Henri Lombardi & Claude Quitté

Commutative algebra: Constructive methods

Finite projective modules

Course and exercises

English translation by Tania K. Roblot

Last corrections January 31, 2025, see page viii

last version `http://hlombardi.free.fr/CACM.pdf`

Henri Lombardi. Maître de Conférences at the Université de Franche-Comté. His research focuses on constructive mathematics, real algebra and algorithmic complexity. He is one of the founders of the international group M.A.P. (Mathematics, Algorithms, Proofs), created in 2003: see the site https://mapcommunity.github.io/

henri.lombardi@univ-fcomte.fr
http://hlombardi.free.fr

Claude Quitté. Maître de Conférences at the Université de Poitiers. His research focuses on effective commutative algebra and computer algebra.

claude.quitte@math.univ-poitiers.fr

Mathematics Subject Classification (2010)
– Primary: 13 Commutative Algebra.
– Secondary:
03F Proof theory and constructive mathematics.
06D Distributive lattices.
14Q Computational aspects of algebraic geometry.

to James Brewer

Preface of the French edition

This book is an introductory course to basic commutative algebra with a particular emphasis on finitely generated projective modules, which constitutes the algebraic version of the vector bundles in differential geometry.

We adopt the constructive point of view, with which all existence theorems have an explicit algorithmic content. In particular, when a theorem affirms the existence of an object – the solution of a problem – a construction algorithm of the object can always be extracted from the given proof.

We revisit with a new and often simplifying eye several abstract classical theories. In particular, we review theories which did not have any algorithmic content in their general natural framework, such as Galois theory, the Dedekind rings, the finitely generated projective modules or the Krull dimension.

Constructive algebra is actually an old discipline, developed among others by Gauss and Kronecker. We are in line with the modern "bible" on the subject, which is the book by Ray Mines, Fred Richman and Wim Ruitenburg, *A Course in Constructive Algebra*, published in 1988. We will cite it in abbreviated form [MRR].

This work corresponds to an MSc graduate level, at least up to Chapter XIV, but only requires as prerequisites the basic notions concerning group theory, linear algebra over fields, determinants, modules over commutative rings, as well as the definition of quotient and localized rings. A familiarity with polynomial rings, the arithmetic properties of $\mathbb{Z}$ and Euclidian rings is also desirable.

Finally, note that we consider the exercises and problems (a little over 320 in total) as an essential part of the book.

We will try to publish the maximum amount of missing solutions, as well as additional exercises on the web page of one of the authors:
`http://hlombardi.free.fr/publis/LivresBrochures.html`

Acknowledgements.

We would like to thank all the colleagues who encouraged us in our project, gave us some truly helpful assistance or provided us with valuable information. Especially MariEmi Alonso, Thierry Coquand, Gema Díaz-Toca, Lionel Ducos, M'hammed El Kahoui, Marco Fontana, Sarah Glaz, Laureano González-Vega, Emmanuel Hallouin, Hervé Perdry, Jean-Claude Raoult, Fred Richman, Marie-Françoise Roy, Peter Schuster and Ihsen Yengui. Last but not least, a special mention for our LaTeX expert, François Pétiard.

Finally, we could not forget to mention the Centre International de Recherches Mathématiques à Luminy and the Mathematisches Forschungsinstitut Oberwolfach, who welcomed us for research visits during the preparation of this book, offering us invaluable working conditions.

Henri Lombardi, Claude Quitté
August 2011

Preface of the English edition

In this edition, we have corrected the errors that we either found ourselves or that were signalled to us.

We have added some exercise solutions as well as some additional content. Most of that additional content is corrections of exercises, or new exercises or problems.

The additions within the course are the following. A paragraph on the null tensors added as the end of Section IV-4. The paragraph on the quotients of flat modules at the end of Section VIII-1 has been fleshed out. We have added Sections 8 and 9 in Chapter XV devoted to the local-global principles.

None of the numbering has changed, except for the local-global principle XII-7.13 which has become XII-7.14.

There are now 297 exercises and 42 problems.

Any useful precisions are on the site:

`http://hlombardi.free.fr/publis/LivresBrochures.html`

Acknowledgements.

We cannot thank Tania K. Roblot enough for the work achieved translating the book into English.

Henri Lombardi, Claude Quitté
May 2014

This is the web updated version of the book

Except for the corrections indicated below, it is the same text as the one of the printed book. The unique structural modifications concern the table of contents: the general table of contents is shortened, and there is a detailed table of contents at the beginning of each chapter.

Corrections to the printed book

Chapter VI: the title of section VI-5 is fixed as “Dualizing linear forms, strictly étale algebras ” instead of “Dualizing linear forms, strictly finite algebras ”

Solution of Problem 3 in Chapter XII: page 736 replace “all nonzero” by “not all zero”.

Chapter XIII. Exercise 17 item *3.* The solution is changed.

In Section XV-9, the proof of Lemma 9.3 is not correct. It is necessary to give directly a proof of the $(a, b, (ab))$ trick for depth 2, allowing us to prove the concrete local-global principle. So 9.3, 9.4, 9.5 and 9.6 become 9.6, 9.3, 9.4 and 9.5.

More details on `http://hlombardi.free.fr/publis/LivresBrochures.html`

Contents

IV Finitely presented modules

V Finitely generated projective modules, 1

VI Strictly finite algebras and Galois algebras

XI Distributive lattices, lattice-groups

XII Prüfer and Dedekind rings

XIII Krull dimension

XIV The number of generators of a module

XV The local-global principle

XVI Extended projective modules

XVII Suslin's stability theorem

Annex. Constructive logic

Foreword

Quant à moi, je proposerais de s'en tenir aux règles suivantes:

1. Ne jamais envisager que des objets susceptibles d'être définis en un nombre fini de mots;
2. Ne jamais perdre de vue que toute proposition sur l'infini doit être la traduction, l'énoncé abrégé de propositions sur le fini;
3. Éviter les classifications et les définitions non prédicatives.

Henri Poincaré,
dans *La logique de l'infini* (Revue de Métaphysique et de Morale, 1909).
Réédité dans *Dernières pensées*, Flammarion.[1]

This book is an introductory course to basic commutative algebra with a particular emphasis on finitely generated projective modules, which constitutes the algebraic version of the vector bundles in differential geometry.

As indicated in the preface, we adopt the constructive method, with which all existence theorems have an explicit algorithmic content. Constructive mathematics can be seen as the most theoretical branch of Computer Algebra, which handles mathematics which "run on a computer." Our course is nevertheless distinguishable from usual Computer Algebra courses in two key aspects.

First of all, our algorithms are often only implied, underlying the proof, and are in no way optimized for the fastest execution, as one might expect when aiming for an efficient implementation.

Second, our theoretical approach is entirely constructive, whereas Computer Algebra courses typically have little concern for this issue. The philosophy here is then not, as is customary "black or white, the good cat is one that catches the mouse"[2] but rather follows "Truth includes not only the result

[1] The official translation by John W. Bolduc (1963) is as follows: "As for me, I would propose that we be guided by the following rules:

1. Never consider any objects but those capable of being defined in a finite number of words;

2. Never lose sight of the fact that every proposition concerning infinity must be the translation, the precise statement of propositions concerning the finite;

3. Avoid nonpredicative classifications and definitions."

[2] Chinese proverb.

but also the path to it. The investigation of truth must itself be true; true investigation is developed truth, the dispersed elements of which are brought together in the result."[3]

We often speak of two points of view on a given subject: classical and constructive. In particular, we have marked with a star the statements (theorems, lemmas, ...) which are true in classical mathematics, but for which we do not give a constructive proof and which often cannot have one. These "starred" statements will then likely never be implemented on a machine, but are often useful as intuition guides, and to at least link with the usual presentations written in the style of classical mathematics.

As for the definitions, we generally first give a constructive variant, even if it means showing the equivalence with the usual definition in the context of classical mathematics.

The reader will notice that in the "starred" proofs we freely use Zorn's lemma and the Law of Excluded Middle (**LEM**)[4], whereas the other proofs always have a direct translation into an algorithm.

Constructive algebra is actually an old discipline, developed by Gauss and Kronecker, among others. As also specified in the preface, we are in line with the modern "bible" on the subject, which is the book by Ray Mines, Fred Richman and Wim Ruitenburg, *A Course in Constructive Algebra*, published in 1988. We will cite it in abbreviated form [MRR]. Our work is however self-contained and we do not demand [MRR] as a prerequisite. The books on constructive mathematics by Harold M. Edwards [Edwards89, Edwards05] and the one of Ihsen Yengui [Yengui] are also recommended.

The work's content

We begin with a brief commentary on the choices that have been made regarding the covered themes.

The theory of finitely generated projective modules is one of the unifying themes of this work. We see this theory in abstract form as an algebraic theory of vector bundles, and in concrete form as that of idempotent matrices. The comparison of the two views is sketched in the introductory chapter.

The theory of finitely generated projective modules itself is treated in Chapters V (first properties), VI (algebras which are finitely generated

[3] Karl Marx, Comments on the latest Prussian censorship instruction, 1843 (cited by Georges Perec in *Les Choses*); transcribed here as by Sally Ryan on `http://www.marxists.org/archive/marx/works/1842/02/10.htm`.

[4] The Law of the Excluded Middle states that $P \vee \neg P$ is true for every proposition P. This principle is accepted in classical mathematics. See page xxvii for a first explanation regarding the refusal of **LEM** in constructive mathematics.

projective modules), X (rank theory and examples), XIV (Serre's Splitting Off theorem) and XVI (extended finitely generated projective modules).

Another unifying theme is provided by local-global principles, as in [Kunz] for example. It is a highly efficient conceptual framework, even though it is a little vague. From a constructive point of view, we replace the localization at an arbitrary prime ideal with a finite number of localizations at comaximal monoids. The notions which respect the local-global principle are considered "good notions," in the sense that they are ready for the passage of commutative rings to Grothendieck schemes, which we will unfortunately be unable to address due to the restricted size of this book.

Finally, one last recurrent theme is found in the method, quite common in computer algebra, called *the lazy evaluation*, or in its most advanced form, *the dynamic evaluation* method. This method is necessary if one wants to set up an algorithmic processing of the questions which a priori require the solution to a factorization problem. This method has also led to the development of the local-global constructive machinery found in Chapters IV and XV, as well as the constructive theory of the Krull dimension (Chapter XIII), with important applications in the last chapters.

We now proceed to a more detailed description of the contents of the book.

In Chapter I, we explain the close relationship that can be established between the notions of vector bundles in differential geometry and of finitely generated projective modules in commutative algebra. This is part of the general algebraization process in mathematics, a process that can often simplify, abstract and generalize surprisingly well concepts from particular theories.

Chapter II is devoted to systems of linear equations over a commutative ring, treated as elementary. It requires almost no theoretical apparatus, apart from the question of localization at a monoid, of which we give a reminder in Section II-1. We then get to our subject matter by putting in place the concrete local-global principle for solving systems of linear equations (Section II-2), a simple and effective tool that will be repeated and varied constantly. From a constructive point of view, solving systems of linear equations immediately renders as central the concept of coherent rings that we treat in Section II-3. Coherent rings are those for which we have a minimal grip on the solution of homogeneous systems of linear equations. Very surprisingly, this concept does not appear in the classical commutative algebra treatises. That is because in general the concept is completely obscured by that of a Noetherian ring. This obscuration does not occur in constructive mathematics where Noetherianity does not necessarily imply coherence. We develop in Section II-4 the question of finite products of rings, with the notion of a fundamental system of orthogonal idempotents and the Chinese Remainder theorem. The long Section II-5 is devoted to many variations on the theme of determinants. Finally, Section II-6 returns to the basic local-global principle in a slightly more general version devoted to exact sequences of modules.

Chapter III develops the method of indeterminate coefficients, first developed by Gauss. Numerous theorems of existence in commutative algebra rely on "algebraic identities under conditions" and thus on memberships $g \in \langle f_1, \ldots, f_s \rangle$ in a ring $\mathbb{Z}[c_1, \ldots, c_r, X_1, \ldots, X_n]$, where the X_i's are the variables and the c_j's are the parameters of the theorem under consideration. In this sense, we can consider that commutative algebra is a vast theory of algebraic identities, which finds its natural framework in the method of indeterminate coefficients, i.e. the method in which the parameters of the given problem are taken as indeterminates. In that assurance we are, to the extent our powers allow to, systematically "chasing algebraic identities." This is the case not only in the "purely computational" Chapters II and III, but throughout the book. In short, rather than simply assert in the context of an existence theorem "there is an algebraic identity which certifies this existence," we have tried each time to give the algebraic identity itself.

Chapter III can be considered as a basic algebra course with 19^{th} century methods. Sections III-1, III-2 and III-3 provide certain generalities about polynomials, featuring in particular the algorithm for partial factorization, the "theory of algebraic identities" (which explains the method of indeterminate coefficients), the elementary symmetric polynomials, the Dedekind-Mertens lemma and the Kronecker's theorem. The last two results are basic tools which give precise information on the coefficients of the product of two polynomials; they are often used in the rest of this manuscript. Section III-4 introduces the universal splitting algebra of a monic polynomial over an arbitrary commutative ring, which is an efficient substitute for the field of the roots of a polynomial over a field. Section III-5 is devoted to the discriminant and explains in what precise sense a generic matrix is diagonalizable. With these tools in hand, we can treat the basic Galois theory in Section III-6. The elementary theory of elimination via the resultant is given in Section III-7. We can then give the basics of algebraic number theory with the theorem of unique decomposition into prime factors for a finitely generated ideal of a number field (Section III-8). Section III-9 shows Hilbert's Nullstellensatz as an application of the resultant. Finally, Section III-10 on Newton's method in algebra closes this chapter.

Chapter IV is devoted to the study of the elementary properties of finitely presented modules. These modules play a role for rings similar to that played by finite dimensional vector spaces for fields: the theory of finitely presented modules is a more abstract, and often profitable, way to address the issue of systems of linear equations. Sections IV-1 to IV-4 show the basic stability properties as well as the important example of the ideal of a zero for a polynomial system (on an arbitrary commutative ring). We then focus on the classification problem of finitely presented modules over a given ring. Working towards principal ideal domains (PID), for which the classification problem is completely solved (Section IV-7), we will encounter pp-rings (Section IV-6), which are the rings where the annihilator of an element is always generated by an idempotent. This will be the opportunity to develop an *elementary local-global machinery* which conveniently reformulates a constructively established result for integral rings into the analogous result for pp-rings. This proof-rewriting machinery is elementary as it is founded on the decomposition of a ring into a finite product of rings. The interesting thing is that this decomposition is obtained via a rereading of the constructive proof written in the integral case; here we see that in constructive mathematics the proof is often even more important than the result. Similarly, we have an *elementary local-global machinery* which conveniently reformulates a constructively established result for discrete fields into the analogous result for reduced zero-dimensional rings (Section IV-8). The zero-dimensional rings elementarily defined here constitute an important intermediate step to generalize specific results regarding discrete fields to arbitrary commutative rings: they are a key tool of commutative algebra. Classically, these appear in the literature in their Noetherian form, i.e. that of Artinian rings. Section IV-9 introduces very important invariants: the Fitting ideals of a finitely presented module. Finally, Section IV-10 applies this notion to introduce the resultant ideal of a finitely generated ideal over a polynomial ring when the ideal contains a monic polynomial, and to prove a theorem of algebraic elimination over an arbitrary ring.

Chapter V is a first approach to the theory of finitely generated projective modules. Sections V-2 to V-5 state basic properties along with the important example of the zero-dimensional rings. Section V-6 states the local structure theorem: a module is finitely generated projective if and only if it becomes free after localization at suitable comaximal elements. Its constructive proof is a rereading of a result established in Chapter II for "well conditioned" systems of linear equations (Theorem II-5.26). Section V-7 develops the example of the locally cyclic projective modules. Section V-8 introduces the determinant of an endomorphism of a finitely generated projective module. This renders the decomposition of such a module into a direct sum of its components of constant rank accessible. Finally, Section V-9, which we were not too sure where to place in this work, hosts some additional considerations on *properties of finite character*, a concept introduced in Chapter II to discuss the connections between concrete local-global principles and abstract local-global principles.

Chapter VI is essentially devoted to algebras which are finitely generated projective modules over their base rings. We call these strictly finite algebras. When applied to commutative rings, they constitute a natural generalization of the concept of a finite algebra over a field. The icing on the cake being the important case of Galois algebras, which generalize Galoisian extensions of discrete fields to commutative rings.

Section VI-1 treats the case where a base ring is a discrete field. It provides the constructive versions of the structure theorem obtained in classical mathematics. The case of étale algebras (when the discriminant is invertible) is particularly enlightening. We discover that the classical theorems always implicitly assume that we know how to factorize the separable polynomials over the base field. The constructive proof of the primitive element theorem VI-1.9 is significant for its deviation from the classical proof. Section VI-2 applies the previous results to complete the basic Galois theory started in Section III-6 by characterizing the Galoisian extensions of discrete fields like the étale and normal extensions. Section VI-3 is a brief introduction to finitely presented algebras, by focusing on integral algebras[5], with a weak Nullstellensatz and the Lying Over lemma. Section VI-4 introduces strictly finite algebras over an arbitrary ring. In Sections VI-5 and VI-6, the related concepts of a strictly étale algebra and of a separable algebra are introduced. These generalize the concept of an étale algebra over a discrete field. In Section VI-7, we constructively present the basics of the theory of Galois algebras for commutative rings. It is in fact an Artin-Galois theory since it adopts the approach Artin had developed for the case of fields, starting directly from a finite group of automorphisms of a field, the base field appearing only as a byproduct of subsequent constructions.

In Chapter VII, the dynamic method – a cornerstone of modern methods in constructive algebra – is implemented to deal with the field of roots of a polynomial and the Galois theory in the separable case. From a constructive point of view, we need to use the dynamic method when we do not know how to factorize the polynomials over the base field.
For training purposes, Section VII-1 begins by establishing results in a constructive form for the Nullstellensatz when we do not know how to factorize the polynomials over the base field. General considerations on the dynamic method are developed in Section VII-2. More details on the course of the festivities are given in the introduction of the chapter.

Chapter VIII is a brief introduction to flat modules and to flat and faithfully flat algebras. Intuitively speaking, an **A**-algebra **B** is flat when the homogeneous systems of linear equations over **A** have "no more" solutions

[5] By "integral algebra" we mean *an algebra that is integral on its base ring*, not to be confused with an algebra that is an integral ring.

in **B** than in **A**, and it is faithfully flat if this statement is also true for nonhomogeneous systems of linear equations. These crucial notions of commutative algebra were introduced by Serre in [173, GAGA,1956]. We will only state the truly fundamental results. This is also when we will introduce the concepts of a pf-ring (i.e. a ring whose principal ideals are flat), of a torsion-free module (for an arbitrary ring), of an arithmetic ring and of a Prüfer ring. As always, we focus on the local-global principle when it applies.

Chapter IX discusses local rings and some generalizations. Section IX-1 introduces the constructive terminology for some common classical concepts, including the important concept of a Jacobson radical. A related concept is that of a residually zero-dimensional ring (a ring **A** such that $\mathbf{A}/\operatorname{Rad}\mathbf{A}$ is zero-dimensional). It is a robust concept, which never uses maximal ideals, and most of the theorems in the literature regarding semi-local rings (in classical mathematics they are the rings which only have a finite number of maximal ideals) apply to residually zero-dimensional rings. Section IX-2 lists some results which show that on a local ring we reduce the solution of particular problems to the case of fields. Sections IX-3 and IX-4 establish, based on geometric examples (i.e. regarding the study of polynomial systems), a link between the notion of a local study in the topological intuitive sense and the study of certain localizations of rings (in the case of polynomial systems over a discrete field these localizations are local rings). In particular we introduce the notions of tangent and cotangent spaces at zero of a polynomial system. Section IX-5 is a brief study of decomposable rings, including the particular case from classical mathematics of decomposed rings (finite products of local rings), which play an important role in the theory of Henselian local rings. Finally, Section IX-6 treats the notion of a local-global ring, which generalizes both the concept of local rings and that of zero-dimensional rings. These rings verify very strong local-global properties; e.g. the projective modules of constant rank are always free. Moreover, the class of local-global rings is stable under integral extensions.

Chapter X continues the study of finitely generated projective modules started in Chapter V. In Section X-1, we return to the question of the characterization of finitely generated projective modules as locally free modules, i.e. of the local structure theorem. We give a matrix version of it (Theorem X-1.7), which summarizes and clarifies the different statements of the theorem. Section X-2 is devoted to the ring of ranks over **A**. In classical mathematics, the rank of a finitely generated projective module is defined as a locally constant function in the Zariski spectrum. We give here an elementary theory of the rank which does not call upon prime ideals. In Section X-3, we provide some simple applications of the local structure theorem. Section X-4 introduces Grassmannians. In Section X-5, we introduce the general problem of the complete classification of the finitely generated projective modules over a fixed ring $\mathbf{A}$. This classification is a fundamental and difficult problem, which does not have a general algorithmic solution. Section X-6 presents a nontrivial example for which this classification can be obtained.

Chapter XI is devoted to distributive lattices and lattice ordered groups (l-groups). The first two sections describe these algebraic structures along with their basic properties. These structures are important in commutative algebra for several reasons.

First, the divisibility theory has as its "ideal model" the natural numbers' divisibility theory. The structure of the multiplicative monoid $(\mathbb{N}^*, \times, 1)$ makes it the positive part of an l-group. In commutative algebra, this can be generalized in two possible ways. The first generalization is the theory of integral rings whose finitely generated ideals form a distributive lattice, called Prüfer domains, which we will study in Chapter XII; their nonzero finitely generated ideals form the positive part of an l-group. The second is the theory of gcd rings that we study in Section XI-3. Let us notify the first appearance of the Krull dimension $\leqslant 1$ in Theorem XI-3.12: an integral gcd ring with dimension $\leqslant 1$ is a Bézout ring.

Secondly, the distributive lattices act as the constructive counterpart of various spectral spaces which have emerged as powerful tools of abstract algebra. The relationship between distributive lattices and spectral spaces will be discussed in Section XIII-1. In Section XI-4, we set up the Zariski lattice of a commutative ring $\mathbf{A}$, which is the constructive counterpart of the famous Zariski spectrum. Our goal here is to establish a parallel between the construction of the zero-dimensional reduced closure of a ring (denoted by $\mathbf{A}^\bullet$) and that of the Boolean algebra generated by a distributive lattice (which is the subject of Theorem XI-4.26). The object $\mathbf{A}^\bullet$ constructed as above essentially contains the same information as the product of the rings $\mathrm{Frac}(\mathbf{A}/\mathfrak{p})$ for all prime ideals $\mathfrak{p}$ of $\mathbf{A}$([6]). This result is closely related to the fact that the Zariski lattice of $\mathbf{A}^\bullet$ is the Boolean algebra generated by the Zariski lattice of $\mathbf{A}$.

A third reason to be interested in distributive lattices is constructive logic (or intuitionistic logic). In this logic, the set of truth values of classical logic, that is the two-element Boolean algebra $\{\mathsf{True}, \mathsf{False}\}$, is replaced by a quite mysterious distributive lattice. Constructive logic is informally discussed in the Annex. In Section XI-5, we set up the tools that provide a framework for a formal algebraic study of constructive logic: entailment relations and Heyting algebras. In addition, entailment relations and Heyting

[6] This product is not accessible in constructive mathematics, $\mathbf{A}^\bullet$ is its perfectly effective constructive substitute.

algebras have their own use in the general study of distributive lattices. For example, the Zariski lattice of a coherent Noetherian ring is a Heyting algebra (Proposition XIII-6.9).

Chapter XII deals with arithmetic rings, Prüfer rings and Dedekind rings. Arithmetic rings are rings for which the lattice of finitely generated ideals is distributive. A Prüfer ring is a reduced arithmetic ring and is characterized by the fact that all of its ideals are flat. A coherent Prüfer ring is the same thing as an arithmetic pp-ring. It is characterized by the fact that its finitely generated ideals are projective. A Dedekind ring is a Noetherian and strongly discrete coherent Prüfer ring (in classical mathematics, with **LEM**, every ring is strongly discrete and every Noetherian ring is coherent). These rings first appeared as the rings of integers of number fields. The paradigm in the integral case is the unique decomposition into prime factors of any nonzero finitely generated ideal. The general arithmetic properties of finitely generated ideals are mostly verified by all the arithmetic rings. For the most subtle properties concerning the factorizations of the finitely generated ideals, and in particular the decomposition into prime factors, a Noetherian assumption, or at least a dimension $\leqslant 1$ assumption, is essential. In this chapter, we wanted to show the progression of the properties satisfied by the rings as we strengthen the assumptions from the arithmetic rings to the total factorization Dedekind rings. We focus on the simple algorithmic character of the definitions in the constructive framework. Certain properties only depend on dimension $\leqslant 1$, and we wanted to do justice to pp-rings of dimension at most 1. We also carried out a more progressive and more elegant study of the problem of the decomposition into prime factors than in the presentations which allow **LEM**. For example, Theorems XII-4.10 and XII-7.12 provide precise constructive versions of the theorem concerning the normal finite extensions of Dedekind rings, with or without the total factorization property.

The chapter begins with a few epistemological remarks on the intrinsic interest of addressing the factorization problems with the partial factorization theorem rather than the total factorization one. To get a good idea of how things unfold, simply refer to the table of contents at the beginning of the chapter on page 679 and to the table of theorems on page 984.

Chapter XIII is devoted to the Krull dimension of commutative rings, of their morphisms and of distributive lattices, and to the valuative dimension of commutative rings.

Several important notions of dimension in classical commutative algebra are dimensions of spectral spaces. These very peculiar topological spaces have the property of being fully described (at least in classical mathematics) by their compact-open subspaces, which form a distributive lattice. It so happens that the corresponding distributive lattice generally has a simple interpretation, without any recourse to spectral spaces. In 1974, Joyal showed how to constructively define the Krull dimension of a distributive lattice. Since this auspicious day, the theory of dimension which seemed bathed in ethereal spaces – that are invisible when you do not trust the axiom of choice – has become (at least in principle) an elementary theory, without any further mysteries.

Section XIII-1 describes the approach of the Krull dimension in classical mathematics. It also explains how to interpret the Krull dimension of such a space in terms of the distributive lattice of its compact-open subspaces. Section XIII-2 states the constructive definition of the Krull dimension of a commutative ring, denoted by $\mathsf{Kdim}\,\mathbf{A}$, and draws some consequences. Section XIII-3 states some more advanced properties, in particular the local-global principle and the closed covering principle for the Krull dimension. Section XIII-4 deals with the Krull dimension of integral extensions and Section XIII-5 that of geometric rings (corresponding to polynomial systems) on the discrete fields. Section XIII-6 states the constructive definition of the Krull dimension of a distributive lattice and shows that the Krull dimension of a commutative ring and that of its Zariski lattice coincide. Section XIII-7 is devoted to the dimension of the morphisms between commutative rings. The definition uses the reduced zero-dimensional closure of the source ring of the morphism. To prove the formula which defines the upper bound of $\mathsf{Kdim}\,\mathbf{B}$ from $\mathsf{Kdim}\,\mathbf{A}$ and $\mathsf{Kdim}\,\rho$ (when we have a morphism $\rho : \mathbf{A} \to \mathbf{B}$), we must introduce the minimal pp-closure of a commutative ring. This object is a constructive counterpart of the product of all the $\mathbf{A}/\mathfrak{p}$, when $\mathfrak{p}$ ranges over the minimal prime ideals of $\mathbf{A}$. Section XIII-8 introduces the valuative dimension of a commutative ring and in particular uses this concept to prove the following important result: for a nonzero arithmetic ring $\mathbf{A}$, we have $\mathsf{Kdim}\,\mathbf{A}[X_1, \dots, X_n] = n + \mathsf{Kdim}\,\mathbf{A}$. Section XIII-9 states constructive versions of the Going up and Going down Theorems.

In Chapter XIV, titled *Number of generators of a module*, we establish the elementary, non-Noetherian and constructive versions of the “great” theorems of commutative algebra, their original form due to Kronecker, Bass, Serre, Forster and Swan. These results relate to the number of radical generators of a finitely generated ideal, the number of generators of a module, the possibility of producing a free submodule as a direct summand in a module, and the possibility to simplifying isomorphisms, in the following way: if $M \oplus N \simeq M' \oplus N$ then $M \simeq M'$. They involve the Krull dimension or other, more sophisticated dimensions introduced by R. Heitmann as well as by the authors of this work and T. Coquand.

Section XIV-1 is devoted to Kronecker's Theorem and its extensions (the most advanced, non-Noetherian, is due to R. Heitmann [101]). Kronecker's

Theorem is usually stated in the following form: an algebraic variety in $\mathbb{C}^n$ can always be defined by $n+1$ equations. The form due to Heitmann is that in a ring of Krull dimension less than or equal to n, for all finitely generated ideal $\mathfrak{a}$ there exists an ideal $\mathfrak{b}$ generated by at most $n+1$ elements of $\mathfrak{a}$ such that $\sqrt{\mathfrak{b}} = \sqrt{\mathfrak{a}}$. The proof also gives Bass' stable range Theorem. The latter theorem was improved by involving "better" dimensions than the Krull dimension. This is the subject of Section XIV-2 where the *Heitmann dimension* is defined, discovered while carefully reading Heitmann's proofs (Heitmann uses another dimension, a priori a little worse, which we also explain in constructive terms). In Section XIV-3, we explain which matrix properties of a ring allow Serre's Splitting Off theorem, Forster-Swan's theorem (controlling the number of generators of a finitely generated module according to the local number of generators) and Bass' simplification theorem. Section XIV-4 introduces the concepts of support (a mapping from a ring to a distributive lattice satisfying certain axioms) and of n-stability. The latter was defined by Thierry Coquand, after having analyzed one of Bass' proofs which establishes that the finitely generated projective modules over a ring $\mathbf{V}[X]$, where $\mathbf{V}$ is a valuation ring of finite Krull dimension, are free. In the final section, we prove that the crucial matrix property introduced in Section XIV-3 is satisfied, on one hand by the n-stable rings, and on the other by the rings of Heitmann dimension $< n$.

Chapter XV is devoted to the local-global principle and its variants. Section XV-1 introduces the notion of the covering of a monoid by a finite family of monoids, which generalizes the notion of comaximal monoids. The covering Lemma XV-1.5 will be decisive in Section XV-5. Section XV-2 states some concrete local-global principles. This is to say that some properties are globally true as soon as they are locally true. Here, "locally" is meant in the constructive sense: after localization at a finite number of comaximal monoids. Most of the results have been established in the previous chapters. Grouping them shows the very broad scope of these principles. Section XV-3 restates some of these principles as abstract local-global principles. Here, "locally" is meant in the abstract sense: after localization at any arbitrary prime ideal. We are mainly interested in comparing the abstract principles and the corresponding concrete local-global principles. Section XV-4 explains the construction of "global" objects from objects of the same type defined only locally, as is usual in differential geometry. It is the impossibility of this construction when seeking to glue certain rings together which is at the root of Grothendieck schemes. In this sense, Sections XV-2 and XV-4 constitute the basis from which we can develop the theory of schemes in a completely constructive framework.

The following sections are of a different nature. Methodologically, they are devoted to the decryption of different variations of the local-global principle in classical mathematics. For example, the localization at every prime ideal, the passage to the quotient by every maximal ideal or the localization at every minimal prime ideal, each of which applies in particular situations. Such a decryption certainly presents a confusing character insofar as it takes as its starting point a classical proof that uses theorems in due and proper form, but where the constructive decryption of this proof is not only given by the use of constructive theorems in due and proper form. One must also look at what the classical proof does with its purely ideal objects (e.g. maximal ideals) to understand how it gives us the means to construct a finite number of elements that will be involved in a constructive theorem (e.g. a concrete local-global principle) to reach the desired result. Decrypting such a proof we use the general dynamic method presented in Chapter VII. We thus describe *local-global machineries* that are significantly less elementary than those in Chapter IV: the basic constructive local-global machinery "with prime ideals" (Section XV-5), the constructive local-global machinery "with maximal ideals" (Section XV-6) and the constructive local-global machinery "with minimal prime ideals" (Section XV-7). By carrying out "Poincaré's program" used as an epigraph for this foreword, our local-global machineries take into account an essential remark made by Lakatos that the most interesting and robust thing in a theorem is always its proof, even if it can be criticized in some respects (see [Lakatos]).

In Sections XV-8 and XV-9, we examine to what extent certain local-global principles remain valid when we replace in the statements the lists of comaximal elements by lists of depth $\geqslant 1$ or of depth $\geqslant 2$.

In Chapter XVI, we treat the question of finitely generated projective modules over rings of polynomials. The decisive question is to establish for which classes of rings the finitely generated projective modules over a polynomial ring are derived by scalar extension of a finitely generated projective module over the ring itself (possibly by putting certain restrictions on the considered finitely generated projective modules or on the number of variables in the polynomial ring). Some generalities on the extended modules are given in Section XVI-1. The case of the projective modules of constant rank 1, which is fully clarified by Traverso-Swan-Coquand's theorem, is dealt with in Section XVI-2. Coquand's constructive proof uses the constructive local-global machinery with minimal prime ideals in a crucial way. Section XVI-3 deals with Quillen and Vaserstein's patching theorems, which state that certain objects are obtained by scalar extension (from the base ring to the polynomial ring) if and only if this property is locally satisfied. We also have a sort of converse to Quillen's patching due to Roitman, in a constructive form. Section XVI-4 is devoted to Horrocks' theorems. The constructive proof of Horrocks' global theorem is obtained from the proof of Horrocks' local theorem by using the basic local-global machinery and concluding with Quillen's constructive patching. Section XVI-5 gives several constructive proofs of Quillen-Suslin's theorem (the finitely generated projective modules over a polynomial ring on a discrete field are free) founded on different classical proofs. Section XVI-6 establishes Lequain-Simis' theorem (the finitely generated projective modules over a polynomial ring on an arithmetic ring are extended). The proof uses the dynamic method presented in Chapter VII. This allows us to establish Yengui's induction theorem, a constructive variation of Lequain-Simis' induction.

In Chapter XVII, we prove "Suslin's Stability Theorem" in the special case of discrete fields. Here also, we use the basic local-global machinery presented in Chapter XV to obtain a constructive proof.

The Annex describes a Bishop style constructive set theory. It can be seen as an introduction to constructive logic. In it we explain the Brouwer-Heyting-Kolmogorov semantic for connectives and quantifiers. We discuss certain weak forms of **LEM** along with several problematic principles in constructive mathematics.

Some epistemological remarks

In this work, we hope to show that classical commutative algebra books such as [Eisenbud], [Kunz], [Lafon & Marot], [Matsumura], [Glaz], [Kaplansky], [Atiyah & Macdonald], [Northcott], [Gilmer], [Lam06] (which we highly recommend), or even [Bourbaki] and the remarkable work available on the web [Stacks-Project], could be entirely rewritten from a constructive point of view, dissipating the veil of mystery which surrounds the nonexplicit existence theorems of classical mathematics. Naturally, we hope that the readers will take advantage of our work to take a fresh look at the classical Computer Algebra books like, for instance, [Cox, Little & O'Shea], [COCOA], [Elkadi & Mourrain], [von zur Gathen & Gerhard], [Mora], [TAPAS] or [SINGULAR].

Since we want an algorithmic processing of commutative algebra we cannot use all the tricks that arise from the systematic use of Zorn's Lemma and the Law of Excluded Middle in classical mathematics. Undoubtedly, the reader understands that it is difficult to implement Zorn's lemma in Computer Algebra. The refusal of **LEM**, however, must seem harder to stomach. It is simply a practical observation on our part. If in a classical proof there is a reasoning that leads to a computation in the form "if x is invertible, do this, otherwise do that," then, clearly, it directly translates into an algorithm only when there is an invertibility test for the ring in question. It is in stressing this difficulty, which we must constantly work around, that we are often led to speak of two points of view on the same subject: classical and constructive.

We could argue forever about whether constructive mathematics is part of classical mathematics, the part that deals exclusively with the explicit aspect of things, or conversely whether it is classical mathematics which is a part of constructive mathematics, the part whose theorems are "starred," i.e. which systematically add **LEM** and the axiom of choice in their assumptions. One of our objectives is to tip the balance in the second direction, not for philosophical debate but for practical purposes.

Finally, let us mention two striking traits of this work compared to classical texts on commutative algebra.

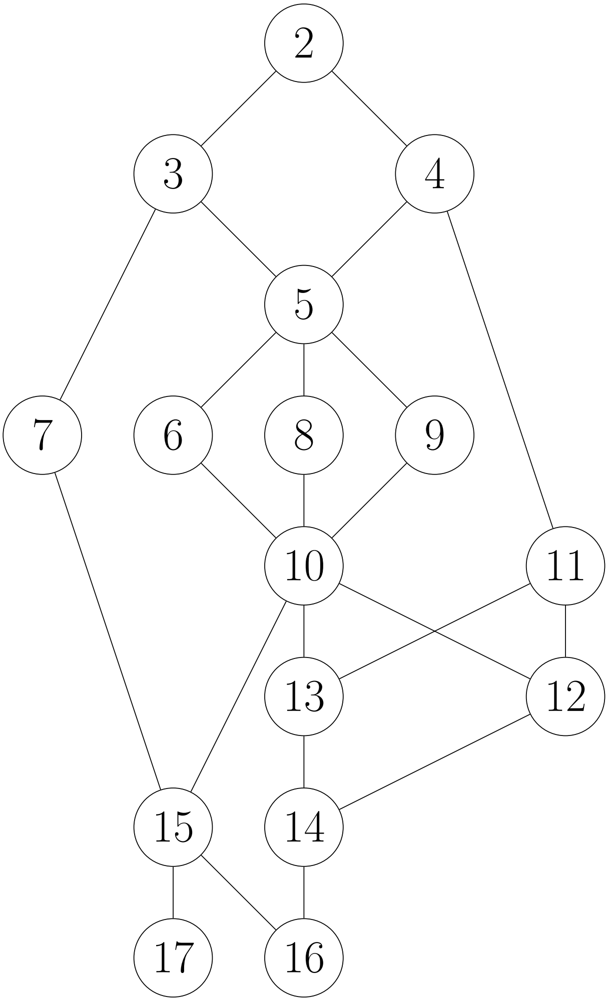
The first is that Noetherianity is left on the backburner. Experience shows that indeed Noetherianity is often too strong an assumption, which hides the true algorithmic nature of things. For example, such a theorem usually stated for Noetherian rings and finitely generated modules, when its proof is examined to extract an algorithm, turns out to be a theorem on coherent rings and finitely presented modules. The usual theorem is but a corollary of the right theorem, but with two nonconstructive arguments allowing us to deduce coherence and finite presentation from Noetherianity and finite generation in classical mathematics. A proof in the more satisfying framework of coherence and finitely presented modules is often already published in research articles, although rarely in an entirely constructive form, but "the right statement" is generally missing.[7]

The second striking trait of this work is the almost total absence of negation in the constructive statements. For example, instead of stating that for a nontrivial ring $\mathbf{A}$, two free modules of respective rank m and n with $m > n$ cannot be isomorphic, we prefer to say without any assumption about the ring that if these modules are isomorphic, then the ring is trivial (Proposition II-5.2). This nuance may seem quite slight at first, but it has an algorithmic importance. It will allow us to substitute a proof from classical mathematics using a ring $\mathbf{A} = \mathbf{B}/\mathfrak{a}$, which would conclude that $1 \in \mathfrak{a}$ by contradiction, with a fully algorithmic proof that constructs 1 as an element of the ideal $\mathfrak{a}$ from an isomorphism between $\mathbf{A}^m$ and $\mathbf{A}^n$.

For a general presentation of the ideas which led to the new methods used in constructive algebra in this work, we suggest to the reader the summary article [42, Coquand&Lombardi, 2006].

Henri Lombardi, Claude Quitté
August 2011

[7] This Noetherian professional bias has produced a linguistic shortcoming in the English literature which consists in taking "local ring" to mean "Noetherian local ring."


2
3
4
5
7
6
8
9
10
11
13
12
15
14
17
16

The flowchart on the previous page shows the dependence relations between the different chapters

2. The basic local-global principle and systems of linear equations
   Coherent rings and modules. A little bit of exterior algebra.
3. The method of undetermined coefficients
   Dedekind-Mertens and Kronecker's lemmas. Basic Galois theory. Classical Nullstellensatz.
4. Finitely presented modules
   Category of finitely presented modules. Zero-dimensional rings. Elementary local-global machineries. Fitting ideals.
5. Finitely generated projective modules, 1
   Local structure theorem. Determinant. Rank.
6. Strictly finite algebras and Galois algebras
7. The dynamic method
   General Nullstellensatz (without algebraic closure). General Galois theory (without factorization algorithm).
8. Flat modules
   Flat and faithfully flat algebras.
9. Local rings, or just about
   Decomposable ring. Local-global ring.
10. Finitely generated projective modules, 2
11. Distributive lattices, lattice-groups
    GCD ring. Zariski lattice of a commutative ring. Entailment relations.
12. Prüfer and Dedekind rings
    Integral extensions. Dimension $\leqslant 1$. Factorization of finitely generated ideals.
13. Krull dimension
    Krull dimension. Dimension of morphisms. Valuative dimension. Dimension of integral and polynomial extensions.
14. The number of generators of a module
    Kronecker's, Bass' and Forster-Swan's theorems. Serre's Splitting Off theorem. Heitmann dimension.
15. The local-global principle
16. Extended projective modules
    Traverso-Swan-Coquand's, Quillen-Suslin's, Bass-Lequain-Simiss theorems.
17. Suslin's stability theorem

Chapter I

Examples

Contents

Introduction

Throughout the manuscript, unless explicitly stated otherwise, rings are commutative and unitary, and a ring homomorphism $\varphi : \mathbf{A} \to \mathbf{B}$ must satisfy $\varphi(1_{\mathbf{A}}) = 1_{\mathbf{B}}$.

Let $\mathbf{A}$ be a ring. We say that an $\mathbf{A}$-module M is a *finite rank free module* when it is isomorphic to a module $\mathbf{A}^n$. We say that it is a *finitely generated projective* module when there exists an $\mathbf{A}$-module N such that $M \oplus N$ is a finite rank free module. This is equivalent to saying that M is isomorphic to the image of a *projection matrix* (a matrix P such that $P^2 = P$). That is, the projection matrix onto M along N, precisely defined as follows:

$$M \oplus N \longrightarrow M \oplus N, \quad x + y \longmapsto x \qquad \text{for } x \in M \text{ and } y \in N.$$

A projection matrix is also called a *projector.*

When we have an isomorphism $M \oplus \mathbf{A}^\ell \simeq \mathbf{A}^k$, the finitely generated projective module M is called *stably free.*

While over a field or over a PID the finitely generated projective modules are free (over a field they are finite dimensional vector spaces), over a general commutative ring the classification of the finitely generated projective modules is both an important and a difficult problem.

Kronecker and Dedekind have proven that a nonzero finitely generated ideal in the ring of integers of a number field is always invertible (thus finitely generated projective), but that it is rarely free (i.e. principal). This is a fundamental phenomenon, which is at the root of the modern development of number theory.

In this chapter, we try to explain why the notion of a finitely generated projective module is important by giving meaningful examples from differential geometry.

The datum of a vector bundle on a smooth compact manifold V is in fact equivalent to the datum of a finitely generated projective module over the ring $\mathbf{A} = C^\infty(V)$ of smooth functions over V; to a vector bundle we associate the $\mathbf{A}$-module of its sections, this is always a finitely generated projective module but it is free only when the bundle is trivial.

The tangent bundle corresponds to a module built by a purely formal procedure from the ring $\mathbf{A}$. In the case where the manifold V is a sphere, the module of the sections of the tangent bundle is stably free. An important result about the sphere is that there exist no smooth everywhere nonzero vector fields. This is equivalent to the fact that the module of sections of the tangent bundle is not free.

We try to be as explicit as possible, but in this motivating chapter we freely use the reasonings of classical mathematics without worrying about being completely rigorous from a constructive point of view.

1. Vector bundles on a smooth compact manifold

Here, we give some motivations for finitely generated projective modules and localization by explaining the example of vector bundles on a compact smooth manifold. Two important particular cases are tangent and cotangent bundles corresponding to C^∞ vector fields and to C^∞ differential forms.

We will use the term “smooth” as a synonym for “of class C^∞.”

We will see that the fact that the sphere cannot be combed admits a purely algebraic interpretation.

In this section, we consider a smooth real differentiable manifold V and we denote by $\mathbf{A} = C^\infty(V)$ the real algebra of global smooth functions on the manifold.

Some localizations of the algebra of continuous functions

Let us first consider an element $f \in \mathbf{A}$ along with the open set (open subset of the manifold V to be precise)

$$U = \{\, x \in V \mid f(x) \neq 0 \,\}$$

and let us see how we can interpret the algebra $\mathbf{A}[1/f]$: two elements g/f^k and h/f^k are equal in $\mathbf{A}[1/f]$ if and only if for some exponent ℓ we have $gf^\ell = hf^\ell$ which means precisely $g|_U = h|_U$.

It follows that we can interpret $\mathbf{A}[1/f]$ as a sub-algebra of the algebra of smooth functions on U: this sub-algebra has as elements the functions which can be written as $(g|_U)/(f|_U)^k$ (for a given exponent k) with $g \in \mathbf{A}$, which a priori introduces certain restrictions on the behavior of the function on the border of U.

To avoid having to deal with this difficult problem, we use the following lemma.

1.1. Lemma. *Let U' be an open subset of V containing the support of a function f. Then, the natural map (by restriction),*

$$\textit{from } C^\infty(V)[1/f] = \mathbf{A}[1/f] \textit{ to } C^\infty(U')[1/f|_{U'}],$$

is an isomorphism.

D Recall that the support of a function f is the adherence of the open subset U. We have a restriction homomorphism $h \mapsto h|_{U'}$ from $C^\infty(V)$ to $C^\infty(U')$ that induces a homomorphism $\varphi : C^\infty(V)[1/f] \to C^\infty(U')[1/f|_{U'}]$. We want to prove that φ is an isomorphism. If $g \in C^\infty(U')$, then the function gf, which equals zero on $U' \setminus \overline{U}$, can be extended to a smooth function on the whole of V by making it zero outside of U'. We continue to denoted it by gf. So, the reciprocal isomorphism of φ is given by $g \mapsto gf/f$ and $g/f^m \mapsto gf/f^{m+1}$. □

A *germ of a smooth function at a point* p of the manifold V is given by a pair (U, f) where U is an open subset containing p and f is a smooth function $U \to \mathbb{R}$. Two pairs (U_1, f_1) and (U_2, f_2) define the same germ if there exist an open subset $U \subseteq U_1 \cap U_2$ containing p such that $f_1|_U = f_2|_U$. The germs of smooth functions at a point p form an $\mathbb{R}$-algebra that we denote by $\mathbf{A}_p$.

We then have the following little "algebraic miracle."

1.2. Lemma. *The algebra* $\mathbf{A}_p$ *is naturally isomorphic to the localization* $\mathbf{A}_{S_p}$*, where* S_p *is the multiplicative part of nonzero functions at a point* p*.*

D First, we have a natural map $\mathbf{A} \to \mathbf{A}_p$ that associates to a function defined on V its germ at p. It follows immediately that the image of S_p is made of invertible elements of $\mathbf{A}_p$. Thus, we have a factorization of the above natural map which provides a homomorphism $\mathbf{A}_{S_p} \to \mathbf{A}_p$.

Next, we define a homomorphism $\mathbf{A}_p \to \mathbf{A}_{S_p}$. If (U, f) defines the germ g then consider a function $h \in \mathbf{A}$ which is equal to 1 on an open subset U' containing p with $\overline{U'} \subseteq U$ and which equals zero outside of U (in a chart we will be able to take U' to be an open ball with center p). So, each of the three pairs (U, f), $(U', f|_{U'})$ and (V, fh) define the same germ g. Now, fh defines an element of $\mathbf{A}_{S_p}$. It remains to check that the correspondence that we have just established does indeed produce a homomorphism of the algebra $\mathbf{A}_p$ on the algebra $\mathbf{A}_{S_p}$: no matter how the germ is represented as a pair (U, f), the element $fh/1$ of $\mathbf{A}_{S_p}$ only depends on the germ g.

Finally, we check that the two homomorphisms of $\mathbb{R}$-algebras that we have defined are indeed inverse isomorphisms of each other. □

In short, we have algebrized the concept of a germ of a smooth function. Except that the monoid S_p is defined from the manifold V, not only from the algebra $\mathbf{A}$.

However, if V is compact, the monoids S_p are precisely the complements of the maximal ideals of $\mathbf{A}$. In fact, on the one hand, whether V is compact or not, the set of $f \in \mathbf{A}$ zero at p always constitutes a maximal ideal $\mathfrak{m}_p$ with a residual field equal to $\mathbb{R}$. On the other hand, if $\mathfrak{m}$ is a maximal ideal of $\mathbf{A}$ the intersection of the $Z(f) = \{\, x \in V \mid f(x) = 0 \,\}$ for each $f \in \mathfrak{m}$ is a non-empty compact subset (note that $Z(f) \cap Z(g) = Z(f^2 + g^2)$). Since the ideal is maximal, this compact subset is necessarily reduced to one point p and we then get $\mathfrak{m} = \mathfrak{m}_p$.

Vector bundles and finitely generated projective modules

Now recall the notion of a *vector bundle* over V.

A vector bundle is given by a smooth manifold W, a smooth surjective mapping $\pi : W \to V$, and a structure of a finite dimensional vector space on every fiber $\pi^{-1}(p)$. In addition, locally, all this must be diffeomorphic to the following simple situation, called trivial:

$$\pi_1 : (U \times \mathbb{R}^m) \to U,\ (p, v) \mapsto p,$$

with m that can depend on U if V is not connected. This means that the structure of the (finite dimensional) vector space on the fiber over p must "properly" depend on p.

Such an open set (or subset) U, which trivializes the bundle, is called a *distinguished open set (or subset)*.

A *section* of the vector bundle $\pi : W \to V$ is by definition a mapping $\sigma : V \to W$ such that $\pi \circ \sigma = \mathrm{Id}_V$. We will denote by $\Gamma(W)$ the set of smooth sections of this bundle. It is equipped with a natural $\mathbf{A}$-module structure.

Now suppose that the manifold V is compact. As the bundle is locally trivial there exists a finite covering of V by distinguished open subsets U_i and a partition of the unity $(f_i)_{i \in [\![1..s]\!]}$ *subordinate to the open cover* U_i: the support of f_i is a compact set K_i contained in U_i.

We notice from Lemma 1.1 that the algebras $\mathbf{A}[1/f_i] = C^\infty(V)[1/f_i]$ and $C^\infty(U_i)[1/f_i]$ are naturally isomorphic.

If we localize the ring $\mathbf{A}$ and the module $M = \Gamma(W)$ by making f_i invertible, we obtain the ring $\mathbf{A}_i = \mathbf{A}[1/f_i]$ and the module M_i. Let $W_i = \pi^{-1}(U_i)$. Then, $W_i \to U_i$ is "isomorphic" to $\mathbb{R}^{m_i} \times U_i \to U_i$. Thus it boils down to taking a section of the bundle W_i, or to taking the m_i functions $U_i \to \mathbb{R}$ which make a section of the bundle $\mathbb{R}^{m_i} \times U_i \to U_i$. In other words, the module of the sections of W_i is free and of rank m.

Since a module that becomes free after localization in a finite number of comaximal elements is finitely generated projective (local-global principle V-2.4), we then get the direct part (point *1*) of the following theorem.

1.3. Theorem. *Let V be a smooth compact manifold, and let $\mathbf{A} = C^\infty(V)$.*

1. *If $W \xrightarrow{\pi} V$ is a vector bundle on V, the $\mathbf{A}$-module of the smooth sections of W is a finitely generated projective module.*
2. *Conversely, every finitely generated projective $\mathbf{A}$-module is isomorphic to the module of the smooth sections of a vector bundle on V.*

Let us consider the converse part of the theorem: if we take a finitely generated projective $\mathbf{A}$-module M, we can construct a vector bundle W over V for which the module of sections is isomorphic to M. We proceed as follows. Consider a projection matrix $F = (f_{ij}) \in \mathbb{M}_n(\mathbf{A})$ such that $\mathrm{Im}\, F \simeq M$ and set

$$W = \{\, (x, h) \in V \times \mathbb{R}^n \mid h \in \mathrm{Im}\, F|_x \,\},$$

where $F|_x$ designates the matrix $(f_{ij}(x))$. The reader will then be able to show that $\mathrm{Im}\, F$ is identified with the module of sections $\Gamma(W)$: to the element $s \in \operatorname{Im} F$ is matched the section $\widetilde{s}$ defined by $x \mapsto \widetilde{s}(x) = (x, s|_x)$. In addition, in the case where F is the standard projection matrix

$$\mathrm{I}_{k,n} = \begin{array}{|c|c|}\hline \mathrm{I}_k & 0 \\ \hline 0 & 0_r \\ \hline \end{array} \quad (k + r = n),$$

then W is clearly trivial; it is equal to $V \times \left(\mathbb{R}^k \times \{0\}^r\right)$. Finally, a finitely generated projective module becomes free after localization at the appropriate comaximal elements (Theorem V-6.1, point *3*, or Theorem X-1.7, more precise matrix form). Consequently, the bundle W defined above is locally trivial; it is indeed a vector bundle.

Tangent vectors and derivations

A decisive example of a vector bundle is the tangent bundle, for which the elements are the pairs (p, v) where $p \in V$ and v is a tangent vector at the point p.

When the manifold V is a manifold immersed in a space $\mathbb{R}^n$, a tangent vector v at the point p can be identified with the derivation at the point p in the direction of v.

When the manifold V is not a manifold immersed in a space $\mathbb{R}^n$, a tangent vector v can be *defined* as a *derivation at the point p,* i.e. as an $\mathbb{R}$-linear form $v : \mathbf{A} \to \mathbb{R}$ which satisfies Leibniz's rule

$$v(fg) = f(p)v(g) + g(p)v(f). \tag{1}$$

We can check with a few computations that the tangent vectors at V indeed form a vector bundle T_V over V.

To a vector bundle $\pi : W \to V$ is associated the $\mathbf{A}$-module $\Gamma(W)$ formed by the smooth sections of the bundle. In the tangent bundle case, $\Gamma(\mathrm{T}_V)$ is nothing else but the $\mathbf{A}$-module of the usual (smooth) vector fields.

Just as a tangent vector at the point p is identified with a derivation at the point p, which can be defined in algebraic terms (equation (1)), a (smooth) tangent vector field can be identified with an element of the $\mathbf{A}$-*module of the derivations of the* $\mathbb{R}$-*algebra* $\mathbf{A}$, defined as follows.

A derivation of an $\mathbb{R}$-algebra $\mathbf{B}$ in a $\mathbf{B}$-module M is an $\mathbb{R}$-linear mapping $v : \mathbf{B} \to M$ which satisfies Leibniz's rule

$$v(fg) = f\,v(g) + g\,v(f). \tag{2}$$

The $\mathbf{B}$-module of derivations of $\mathbf{B}$ in M is denoted by $\mathrm{Der}_{\mathbb{R}}(\mathbf{B}, M)$.

When we "simply" refer to a derivation of an $\mathbb{R}$-algebra gB, what we mean is a derivation with values in $\mathbf{B}$. When the context is clear we write $\mathrm{Der}(\mathbf{B})$ as an abbreviation for $\mathrm{Der}_{\mathbb{R}}(\mathbf{B}, \mathbf{B})$.

The derivations at a point p are then the elements of $\operatorname{Der}_{\mathbb{R}}(\mathbf{A}, \mathbb{R}_p)$ where $\mathbb{R}_p = \mathbb{R}$ is equipped with the $\mathbf{A}$-module structure given by the homomorphism $f \mapsto f(p)$ of $\mathbf{A}$ in $\mathbb{R}$. Thus $\operatorname{Der}_{\mathbb{R}}(\mathbf{A}, \mathbb{R}_p)$ is an abstract algebraic version of the tangent space at the point p at the manifold V.

A smooth manifold is called *parallelizable* if it has a (smooth) field of bases (n smooth sections of the tangent bundle that give a base at every point). This boils down to saying that the tangent bundle is trivial, or even that the $\mathbf{A}$-module of sections of this bundle, the module $\operatorname{Der}(\mathbf{A})$ of derivations of $\mathbf{A}$, is free.

Differentials and cotangent bundle

The dual bundle of the tangent bundle, called the cotangent bundle, has the differential forms on the manifold V as its sections.

The corresponding $\mathbf{A}$-module, called the module of differentials, can be defined *by generators and relations* in the following way.

Generally, if $(f_i)_{i\in I}$ is a family of elements that generate an $\mathbb{R}$-algebra $\mathbf{B}$, the $\mathbf{B}$-*module of (Kähler) differentials* of $\mathbf{B}$, denoted by $\Omega_{\mathbf{B}/\mathbb{R}}$, is generated by the (purely formal) $\mathrm{d}f_i$'s subject to the relations "derived from" the relations that bind the f_i's: if $P \in \mathbb{R}[z_1, \dots, z_n]$ and if $P(f_{i_1}, \dots, f_{i_n}) = 0$, the derived relation is

$$\sum\nolimits_{k=1}^{n} \frac{\partial P}{\partial z_k}(f_{i_1}, \dots, f_{i_n})\mathrm{d}f_{i_k} = 0.$$

Furthermore, we have the canonical mapping $\mathrm{d} : \mathbf{B} \to \Omega_{\mathbf{B}/\mathbb{R}}$ available, defined by $\mathrm{d}f =$ the class of f (if $f = \sum \alpha_i f_i$, with $\alpha_i \in \mathbb{R}$, $\mathrm{d}f = \sum \alpha_i \mathrm{d}f_i$), which is a derivation.[1]

We then prove that, for every $\mathbb{R}$-algebra $\mathbf{B}$, the $\mathbf{B}$-module of derivations of $\mathbf{B}$ is the dual module of the $\mathbf{B}$-module of Kähler differentials.

In the case where the $\mathbf{B}$-module of differentials of $\mathbf{B}$ is a finitely generated projective module (for example when $\mathbf{B} = \mathbf{A}$), then it is itself the dual module of the $\mathbf{B}$-module of derivations of $\mathbf{B}$.

The smooth algebraic compact manifolds case

In the case of a smooth compact real *algebraic* manifold V, the algebra $\mathbf{A}$ of smooth functions on V has as sub-algebra that of the polynomial functions, denoted by $\mathbb{R}[V]$.

The modules of vector fields and differential forms can be defined as above in terms of the algebra $\mathbb{R}[V]$.

Every finitely generated projective module M on $\mathbb{R}[V]$ corresponds to a vector bundle $W \to V$ that we qualify as *strongly algebraic*. The smooth

[1] For further details on the subject see Theorems VI-6.6 and VI-6.7.

sections of this vector bundle form an $\mathbf{A}$-module that is (isomorphic to) the module obtained from M by scalar extension to $\mathbf{A}$.

So, the fact that the manifold is parallelizable can be tested on an elementary level, that of the module M.

Indeed the assertion "the $\mathbf{A}$-module of smooth sections of W is free" concerning the smooth case is equivalent to the corresponding assertion in the algebraic case "the $\mathbb{R}[V]$-module M is free." Proof sketch: Weierstrass' approximation theorem allows us to approximate a smooth section by a polynomial section, and a "smooth basis" (n smooth sections of the bundle that at every point give a basis), by a polynomial one.

Let us now examine the smooth compact surfaces case. Such a surface is parallelizable if and only if it is orientable and has an everywhere nonzero vector field. Figuratively the latter condition reads: the surface can be combed. The integral curves of the vector field then form a *beautiful curve family*, i.e. a locally rectifiable curve family.

Thus for an orientable smooth compact algebraic surface V the following properties are equivalent.

1. There exists an everywhere nonzero vector field.
2. There exists a beautiful curve family.
3. The manifold is parallelizable.
4. The Kähler module of differentials of $\mathbb{R}[V]$ is free.

As previously explained, the latter condition stems from pure algebra (see also Section 2).

Hence the possibility of an "algebraic" proof of the fact that the sphere cannot be combed. This has been done by Richard Swan in [189]. He uses some advanced tools out of the scope of our book.

The differential module and the module of derivations of a finitely presented algebra

Let $\mathbf{R}$ be a commutative ring. For a finitely presented $\mathbf{R}$-algebra

$$\mathbf{A} = \mathbf{R}[X_1, \dots, X_n]/\langle f_1, \dots, f_s\rangle = \mathbf{R}[x_1, \dots, x_n],$$

the definitions of the module of derivations and the module of differentials are updated as follows.

We denote by $\pi : \mathbf{R}[X_1, \dots, X_n] \to \mathbf{A},\ g(\underline{X}) \mapsto g(\underline{x})$ the canonical projection.

We consider the Jacobian matrix of the system of equations $f_1, \ldots, f_s$,

$$J(\underline{X}) = \begin{bmatrix} \frac{\partial f_1}{\partial X_1}(\underline{X}) & \cdots & \frac{\partial f_1}{\partial X_n}(\underline{X}) \\ \vdots & & \vdots \\ \frac{\partial f_s}{\partial X_1}(\underline{X}) & \cdots & \frac{\partial f_s}{\partial X_n}(\underline{X}) \end{bmatrix}.$$

The matrix $J(\underline{x})$ defines an $\mathbf{A}$-linear map $\mathbf{A}^n \to \mathbf{A}^s$. So, we have two natural isomorphisms $\Omega_{\mathbf{A}/\mathbf{R}} \simeq \mathrm{Coker}\ {}^{\mathrm{t}}J(\underline{x})$ and $\mathrm{Der}(\mathbf{A}) \simeq \mathrm{Ker}\, J(\underline{x})$. The first isomorphism results from the definition of the module of differentials. The second can be clarified as follows: if $u = (u_1, \ldots, u_n) \in \mathrm{Ker}\, J(\underline{x})$, we associate with it "the partial derivation in the direction of the tangent vector u" (actually it is rather a vector field) defined by

$$\delta_u : \mathbf{A} \to \mathbf{A},\ \pi(g) \mapsto \sum\nolimits_{i=1}^{n} u_i \frac{\partial g}{\partial X_i}(\underline{x}).$$

So, $u \mapsto \delta_u$ is the isomorphism in question.

Exercise 1. *Prove the statement made about the module of derivations. Then confirm from it that* $\mathrm{Der}(\mathbf{A})$ *is the dual module of* $\Omega_{\mathbf{A}/\mathbf{R}}$*: if* $\varphi : E \to F$ *is a linear map between finite rank free modules, we always have* $\mathrm{Ker}\,\varphi \simeq (E^\star / \mathrm{Im}\ {}^{\mathrm{t}}\varphi)^\star$.

In the remainder of this chapter we are interested in the smooth case, in which the purely algebraic concepts coincide with the analogous concepts from differential geometry.

2. Differential forms with polynomial coefficients on a smooth affine manifold

The module of differential forms with polynomial coefficients on the sphere

Let $S = \left\{ (\alpha, \beta, \gamma) \in \mathbb{R}^3 \,|\, \alpha^2 + \beta^2 + \gamma^2 = 1 \right\}$. The ring of polynomial functions over S is the $\mathbb{R}$-algebra

$$\mathbf{A} = \mathbb{R}[X, Y, Z] / \langle X^2 + Y^2 + Z^2 - 1 \rangle = \mathbb{R}[x, y, z].$$

The $\mathbf{A}$-module of differential forms with polynomial coefficients on S is

$$\Omega_{\mathbf{A}/\mathbb{R}} = (\mathbf{A}\ \mathrm{d}x \oplus \mathbf{A}\ \mathrm{d}y \oplus \mathbf{A}\ \mathrm{d}z) / \langle x\mathrm{d}x + y\mathrm{d}y + z\mathrm{d}z \rangle \simeq \mathbf{A}^3 / \mathbf{A}v,$$

where v is the column vector ${}^{\mathrm{t}}[\, x\ y\ z \,]$.

This vector is *unimodular* (this means that its coordinates are comaximal elements of $\mathbf{A}$) since $[\,x\;y\;z\,]\cdot v = 1$. Thus, the matrix

$$P = v \cdot [\,x\;y\;z\,] = \begin{bmatrix} x^2 & xy & xz \\ xy & y^2 & yz \\ xz & yz & z^2 \end{bmatrix}$$

satisfies $P^2 = P$, $P \cdot v = v$, $\mathrm{Im}(P) = \mathbf{A}v$ such that by posing $Q = \mathrm{I}_3 - P$ we get

$$\mathrm{Im}(Q) \simeq \mathbf{A}^3/\,\mathrm{Im}(P) \simeq \Omega_{\mathbf{A}/\mathbb{R}}, \text{ and } \Omega_{\mathbf{A}/\mathbb{R}} \oplus \mathrm{Im}(P) \simeq \Omega_{\mathbf{A}/\mathbb{R}} \oplus \mathbf{A} \simeq \mathbf{A}^3.$$

This highlights the fact that $\Omega_{\mathbf{A}/\mathbb{R}}$ is a stably free projective $\mathbf{A}$-module of rank 2.

The previous considerations continue to hold if we substitute $\mathbb{R}$ by a field of characteristic $\neq 2$ or even by a commutative ring $\mathbf{R}$ where 2 is invertible.

An interesting problem that arises is to ask for which rings $\mathbf{R}$, precisely, is the $\mathbf{A}$-module $\Omega_{\mathbf{A}/\mathbf{R}}$ free.

The module of differential forms with polynomial coefficients on a smooth algebraic manifold

The smooth hypersurface case

Let $\mathbf{R}$ be a commutative ring, and $f(X_1, \ldots, X_n) \in \mathbf{R}[X_1, \ldots, X_n] = \mathbf{R}[\underline{X}]$. Consider the $\mathbf{R}$-algebra

$$\mathbf{A} = \mathbf{R}[X_1, \ldots, X_n]/\langle f \rangle = \mathbf{R}[x_1, \ldots, x_n] = \mathbf{R}[\underline{x}].$$

We say that *the hypersurface S defined by $f = 0$ is smooth* if for every field $\mathbf{K}$ "extension of $\mathbf{R}$" ([2]) and for every point $\underline{\xi} = (\xi_1, \ldots, \xi_n) \in \mathbf{K}^n$ satisfying $f(\underline{\xi}) = 0$ one of the coordinates $(\partial f/\partial X_i)(\underline{\xi})$ is nonzero. By the formal Nullstellensatz, this is equivalent to the existence of F, B_1, …, B_n in $\mathbf{R}[\underline{X}]$ satisfying

$$Ff + B_1 \frac{\partial f}{\partial X_1} + \cdots + B_n \frac{\partial f}{\partial X_n} = 1.$$

Let $b_i = B_i(\underline{x})$ be the image of B_i in $\mathbf{A}$ and $\partial_i f = (\partial f/\partial X_i)(\underline{x})$. We thus have in $\mathbf{A}$

$$b_1\,\partial_1 f + \cdots + b_n\,\partial_n f = 1.$$

[2] In this introductory chapter, when we use the incantatory figurative expression *field* $\mathbf{K}$ *"extension of* $\mathbf{R}$*,"* we simply mean that $\mathbf{K}$ is a field with an $\mathbf{R}$-algebra structure. This boils down to saying that a subring of $\mathbf{K}$ is isomorphic to a (integral) quotient of $\mathbf{R}$, and that the isomorphism is given. Consequently the coefficients of f can be "seen" in $\mathbf{K}$ and the speech following the incantatory expression does indeed have a precise algebraic meaning. In Chapter III we will define a ring extension as an *injective* homomorphism. This definition directly conflicts with the figurative expression used here if $\mathbf{R}$ is not a field. This explains the inverted commas used in the current chapter.

The **A**-module of differential forms with polynomial coefficients on S is

$$\Omega_{\mathbf{A}/\mathbf{R}} = (\mathbf{A}\ \mathrm{d}x_1 \oplus \cdots \oplus \mathbf{A}\ \mathrm{d}x_n)/\langle \mathrm{d}f\rangle \simeq \mathbf{A}^n/\mathbf{A}v,$$

where v is the column vector ${}^{\mathrm{t}}[\,\partial_1 f\ \cdots\ \partial_n f\,]$. This vector is unimodular since $[\,b_1\ \cdots\ b_n\,]\cdot v = 1$. So, the matrix

$$P = v\cdot[\,b_1\ \cdots\ b_n\,] = \begin{bmatrix} b_1\partial_1 f & \dots & b_n\partial_1 f \\ \vdots & & \vdots \\ b_1\partial_n f & \dots & b_n\partial_n f \end{bmatrix}$$

satisfies $P^2 = P$, $P\cdot v = v$, $\mathrm{Im}(P) = \mathbf{A}v$ such that by posing $Q = \mathrm{I}_n - P$ we get

$$\mathrm{Im}(Q) \simeq \mathbf{A}^n/\,\mathrm{Im}(P) \simeq \Omega_{\mathbf{A}/\mathbf{R}} \ \text{ and }\ \Omega_{\mathbf{A}/\mathbf{R}} \oplus \mathrm{Im}(P) \simeq \Omega_{\mathbf{A}/\mathbf{R}} \oplus \mathbf{A} \simeq \mathbf{A}^n.$$

This highlights the fact that $\Omega_{\mathbf{A}/\mathbf{R}}$ is a stably free projective **A**-module of rank $n-1$.

The smooth complete intersection case

We treat the case of using two equations to define a smooth complete intersection. The generalization to an arbitrary number of equations is straightforward.

Let **R** be a commutative ring, and $f(\underline{X})$, $g(\underline{X}) \in \mathbf{R}[X_1,\dots,X_n]$. Consider the **R**-algebra

$$\mathbf{A} = \mathbf{R}[X_1,\dots,X_n]/\langle f,g\rangle = \mathbf{R}[x_1,\dots,x_n] = \mathbf{R}[\underline{x}].$$

The Jacobian matrix of the system of equations (f,g) is

$$J(\underline{X}) = \begin{bmatrix} \frac{\partial f}{\partial X_1}(\underline{X}) & \cdots & \frac{\partial f}{\partial X_n}(\underline{X}) \\ \frac{\partial g}{\partial X_1}(\underline{X}) & \cdots & \frac{\partial g}{\partial X_n}(\underline{X}) \end{bmatrix}.$$

We say that *the algebraic manifold S defined by $f = g = 0$ is smooth and of codimension* 2 if, for every field **K** "extension of **R**" and for every point $(\underline{\xi}) = (\xi_1,\dots,\xi_n) \in \mathbf{K}^n$ satisfying $f(\underline{\xi}) = g(\underline{\xi}) = 0$, then one of the 2×2 minors of the Jacobian matrix $J_{k,\ell}(\underline{\xi})$, where

$$J_{k,\ell}(\underline{X}) = \begin{vmatrix} \frac{\partial f}{\partial X_k}(\underline{X}) & \frac{\partial f}{\partial X_\ell}(\underline{X}) \\ \frac{\partial g}{\partial X_k}(\underline{X}) & \frac{\partial g}{\partial X_\ell}(\underline{X}) \end{vmatrix}$$

is nonzero.

By the formal Nullstellensatz, this is equivalent to the existence of polynomials F, G and $(B_{k,\ell})_{1\leqslant k<\ell\leqslant n}$ in $\mathbf{R}[\underline{X}]$ which satisfy

$$Ff + Gg + \textstyle\sum_{1\leqslant k<\ell\leqslant n} B_{k,\ell}(\underline{X})J_{k,\ell}(\underline{X}) = 1.$$

Let $b_{k,\ell} = B_{k,\ell}(\underline{x})$ be the image of $B_{k,\ell}$ in **A** and $j_{k,\ell} = J_{k,\ell}(\underline{x})$. We therefore have in $\mathbf{A}$

$$\sum\nolimits_{1 \leqslant k < \ell \leqslant n} b_{k,\ell}\, j_{k,\ell} = 1. \tag{$*$}$$

The $\mathbf{A}$-module of differential forms with polynomial coefficients on S is

$$\Omega_{\mathbf{A}/\mathbf{R}} = (\mathbf{A}\ \mathrm{d}x_1 \oplus \cdots \oplus \mathbf{A}\ \mathrm{d}x_n)/\langle \mathrm{d}f, \mathrm{d}g\rangle \simeq \mathbf{A}^n/\operatorname{Im}{}^{\mathrm{t}}J,$$

where ${}^{\mathrm{t}}J$ is the Jacobian matrix transpose (taken in $\mathbf{A}$):

$${}^{\mathrm{t}}J = {}^{\mathrm{t}}J(\underline{x}) = \begin{bmatrix} \partial_1 f & \partial_1 g \\ \vdots & \vdots \\ \partial_n f & \partial_n g \end{bmatrix}.$$

Equality $(*)$ implies that the Jacobian matrix $J(\underline{x})$ defines a surjective linear map, and its transpose defines an injective linear map: more precisely, if we let

$$T_{k,l}(\underline{x}) = \begin{bmatrix} 0 & \cdots & 0 & \partial_\ell g & 0 & \cdots & 0 & -\partial_k g & 0 & \cdots & 0 \\ 0 & \cdots & 0 & -\partial_\ell f & 0 & \cdots & 0 & \partial_k f & 0 & \cdots & 0 \end{bmatrix}$$

and $T = \sum_{1 \leqslant k < \ell \leqslant n} b_{k,\ell} T_{k,l}$, then $T \cdot {}^{\mathrm{t}}J = \mathrm{I}_2 = J \cdot {}^{\mathrm{t}}T$ and the matrix $P = {}^{\mathrm{t}}J \cdot T$ satisfies

$$P^2 = P,\ P \cdot {}^{\mathrm{t}}J = {}^{\mathrm{t}}J,\ \operatorname{Im} P = \operatorname{Im}{}^{\mathrm{t}}J \simeq \mathbf{A}^2,$$

so that by posing $Q = \mathrm{I}_n - P$ we get

$$\operatorname{Im} Q \simeq \mathbf{A}^n/\operatorname{Im} P \simeq \Omega_{\mathbf{A}/\mathbf{R}} \text{ and } \Omega_{\mathbf{A}/\mathbf{R}} \oplus \operatorname{Im} P \simeq \Omega_{\mathbf{A}/\mathbf{R}} \oplus \mathbf{A}^2 \simeq \mathbf{A}^n.$$

This highlights the fact that $\Omega_{\mathbf{A}/\mathbf{R}}$ is a stably free projective $\mathbf{A}$-module of rank $n-2$.

The general case

We treat the case of using m equations to define a smooth manifold of codimension r.

Let $\mathbf{R}$ be a commutative ring, and $f_i(\underline{X}) \in \mathbf{R}[X_1, \ldots, X_n]$, $i = 1, \ldots, m$. Consider the $\mathbf{R}$-algebra

$$\mathbf{A} = \mathbf{R}[X_1, \ldots, X_n]/\langle f_1, \ldots, f_m\rangle = \mathbf{R}[x_1, \ldots, x_n] = \mathbf{R}[\underline{x}].$$

The Jacobian matrix of the system of equations $(f_1, \ldots, f_m)$ is

$$J(\underline{X}) = \begin{bmatrix} \frac{\partial f_1}{\partial X_1}(\underline{X}) & \cdots & \frac{\partial f_1}{\partial X_n}(\underline{X}) \\ \vdots & & \vdots \\ \frac{\partial f_m}{\partial X_1}(\underline{X}) & \cdots & \frac{\partial f_m}{\partial X_n}(\underline{X}) \end{bmatrix}.$$

We say that *the algebraic manifold S defined by $f_1 = \cdots = f_m = 0$ is smooth and of codimension* r if the Jacobian matrix taken in $\mathbf{A}$ is "of rank r," i.e.

every minor of order $r+1$ is zero,
and the minors of order r are comaximal.

This implies that for every field $\mathbf{K}$ "extension of $\mathbf{R}$" and at every point $(\underline{\xi}) \in \mathbf{K}^n$ of the manifold of the zeros of the f_i's in $\mathbf{K}^n$, the tangent space is of codimension r. If the ring $\mathbf{A}$ is reduced, this "geometric" condition is in fact sufficient (in classical mathematics).

Let $J^{i_1,\dots,i_r}_{k_1,\dots,k_r}(\underline{X})$ be the $r \times r$ minor extracted from the rows $i_1, \dots, i_r$ and from the columns $k_1, \dots, k_r$ of $J(\underline{X})$, and taken in $\mathbf{A}$: $j^{i_1,\dots,i_r}_{k_1,\dots,k_r} = J^{i_1,\dots,i_r}_{k_1,\dots,k_r}(\underline{x})$.

The condition on $r \times r$ minors indicates the existence of elements $b^{i_1,\dots,i_r}_{k_1,\dots,k_r}$ of $\mathbf{A}$ such that

$$\sum_{1 \leqslant k_1 < \cdots < k_r \leqslant n, 1 \leqslant i_1 < \cdots < i_r \leqslant m} b^{i_1,\dots,i_r}_{k_1,\dots,k_r}\, j^{i_1,\dots,i_r}_{k_1,\dots,k_r} = 1.$$

The $\mathbf{A}$-module of differential forms with polynomial coefficients on S is

$$\Omega_{\mathbf{A}/\mathbf{R}} = (\mathbf{A}\ \mathrm{d}x_1 \oplus \cdots \oplus \mathbf{A}\ \mathrm{d}x_n)/\langle \mathrm{d}f_1, \dots, \mathrm{d}f_m \rangle \simeq \mathbf{A}^n / \operatorname{Im}\, {}^{\mathrm{t}}\!J,$$

where ${}^{\mathrm{t}}\!J = {}^{\mathrm{t}}\!J(\underline{x})$ is the Jacobian matrix transpose (seen in $\mathbf{A}$).

We will see that $\operatorname{Im}\, {}^{\mathrm{t}}\!J$ is the image of a projection matrix of rank $n - r$. This will highlight the fact that $\Omega_{\mathbf{A}/\mathbf{R}}$ is a projective $\mathbf{A}$-module of rank $n - r$ (but a priori it is not stably free).

To do so it suffices to compute a matrix H of $\mathbf{A}^{m \times n}$ such that ${}^{\mathrm{t}}\!J\, H\, {}^{\mathrm{t}}\!J = {}^{\mathrm{t}}\!J$, as then the matrix $P = {}^{\mathrm{t}}\!J\, H$ is the sought projection matrix.

We are therefore reduced to solve a system of linear equations whose unknowns are the coefficients of the matrix H. However, the solution of a system of linear equations is essentially a local matter, and if we localize by rendering a minor of order r invertible, the solution is not too difficult to find, knowing that every minor of order $r+1$ is zero.

Here is an example of how this can work.

Exercise 2. In this exercise, we perform a patching in the most naive way possible. Let $A \in \mathbf{A}^{n \times m}$ be a matrix of rank r. We want to construct a matrix $B \in \mathbf{A}^{m \times n}$ such that $ABA = A$. Note that if we have a solution for a matrix A, we ipso facto have a solution for every equivalent matrix.

1. Treat the case where $A = \mathrm{I}_{r,n,m} = \begin{array}{|c|c|} \hline \mathrm{I}_r & 0 \\ \hline 0 & 0 \\ \hline \end{array}$

2. Treat the case where $PAQ = \mathrm{I}_{r,n,m}$ with P and Q invertible.

3. Treat the case where A has an invertible minor of order r.

4. Treat the general case.

Solution. *1.* Take $B = {}^{\mathrm{t}}A$.

2. Take $B = Q\,{}^{\mathrm{t}}(PAQ)P$.

3. Suppose without loss of generality that the invertible minor is in the north-west corner. Let $s = n - r$, $t = m - r$. We write $\delta_1 = \det R$,

$$A = \begin{array}{|c|c|}\hline R & -V \\ \hline -U & W \\ \hline \end{array}\,,\ L = \begin{array}{|c|c|}\hline \mathrm{I}_r & 0 \\ \hline U\widetilde{R} & \delta_1 \mathrm{I}_s \\ \hline \end{array}\,,\ C = \begin{array}{|c|c|}\hline \mathrm{I}_r & \widetilde{R}V \\ \hline 0 & \delta_1 \mathrm{I}_t \\ \hline \end{array}\,.$$

We get $LA = \begin{array}{|c|c|}\hline R & -V \\ \hline 0 & W' \\ \hline \end{array}$ with $W' = -\delta_1 U\widetilde{R}V + W$, then

$$LAC = \begin{array}{|c|c|}\hline R & 0 \\ \hline 0 & \delta_1 W' \\ \hline \end{array}\,.$$

Since the minors of order $r + 1$ of A are zero, we get $\delta_1^2 W' = 0$. Thus let $M = \begin{array}{|c|c|}\hline \widetilde{R} & 0 \\ \hline 0 & 0 \\ \hline \end{array}$, hence $(LAC)M(LAC) = \begin{array}{|c|c|}\hline \delta_1 R & 0 \\ \hline 0 & 0 \\ \hline \end{array} = \delta_1 LAC$.

With $B_1 = CML$ this gives

$$LAB_1AC = (LAC)M(LAC) = \delta_1 LAC,$$

thus by multiplying on the left by $\widetilde{L}$ and on the right by $\widetilde{C}$

$$\delta_1^{s+t} AB_1A = \delta_1^{s+t+1} A.$$

Whence the solution $B = B_1/\delta_1$ since we supposed that δ_1 is invertible.

4. The precomputation made with the minor δ_1 did not require that it be invertible. It can be done with each of the minors δ_ℓ of order r of A. This results in as many equalities $\delta_\ell^{s+t} AB_\ell A = \delta_\ell^{s+t+1} A$.

A linear combination $\sum_\ell a_\ell \delta_\ell = 1$, raised to a sufficient power, results in an equality $\sum_\ell b_\ell \delta_\ell^{s+t+1} = 1$, hence $ABA = A$ for $B = \sum_\ell b_\ell \delta_\ell^{s+t} B_\ell$. □

Remarks.
1) We will return to the equality $ABA = A$ when using a Cramer-style magical formula, cf. Theorem II-5.14.

2) In the last example, we were directly inspired by the "Rank Theorem" which states that if a smooth mapping $\varphi : U \to \mathbb{R}^k$ has constant rank r at every point of $V = \{\, x \in U \mid \varphi(x) = 0 \,\}$, then V is a smooth sub-manifold of codimension r of the open subset $U \subseteq \mathbb{R}^n$. It turns out that the analogue we have developed here does not always work correctly. For example with $\mathbf{R} = \mathbb{F}_2$, $f_1 = X^2 + Y$ and $f_2 = Y^2$, the manifold V is reduced to a point, the origin (even if we pass to the algebraic closure of $\mathbb{F}_2$), in which the Jacobian matrix is of rank 1: $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$. However, V is not a curve, it is a multiple point. This means that the Rank Theorem poses some problems in nonzero characteristic. Our definition is therefore abusive when $\mathbf{R}$ is not a $\mathbb{Q}$-algebra. ■

Chapter II

The basic local-global principle and systems of linear equations

Contents

In this Chapter, as in the entirety of this manuscript unless explicitly stated otherwise, rings are commutative and unitary, and homomorphisms between rings preserve the multiplicative identities. In particular, a subring has the same multiplicative identity as the whole ring.

Introduction

Solving systems of linear equations is an omnipresent theme of commutative algebra, in particular in its most developed form for which homological methods are at use. In this chapter, we recall some classical results on this topic, which we will come back to often throughout this work.

Particular attention is given to the basic local-global principle, the notion of a coherent module and some variants of Cramer's formula.

1. Some facts concerning quotients and localizations

Let us begin by recalling the following result on quotients. Let $\mathfrak{a}$ be an ideal of a ring $\mathbf{A}$. When needed, the canonical mapping will be denoted by $\pi_{\mathbf{A},\mathfrak{a}} : \mathbf{A} \to \mathbf{A}/\mathfrak{a}$.

The quotient ring $(\mathbf{A}/\mathfrak{a}\,, \pi_{\mathbf{A},\mathfrak{a}})$ is characterized, *up to unique isomorphism*, by the following universal property.

1.1. Fact. (Characteristic property of the quotient by the ideal $\mathfrak{a}$)
A ring homomorphism $\psi : \mathbf{A} \to \mathbf{B}$ is factorized by $\pi_{\mathbf{A},\mathfrak{a}}$ if and only if $\mathfrak{a} \subseteq \operatorname{Ker}\psi$, meaning $\psi(\mathfrak{a}) \subseteq \{0_{\mathbf{B}}\}$. In this case, the factorization is unique.

$$\begin{tikzcd}
\mathbf{A} \arrow[d, "\pi_{\mathbf{A},\mathfrak{a}}"'] \arrow[dr, "\psi"] & \\
\mathbf{A}/\mathfrak{a} \arrow[r, dashed, "\theta\,!"'] & \mathbf{B}
\end{tikzcd}$$

homomorphisms vanishing on $\mathfrak{a}$.

Explanation regarding the figure. *In a figure of the type found above, everything but the morphism θ corresponding to the dotted arrow is given. The exclamation mark signifies that θ makes the diagram commute and that it is* the unique *morphism with this property.*

We denote by $M/\mathfrak{a}M$ the $\mathbf{A}/\mathfrak{a}$-module obtained from the quotient of the $\mathbf{A}$-module M by the submodule generated by the elements ax for $a \in \mathfrak{a}$ and $x \in M$. This module can thus be defined through the extension of scalars to $\mathbf{A}/\mathfrak{a}$ from the $\mathbf{A}$-module M (see page 196, and exercise IV-5).

Let us move on to localizations, which are very analogous to quotients (we will return to this analogy in further detail on page 644). In this work, when referring to a *monoid* contained within a ring (i.e. a submonoid of a ring) we always assume a subset of the ring which contains 1 and is closed under multiplication.

For a given ring $\mathbf{A}$, we denote by $\mathbf{A}^\times$ the multiplicative group of invertible elements, also called the *group of units*.

If S is a monoid, we denote by $\mathbf{A}_S$ or $S^{-1}\mathbf{A}$ the localization of $\mathbf{A}$ at S. Every element of $\mathbf{A}_S$ can be written in the form x/s with $x \in \mathbf{A}$ and $s \in S$. By definition we have $x_1/s_1 = x_2/s_2$ if there exists an $s \in S$ such that $ss_2x_1 = ss_1x_2$. When needed, we will denote by $j_{\mathbf{A},S} : \mathbf{A} \to \mathbf{A}_S$ the canonical mapping $x \mapsto x/1$.

The localized ring $(\mathbf{A}_S, j_{\mathbf{A},S})$ is characterized, *up to unique isomorphism*, by the following universal property.

1.2. Fact. (Characteristic property of the localization at S)
A ring homomorphism $\psi : \mathbf{A} \to \mathbf{B}$ is factorized by $j_{\mathbf{A},S}$ if and only if $\psi(S) \subseteq \mathbf{B}^\times$. When this is the case, the factorization is unique.

$$\begin{tikzcd}
\mathbf{A} \arrow[d, "j_{\mathbf{A},S}"'] \arrow[dr, "\psi"] & \\
S^{-1}\mathbf{A} \arrow[r, dashed, "\theta\,!"'] & \mathbf{B}
\end{tikzcd}$$

homomorphisms which send S into $\mathbf{B}^\times$.

Similarly, we denote by $M_S = S^{-1}M$ the $\mathbf{A}_S$-module obtained by localization of the $\mathbf{A}$-module M at S. Every element of M_S is of the form x/s with $x \in M$ and $s \in S$. By definition, we have $x_1/s_1 = x_2/s_2$ if there exists an $s \in S$ such that $ss_2x_1 = ss_1x_2$. This module M_S can also be defined through an extension of scalars to $\mathbf{A}_S$ from the $\mathbf{A}$-module M (see page 196, and exercise IV-5).

The monoid S contained in a ring $\mathbf{A}$ is called *saturated* when

$$\forall s, t \in \mathbf{A} \ \ (st \in S \ \Rightarrow \ s \in S)$$

is satisfied. A saturated monoid is also called a *filter.* A *principal filter* is a filter generated by a single element; that is, it is just the set of divisors of some arbitrary power of that element. We denote by S^{sat} the saturation of the monoid S; it is obtained by adding all elements dividing an element of S. When we saturate a monoid, the localization remains unchanged.[1] Two monoids S_1 and S_2 are said to be *equivalent* if they have the same saturation. We then write $\mathbf{A}_{S_1} = \mathbf{A}_{S_2}$.

It is possible to localize by a monoid which contains 0.
The result is then the *trivial* ring (recall that a ring is trivial if it is reduced to a single element, i.e. if $1 = 0$).

If S is generated by $s \in \mathbf{A}$, i.e. if $S = s^{\mathbb{N}} \overset{\mathrm{def}}{=} \left\{ s^k \mid k \in \mathbb{N} \right\}$, we denote by $\mathbf{A}_s$ or $\mathbf{A}[1/s]$ the localized ring $S^{-1}\mathbf{A}$, which is isomorphic to $\mathbf{A}[T]/\langle sT - 1\rangle$.

In a ring, the *conductor* of an ideal $\mathfrak{a}$ into an ideal $\mathfrak{b}$ is the ideal

$$(\mathfrak{b} : \mathfrak{a})_{\mathbf{A}} = \{ a \in \mathbf{A} \mid a\mathfrak{a} \subseteq \mathfrak{b} \}.$$

More generally, if N and P are submodules of an $\mathbf{A}$-module M, we define the *conductor* of N into P as the ideal

$$(P : N)_{\mathbf{A}} = \{ a \in \mathbf{A} \mid aN \subseteq P \}.$$

Recall also that the *annihilator* of an element x from an $\mathbf{A}$-module M is the ideal $\mathrm{Ann}_{\mathbf{A}}(x) = (\langle 0_{\mathbf{A}} \rangle : \langle x \rangle) = \{ a \in \mathbf{A} \mid ax = 0 \}$.

The *annihilator of a module* M is the ideal $\mathrm{Ann}_{\mathbf{A}}(M) = (\langle 0_M \rangle : M)_{\mathbf{A}}$. A module or an ideal is *faithful* if its annihilator is reduced to 0.

The following notations are also useful for a submodule N of M.

$$(N : \mathfrak{a})_M = \{ x \in M \mid x\,\mathfrak{a} \subseteq N \}.$$

$$(N : \mathfrak{a}^{\infty})_M = \{ x \in M \mid \exists n,\, x\,\mathfrak{a}^n \subseteq N \}.$$

The latter submodule is called the *saturation* of N by $\mathfrak{a}$ in M.

We say that an element x of an $\mathbf{A}$-module M is *regular* (if $M = \mathbf{A}$ we also say that x is a *nonzerodivisor*) if the sequence

$$0 \longrightarrow \mathbf{A} \xrightarrow{.x} M$$

is exact; in other words if $\mathrm{Ann}(x) = 0$. If $0_{\mathbf{A}}$ is a regular in $\mathbf{A}$, the ring is trivial.

[1] In fact, depending on the specific construction chosen to define localization, we would either have an equality or a canonical isomorphism between the two localizations.

When the context is unambiguous, we omit the $\mathbf{A}$ or M subscript to simplify the previous notations regarding conductors.

The *total ring of fractions* or *total quotient ring* of $\mathbf{A}$, denoted by $\operatorname{Frac}\mathbf{A}$, is the localized ring $\mathbf{A}_S$, where S is the monoid of regular elements of $\mathbf{A}$, denoted by $\operatorname{Reg}\mathbf{A}$.

1.3. Fact.

1. *The kernel of the natural homomorphism* $j_{\mathbf{A},s} : \mathbf{A} \to \mathbf{A}_s = \mathbf{A}[1/s]$ *is the ideal* $(0 : s^\infty)_\mathbf{A}$. *It is reduced to* 0 *if and only if* s *is regular.*
2. *Similarly, the kernel of the natural homomorphism of* M *to* $M_s = M[1/s]$ *is the* $\mathbf{A}$*-submodule* $(0 : s^\infty)_M$.
3. *The natural homomorphism* $\mathbf{A} \to \operatorname{Frac}\mathbf{A}$ *is injective.*

1.4. Fact. *If* $S \subseteq S'$ *are two monoids of* $\mathbf{A}$ *and* M *is an* $\mathbf{A}$*-module, we have two canonical identifications* $(\mathbf{A}_S)_{S'} \simeq \mathbf{A}_{S'}$ *and* $(M_S)_{S'} \simeq M_{S'}$.

2. The basic local-global principle

We will study the general workings of the local-global principle in commutative algebra in Chapter XV. However, we will encounter it at every turn, under different forms adapted to each situation. In this section, an essential instance of this principle is given as it is so simple and efficient that it would be a pity to go without it any longer.

The local-global principle affirms that certain properties are true if and only if they are true after "sufficiently many" localizations. In classical mathematics we often invoke localization at every maximal ideal. It is a lot of work and seems a bit mysterious, especially from an algorithmic point of view. We will use simpler (and less intimidating) versions in which only a finite number of localizations are used.

Comaximal localizations and the local-global principle

The following definition corresponds to the intuitive idea that certain (finite) systems of localizations of a ring $\mathbf{A}$ are "sufficiently numerous" to capture all the information contained within $\mathbf{A}$.

2.1. Definition.

1. Let s_1, …, s_n be elements. if $\langle 1 \rangle = \langle s_1, \dots, s_n \rangle$ then s_1, …, s_n are said to be *comaximal.*
2. Let S_1, …, S_n be monoids. If for every $s_1 \in S_1$, …, $s_n \in S_n$, the s_i's are comaximal then S_1, …, S_n are called *comaximal.*

Two fundamental examples.

1) If $s_1, \ldots, s_n$ are comaximal then the monoids they generate are comaximal. Indeed, consider every $s_i^{m_i}$ ($m_i \geqslant 1$) in the monoids $s_i^{\mathbb{N}}$ and let $a_1, \ldots, a_n$ be such that $\sum_{i=1}^n a_i s_i = 1$. By raising the latter equality to the power of $1 - n + \sum_{i=1}^n m_i$ and by conveniently regrouping the terms in the resulting sum, we get an equality of the form $\sum_{i=1}^n b_i s_i^{m_i} = 1$, as required.

2) If $a = a_1 \cdots a_n \in \mathbf{A}$, then the monoids $a^{\mathbb{N}}$, $1 + a_1\mathbf{A}$, ..., $1 + a_n\mathbf{A}$ are comaximal. Indeed, take an element $b_i = 1 - a_i x_i$ in each monoid $1 + a_i\mathbf{A}$ and an element a^m in the monoid $a^{\mathbb{N}}$. We need to prove that the ideal $\mathfrak{m} = \langle a^m, b_1, \ldots, b_n \rangle$ contains 1. However, modulo $\mathfrak{m}$ we have $1 = a_i x_i$, thus $1 = a \prod_i x_i = ax$, and we finally obtain $1 = 1^m = a^m x^m = 0$. ∎

Here is a characterization from classical mathematics.

2.2. Fact*. Let S_1, ..., S_n be monoids in a nontrivial ring $\mathbf{A}$ (i.e., $1 \neq_{\mathbf{A}} 0$). The monoids S_i are comaximal if and only if for every prime ideal (resp. for every maximal ideal) $\mathfrak{p}$ one of the S_i is contained within $\mathbf{A} \setminus \mathfrak{p}$.

D Let $\mathfrak{p}$ be a prime ideal. If none of the S_i's are contained in $\mathbf{A} \setminus \mathfrak{p}$ then for each i there exists some $s_i \in S_i \cap \mathfrak{p}$. Consequently, s_1, ..., s_n are not comaximal.

Conversely, suppose that for every maximal ideal $\mathfrak{m}$ one of the S_i's is contained within $\mathbf{A} \setminus \mathfrak{m}$ and let $s_1 \in S_1$, ..., $s_n \in S_n$ then the ideal $\langle s_1, \ldots, s_n \rangle$ is not contained in any maximal ideal. Thus it contains 1. □

We denote by $\mathbf{A}^{m \times p}$ or $\mathbb{M}_{m,p}(\mathbf{A})$ the $\mathbf{A}$-module of m-by-p matrices with coefficients in $\mathbf{A}$, and $\mathbb{M}_n(\mathbf{A})$ means $\mathbb{M}_{n,n}(\mathbf{A})$. The group of invertible matrices is denoted by $\mathbb{GL}_n(\mathbf{A})$, the subgroup consisting of the matrices of determinant 1 is denoted by $\mathbb{SL}_n(\mathbf{A})$. The subset of $\mathbb{M}_n(\mathbf{A})$ consisting of the projection matrices (i.e. matrices F such that $F^2 = F$) is denoted by $\mathbb{AG}_n(\mathbf{A})$. The acronyms are explained as follows: $\mathbb{GL}$ for linear group, $\mathbb{SL}$ for special linear group and $\mathbb{AG}$ for affine Grassmannian.

2.3. Concrete local-global principle. (Basic local-global principle, concrete gluing of solutions of a system of linear equations)

Let S_1, ..., S_n be comaximal monoids of $\mathbf{A}$, B a matrix of $\mathbf{A}^{m \times p}$ and C a column vector of $\mathbf{A}^m$. Then the following properties are equivalent.

1. *The system of linear equations $BX = C$ has a solution in $\mathbf{A}^p$.*
2. *For $i \in [\![1..n]\!]$, the system of linear equations $BX = C$ has a solution in $\mathbf{A}_{S_i}^p$.*

This principle also holds for systems of linear equations with coefficients in an $\mathbf{A}$-module M.

D *1* ⇒ *2.* Clearly true.

2 ⇒ *1.* For each i, we have $Y_i \in \mathbf{A}^p$ and $s_i \in S_i$ such that $B(Y_i/s_i) = C$

in $\mathbf{A}_{S_i}^m$. This means that we have some $t_i \in S_i$ such that $t_i\, BY_i = s_i t_i\, C$ in $\mathbf{A}^m$. Using $\sum_i a_i s_i t_i = 1$, we get a solution in $\mathbf{A}$: $X = \sum_i a_i t_i Y_i$. □

Remark. As to the merits, this concrete local-global principle boils down to the following remark when speaking of an integral ring (a ring is said to be *integral* if every element is null or regular[2]). If every s_i is regular and if

$$\frac{x_1}{s_1} = \frac{x_2}{s_2} = \cdots = \frac{x_n}{s_n},$$

then the common value of these fractions, when $\sum_i s_i u_i = 1$, is also equal to

$$\frac{x_1 u_1 + \cdots + x_n u_n}{s_1 u_1 + \cdots + s_n u_n} = x_1 u_1 + \cdots + x_n u_n.$$

This principle could then also be called "the art of shrewdly getting rid of denominators." Arguably, the most remarkable thing is that this holds in full generality, even if the ring is not integral. Our thanks go to Claude Chevalley for introducing arbitrary localizations. In some scholarly works, we find the following reformulation (at the cost of an information loss regarding the concreteness of the result): the $\mathbf{A}$-module $\bigoplus_{\mathfrak{m}} \mathbf{A}_{1+\mathfrak{m}}$ (where $\mathfrak{m}$ ranges over every maximal ideal of $\mathbf{A}$) is faithfully flat. ■

2.4. Corollary. *Let S_1, …, S_n be comaximal monoids of $\mathbf{A}$, $x \in \mathbf{A}$ and $\mathfrak{a}$, $\mathfrak{b}$ be two finitely generated ideals of $\mathbf{A}$. Then, we have the following equivalences.*

1. *$x = 0$ in $\mathbf{A}$ if and only if for $i \in [\![1..n]\!]$, $x = 0$ on $\mathbf{A}_{S_i}$.*
2. *x is regular in $\mathbf{A}$ if and only if for $i \in [\![1..n]\!]$, x is regular in $\mathbf{A}_{S_i}$.*
3. *$\mathfrak{a} = \langle 1 \rangle$ in $\mathbf{A}$ if and only if for $i \in [\![1..n]\!]$, $\mathfrak{a} = \langle 1 \rangle$ in $\mathbf{A}_{S_i}$.*
4. *$\mathfrak{a} \subseteq \mathfrak{b}$ in $\mathbf{A}$ if and only if for $i \in [\![1..n]\!]$, $\mathfrak{a} \subseteq \mathfrak{b}$ in $\mathbf{A}_{S_i}$.*

D The proof is left to the reader. □

Remark. In fact, as we will see in the local-global principle 6.7, ideals do not need to be finitely generated. ■

Examples

Let us give some simple examples of applications of the basic concrete local-global principle. A typical application of the first example (Fact 2.5) is where the module M in the statement is a nonzero ideal of a Dedekind ring. A module M is said to be *locally cyclic* if after each localization at comaximal monoids $S_1, \ldots, S_n$, it is generated by a single element.

[2] This notion is discussed in further detail on page 202.

2.5. Fact. *Let $M = \langle a, b \rangle = \langle c, d \rangle$ be a module with two generator sets. Suppose this module is faithful and locally cyclic. Then, there exists a matrix $A \in \mathbb{SL}_2(\mathbf{A})$ such that $[\,a\;b\,]\,A = [\,c\;d\,]$.*

D If $A = \begin{bmatrix} x & y \\ z & t \end{bmatrix}$, the cotransposed matrix must be equal to

$$B = \operatorname{Adj} A = \begin{bmatrix} t & -y \\ -z & x \end{bmatrix}.$$

In particular, we mean to solve the following system of linear equations:

$$[\,a\;b\,]\,A = [\,c\;d\,], \quad [\,c\;d\,]\,B = [\,a\;b\,] \qquad (*)$$

where the unknowns are x, y, z, t. Note that $A\,B = \det(A)\,\mathrm{I}_2$.
Conversely, if this system of linear equations is solved, we will have $[\,a\;b\,] = [\,a\;b\,]\,A\,B$. So $\big(1 - \det(A)\big)[\,a\;b\,] = [\,0\;0\,]$, and since the module is faithful, $\det(A) = 1$.
We have some comaximal monoids S_i such that M_{S_i} is generated by $g_i/1$ for some $g_i \in M$. To solve the system of linear equations it suffices to solve it after localizing at each of the S_i's.
In the ring $\mathbf{A}_{S_i}$, we have the equalities $a = \alpha_i g_i$, $b = \beta_i g_i$, $g_i = \mu_i a + \nu_i b$, thus $\big(1 - (\alpha_i \mu_i + \beta_i \nu_i)\big)\,g_i = 0$.
The module $M_{S_i} = \langle g_i \rangle$ stays faithful, so $1 = \alpha_i \mu_i + \beta_i \nu_i$ in $\mathbf{A}_{S_i}$. Therefore:

$$[\,a\;b\,]\,E_i = [\,g_i\;0\,] \text{ with } E_i = \begin{bmatrix} \mu_i & -\beta_i \\ \nu_i & \alpha_i \end{bmatrix} \text{ and } \det(E_i) = 1.$$

Similarly we obtain $[\,c\;d\,]\,C_i = [\,g_i\;0\,]$ for some matrix C_i with determinant 1 in $\mathbf{A}_{S_i}$. By taking $A_i = E_i \operatorname{Adj}(C_i)$ we get $[\,a\;b\,]\,A_i = [\,c\;d\,]$ and $\det(A_i) = 1$ in $\mathbf{A}_{S_i}$. Thus the system of linear equations $(*)$ has a solution in $\mathbf{A}_{S_i}$. □

Our second example is given by the Gauss-Joyal Lemma: point *1* in the following lemma is proven by applying the basic local-global principle. Before stating this result, we first need to recall some definitions.

An element a of a ring is said to be *nilpotent* if $a^n = 0$ some integer $n \in \mathbb{N}$. The nilpotent elements of a ring $\mathbf{A}$ form an ideal called *the nilradical*, or the *nilpotent radical* of the ring. A ring is *reduced* if its nilradical equals 0. More generally, the nilradical of an ideal $\mathfrak{a}$ of $\mathbf{A}$ is the ideal consisting of elements $x \in \mathbf{A}$, such that each x has some power in $\mathfrak{a}$. We denote the nilradical of an ideal $\mathfrak{a}$ of $\mathbf{A}$ by $\sqrt{\mathfrak{a}}$ or by $\mathrm{D}_{\mathbf{A}}(\mathfrak{a})$. We also use $\mathrm{D}_{\mathbf{A}}(x)$ to denote $\mathrm{D}_{\mathbf{A}}(\langle x \rangle)$. An ideal $\mathfrak{a}$ is called *a radical ideal* when it is equal to its nilradical. The ring $\mathbf{A}/\mathrm{D}_{\mathbf{A}}(0) = \mathbf{A}_{\mathrm{red}}$ is *the reduced ring associated with* $\mathbf{A}$.
For some polynomial f of $\mathbf{A}[X_1, \ldots, X_n] = \mathbf{A}[\underline{X}]$, we call the *content* of f and denote by $\mathrm{c}_{\mathbf{A},\underline{X}}(f)$ or $\mathrm{c}(f)$ the ideal generated by the coefficients of f. The polynomial f is said to be *primitive* (in $\underline{X}$) when $\mathrm{c}_{\mathbf{A},\underline{X}}(f) = \langle 1 \rangle$.

When a polynomial f of $\mathbf{A}[X]$ is given in the form $f(X) = \sum_{k=0}^{n} a_k X^k$, we say that n is the *formal degree* of f, and a_n is its *formally leading coefficient.* Finally, if f is null, its formal degree is -1.

2.6. Lemma.

1. (Poor man's Gauss-Joyal) *The product of two primitive polynomials is a primitive polynomial.*
2. (Gauss-Joyal) *For f, $g \in \mathbf{A}[\underline{X}]$, there exists a $p \in \mathbb{N}$ such that*
$$\big(\mathrm{c}(f)\mathrm{c}(g)\big)^p \subseteq \mathrm{c}(fg).$$
3. (Nilpotent elements in $\mathbf{A}[\underline{X}]$) *An element f of $\mathbf{A}[\underline{X}]$ is nilpotent if and only if all of its coefficients are nilpotent. In other words, we have the following equality: $(\mathbf{A}[\underline{X}])_{\mathrm{red}} = \mathbf{A}_{\mathrm{red}}[\underline{X}]$.*
4. (Invertible elements in $\mathbf{A}[\underline{X}]$) *An element f of $\mathbf{A}[\underline{X}]$ is invertible if and only if $f(\underline{0})$ is invertible and $f - f(\underline{0})$ is nilpotent. In other words, $\mathbf{A}[\underline{X}]^{\times} = \mathbf{A}^{\times} + \mathrm{D}_{\mathbf{A}}(0)[\underline{X}]$ and in particular $(\mathbf{A}_{\mathrm{red}}[\underline{X}])^{\times} = (\mathbf{A}_{\mathrm{red}})^{\times}$.*

D Note that, a priori, we have the following inclusion: $\mathrm{c}(fg) \subseteq \mathrm{c}(f)\mathrm{c}(g)$.

1. For univariate polynomials f, $g \in \mathbf{A}[X]$. We have $\mathrm{c}(f) = \mathrm{c}(g) = \langle 1 \rangle$. Consider the quotient ring $\mathbf{B} = \mathbf{A}\big/\mathrm{D}_{\mathbf{A}}\big(\mathrm{c}(fg)\big)$. We need to prove that this ring is trivial. It suffices to do so after localization at comaximal elements, for example at the coefficients of f. That is, we can suppose that some coefficient of f is invertible. Let us give a proof of a sufficiently general example. Suppose

$$f(X) = a + bX + X^2 + cX^3 + \ldots \text{ and } g(X) = g_0 + g_1X + g_2X^2 + \ldots$$

In the ring $\mathbf{B}$ we have $ag_0 = 0$, $ag_1 + bg_0 = 0$, $ag_2 + bg_1 + g_0 = 0$, thus $bg_0^2 = 0$, then $g_0^3 = 0$, thus $g_0 = 0$. We then have $g = Xh$ and $c(fg) = c(fh)$. Moreover, since the formal degree of h is smaller than that of g, we can conclude by induction on the formal degree that $g = 0$. As $\mathrm{c}(g) = \langle 1 \rangle$, the ring is trivial.

2. For univariate polynomials. Consider a coefficient a of f and a coefficient b of g. We prove that ab is nilpotent in $\mathbf{B} = \mathbf{A}/\mathrm{c}(fg)$. This boils down to proving that $\mathbf{C} = \mathbf{B}[1/(ab)]$ is trivial. However, in $\mathbf{C}$, f and g are primitive, so point *1* implies that $\mathbf{C}$ is trivial.

2 and *1. General case.* Point *2.* is proved by induction on the number of variables from the univariate case. Indeed, for $f \in \mathbf{A}[X][Y]$ we have the equality $\mathrm{c}_{\mathbf{A},X,Y}(f) = \big\langle \mathrm{c}_{\mathbf{A},X}(h) \mid h \in \mathrm{c}_{\mathbf{A}[X],Y}(f) \big\rangle$. Then we deduce point *1* from it.

3. Note that $f^2 = 0$ implies $\mathrm{c}(f)^p = 0$ for some p from point *2.*

4. The condition is sufficient: in a ring, if x is nilpotent, then $1 - x$ is invertible because $(1 - x)(1 + x + \cdots + x^n) = 1 - x^{n+1}$. Thus if u is invertible and x nilpotent, $u + x$ is invertible. To see that the condition is necessary it suffices to deal with the univariate case (we conclude by induction on the number of variables). Let $fg = 1$ with $f = f(0) + XF(X)$ and $g = g(0) + XG(X)$. We obtain $f(0)g(0) = 1$. Let n be the formal degree of F and m that of G. We must prove that F and G are nilpotent.

If $n = -1$ or $m = -1$, the result is obvious. We reason by induction on $n+m$ assuming that n, $m \geqslant 0$, F_n and G_m being the formally leading coefficients. By induction hypothesis the result is obtained for the rings $(\mathbf{A}/\langle F_n\rangle)[X]$ and $(\mathbf{A}/\langle G_m\rangle)[X]$. Since $F_nG_m = 0$, we can conclude with the following lemma.

NB: some details are given in exercise VII-8. □

2.7. Lemma. *Let a, b, $c \in \mathbf{A}$. If c is nilpotent modulo a and modulo b, and if $ab = 0$, then c is nilpotent.*

D We have $c^n = xa$ and $c^m = yb$ therefore $c^{n+m} = xyab = 0$. □

Remark. We can reformulate this lemma in a more structural manner as follows. For two ideals $\mathfrak{a}$, $\mathfrak{b}$ consider the canonical morphism

$$\mathbf{A} \to \mathbf{A}/\mathfrak{a} \times \mathbf{A}/\mathfrak{b}$$

whose kernel is $\mathfrak{a} \cap \mathfrak{b}$. If an element of $\mathbf{A}$ is nilpotent modulo $\mathfrak{a}$ and modulo $\mathfrak{b}$, it is also nilpotent modulo $\mathfrak{a} \cap \mathfrak{b}$, thus also modulo $\mathfrak{a}\mathfrak{b}$, as $(\mathfrak{a} \cap \mathfrak{b})^2 \subseteq \mathfrak{a}\mathfrak{b}$. This touches on the "closed covering principle," see page 649. ■

Finite character properties

The basic concrete local-global principle can be reformulated as a "transfer principle."

2.8. Basic Transfer principle.
For some system of linear equations in a ring $\mathbf{A}$ the elements s such that the system of linear equations has a solution in $\mathbf{A}[1/s]$ form an ideal of $\mathbf{A}$.

Firstly, we invite the reader to prove that this transfer principle is equivalent to the basic concrete local-global principle.

We now provide a detailed analysis of what is going on. The equivalence actually relies on the following notion.

2.9. Definition. A property P concerning commutative rings and modules is called a *finite character property* if it is preserved by localization and if, when it holds for $S^{-1}\mathbf{A}$, then it also holds for $\mathbf{A}[1/s]$ for some $s \in S$.

2.10. Fact. *Let P be a finite character property. Then the concrete local-global principle for P is equivalent to the transfer principle for P. In other words, the following principles are equivalent.*

1. *If the property P is true after localization at every monoid in a family of comaximal monoids, then it is true.*
2. *The set of elements s (in a given ring) such that the property P is true after localization at s is an ideal.*

D Let $\mathbf{A}$ be a ring which provides the context for the property P. Now consider the set $I = \{\, s \in \mathbf{A} \mid \mathsf{P} \text{ is true for } \mathbf{A}_s \,\}$.

1 ⇒ *2*. Suppose *1*. Let $s, t \in I$, $a, b \in \mathbf{A}$ and $u = as + bt$. The elements s and t are comaximal in $\mathbf{A}_u$. Since P is closed under localization, P is true for $(\mathbf{A}_u)_s = (\mathbf{A}_s)_u$ and $(\mathbf{A}_u)_t = (\mathbf{A}_t)_u$. By applying *1*, P is true for $\mathbf{A}_u$, i.e., $u = as + bt \in I$.

2 ⇒ *1*. Suppose *2* and let (S_i) be the considered family of comaximal monoids. Since we have a property of finite character, we find in each S_i an element s_i such that P is true after localization at s_i. Since the S_i's are comaximal the s_i's are comaximal elements. By applying *2*, we get $I = \langle 1 \rangle$. Finally, the localization at 1 provides the answer. □

Most of the concrete local-global principles which we will consider in this manuscript apply to finite character properties. One may thus replace any concrete local-global principle with its corresponding transfer principle.

For finite character properties we have an equivalence in classical mathematics between two notions, one concrete and the other abstract.

2.11. Fact*. *Let* P *be a finite character property. Then, in classical mathematics the following properties are equivalent.*

1. *There exist comaximal monoids such that the property* P *is true after localization at each monoid.*
2. *The property* P *is true after localization at every maximal ideal.*

D *1* ⇒ *2*. Let (S_i) be the family of comaximal monoids under consideration. Since it is a finite character property, we find in each S_i some element s_i such that P is true after localization at s_i. Since the S_i's are comaximal the s_i's are comaximal elements. Let $\mathfrak{m}$ be a maximal ideal. Some s_i is not in $\mathfrak{m}$. The localization at $1 + \mathfrak{m}$ is a localization of the localization at s_i. Thus P is true after localization at $1 + \mathfrak{m}$.

2 ⇒ *1*. For each maximal ideal $\mathfrak{m}$ select an $s_\mathfrak{m} \notin \mathfrak{m}$ such that the property P is true after localization at $s_\mathfrak{m}$. The set of $s_\mathfrak{m}$ generates an ideal which is not contained in any maximal ideal, therefore it is the ideal $\langle 1 \rangle$. A finite family of some of these $s_\mathfrak{m}$ is then a system of comaximal elements. The family of monoids generated by these elements is suitable. □

We immediately obtain the following corollary.

2.12. Fact*. *Let* P *a finite character property. Then the concrete local-global principle for* P *is equivalent (in classical mathematics) to the abstract local-global principle for* P*. In other words, the following principles are equivalent.*

1. *If the property* P *is true after localization at each monoid in a family of comaximal monoids, then it is true.*
2. *If the property* P *is true after localization at every maximal ideal, then it is true.*

Remark. Let us give a direct proof of the equivalence from classical mathematics between the transfer principle and the abstract local-global principle for the property P (which we assume is of finite character).

Transfer ⇒ Abstract. Suppose the property is true after localization at every maximal ideal. The ideal given by the transfer principle cannot be strict,[3] otherwise it would be contained in a maximal ideal $\mathfrak{m}$, which contradicts the fact that the property is true after localization at some $s \notin \mathfrak{m}$.

Abstract ⇒ Transfer. For each maximal ideal $\mathfrak{m}$ select an $s_{\mathfrak{m}} \notin \mathfrak{m}$ such that the property P is true after localization at $s_{\mathfrak{m}}$. The set of $s_{\mathfrak{m}}$ generates an ideal not contained in any maximal ideal, thus it is the ideal $\langle 1 \rangle$. We can then conclude by the transfer principle: the property is true after localization at 1! ■

Comment. The advantage of localizing at a prime ideal is that the result is a local ring, which has very nice properties (see Chapter IX). The disadvantage is that the proofs which use an abstract local-global principle instead of its corresponding concrete local-global principle are non-constructive to the extent that the only access we have (in a general situation) to the prime ideals is given by Zorn's Lemma. Furthermore even Fact 2.2 is obtained by contradiction, which removes any algorithmic trait from the corresponding "construction."

Some concrete local-global principles do not have a corresponding abstract version as the property they are affiliated with is not of finite character. This is the case with the concrete local-global principles for finitely generated modules and for coherent rings (3.6 and 3.5 respectively).

We will systematically make efficient and constructive use of the basic concrete local-global principle and its consequences. Often, we will draw inspiration from some abstract local-global principle's proof found in classical mathematics. In Chapter XV we will develop a general local-global machinery to fully exploit the classical local-global proofs in a constructive manner. ■

[3] An ideal $\mathfrak{a}$ is said to be strict when $1 \notin \mathfrak{a}$.

Abstract version of the basic local-global principle

Since we are dealing with a finite character property, classical mathematics provides the following abstract version of the basic local-global principle.

2.13. Abstract local-global principle*. (Abstract basic local-global principle: abstract patching of solutions of a system of linear equations)
Let B be a matrix $\in \mathbf{A}^{m\times p}$ and C a column vector of $\mathbf{A}^m$. Then the following properties are equivalent.

1. *The system of linear equations $BX = C$ has a solution in $\mathbf{A}^p$.*
2. *For every maximal ideal $\mathfrak{m}$ the system of linear equations $BX = C$ has a solution in $(\mathbf{A}_{1+\mathfrak{m}})^p$.*

Forcing comaximality

Localization at an element $s \in \mathbf{A}$ is a fundamental operation in commutative algebra for forcing the invertibility of s.

Sometimes you may need to make n elements $a_1, \dots, a_n$ of a ring $\mathbf{A}$ comaximal. To this end we introduce the ring

$$\mathbf{B} = \mathbf{A}[X_1, \dots, X_n]\big/\big\langle 1 - \textstyle\sum_i a_i X_i \big\rangle = \mathbf{A}[x_1, \dots, x_n].$$

2.14. Lemma. *The kernel of the natural homomorphism $\psi : \mathbf{A} \to \mathbf{B}$ is the ideal $(0 : \mathfrak{a}^\infty)$, where $\mathfrak{a} = \langle a_1, \dots, a_n \rangle$. In particular, the homomorphism is injective if and only if* $\operatorname{Ann} \mathfrak{a} = 0$.

D Let c be an element of the kernel. Considering the isomorphism

$$\mathbf{B}/\langle (x_j)_{j\neq i} \rangle \simeq \mathbf{A}[1/a_i],$$

we have $c =_{\mathbf{A}[1/a_i]} 0$. Thus $c \in (0 : a_i^\infty)$. From this we deduce that $c \in (0 : \mathfrak{a}^\infty)$. Conversely if $c \in (0 : \mathfrak{a}^\infty)$, there exists an r such that $ca_i^r = 0$ for each i, and therefore $\psi(c) = \psi(c)(\sum a_i x_i)^{nr} = 0$. □

3. Coherent rings and modules

A fundamental notion

A ring $\mathbf{A}$ is called *coherent* if every linear equation

$$LX = 0 \ \text{ with } \ L \in \mathbf{A}^{1\times n} \ \text{ and } \ X \in \mathbf{A}^{n\times 1}$$

has for solutions the elements of a finitely generated $\mathbf{A}$-submodule of $\mathbf{A}^{n\times 1}$. In other words,

$$\left\{ \begin{array}{l} \forall n \in \mathbb{N},\, \forall L \in \mathbf{A}^{1\times n},\, \exists m \in \mathbb{N},\, \exists G \in \mathbf{A}^{n\times m},\, \forall X \in \mathbf{A}^{n\times 1}, \\ \qquad LX = 0 \quad \iff \quad \exists Y \in \mathbf{A}^{m\times 1},\ X = GY \ . \end{array} \right. \tag{1}$$

This means that we have some control over the solution space of the homogeneous system of linear equations $LX = 0$.

Clearly, a finite product of rings is coherent if and only if each factor is coherent.

More generally, given $V = (v_1, \ldots, v_n) \in M^n$ where M is an $\mathbf{A}$-module, the $\mathbf{A}$-submodule of $\mathbf{A}^n$ defined as the kernel of the linear map

$$\check{V} : \mathbf{A}^n \longrightarrow M, \quad (x_1, \ldots, x_n) \longmapsto \textstyle\sum_i x_i v_i$$

is called the *syzygy module between the v_i's.* More specifically, we say that it is the *syzygy module of (the vector) V.* An element $(x_1, \ldots, x_n)$ of this kernel is called a *linear dependence relation* or a *syzygy* between the v_i's. When V is a generator set of M the syzygy module between the v_i's is often called the *(first) syzygy module of M.*

By slight abuse of terminology, we indifferently refer to the term *syzygy* to mean the equality $\sum_i x_i v_i = 0$ or the element $(x_1, \ldots, x_n) \in \mathbf{A}^n$. The $\mathbf{A}$-module M is said to be *coherent* if for every $V \in M^n$ the syzygy module is finitely generated, in other words if we have:

$$\left\{ \begin{array}{l} \forall n \in \mathbb{N},\, \forall V \in M^{n\times 1},\, \exists m \in \mathbb{N},\, \exists G \in \mathbf{A}^{m\times n},\, \forall X \in \mathbf{A}^{1\times n}\,, \\ \qquad XV = 0 \quad \Longleftrightarrow \quad \exists Y \in \mathbf{A}^{1\times m},\ X = YG\,. \end{array} \right. \tag{2}$$

A ring $\mathbf{A}$ is then coherent if and only if it is coherent as an $\mathbf{A}$-module.

Notice that we used a transposed notation in equation (2) with respect to equation (1). This was to avoid writing the sum $\sum_i x_i v_i$ as $\sum_i v_i x_i$ with $v_i \in M$ and $x_i \in \mathbf{A}$. For the remainder of this work, we will generally not use this transposition, as it seems preferable to keep to the usual form $AX = V$ for a system of linear equations, even when the matrices A and V have their coefficients in a module M.

3.1. Proposition. *Let M be a coherent $\mathbf{A}$-module.*
Any homogeneous system of linear equations $BX = 0$, where $B \in M^{k\times n}$ and $X \in \mathbf{A}^{n\times 1}$*, has the elements of a finitely generated $\mathbf{A}$-submodule of $\mathbf{A}^{n\times 1}$ as its solution set.*

D The general proof is by induction on the number of linear equations k, where the procedure is as follows: solve the first equation, then substitute the obtained general solution into the second equation, and so on. So let us for example do the proof for $k = 2$ and take a closer look at this process. The matrix B is composed of the rows L and L'. We then have a matrix G such that

$$LX = 0 \quad \Longleftrightarrow \quad \exists Y \in \mathbf{A}^{m\times 1},\ X = GY.$$

We now need to solve $L'GY = 0$ which is equivalent to the existence of a column vector Z such that $Y = G'Z$ for a suitable matrix G'. Thus $BX = 0$ if and only if X can be expressed as $GG'Z$. □

The above proposition is particularly important for systems of linear equations on $\mathbf{A}$ (i.e. when $M = \mathbf{A}$).

Comment. The notion of a coherent ring is then fundamental from an algorithmic point of view in commutative algebra. Usually, this notion is hidden behind that of a *Noetherian* ring,[4] and rarely put forward as we have here. In classical mathematics every Noetherian ring $\mathbf{A}$ is coherent because every submodule of $\mathbf{A}^n$ is finitely generated, and every finitely generated module is coherent for the same reason. Furthermore, we have the Hilbert theorem, which states that *if* $\mathbf{A}$ *is Noetherian, every finitely generated* $\mathbf{A}$*-algebra is also a Noetherian ring,* whereas the same statement does not hold if one replaces "Noetherian" with "coherent."

From an algorithmic point of view however, it seems impossible to find a satisfying constructive formulation of Noetherianity which implies coherence (see exercise 8), and coherence is often the most important property from an algorithmic point of view. Consequently, coherence cannot be implied (as is the case in classical mathematics) when we speak of a Noetherian ring or module.

The classical theorem stating that in a Noetherian ring every finitely generated $\mathbf{A}$-module is Noetherian is often advantageously replaced by the following constructive theorem.[5]

Over a coherent (resp. Noetherian coherent) ring every finitely presented $\mathbf{A}$*-module is coherent (resp. Noetherian coherent).*

In fact, as this example shows, Noetherianity is often an unnecessarily strong assumption. ■

The following definition of a Noetherian module is equivalent in classical mathematics to the usual definition but it is much better adapted to constructive algebra (only the trivial ring constructively satisfies the usual definition).

3.2. Definition. *(Richman-Seidenberg theory of Noetherianity, [161, 171])* An $\mathbf{A}$-module is called *Noetherian* if it satisfies the following *ascending chain condition*: any ascending sequence of finitely generated submodules has two equal consecutive terms. A ring $\mathbf{A}$ is called *Noetherian* if it is Noetherian as an $\mathbf{A}$-module.

Here is a corollary of proposition 3.1.

[4] The constructive definition of this notion is given after this comment.

[5] For the non-Noetherian version see Theorem IV-4.3, and for the Noetherian version see [MRR, corollary 3.2.8 p. 83].

3.3. Corollary. (Conductors and coherence)
Let $\mathbf{A}$ *be a coherent ring. Then, the conductor of a finitely generated ideal into another is a finitely generated ideal. More generally, if* N *and* P *are two finitely generated submodules of a coherent* $\mathbf{A}$*-module, then* $(P : N)$ *is a finitely generated ideal.*

3.4. Theorem. *An* $\mathbf{A}$*-module* M *is coherent if and only if the following two conditions hold.*

1. *The intersection of two arbitrary finitely generated submodules is a finitely generated module.*
2. *The annihilator of an arbitrary element is a finitely generated ideal.*

D *The first condition is necessary.* Let g_1, …, g_n be the generators of the first submodule and g_{n+1}, …, g_m be the generators of the second. Taking an element of the intersection reduces to finding a syzygy $\sum_{i=1}^{m} \alpha_i g_i = 0$ between the g_i's. To such a syzygy $\alpha = (\alpha_1, \ldots, \alpha_m) \in \mathbf{A}^m$ corresponds the element $\varphi(\alpha) = \alpha_1 g_1 + \cdots + \alpha_n g_n = -(\alpha_{n+1} g_{n+1} + \cdots + \alpha_m g_m)$ in the intersection. Thus if S is a generator set for the syzygies between the g_i's, $\varphi(S)$ generates the intersection of the two submodules.

The second condition is necessary by definition.

The two conditions together are sufficient. Here we give the key idea of the proof and leave the details to the reader. Consider the syzygy module of some $L \in M^n$. We perform induction on n. For $n = 1$ the second condition applies and gives a generator set for the syzygies connecting the single element of L.
Suppose that the syzygy module of every $L \in M^n$ is finitely generated and consider some $L' \in M^{n+1}$. Let $k \in [\![1..n]\!]$, we write $L' = L_1 \bullet L_2$ where $L_1 = (a_1, \ldots, a_k)$ and $L_2 = (a_{k+1}, \ldots, a_{n+1})$. Let $M_1 = \langle a_1, \ldots, a_k \rangle$ and $M_2 = \langle a_{k+1}, \ldots, a_{n+1} \rangle$. Taking a syzygy $\sum_{i=1}^{n+1} \alpha_i a_i = 0$ reduces to taking an element of the intersection $M_1 \cap M_2$ (as above). We thus obtain a generator set for the syzygies between the a_i's by taking the union of the three following systems of syzygies: the system of syzygies between the elements of L_1, the system of syzygies between the elements of L_2, and that which comes from the generator set of the intersection $M_1 \cap M_2$. □

In particular, *a ring is coherent if and only if on the one hand the intersection of the two finitely generated ideals is always a finitely generated ideal, and on the other hand the annihilator of an element is always a finitely generated ideal.*

Examples. If $\mathbf{K}$ is a discrete field, every finitely presented algebra over $\mathbf{K}$ is a coherent ring (Theorem VII-1.10). It is also clear that every Bézout domain (cf. page 206) is a coherent ring. ■

Local character of coherence

Coherence is a local notion in the following sense.

3.5. Concrete local-global principle. (Coherent modules)
Consider a ring $\mathbf{A}$*, let* $S_1, \ldots, S_n$ *be comaximal monoids and* M *an* $\mathbf{A}$*-module.*

1. *The module* M *is coherent if and only if each* M_{S_i} *is coherent.*
2. *The ring* $\mathbf{A}$ *is coherent if and only if each* $\mathbf{A}_{S_i}$ *is coherent.*

D Let $a = (a_1, \ldots, a_m) \in M^m$, and $N \subseteq \mathbf{A}^m$ be the syzygy module of a. We find that for any monoid S, N_S is the syzygy module of a in M_S. This brings us to prove the following concrete local-global principle. □

3.6. Concrete local-global principle. (Finitely generated modules)
Let $S_1, \ldots, S_n$ *be comaximal monoids of* $\mathbf{A}$ *and* M *an* $\mathbf{A}$*-module. Then,* M *is finitely generated if and only if each* M_{S_i} *is finitely generated.*

D Suppose that M_{S_i} is a finitely generated $\mathbf{A}_{S_i}$-module for each i. Let us prove that M is finitely generated. Let $g_{i,1}, \ldots, g_{i,q_i}$ be elements of M which generate M_{S_i}. Let $x \in M$ be arbitrary. For each i we have some $s_i \in S_i$ and some $a_{i,j} \in \mathbf{A}$ such that:

$$s_i x = a_{i,1} g_{i,1} + \cdots + a_{i,q_i} g_{i,q_i} \quad \text{in} \quad M.$$

When writing $\sum_{i=1}^{n} b_i s_i = 1$, we observe that x is a linear combination of the $g_{i,j}$'s. □

Remark. Consider the $\mathbb{Z}$-submodule M of $\mathbb{Q}$ generated by the elements $1/p$ where p ranges over the set of prime numbers. We can easily check that M is not finitely generated but that it becomes finitely generated after localization at any prime ideal. This means that the concrete local-global principle 3.6 does not have a corresponding “abstract” version, in which the localization at some comaximal monoids would be replaced by the localization at every prime ideal. Actually, the property P for a module to be finitely generated is not a finite character property, as we can see with the module M above and the monoids $\mathbb{Z} \setminus \{0\}$ or $1 + p\mathbb{Z}$. Moreover, the property satisfies the transfer principle, but it so happens here that it is of no use. ■

About the equality and the membership tests

We now introduce several constructive notions relating to the equality test and the membership test.

A set E is well defined when we have indicated how to construct its elements and when we have constructed an equivalence relation which defines the equality of two elements in a set. We denote by $x = y$ the equality in E, or $x =_E y$ if necessary. The set E is called *discrete* when the following axiom holds

$$\forall x, y \in E \qquad x = y \ \text{ or } \ \neg(x = y).$$

Classically, every set is discrete, as the "or" present in the definition is understood in an abstract manner. Constructively, this same "or" is understood according to the usual language's meaning: at least one of the two alternatives must occur. It is thus an "or" of an algorithmic nature. In short, a set is discrete if we have a test for the equality of two arbitrary elements of this set.

If we want to be more precise and explain in detail what comprises an equality test in the set E, we will say that it is a construction which, from two given elements of E, provides a "yes" or "no" answer to the posed question (are these elements equal?). However, we could not go into much further detail. In constructive mathematics the notions of integers and of construction are basic concepts. They can be explained and commented on, but not strictly speaking "defined." The constructive meaning of the "or" and that of the "there exists" are as such directly dependent of the notion of construction,[6] which we do not attempt to define.

A *discrete field* is simply a ring where the following axiom is satisfied:

$$\forall x \in \mathbf{A} \qquad x = 0 \ \text{ or } \ x \in \mathbf{A}^\times \tag{3}$$

The trivial ring is a discrete field.

Remark. The Chinese pivot method (often called Gaussian elimination) works algorithmically with discrete fields. This means that the basic linear algebra is explicit over discrete fields. ■

Note that a discrete field $\mathbf{A}$ is a discrete set if and only if the test "$1 =_{\mathbf{A}} 0$?" is explicit.[7] Sometimes, however, it is known that a ring constructed during an algorithm is a discrete field without knowing whether it is trivial or not.

If $\mathbf{A}$ is a nontrivial discrete field, the statement "M is a free finite dimensional vector space" is more precise than the statement "M is a finitely generated vector space" as in the first case knowing how to extract a basis of the generator set is similar to having a test of linear independence in M.

[6] In classical mathematics we may wish to define the notion of construction from the notion of a "correct program." However, what we define in this way is rather the notion of "mechanized construction," and especially in the notion of a "correct program," there is the fact that the program must halt after a finite number of steps. This hides a "there exists," which in constructive mathematics refers in an irreducible manner to the notion of construction. On this matter, see Section A-4 of the Annex.

[7] The general notion of a field in constructive mathematics will be defined page 489. We will then see that if a field is a discrete set, then it is a discrete field.

A subset P of a set E is said to be *detachable* when the following property is satisfied:

$$\forall x \in E \qquad x \in P \text{ or } \neg(x \in P).$$

It amounts to the same to take a detachable part P of E or to take its characteristic function $\chi_P : E \to \{0, 1\}$.

In constructive mathematics, if two sets E and F are correctly defined, then so is the *set of functions from E to F*, which is denoted by F^E. Consequently, the *set of detachable subsets* of a set E is itself correctly defined since it is identified with the set $\{0, 1\}^E$ of characteristic functions over E.

Strongly discrete coherent rings and modules

A ring (resp. a module) is said to be *strongly discrete* when the finitely generated ideals (resp. the finitely generated submodules) are detachable, i.e. if the quotients by the finitely generated ideals (resp. by the finitely generated submodules) are discrete.

This means that we have a test for deciding whether a linear equation $LX = c$ has a solution or not, and by computing one in the affirmative case.

A key result in constructive algebra and Computer Algebra states that $\mathbb{Z}[X_1, \dots, X_n]$ is a strongly discrete coherent ring.

More generally, we have the following constructive version of the Hilbert theorem (see [MRR, Adams & Loustaunau]).

If $\mathbf{A}$ is a strongly discrete Noetherian coherent ring, so is any finitely presented $\mathbf{A}$-algebra.

The following proposition is proven similarly to proposition 3.1.

3.7. Proposition. *Over a strongly discrete coherent module M, every system of linear equations $BX = C$ ($B \in M^{k\times n}$, $C \in M^{k\times 1}$, $X \in \mathbf{A}^{n\times 1}$) can be tested. In the affirmative case, a particular solution X_0 can be computed. Furthermore the solutions X are all the elements of $X_0 + N$ where N is a finitely generated $\mathbf{A}$-submodule of $\mathbf{A}^{n\times 1}$.*

4. Fundamental systems of orthogonal idempotents

An element e of a ring is said to be *idempotent* if $e^2 = e$. In this case, $1 - e$ is also an idempotent, called the *complementary idempotent of* e, or the *complement of* e. For two idempotents e_1 and e_2, we have

$$\langle e_1 \rangle \cap \langle e_2 \rangle = \langle e_1 e_2 \rangle\,, \quad \langle e_1 \rangle + \langle e_2 \rangle = \langle e_1, e_2 \rangle = \langle e_1 + e_2 - e_1 e_2 \rangle\,,$$

where $e_1 e_2$ and $e_1 + e_2 - e_1 e_2$ are idempotents. Two idempotents e_1 and e_2 are said to be *orthogonal* when $e_1 e_2 = 0$. We then have $\langle e_1 \rangle + \langle e_2 \rangle = \langle e_1 + e_2 \rangle$.

A ring is said to be *connected* if every idempotent is equal to 0 or 1.

In the following, we implicitly use the following obvious fact: for an idempotent e and an element x, e divides x if and only if $x = ex$.

The presence of an idempotent $\neq 0$, 1 means that the ring $\mathbf{A}$ is isomorphic to a product of two rings $\mathbf{A}_1$ and $\mathbf{A}_2$, and that any computation in $\mathbf{A}$ can be split into two "simpler" computations in $\mathbf{A}_1$ and $\mathbf{A}_2$. We describe the situation as follows.

4.1. Fact. *For every isomorphism $\lambda : \mathbf{A} \to \mathbf{A}_1 \times \mathbf{A}_2$, there exists a unique element $e \in \mathbf{A}$ satisfying the following properties.*

1. *The element e is idempotent (its complement is denoted by $f = 1 - e$).*
2. *The homomorphism $\mathbf{A} \to \mathbf{A}_1$ identifies $\mathbf{A}_1$ with $\mathbf{A}/\langle e \rangle$ and with $\mathbf{A}[1/f]$.*
3. *The homomorphism $\mathbf{A} \to \mathbf{A}_2$ identifies $\mathbf{A}_2$ with $\mathbf{A}/\langle f \rangle$ and with $\mathbf{A}[1/e]$.*

Conversely, if e is an idempotent and f is its complement, the canonical homomorphism $\mathbf{A} \to \mathbf{A}/\langle e \rangle \times \mathbf{A}/\langle f \rangle$ is an isomorphism.

D The element e is defined by $\lambda(e) = (0, 1)$. □

Here are some often useful facts.

4.2. Fact. *Let e be an idempotent of $\mathbf{A}$, $f = 1 - e$ and M be an $\mathbf{A}$-module.*

1. *The monoids $e^{\mathbb{N}} = \{1, e\}$ and $1 + f\mathbf{A}$ have the same saturation.*
2. *As an $\mathbf{A}$-module, $\mathbf{A}$ is the direct sum of $\langle e \rangle = e\mathbf{A}$ and $\langle f \rangle = f\mathbf{A}$. The ideal $e\mathbf{A}$ is a ring where e is a neutral element of the multiplication. We then have three isomorphic rings*
$$\mathbf{A}[1/e] = (1 + f\mathbf{A})^{-1}\mathbf{A} \;\simeq\; \mathbf{A}/\langle f \rangle \;\simeq\; e\mathbf{A}.$$
These isomorphisms stem from the three canonical mappings
$$\begin{array}{lcl} \mathbf{A} \to \mathbf{A}[1/e] & : & x \mapsto x/1, \\ \mathbf{A} \to \mathbf{A}/\langle f \rangle & : & x \mapsto x \bmod \langle f \rangle\,, \\ \mathbf{A} \to e\mathbf{A} & : & x \mapsto e\,x, \end{array}$$
which are surjective and have the same kernel.

3. *We have three isomorphic* $\mathbf{A}$*-modules* $M[1/e] \simeq M/fM \simeq eM$. *These isomorphisms stem from the three canonical mappings*

$$\begin{array}{lll} M \to M[1/e] & : & x \mapsto x/1, \\ M \to M/fM & : & x \mapsto x \bmod \langle f \rangle, \\ M \to eM & : & x \mapsto e\,x, \end{array}$$

which are surjective and have the same kernel.

In addition, care must be taken that the ideal $e\mathbf{A}$, which is a ring with e as its neutral element, is not a subring of $\mathbf{A}$ (unless $e = 1$).

In a ring $\mathbf{A}$ a *fundamental system of orthogonal idempotents* is a list $(e_1, \ldots, e_n)$ of elements of $\mathbf{A}$ which satisfy the following equalities:

$$e_i e_j = 0 \text{ for } i \neq j, \quad \text{and} \quad \textstyle\sum_{i=1}^{n} e_i = 1.$$

This implies that the e_i's are idempotents. We do not claim that none of them are null.[8]

4.3. Theorem. (Fundamental systems of orthogonal idempotents)
Let $(e_1, \ldots, e_n)$ *be a fundamental system of orthogonal idempotents of a ring* $\mathbf{A}$*, and* M *be an* $\mathbf{A}$*-module. Note that* $\mathbf{A}_i = \mathbf{A}/\langle 1 - e_i \rangle \simeq \mathbf{A}[1/e_i]$. *Then:*

$$\begin{array}{rcl} \mathbf{A} & \simeq & \mathbf{A}_1 \times \cdots \times \mathbf{A}_n, \\ M & = & e_1 M \oplus \cdots \oplus e_n M. \end{array}$$

Take note that $e_1 M$ is an $\mathbf{A}$-module and an $\mathbf{A}_1$-module, but that it is not an $\mathbf{A}_2$-module (unless it is null).

The following lemma gives a converse of Theorem 4.3.

4.4. Lemma. *Let* $(\mathfrak{a}_i)_{i \in [\![1..n]\!]}$ *be ideals of* $\mathbf{A}$. *We have* $\mathbf{A} = \bigoplus_{i \in [\![1..n]\!]} \mathfrak{a}_i$ *if and only if there exists a fundamental system of orthogonal idempotents* $(e_i)_{i \in [\![1..n]\!]}$ *such that* $\mathfrak{a}_i = \langle e_i \rangle$ *for* $i \in [\![1..n]\!]$. *In this case, the fundamental system of orthogonal idempotents is uniquely determined.*

D Assume that $\mathbf{A} = \bigoplus_{i \in [\![1..n]\!]} \mathfrak{a}_i$. We have $e_i \in \mathfrak{a}_i$ such that $\sum_i e_i = 1$, and since $e_i e_j \in \mathfrak{a}_i \cap \mathfrak{a}_j = \{0\}$ for $i \neq j$, we indeed obtain a fundamental system of orthogonal idempotents. Furthermore if $x \in \mathfrak{a}_j$, we have $x = x \sum_i e_i = x e_j$ and thus $\mathfrak{a}_j = \langle e_j \rangle$. The converse is immediate. The uniqueness follows from that of writing an element as a direct sum. □

Next we give two very useful lemmas.

[8] This is much nicer to obtain uniform statements. Furthermore this is virtually necessary when we do not have at our disposal an equality to zero test for idempotents in the given ring.

4.5. Lemma. (Lemma of the ideal generated by an idempotent)
An ideal $\mathfrak{a}$ is generated by an idempotent if and only if

$$\mathfrak{a} + \operatorname{Ann}\mathfrak{a} = \langle 1 \rangle .$$

D First, if e is idempotent, we have $\operatorname{Ann}\langle e\rangle = \langle 1-e\rangle$. For the reciprocal implication, let $e \in \mathfrak{a}$ such that $1-e \in \operatorname{Ann}\mathfrak{a}$. Then $e(1-e)=0$, therefore e is idempotent, and for every $y \in \mathfrak{a}$, $y = ye$, thus $\mathfrak{a} \subseteq \langle e \rangle$. □

4.6. Lemma. (Lemma of the finitely generated idempotent ideal)
If $\mathfrak{a}$ is a finitely generated idempotent ideal (i.e., $\mathfrak{a} = \mathfrak{a}^2$) in $\mathbf{A}$, then $\mathfrak{a} = \langle e \rangle$ where $e^2 = e$ is entirely determined by $\mathfrak{a}$.

D We use the determinant trick. Consider a generator set $(a_1, \dots a_q)$ of $\mathfrak{a}$ and the column vector $\underline{a} = {}^{\mathrm{t}}[\, a_1 \ \cdots \ a_q \,]$.
Since $a_j \in \mathfrak{a}^2$ for $j \in \llbracket 1..q \rrbracket$, there exists a $C \in \mathbb{M}_q(\mathfrak{a})$ such that $\underline{a} = C\,\underline{a}$, so $(\mathrm{I}_q - C)\,\underline{a} = \underline{0}$ and $\det(\mathrm{I}_q - C)\,\underline{a} = \underline{0}$. However, $\det(\mathrm{I}_q - C) = 1 - e$ where $e \in \mathfrak{a}$. Hence $(1-e)\mathfrak{a} = 0$, and we apply Lemma 4.5.
Finally, the uniqueness of e follows immediately from Lemma 4.4. □

Let us finally recall the Chinese remainder theorem, a very efficient tool which hides a fundamental system of orthogonal idempotents. Some ideals $\mathfrak{b}_1, \dots, \mathfrak{b}_\ell$ of a ring $\mathbf{A}$ are called *comaximal* when $\mathfrak{b}_1 + \cdots + \mathfrak{b}_\ell = \langle 1 \rangle$.

4.7. Chinese Remainder Theorem.
*Let $(\mathfrak{a}_i)_{i \in \llbracket 1..n \rrbracket}$ be pairwise comaximal ideals in $\mathbf{A}$ and $\mathfrak{a} = \bigcap_i \mathfrak{a}_i$.
Then $\mathfrak{a} = \prod_i \mathfrak{a}_i$, and the canonical mapping $\mathbf{A}/\mathfrak{a} \to \prod_i \mathbf{A}/\mathfrak{a}_i$ is an isomorphism. Now, there exist $e_1, \dots, e_n$ in $\mathbf{A}$ such that $\mathfrak{a}_i = \mathfrak{a} + \langle 1 - e_i \rangle$ and the $\pi_{\mathbf{A},\mathfrak{a}}(e_i)$'s form a fundamental system of orthogonal idempotents of $\mathbf{A}/\mathfrak{a}$.*

As a corollary we obtain the following result.

4.8. Lemma. (Kernels' Lemma)
Let $P = P_1 \cdots P_\ell \in \mathbf{A}[X]$ and an $\mathbf{A}$-linear map $\varphi : M \to M$ satisfying $P(\varphi) = 0$. Assume the P_i's are pairwise comaximal and let $K_i = \operatorname{Ker}\big(P_i(\varphi)\big)$, $Q_i = \prod_{j \neq i} P_j$. Then we have

$$K_i = \operatorname{Im}\big(Q_i(\varphi)\big),\ M = \textstyle\bigoplus_{j=1}^{\ell} K_j \ \text{ and } \operatorname{Im}\big(P_i(\varphi)\big) = \operatorname{Ker}\big(Q_i(\varphi)\big) = \bigoplus_{j \neq i} K_i.$$

D Consider the ring $\mathbf{B} = \mathbf{A}[X]/\langle P \rangle$. The module M can be seen as a $\mathbf{B}$-module by the operation $(Q, y) \mapsto Q \cdot y = Q(\varphi)(y)$. We then apply the Chinese remainder theorem and Theorem 4.3.
This proof summarizes the following computation. From the equalities $U_{ij}P_i + U_{ji}P_j = 1$, we get the equalities $U_iP_i + V_iQ_i = 1$ together with an equality $\sum_i W_iQ_i = 1$. Let $p_i = P_i(\varphi)$, $q_i = Q_i(\varphi)$, and so on.
Then, every obtained endomorphism commutes and we obtain the equalities $p_iq_i = 0$, $u_ip_i + v_iq_i = \mathrm{Id}_M$, $\sum_i w_iq_i = \mathrm{Id}_M$. The claimed result readily follows. □

5. A little exterior algebra

> *That a homogeneous system of n linear equations with n unknowns*
> *admits (over a discrete field) a nontrivial solution*
> *if and only if the determinant of the system is zero,*
> *here is a fact of utmost importance whose scope we*
> *will never finish measuring.*
> Anonymous

> *Eliminate, eliminate, eliminate*
> *Eliminate the eliminators of elimination theory!*
> Mathematical poem (extract)
> S. Abhyankar

Some simple examples illustrating these ideas are given in this section.

Free submodules as direct summands (Splitting Off)

Let $k \in \mathbb{N}$. A *free module of rank k* is by definition an $\mathbf{A}$-module isomorphic to $\mathbf{A}^k$. If k is not specified, we will say *free module of finite rank.*

When $\mathbf{A}$ is a discrete field we speak of a *finite dimensional vector space* or a *finite rank vector space* interchangeably.

The modules whose structure is the simplest are the free modules of finite rank. We are thus interested in the possibility of constructing an arbitrary module M in the form $L \oplus N$ where L is a free module of finite rank. A (partial) answer to this question is given by the exterior algebra.

5.1. Proposition. (Splitting Off)
Let $a_1, \ldots, a_k$ be elements of an $\mathbf{A}$-module M, then the following properties are equivalent.

1. *The submodule $L = \langle a_1, \ldots, a_k \rangle$ of M is free with basis $(a_1, \ldots, a_k)$ and is a direct summand of M.*
2. *There exists a k-multilinear alternating form $\varphi : M^k \to \mathbf{A}$ which satisfies the equality $\varphi(a_1, \ldots, a_k) = 1$.*

D *1 ⇒ 2.* If $L \oplus N = M$, if $\pi : M \to L$ is the projection parallel to N, and if $\theta_j : L \to \mathbf{A}$ is the j-th coordinate form for the basis $(a_1, \ldots, a_k)$, we define

$$\varphi(x_1, \ldots, x_k) = \det\Big(\big(\theta_j(\pi(x_i))\big)_{i,j \in [\![1..k]\!]}\Big).$$

2 ⇒ 1. We define the linear map $\pi : M \to M$ as

$$\pi(x) = \sum\nolimits_{j=1}^{k} \varphi(\underbrace{a_1, \ldots, x, \ldots, a_k}_{(x \text{ is in position } j)})\, a_j.$$

We immediately have $\pi(a_i) = a_i$ and $\operatorname{Im}\pi \subseteq L := \langle a_1, \ldots, a_k \rangle$, thus $\pi^2 = \pi$ and $\operatorname{Im}\pi = L$. Finally, if $x = \sum_j \lambda_j a_j = 0$, then $\varphi(a_1, \ldots, x, \ldots, a_k) = \lambda_j = 0$ (with x in position j). □

Special case: for $k = 1$ we say that the element a_1 of M is *unimodular* when there exists a linear form $\varphi : M \to \mathbf{A}$ such that $\varphi(a_1) = 1$. The vector $b = (b_1, \dots, b_n) \in \mathbf{A}^n$ is unimodular if and only if the b_i's are comaximal. In this case we also say that the sequence $(b_1, \dots, b_n)$ is *unimodular*.

The rank of a free module

As we will see, the rank of a free module is a well-determined integer if the ring is nontrivial. In other words, two $\mathbf{A}$-modules $M \simeq \mathbf{A}^m$ and $P \simeq \mathbf{A}^p$ with $m \neq p$ can only be isomorphic if $1 =_{\mathbf{A}} 0$.

We will use the notation $\mathrm{rk}_{\mathbf{A}}(M) = k$ (or $\mathrm{rk}(M) = k$ if $\mathbf{A}$ is clear from the context) to indicate that a (supposedly free) module has rank k.

A scholarly proof consists to say that, if $m > p$, the m-th exterior power of P is $\{0\}$ whereas that of M is isomorphic to $\mathbf{A}$ (this is essentially the proof for Corollary 5.23).

The same proof can be presented in a more elementary way as follows. First recall the basic Cramer formula. If B is a square matrix of order n, we denote by $\widetilde{B}$ or $\mathrm{Adj}\,B$ the *cotransposed* matrix (sometimes called *adjoint*). The elementary form of Cramer's identities is then expressed as:

$$A\ \mathrm{Adj}(A) = \mathrm{Adj}(A)\ A = \det(A)\ \mathrm{I}_n. \tag{4}$$

This formula, in combination with the product formula

$$\det(AB) = \det(A)\det(B),$$

has a couple of implications regarding square matrices. First, that a square matrix A is invertible on one side if and only if A is invertible if and only if its determinant is invertible. Second, that the inverse of A is equal to $(\det A)^{-1}\,\mathrm{Adj}\,A$.

We now consider two $\mathbf{A}$-modules $M \simeq \mathbf{A}^m$ and $P \simeq \mathbf{A}^p$ with $m \geqslant p$ and a surjective linear map $\varphi : P \to M$. Therefore there exists a linear map $\psi : M \to P$ such that $\varphi \circ \psi = \mathrm{Id}_M$. This corresponds to two matrices $A \in \mathbf{A}^{m \times p}$ and $B \in \mathbf{A}^{p \times m}$ with $AB = \mathrm{I}_m$. If $m = p$, the matrix A is invertible with inverse B and φ and ψ are reciprocal isomorphisms. If $m > p$, we have $AB = A_1B_1$ with square A_1 and B_1 respectively obtained from A and B by filling in with zeros ($m - p$ columns for A_1, $m - p$ rows for B_1).

$$A_1 = \left[\begin{array}{c|c} 0 & \\ \vdots & A \\ 0 & \end{array}\right], \qquad B_1 = \left[\begin{array}{c} 0 \ \cdots \ 0 \\ \hline \\ B \\ \end{array}\right], \qquad A_1B_1 = \mathrm{I}_m.$$

Thus $1 = \det \mathrm{I}_m = \det(AB) = \det(A_1B_1) = \det(A_1)\det(B_1) = 0$.

In this proof we clearly see the commutativity of the ring appear (which is truly necessary). Let us summarize.

5.2. Proposition. *Let two* $\mathbf{A}$*-modules* $M \simeq \mathbf{A}^m$ *and* $P \simeq \mathbf{A}^p$ *and a surjective linear map* $\varphi : P \to M$*.*

1. *If* $m = p$*, then* φ *is an isomorphism. In other words, in a module* $\mathbf{A}^m$ *every generator set of* m *elements is a basis.*
2. *If* $m > p$*, then* $1 =_{\mathbf{A}} 0$*, and if the ring is nontrivial,* $m > p$ *is impossible.*

In the following, this important classification theorem will often appear as a corollary of more subtle theorems, as for example Theorem IV-5.1 or Theorem IV-5.2.

Exterior powers of a module

Terminology. Recall that any determinant of a square matrix extracted from A on certain rows and columns is called a *minor* of A. We speak of a *minor of order* k when the extracted square matrix is in $\mathbb{M}_k(\mathbf{A})$. When A is a square matrix, a *principal minor* is a minor corresponding to a matrix extracted on the same set of indices for both the rows and the columns. For example if $A \in \mathbb{M}_n(\mathbf{A})$, the coefficient of X^k in the polynomial $\det(\mathrm{I}_n + XA)$ is the sum of the principal minors of order k of A. Finally, a principal minor in the north-west position, i.e. obtained by extracting the matrix on the first lines and first columns, is called a *dominant principal minor.* ■

Let M be an $\mathbf{A}$-module. A k-multilinear alternating map $\varphi : M^k \to P$ is called a k-th *exterior power* of the $\mathbf{A}$-module M if every multilinear alternating map $\psi : M^k \to R$ is uniquely expressible in the form $\psi = \theta \circ \varphi$, where θ is an $\mathbf{A}$-linear map from P to R.

$$\begin{tikzcd}
M^k \arrow[d, "\varphi"'] \arrow[dr, "\psi"] & & \text{k-multilinear alternating maps} \\
P \arrow[r, dashed, "\theta\,!"'] & R & \text{linear maps.}
\end{tikzcd}$$

Clearly $\varphi : M^k \to P$ is unique in the categorical sense, i.e. that for every other exterior power $\varphi' : M^k \to P'$ there is a unique linear map $\theta : P \to P'$ which makes the suitable diagram commutative, and that θ is an isomorphism.

We then denote P by $\bigwedge^k M$ or $\bigwedge^k_{\mathbf{A}} M$ and $\varphi(x_1, \dots, x_k)$ by $\lambda_k(x_1, \dots, x_k)$ or $x_1 \wedge \cdots \wedge x_k$.

The existence of a k-th exterior power for every module M results from general considerations analogous to those that we will detail for the tensor product on page 191 in Section IV-4.

The simplest theory of exterior powers, analogous to the elementary theory of the determinant, shows that if M is a free module with a basis of n elements $(a_1, \dots, a_n)$, then $\bigwedge^k M$ is zero if $k > n$, and otherwise it is a free

module whose basis is the $\binom{n}{k}$ k-vectors $a_{i_1} \wedge \cdots \wedge a_{i_k}$, where $(i_1, \ldots, i_k)$ ranges over the set of strictly increasing k-tuples of elements of $[\![1..n]\!]$.
In particular, $\bigwedge^n M$ is free and of rank 1 with $a_1 \wedge \cdots \wedge a_n$ as its basis.

To every $\mathbf{A}$-linear map $\alpha : M \to N$ corresponds a unique $\mathbf{A}$-linear map $\bigwedge^k \alpha : \bigwedge^k M \to \bigwedge^k N$ satisfying the equality

$$\big(\bigwedge^k \alpha\big)(x_1 \wedge \cdots \wedge x_k) = \alpha(x_1) \wedge \cdots \wedge \alpha(x_k)$$

for every k-vector $x_1 \wedge \cdots \wedge x_k$ of $\bigwedge^k M$. The linear map $\bigwedge^k \alpha$ is called the k-th *exterior power* of the linear map α.

Moreover we have $\big(\bigwedge^k \alpha\big) \circ \big(\bigwedge^k \beta\big) = \bigwedge^k(\alpha \circ \beta)$ when $\alpha \circ \beta$ is defined. In short, each $\bigwedge^k(\bullet)$ is a functor.

If M and N are free with respective bases $(a_1, \ldots, a_n)$ and $(b_1, \ldots, b_m)$, and if α admits the matrix H on its bases, then $\bigwedge^k \alpha$ admits the matrix denoted by $\bigwedge^k H$ on the corresponding bases of $\bigwedge^k M$ and $\bigwedge^k N$. The coefficients of this matrix are all the minors of order k of the matrix H.

Determinantal ideals

5.3. Definition. Let $G \in \mathbf{A}^{n \times m}$ and $k \in [\![1..\min(m,n)]\!]$, *the determinantal ideal of order k of the matrix G* is the ideal, denoted by $\mathcal{D}_{\mathbf{A},k}(G)$ or $\mathcal{D}_k(G)$, generated by the minors of order k of G. For $k \leqslant 0$ we set by convention $\mathcal{D}_k(G) = \langle 1 \rangle$, and for $k > \min(m,n)$, $\mathcal{D}_k(G) = \langle 0 \rangle$.

These conventions are natural because they allow us to obtain in full generality the following equalities.

- If $H = \begin{array}{|c|c|}\hline \mathrm{I}_r & 0 \\ \hline 0 & G \\ \hline \end{array}$, for all $k \in \mathbb{Z}$ we have $\mathcal{D}_k(G) = \mathcal{D}_{k+r}(H)$.
- If $H = \begin{array}{|c|c|}\hline 0 & 0 \\ \hline 0 & G \\ \hline \end{array}$, for all $k \in \mathbb{Z}$ we have $\mathcal{D}_k(H) = \mathcal{D}_k(G)$.

5.4. Fact. *For every matrix G of type $n \times m$ we have the inclusions*

$$\{0\} = \mathcal{D}_{1+\min(m,n)}(G) \subseteq \cdots \subseteq \mathcal{D}_1(G) \subseteq \mathcal{D}_0(G) = \langle 1 \rangle = \mathbf{A} \qquad (5)$$

More precisely for all $k, r \in \mathbb{N}$ we have one inclusion

$$\mathcal{D}_{k+r}(G) \subseteq \mathcal{D}_k(G)\,\mathcal{D}_r(G) \qquad (6)$$

Indeed, every minor of order $h+1$ is expressed as a linear combination of minors of order h, and the inclusion (6) is obtained via the Laplace expansion of the determinant.

5.5. Fact. *Let $G_1 \in \mathbf{A}^{n\times m_1}$, $G_2 \in \mathbf{A}^{n\times m_2}$ and $H \in \mathbf{A}^{p\times n}$.*

1. *If $\operatorname{Im} G_1 \subseteq \operatorname{Im} G_2$, then for any integer k we have $\mathcal{D}_k(G_1) \subseteq \mathcal{D}_k(G_2)$.*
2. *For any integer k, we have $\mathcal{D}_k(HG_1) \subseteq \mathcal{D}_k(G_1)$.*
3. *The determinantal ideals of a matrix $G \in \mathbf{A}^{n\times m}$ only depend on the equivalence class of the submodule image of G (i.e., they only depend on $\operatorname{Im} G$, up to automorphism of the module $\mathbf{A}^n$).*
4. *In particular, if φ is a linear map between free modules of finite rank, the determinantal ideals of a matrix of φ do not depend on the chosen bases. We denote them by $\mathcal{D}_k(\varphi)$ and we call them the* determinantal ideals of the linear map *φ.*

D *1.* Each column of G_1 is a linear combination of columns of G_2. We conclude with the multilinearity of the determinant.
2. Same reasoning by replacing the columns with the rows.
Finally, *3* implies *4* and results from the two preceding items. □

Remark. A determinantal ideal is therefore essentially attached to a finitely generated submodule M of a free module L. However, it is the structure of the inclusion $M \subseteq L$ and not only the structure of M which intervenes to determine the determinantal ideals. For example $M = 3\mathbb{Z} \times 5\mathbb{Z}$ is a free $\mathbb{Z}$-submodule of $L = \mathbb{Z}^2$ and its determinantal ideals are $\mathcal{D}_1(M) = \langle 1\rangle$, $\mathcal{D}_2(M) = \langle 15\rangle$. If we replace 3 and 5 with 6 and 10 for example, we obtain another free submodule, but the structure of the inclusion is different since the determinantal ideals are now $\langle 2\rangle$ and $\langle 60\rangle$. ■

5.6. Fact. *If G and H are matrices such that GH is defined, then, for all $n \geqslant 0$ we have*

$$\mathcal{D}_n(GH) \subseteq \mathcal{D}_n(G)\,\mathcal{D}_n(H) \tag{7}$$

D The result is clear for $n = 1$. For $n > 1$, we reduce to the case $n = 1$ by noting that the minors of order n of G, H and GH represent the coefficients of the matrices "n-th exterior power of G, H and GH" $\big($taking into account the equality $\bigwedge^n(\varphi\psi) = \bigwedge^n \varphi \circ \bigwedge^n \psi\big)$. □

The following equality is immediate.

$$\mathcal{D}_n(\varphi \oplus \psi) = \sum\nolimits_{k=0}^{n} \mathcal{D}_k(\varphi)\,\mathcal{D}_{n-k}(\psi) \tag{8}$$

The rank of a matrix

5.7. Definition.
A linear map φ between free modules of finite rank is said to be

- *of rank* $\leqslant k$ if $\mathcal{D}_{k+1}(\varphi) = 0$,
- *of rank* $\geqslant k$ if $\mathcal{D}_k(\varphi) = \langle 1 \rangle$,
- *of rank* k if it is both of rank $\geqslant k$ and of rank $\leqslant k$.

We will use the notations $\operatorname{rk}(\varphi) \geqslant k$ and $\operatorname{rk}(\varphi) \leqslant k$, in accordance with the preceding definition, without presupposing that $\operatorname{rk}(\varphi)$ is defined. Only the notation $\operatorname{rk}(\varphi) = k$ will mean that the rank is defined.

We will later generalize this definition to the case of linear maps between finitely generated projective modules: see the notation X-6.5 as well as exercices X-21, X-22 and X-23.

Comment. The reader is cautioned that there is no universally accepted definition for “matrix of rank k” in the literature. When reading another book, one must first ascertain the definition adopted by the author. For example in the case of an integral ring $\mathbf{A}$, we often find the rank defined as that of the matrix over the quotient field of $\mathbf{A}$. Nevertheless a matrix of rank k in the sense of Definition 5.7 is generally of rank k in the sense of other authors. ■

The following concrete local-global principle is an immediate consequence of the basic local-global principle.

5.8. Concrete local-global principle. (Rank of a matrix)
Let S_1, …, S_n be comaximal monoids of $\mathbf{A}$ and B be a matrix $\in \mathbf{A}^{m\times p}$. Then the following properties are equivalent.

1. *The matrix is of rank $\leqslant k$ (resp. of rank $\geqslant k$) over $\mathbf{A}$.*
2. *For $i \in [\![1..n]\!]$, the matrix is of rank $\leqslant k$ (resp. of rank $\geqslant k$) over $\mathbf{A}_{S_i}$.*

Generalized pivot method

Terminology.

1) Two matrices are said to be *equivalent* if we can pass from one to the other by left- and right-multiplying by invertible matrices.

2) Two square matrices in $\mathbb{M}_n(\mathbf{A})$ are said to be *similar* when they represent the same endomorphism of $\mathbf{A}^n$ over two bases (distinct or not), in other words when they are conjugate with respect to the action $(G, M) \mapsto GMG^{-1}$ of $\mathbb{GL}_n(\mathbf{A})$ over $\mathbb{M}_n(\mathbf{A})$.

3) An *elementary row operation* on a matrix of n rows consists in replacing a row L_i with a row $L_i + \lambda L_j$ where $i \neq j$.

We also denote this by $L_i \leftarrow L_i + \lambda L_j$. This corresponds to the left-multiplication by a matrix, said to be *elementary*, denoted by $\mathrm{E}_{i,j}^{(n)}(\lambda)$ (or, if the context allows it, $\mathrm{E}_{i,j}(\lambda)$). This matrix is obtained from I_n by means of the same elementary row operation.
The right-multiplication by the same matrix $\mathrm{E}_{i,j}(\lambda)$ corresponds to the *elementary column operation* (for a matrix having n columns) which transforms the matrix I_n into $\mathrm{E}_{i,j}(\lambda)$: $C_j \leftarrow C_j + \lambda C_i$.
4) The subgroup of $\mathbb{SL}_n(\mathbf{A})$ generated by the elementary matrices is called the *elementary group* and it is denoted by $\mathbb{E}_n(\mathbf{A})$. Two matrices are said to be *elementarily equivalent* when we can pass from one to the other via elementary row and column operations. ■

5.9. Invertible minor lemma. (Generalized pivot)
If a matrix $G \in \mathbf{A}^{q\times m}$ has an invertible minor of order $k \leqslant \min(m,q)$, it is equivalent to a matrix

$$\begin{bmatrix} \mathrm{I}_k & 0_{k,m-k} \\ 0_{q-k,k} & G_1 \end{bmatrix},$$

where $\mathcal{D}_r(G_1) = \mathcal{D}_{k+r}(G)$ for all $r \in \mathbb{Z}$.

D By eventually permuting the rows and the columns we bring the invertible minor to the top left. Next, by right-multiplying (or left-multiplying) by an invertible matrix, we reduce to the form

$$G' = \begin{bmatrix} \mathrm{I}_k & A \\ B & C \end{bmatrix},$$

then by elementary row and column operations, we obtain

$$G'' = \begin{bmatrix} \mathrm{I}_k & 0_{k,m-k} \\ 0_{q-k,k} & G_1 \end{bmatrix}.$$

Finally, $\mathcal{D}_r(G_1) = \mathcal{D}_{k+r}(G'') = \mathcal{D}_{k+r}(G)$ for all $r \in \mathbb{Z}$. □

As an immediate consequence we obtain the freeness lemma.

5.10. Freeness lemma. *Consider a matrix $G \in \mathbf{A}^{q\times m}$ of rank $\leqslant k$ with $1 \leqslant k \leqslant \min(m,q)$. If the matrix G has an invertible minor of order k, then it is equivalent to the matrix*

$$\mathrm{I}_{k,q,m} = \begin{bmatrix} \mathrm{I}_k & 0_{k,m-k} \\ 0_{q-k,k} & 0_{q-k,m-k} \end{bmatrix}.$$

In this case, the image, the kernel and the cokernel of G are free, respectively of ranks k, $m-k$ and $q-k$. Moreover the image and the kernel have free summands.
If $i_1, \ldots, i_k$ (resp. $j_1, \ldots, j_k$) are the indexes of rows (resp. of columns) of the invertible minor, then the columns $j_1, \ldots, j_k$ form a basis of the module $\operatorname{Im} G$, *and* $\operatorname{Ker} G$ *is the module of vectors annihilated by the linear forms corresponding to the rows $i_1, \ldots, i_k$.*

D With the notations of the previous lemma we have $\mathcal{D}_1(G_1)=\mathcal{D}_{k+1}(G)=0$, so $G_1 = 0$. The rest is left to the reader. □

The matrix $\mathrm{I}_{k,q,m}$ is called a *standard simple matrix.* We denote the matrix $\mathrm{I}_{k,n,n}$ by $\mathrm{I}_{k,n}$ and we call it a *standard projection matrix.*

5.11. Definition. A linear map between free modules of finite rank is said to be *simple* if it can be represented by a matrix $\mathrm{I}_{k,q,m}$ over suitable bases. Similarly a matrix is said to be *simple* when it is equivalent to a matrix $\mathrm{I}_{k,q,m}$.

Generalized Cramer formula

We study in this subsection some generalizations of the usual Cramer formulas. We will exploit these in the following paragraphs.

For a matrix $A \in \mathbf{A}^{m\times n}$ we denote by $A_{\alpha,\beta}$ the matrix extracted on the rows $\alpha = \{\alpha_1, \ldots, \alpha_r\} \subseteq [\![1..m]\!]$ and the columns $\beta = \{\beta_1, \ldots, \beta_s\} \subseteq [\![1..n]\!]$.

Suppose that the matrix A is of rank $\leqslant k$. Let $V \in \mathbf{A}^{m\times 1}$ be a column vector such that the bordered matrix $[\,A\,|\,V\,]$ is also of rank $\leqslant k$. Let us call A_j the j-th column of A. Let $\mu_{\alpha,\beta} = \det(A_{\alpha,\beta})$ be the minor of order k of the matrix A extracted on the rows $\alpha = \{\alpha_1, \ldots, \alpha_k\}$ and the columns $\beta = \{\beta_1, \ldots, \beta_k\}$. For $j \in [\![1..k]\!]$ let $\nu_{\alpha,\beta,j}$ be the determinant of the same extracted matrix, except that the column j has been replaced with the extracted column of V on the rows α. Then, we obtain for each pair (α, β) of multi-indices a Cramer identity:

$$\mu_{\alpha,\beta}\, V = \sum\nolimits_{j=1}^{k} \nu_{\alpha,\beta,j}\, A_{\beta_j} \tag{9}$$

due to the fact that the rank of the bordered matrix $[\,A_{1..m,\beta}\,|\,V\,]$ is $\leqslant k$. This can be read as follows:

$$\begin{aligned}
\mu_{\alpha,\beta}\, V &= \begin{bmatrix} A_{\beta_1} & \ldots & A_{\beta_k} \end{bmatrix} \cdot \begin{bmatrix} \nu_{\alpha,\beta,1} \\ \vdots \\ \nu_{\alpha,\beta,k} \end{bmatrix} \\
&= \begin{bmatrix} A_{\beta_1} & \ldots & A_{\beta_k} \end{bmatrix} \cdot \mathrm{Adj}(A_{\alpha,\beta}) \cdot \begin{bmatrix} v_{\alpha_1} \\ \vdots \\ v_{\alpha_k} \end{bmatrix} \\
&= A \cdot (\mathrm{I}_n)_{1..n,\beta} \cdot \mathrm{Adj}(A_{\alpha,\beta}) \cdot (\mathrm{I}_m)_{\alpha,1..m} \cdot V \qquad (10)
\end{aligned}$$

This leads us to introduce the following notation.

5.12. Notation. We denote by $\mathcal{P}_\ell$ the set of parts of $[\![1..\ell]\!]$ and $\mathcal{P}_{k,\ell}$ the set of parts of $[\![1..\ell]\!]$ with k elements. For $A \in \mathbf{A}^{m\times n}$ and $\alpha \in \mathcal{P}_{k,m}$, $\beta \in \mathcal{P}_{k,n}$ we define

$$\mathrm{Adj}_{\alpha,\beta}(A) := (\mathrm{I}_n)_{1..n,\beta} \cdot \mathrm{Adj}(A_{\alpha,\beta}) \cdot (\mathrm{I}_m)_{\alpha,1..m}.$$

For example with the matrix

$$A = \begin{bmatrix} 5 & -5 & 7 & 4 \\ 9 & -1 & 2 & 7 \\ 13 & 3 & -3 & 10 \end{bmatrix},$$

and the parts $\alpha = \{1, 2\}$ and $\beta = \{2, 3\}$, we obtain

$$A_{\alpha,\beta} = \begin{bmatrix} -5 & 7 \\ -1 & 2 \end{bmatrix}, \ \mathrm{Adj}(A_{\alpha,\beta}) = \begin{bmatrix} 2 & -7 \\ 1 & -5 \end{bmatrix} \text{ and } \mathrm{Adj}_{\alpha,\beta}(A) = \begin{bmatrix} 0 & 0 & 0 \\ 2 & -7 & 0 \\ 1 & -5 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

When $\mathcal{D}_{k+1}([\,A\,|\,V\,]) = 0$, equality (10) is written as follows.

$$\mu_{\alpha,\beta}\, V \ = \ A \cdot \mathrm{Adj}_{\alpha,\beta}(A) \cdot V \tag{11}$$

We thus obtain the following equality, under the assumption that A is of rank $\leqslant k$.

$$\mu_{\alpha,\beta}\, A \ = \ A \cdot \mathrm{Adj}_{\alpha,\beta}(A) \cdot A \tag{12}$$

The Cramer's identities (11) and (12) provide the congruences which are not subject to any hypothesis: it suffices for example to read (11) in the quotient ring $\mathbf{A}/\mathcal{D}_{k+1}([\,A\,|\,V\,])$ to obtain the congruence (13).

5.13. Lemma. (Generalized Cramer formula) *Without any assumption on the matrix A or the vector V, we have for $\alpha \in \mathcal{P}_{k,m}$ and $\beta \in \mathcal{P}_{k,n}$ the following congruences.*

$$\mu_{\alpha,\beta}\, V \equiv A \cdot \mathrm{Adj}_{\alpha,\beta}(A) \cdot V \quad \bmod \quad \mathcal{D}_{k+1}(\,[\,A\,|\,V\,]\,), \tag{13}$$

$$\mu_{\alpha,\beta}\, A \equiv A \cdot \mathrm{Adj}_{\alpha,\beta}(A) \cdot A \quad \bmod \quad \mathcal{D}_{k+1}(A). \tag{14}$$

A simple special case is the following where $k = m \leqslant n$.

$$\mu_{1..m,\beta}\, \mathrm{I}_m \ = \ A \cdot \mathrm{Adj}_{1..m,\beta}(A) \quad (\beta \in \mathcal{P}_{m,n}). \tag{15}$$

This equality is in fact a direct consequence of the basic Cramer's identity (4). Similarly we obtain

$$\mu_{\alpha,1..n}\, \mathrm{I}_n \ = \ \mathrm{Adj}_{\alpha,1..n}(A) \cdot A \quad (\alpha \in \mathcal{P}_{n,m},\ n \leqslant m) \tag{16}$$

A magic formula

An immediate consequence of the Cramer's identity (12) is the less usual identity (17) given in the following theorem. Similarly the equalities (18) and (19) easily result from (15) and (16).

5.14. Theorem. *Let $A \in \mathbf{A}^{m\times n}$ be a matrix of rank k. We thus have an equality $\sum_{\alpha\in\mathcal{P}_{k,m},\beta\in\mathcal{P}_{k,n}} c_{\alpha,\beta}\, \mu_{\alpha,\beta} = 1$. Let*

$$B \;=\; \textstyle\sum_{\alpha\in\mathcal{P}_{k,m},\beta\in\mathcal{P}_{k,n}} c_{\alpha,\beta}\, \mathrm{Adj}_{\alpha,\beta}(A).$$

1. *We have*
$$A\cdot B\cdot A = A. \tag{17}$$
Consequently $A\,B$ is a projection matrix of rank k and the submodule $\mathrm{Im}\,A = \mathrm{Im}\,AB$ is a direct summand in $\mathbf{A}^m$.
2. *If $k = m$, then*
$$A\cdot B = \mathrm{I}_m. \tag{18}$$
3. *If $k = n$, then*
$$B\cdot A = \mathrm{I}_n. \tag{19}$$

The following identity, which we will not use in this work, is even more miraculous.

5.15. Proposition. (Prasad and Robinson)
With the assumptions and the notations of Theorem 5.14, if we have

$$\forall \alpha,\alpha' \in \mathcal{P}_{k,m},\ \forall \beta,\beta' \in \mathcal{P}_{k,n}\ \ c_{\alpha,\beta}\, c_{\alpha',\beta'} = c_{\alpha,\beta'}\, c_{\alpha',\beta},$$

then

$$B\cdot A\cdot B = B. \tag{20}$$

Generalized inverses and locally simple maps

Let E and F be two $\mathbf{A}$-modules, and $\varphi : E \to F$ be a linear map. We can see this as some sort of generalized system of linear equations (a usual system of linear equations corresponds to the free modules of finite rank case). Informally such a system of linear equations is considered to be “well-conditioned” if there is a systematic way to solve the equation $\varphi(x) = y$ for x from a given y, when such a solution exists. More precisely, we ask if there exists a linear map $\psi : F \to E$ satisfying $\varphi\big(\psi(y)\big) = y$ each time there exists a solution x. This amounts to asking $\varphi\big(\psi\big(\varphi(x)\big)\big) = \varphi(x)$ for all $x \in E$.

This clarifies the importance of the equation (17) and leads to the notion of a generalized inverse.

The terminology regarding generalized inverses does not seem fully fixed. We adopt that of [Lancaster & Tismenetsky].
In the book [Bhaskara Rao], the author uses the term “reflexive g-inverse.”

5.16. Definition. Let E and F be two $\mathbf{A}$-modules, and $\varphi : E \to F$ be a linear map. A linear map $\psi : F \to E$ is called a *generalized inverse* of φ if we have

$$\varphi \circ \psi \circ \varphi = \varphi \quad \text{and} \quad \psi \circ \varphi \circ \psi = \psi. \tag{21}$$

A linear map is said to be *locally simple* when it has a generalized inverse.

The following fact is immediate.

5.17. Fact. *When ψ is a generalized inverse of φ, we have:*

- $\varphi\,\psi$ *and* $\psi\,\varphi$ *are projections,*
- $\mathrm{Im}\,\varphi = \mathrm{Im}\,\varphi\,\psi$*,* $\mathrm{Im}\,\psi = \mathrm{Im}\,\psi\,\varphi$*,* $\mathrm{Ker}\,\varphi = \mathrm{Ker}\,\psi\,\varphi$*,* $\mathrm{Ker}\,\psi = \mathrm{Ker}\,\varphi\,\psi$*,*
- $E = \mathrm{Ker}\,\varphi \oplus \mathrm{Im}\,\psi$ *and* $F = \mathrm{Ker}\,\psi \oplus \mathrm{Im}\,\varphi$*,*
- $\mathrm{Ker}\,\varphi \simeq \mathrm{Coker}\,\psi$ *and* $\mathrm{Ker}\,\psi \simeq \mathrm{Coker}\,\varphi$*.*

Moreover φ and ψ provide by restriction reciprocal isomorphisms φ_1 and ψ_1 between $\mathrm{Im}\,\psi$ *and* $\mathrm{Im}\,\varphi$*. In matrix form we obtain:*

$$\begin{array}{c|cc} & \mathrm{Im}\,\psi & \mathrm{Ker}\,\varphi \\ \hline \mathrm{Im}\,\varphi & \varphi_1 & 0 \\ \mathrm{Ker}\,\psi & 0 & 0 \end{array} = \varphi, \qquad \begin{array}{c|cc} & \mathrm{Im}\,\varphi & \mathrm{Ker}\,\psi \\ \hline \mathrm{Im}\,\psi & \psi_1 & 0 \\ \mathrm{Ker}\,\varphi & 0 & 0 \end{array} = \psi.$$

Remarks.

1) If we have a linear map ψ_0 satisfying as in Theorem 5.14 the equality $\varphi\,\psi_0\,\varphi = \varphi$, we obtain a generalized inverse of φ by stating $\psi = \psi_0\,\varphi\,\psi_0$. In other words, a linear map φ is locally simple if and only if there exists a ψ satisfying $\varphi\,\psi\,\varphi = \varphi$.

2) A simple linear map between free modules of finite rank is locally simple (immediate verification).

3) Theorem 5.14 informs us that a linear map which has rank k in the sense of definition 5.7 is locally simple. ■

5.18. Fact. *Let $\varphi : \mathbf{A}^n \to \mathbf{A}^m$ be a linear map. The following properties are equivalent.*

1. *The linear map φ is locally simple.*
2. *There exists a $\varphi^\bullet : \mathbf{A}^m \to \mathbf{A}^n$ such that*
$$\mathbf{A}^n = \mathrm{Ker}\,\varphi \oplus \mathrm{Im}\,\varphi^\bullet \ \textit{and}\ \mathbf{A}^m = \mathrm{Ker}\,\varphi^\bullet \oplus \mathrm{Im}\,\varphi.$$
3. *The submodule* $\mathrm{Im}\,\varphi$ *is a direct summand in* $\mathbf{A}^m$*.*

D *1 ⇒ 2.* If ψ is a generalized inverse of φ, we can take $\varphi^\bullet = \psi$.
2 ⇒ 3. Obvious.
3 ⇒ 1. If $\mathbf{A}^m = P \oplus \mathrm{Im}\,\varphi$, denote by $\pi : \mathbf{A}^m \to \mathbf{A}^m$ the projection over $\mathrm{Im}\,\varphi$ parallel to P. For each vector e_i of the canonical basis of $\mathbf{A}^m$ there exists an element a_i of $\mathbf{A}^n$ such that $\varphi(a_i) = \pi(e_i)$. We define $\psi : \mathbf{A}^m \to \mathbf{A}^n$ as $\psi(e_i) = a_i$. Then, $\varphi \circ \psi = \pi$ and $\varphi \circ \psi \circ \varphi = \pi \circ \varphi = \varphi$, and $\psi \circ \varphi \circ \psi$ is a generalized inverse of φ. □

The notion of a locally simple linear map is a local notion in the following sense.

5.19. Concrete local-global principle. (Locally simple linear maps) *Let S_1, …, S_n be comaximal monoids of a ring $\mathbf{A}$. Let $\varphi : \mathbf{A}^m \to \mathbf{A}^q$ be a linear map. If every $\varphi_{S_i} : \mathbf{A}_{S_i}^m \to \mathbf{A}_{S_i}^q$ is simple, then φ is locally simple. More generally φ is locally simple if and only if all the φ_{S_i}'s are locally simple.*

D Let us focus on the second statement. To prove that φ is locally simple amounts to finding a ψ which satisfies $\varphi\,\psi\,\varphi = \varphi$. This is a system of linear equations in the coefficients of the matrix of ψ and we can therefore apply the basic concrete local-global principle 2.3. □

The terminology of a locally simple linear map is justified by the previous local-global principle and by the converse given in item *8* of Theorem 5.26 (also see the locally simple map lemma in the local ring case, page 495).

Grassmannians

The following theorem serves as an introduction to the grassmannian varieties. It results from Fact 5.18 and Theorem 5.14.

5.20. Theorem. (Finitely generated submodules as direct summands of a free module) *Let $M = \langle C_1, \dots, C_m \rangle$ be a finitely generated submodule of $\mathbf{A}^n$ and $C = [\,C_1 \;\cdots\; C_m\,] \in \mathbf{A}^{n\times m}$ be the corresponding matrix.*

1. *The following properties are equivalent.*
   - a. *The matrix C is locally simple.*
   - b. *The module M is a direct summand of $\mathbf{A}^n$.*
   - c. *The module M is the image of a matrix $F \in \mathbb{AG}_n(\mathbf{A})$.*
2. *The following properties are equivalent.*
   - a. *The matrix C is of rank k.*
   - b. *The module M is image of a matrix $F \in \mathbb{AG}_n(\mathbf{A})$ of rank k.*

The "variety" of vector lines in a $\mathbf{K}$-vector space of dimension $n+1$ is, intuitively, of dimension n, as a vector line essentially depends on n parameters (a nonzero vector, up to a multiplicative constant, that makes $(n+1)-1$ independent parameters). We call this variety the projective space of dimension n over $\mathbf{K}$.

Furthermore, passing from a field $\mathbf{K}$ to an arbitrary ring $\mathbf{A}$, the correct generalization of a "vector line in $\mathbf{K}^{n+1}$" is "the image of a projection matrix of rank 1 in $\mathbf{A}^{n+1}$." This leads to the following definitions.

5.21. Definition.

1. We define the space $\mathbb{AG}_{n,k}(\mathbf{A}) \subseteq \mathbb{AG}_n(\mathbf{A})$ as the set of projection matrices of rank k and $\mathbb{G}_{n,k}(\mathbf{A})$ as the set of submodules of $\mathbf{A}^n$ which are images of matrices of $\mathbb{AG}_{n,k}(\mathbf{A})$.
2. The space $\mathbb{G}_{n+1,1}(\mathbf{A})$ is again denoted by $\mathbb{P}^n(\mathbf{A})$ and we call it the *projective space of dimension n over* $\mathbf{A}$.
3. We denote by $\mathbb{G}_n(\mathbf{A})$ the space of all the submodules that are direct summands of $\mathbf{A}^n$ (i.e., images of a projection matrix).

The above definition is a little unsatisfactory, insofar as we have not explained how the set $\mathbb{G}_{n,k}(\mathbf{A})$ is structured. Only this structure makes it worthy of the label "space."

A partial answer is given by the observation that $\mathbb{G}_{n,k}$ is a functor. More precisely, to every homomorphism $\varphi : \mathbf{A} \to \mathbf{B}$ we associate a natural map $\mathbb{G}_{n,k}(\varphi) : \mathbb{G}_{n,k}(\mathbf{A}) \to \mathbb{G}_{n,k}(\mathbf{B})$, so that

$$\mathbb{G}_{n,k}(\mathrm{Id}_{\mathbf{A}}) = \mathrm{Id}_{\mathbb{G}_{n,k}(\mathbf{A})}, \text{ and } \mathbb{G}_{n,k}(\psi \circ \varphi) = \mathbb{G}_{n,k}(\psi) \circ \mathbb{G}_{n,k}(\varphi),$$

when $\psi \circ \varphi$ is defined.

Injectivity and surjectivity criteria

Two famous propositions are contained in the following theorem.

5.22. Theorem. *Let $\varphi : \mathbf{A}^n \to \mathbf{A}^m$ be a linear map with matrix A.*

1. *The map φ is surjective if and only if φ is of rank m, i.e. here $\mathcal{D}_m(\varphi) = \langle 1 \rangle$ (we then say that A is* unimodular*).*
2. (McCoy's theorem) *The map φ is injective if and only if $\mathcal{D}_n(\varphi)$ is faithful, i.e. if the annihilator of $\mathcal{D}_n(\varphi)$ is reduced to $\{0\}$.*

D *1.* If φ is surjective, it admits a right inverse ψ, and Fact 5.6 gives $\langle 1 \rangle = \mathcal{D}_m(\mathrm{I}_m) \subseteq \mathcal{D}_m(\varphi)\mathcal{D}_m(\psi)$, so $\mathcal{D}_m(\varphi) = \langle 1 \rangle$. Conversely, if A is of rank m, equation (18) shows that A admits a right inverse, and φ is surjective.

2. Assume that $\mathcal{D}_n(A)$ is faithful. By equality (16), if $AV = 0$, then $\mu_{\alpha,1..n}V = 0$ for all the generators $\mu_{\alpha,1..n}$ of $\mathcal{D}_n(A)$, and so $V = 0$.

For the converse, we will prove by induction on k the following property: *if k column vectors $x_1, \dots, x_k$ are linearly independent, then the annihilator of the vector $x_1 \wedge \cdots \wedge x_k$ is reduced to* 0. For $k = 1$ it is trivial. To pass from k to $k+1$ we proceed as follows. Let z be a scalar that annihilates $x_1 \wedge \cdots \wedge x_{k+1}$. For $\alpha \in \mathcal{P}_{k,m}$, we denote by $d_\alpha(y_1, \dots, y_k)$ the minor extracted on the index rows of α for the column vectors $y_1, \dots, y_k$ of $\mathbf{A}^m$. Since $z(x_1 \wedge \cdots \wedge x_{k+1}) = 0$, and by the Cramer formulas, we have the equality

$$z \left(d_\alpha(x_1, \dots, x_k)x_{k+1} - d_\alpha(x_1, \dots, x_{k-1}, x_{k+1})x_k + \cdots \right) = 0,$$

so $z\,d_\alpha(x_1,\dots,x_k)=0$.
As this is true for any α, this gives $z(x_1\wedge\cdots\wedge x_k)=0$, and by the induction hypothesis, $z=0$. □

Remark. Theorem 5.22 can also be read in the following way.

1. The linear map $\varphi:\mathbf{A}^n\to\mathbf{A}^m$ is surjective if and only if the map $\bigwedge^m\varphi:\mathbf{A}^{\binom{n}{m}}\to\mathbf{A}$ is surjective.
2. The linear map $\varphi:\mathbf{A}^n\to\mathbf{A}^m$ is injective if and only if the map $\bigwedge^n\varphi:\mathbf{A}\to\mathbf{A}^{\binom{m}{n}}$ is injective. ■

5.23. Corollary. *Let $\varphi:\mathbf{A}^n\to\mathbf{A}^m$ be an $\mathbf{A}$-linear map.*

1. *If φ is surjective and $n<m$, the ring is trivial.*
2. *If φ is injective and $n>m$, the ring is trivial.*

Remark. A more positive, equivalent, but probably even more bewildering formulation of the results of the previous corollary is the following.

1. If φ is surjective, then X^m divides X^n in $\mathbf{A}[X]$.
2. If φ is injective, then X^n divides X^m in $\mathbf{A}[X]$.

In some way, this is closer to the formulation found in classical mathematics: if the ring is nontrivial, then $m\leqslant n$ in the first case (resp. $n\leqslant m$ in the second case).
The advantage of our formulations is that they work in all cases, without the need to assume that we know how to decide if the ring is trivial or not. ■

5.24. Corollary. *If $\varphi:\mathbf{A}^n\to\mathbf{A}^m$ is injective, the same applies for every exterior power of φ.*

D The annihilator of $\mathcal{D}_n(\varphi)$ is reduced to 0 by the previous theorem. There exists a ring $\mathbf{B}\supseteq\mathbf{A}$ such that the generators of $\mathcal{D}_n(\varphi)$ become comaximal in $\mathbf{B}$ (Lemma 2.14). The $\mathbf{B}$-linear map $\varphi_1:\mathbf{B}^n\to\mathbf{B}^m$ obtained by extending φ to $\mathbf{B}$ is thus of rank n and admits a left inverse ψ (item *3* of Theorem 5.14), i.e. $\psi\circ\varphi_1=\mathrm{Id}_{\mathbf{B}^n}$. Therefore

$$\textstyle\bigwedge^k\psi\circ\bigwedge^k\varphi_1=\mathrm{Id}_{\bigwedge^k\mathbf{B}^n}.$$

Thus the matrix of $\bigwedge^k\varphi_1$ is injective, and since it is the same matrix as that of $\bigwedge^k\varphi$, the linear map $\bigwedge^k\varphi$ is injective. □

Characterization of locally simple maps

The following lemma places a bijective correspondence between the fundamental systems of orthogonal idempotents and the non-decreasing sequences of idempotents for divisibility.

5.25. Lemma. *Let ($e_{q+1} = 0$, e_q, …, e_1, $e_0 = 1$) be a list of idempotents such that e_i divides e_{i+1} for $i = 0, \ldots, q$. Then, the elements $r_i := e_i - e_{i+1}$, for $i \in [\![0..q]\!]$, form a fundamental system of orthogonal idempotents. Conversely, every fundamental system of orthogonal idempotents $(r_0, \ldots, r_q)$ defines such a list of idempotents by letting*

$$e_j = \textstyle\sum_{k \geqslant j} r_k \text{ for } j \in [\![0..q+1]\!].$$

D It is clear that $\sum_i r_i = 1$. For $0 \leqslant i < q$, we have $e_{i+1} = e_i e_{i+1}$. Hence $(e_i - e_{i+1})e_{i+1} = 0$, i.e. $(r_q + \cdots + r_{i+1}) \cdot r_i = 0$. We can now easily deduce that $r_i r_j = 0$ for $j > i$. □

We denote by $\mathrm{Diag}(a_1, \ldots, a_n)$ the diagonal matrix of order n whose coefficient in position (i, i) is the element a_i.

In the following theorem some of the idempotents r_i in the fundamental system of orthogonal idempotents can very well be equal to zero. For example if the ring is connected and nontrivial, all but one are equal to zero.

5.26. Theorem. (Locally simple matrix)
Let $G \in \mathbf{A}^{m \times n}$ be the matrix of $\varphi : \mathbf{A}^n \to \mathbf{A}^m$ and $q = \inf(m, n)$.
The following properties are equivalent.

1. *The linear map φ is locally simple.*
2. *The submodule $\operatorname{Im}\varphi$ is a direct summand of $\mathbf{A}^m$.*
3. *$\operatorname{Im}\varphi$ is a direct summand of $\mathbf{A}^m$ and $\operatorname{Ker}\varphi$ is a direct summand of $\mathbf{A}^n$.*
4. *There exists a linear map $\varphi^\bullet : \mathbf{A}^m \to \mathbf{A}^n$ with $\mathbf{A}^n = \operatorname{Ker}\varphi \oplus \operatorname{Im}\varphi^\bullet$ and $\mathbf{A}^m = \operatorname{Ker}\varphi^\bullet \oplus \operatorname{Im}\varphi$.*
5. *Each determinantal ideal $\mathcal{D}_k(\varphi)$ is idempotent.*
6. *There exists a (unique) fundamental system of orthogonal idempotents $(r_0, r_1, \ldots, r_q)$ such that on each localized ring $\mathbf{A}[1/r_k]$ the map φ is of rank k.*
7. *Each determinantal ideal $\mathcal{D}_k(\varphi)$ is generated by an idempotent e_k. Then let $r_k = e_k - e_{k+1}$. The r_k's form a fundamental system of orthogonal idempotents. For every minor μ of order k of G, on the localized ring $\mathbf{A}[1/(r_k\,\mu)]$ the linear map φ becomes simple of rank k.*
8. *The linear map φ becomes simple after localization at suitable comaximal elements.*
9. *Each determinantal ideal $\mathcal{D}_k(\varphi)$ is generated by an idempotent e_k and the matrix of φ becomes equivalent to the matrix $\mathrm{Diag}(e_1, e_2, \ldots, e_q)$, eventually filled-in with zeros (for both rows and columns), after localization at suitable comaximal elements.*
10. * *The linear map φ becomes simple after localization at any arbitrary maximal ideal.*

D The equivalence of items *1*, *2*, *3*, *4* is already clear (see Facts 5.17 and 5.18). Furthermore, we trivially have *7* ⇒ *6* ⇒ *5* and *9* ⇒ *5*.

Since $q = \inf(m, n)$, we have $\mathcal{D}_{q+1}(\varphi) = 0$.

1 ⇒ *5*. We have $GHG = G$ for some matrix H and we apply Fact 5.6.

5 ⇒ *7*. The fact that each $\mathcal{D}_k(\varphi)$ is generated by an idempotent e_k results from Fact 4.6. The fact that $(r_0, \ldots, r_q)$ is a fundamental system of orthogonal idempotents results from Lemma 5.25 (and Fact 5.4).
As $r_k e_{k+1} = 0$, over the ring $\mathbf{A}[1/r_k]$, and thus over the ring $\mathbf{A}[1/(\mu r_k)]$, where μ is a minor of order k, every minor of order $k+1$ of the matrix G is null. Thus, by the freeness lemma 5.10, G is simple of rank k.

7 ⇒ *9*. Over $\mathbf{A}[1/r_k]$ and so over $\mathbf{A}[1/(\mu r_k)]$ (μ a minor of order k), we have $\mathrm{Diag}(e_1, \ldots, e_q) = \mathrm{Diag}(1, \ldots, 1, 0, \ldots, 0)$ with 1 appearing k times.

7 ⇒ *8*. Let $t_{k,j}$ be the minors of order k of G. The localizations are those at $t_{k,j} r_k$. We must verify that they are comaximal. Each e_k is in the form $\sum t_{k,j} v_{k,j}$, so $\sum_{k,j} v_{k,j}(t_{k,j} r_k) = \sum_k e_k r_k = \sum r_k = 1$.

8 ⇒ *1*. By application of the local-global principle 5.19 since every simple map is locally simple.

8 ⇒ *10*. (In classical mathematics.) Because the complement of a maximal ideal always contains at least one element in a system of comaximal elements (we can assume that the ring is nontrivial).

10 ⇒ *8*. (In classical mathematics.) For each maximal ideal $\mathfrak{m}$ we obtain a $s_{\mathfrak{m}} \notin \mathfrak{m}$ and a matrix $H_{\mathfrak{m}}$ such that we have $GH_{\mathfrak{m}}G = G$ in $\mathbf{A}[1/s_{\mathfrak{m}}]$. The ideal generated by the $s_{\mathfrak{m}}$'s is not contained in any maximal ideal and so it is the ideal $\langle 1 \rangle$. Thus there is a finite number of these $s_{\mathfrak{m}}$'s which are comaximal.

Let us finish by giving a direct proof for the implication *6* ⇒ *1*.
On the ring $\mathbf{A}[1/r_k]$ the matrix G is of rank k so there exists a matrix B_k satisfying $GB_kG = G$ (Theorem 5.14). This means that on the ring $\mathbf{A}$ we have a matrix H_k in $\mathbf{A}^{n \times m}$ satisfying $r_k H_k = H_k$ and $r_k G = GH_kG$. We then take $H = \sum_k H_k$ and obtain $G = GHG$. □

The equivalence of items *1* to *9* has been established constructively, whilst item *10* only implies the previous ones in classical mathematics.

Trace, norm, discriminant, transitivity

We denote by $\mathrm{Tr}(\varphi)$ and $\mathrm{C}_{\varphi}(X)$ the trace and the *characteristic polynomial* of an endomorphism φ of a free module of finite rank (we take as characteristic polynomial of a matrix $F \in \mathbb{M}_n(\mathbf{A})$ the polynomial $\det(X\mathrm{I}_n - F)$, which has the advantage of being monic).

5.27. Notation.

- If $\mathbf{A} \subseteq \mathbf{B}$ and if $\mathbf{B}$ is a free $\mathbf{A}$-module of finite rank, we denote $\mathrm{rk}_{\mathbf{A}}(\mathbf{B})$ by $[\,\mathbf{B} : \mathbf{A}\,]$.
- For $a \in \mathbf{B}$ we then denote by $\mathrm{Tr}_{\mathbf{B}/\mathbf{A}}(a)$, $\mathrm{N}_{\mathbf{B}/\mathbf{A}}(a)$ and $\mathrm{C}_{\mathbf{B}/\mathbf{A}}(a)(X)$ the trace, the determinant and the characteristic polynomial of the multiplication by a, seen as an endomorphism of the $\mathbf{A}$-module $\mathbf{B}$.

5.28. Lemma. *Assume that $\mathbf{A} \subseteq \mathbf{B}$ and that $\mathbf{B}$ is a free $\mathbf{A}$-module of finite rank m.*

1. *Let E be a free $\mathbf{B}$-module of finite rank n. If $\underline{e} = (e_i)_{i\in[\![1..m]\!]}$ is a basis of $\mathbf{B}$ over $\mathbf{A}$ and $\underline{f} = (f_j)_{j\in[\![1..n]\!]}$ a basis of E over $\mathbf{B}$, then $(e_i f_j)_{i,j}$ is a basis of E over $\mathbf{A}$. Consequently, E is free over $\mathbf{A}$ and*
$$\mathrm{rk}_{\mathbf{A}}(E) = \mathrm{rk}_{\mathbf{B}}(E) \times \mathrm{rk}_{\mathbf{A}}(\mathbf{B}).$$
2. *If $\mathbf{B} \subseteq \mathbf{C}$ and if $\mathbf{C}$ is a free $\mathbf{B}$-module of finite rank, we have*
$$[\,\mathbf{C} : \mathbf{A}\,] = [\,\mathbf{C} : \mathbf{B}\,]\,[\,\mathbf{B} : \mathbf{A}\,].$$

Remark. Let $\mathbf{C} = \mathbf{A}[Y]/\langle Y^3\rangle = \mathbf{A}[y]$, a free $\mathbf{A}$-algebra of rank 3. Since $y^4 = 0$, $\mathbf{B} = \mathbf{A} \oplus \mathbf{A}y^2$ is a sub-algebra of $\mathbf{C}$, free over $\mathbf{A}$, whose rank (equal to 2) does not divide the rank of $\mathbf{C}$ (equal to 3). The equality $[\,\mathbf{C} : \mathbf{A}\,] = [\,\mathbf{C} : \mathbf{B}\,][\,\mathbf{B} : \mathbf{A}\,]$ does not apply because $\mathbf{C}$ is not free over $\mathbf{B}$. ■

5.29. Theorem. (Transitivity formulas for the trace, the determinant and the characteristic polynomial) *Under the same assumptions, let $u_{\mathbf{B}} : E \to E$ be a $\mathbf{B}$-linear map. We denote by $u_{\mathbf{A}}$ this map when considered as an $\mathbf{A}$-linear map. We then have the equalities:*

$$\det(u_{\mathbf{A}}) = \mathrm{N}_{\mathbf{B}/\mathbf{A}}\big(\det(u_{\mathbf{B}})\big),\ \ \mathrm{Tr}(u_{\mathbf{A}}) = \mathrm{Tr}_{\mathbf{B}/\mathbf{A}}\,\big(\mathrm{Tr}(u_{\mathbf{B}})\big),$$
$$\mathrm{C}_{u_{\mathbf{A}}}(X) = \mathrm{N}_{\mathbf{B}[X]/\mathbf{A}[X]}\big(\mathrm{C}_{u_{\mathbf{B}}}(X)\big).$$

D We use the notations of Lemma 5.28. Let u_{kj} be the elements of $\mathbf{B}$ defined by $u(f_j) = \sum_{k=1}^{n} u_{kj} f_k$. Then the matrix M of $u_{\mathbf{A}}$ with respect to the basis $(e_i f_j)_{i,j}$ is expressed as a block matrix

$$M = \begin{bmatrix} M_{11} & \cdots & M_{1n} \\ \vdots & & \vdots \\ M_{n1} & \cdots & M_{nn} \end{bmatrix},$$

where M_{kj} represents the $\mathbf{A}$-linear map $b \mapsto bu_{kj}$ of $\mathbf{B}$ in $\mathbf{B}$ to with respect to the basis $\underline{e}$. This provides the desired equality regarding the trace of u_A

since

$$\begin{aligned}\operatorname{Tr}(u_{\mathbf{A}}) = \ & \sum\nolimits_{i=1}^{n} \operatorname{Tr}(M_{ii}) \ = \sum\nolimits_{i=1}^{n} \operatorname{Tr}_{\mathbf{B}/\mathbf{A}}(u_{ii}) \\ = \ & \operatorname{Tr}_{\mathbf{B}/\mathbf{A}}\big(\sum\nolimits_{i=1}^{n} u_{ii}\big) \ = \ \operatorname{Tr}_{\mathbf{B}/\mathbf{A}}\big(\operatorname{Tr}(u_{\mathbf{B}})\big).\end{aligned}$$

As for the equality for the determinant, note that the matrices M_{ij} pairwise commute (M_{ij} is the matrix of the multiplication by u_{ij}). We can then apply the following Lemma 5.30, which gives us:

$$\det(M) = \det(\Delta) \quad \text{with} \quad \Delta = \sum\nolimits_{\sigma\in \mathrm{S}_n} \varepsilon(\sigma) M_{1\sigma_1} M_{2\sigma_2} \ldots M_{n\sigma_n}.$$

However, Δ is none other than the matrix of the multiplication by the element $\sum_{\sigma\in \mathrm{S}_n} \varepsilon(\sigma) u_{1\sigma_1} u_{2\sigma_2} \ldots u_{n\sigma_n}$, i.e., by $\det(u_{\mathbf{B}})$, thus:

$$\det(u_{\mathbf{A}}) = \det(M) = \mathrm{N}_{\mathbf{B}/\mathbf{A}}\big(\det(u_{\mathbf{B}})\big).$$

Finally, the equality for the characteristic polynomial is deduced from the one for determinants by using the fact that $\mathrm{C}_{u_{\mathbf{A}}}(X)$ is the determinant of the endomorphism $X\mathrm{Id}_{E[X]} - u_{\mathbf{A}}$ of the $\mathbf{A}[X]$-module $E[X]$ whereas $\mathrm{C}_{u_{\mathbf{B}}}(X)$ is that of the same map seen as an endomorphism of the $\mathbf{B}[X]$-module $E[X]$.□

In a noncommutative ring, two elements a and b are said to be *permutable* or *commuting* if $ab = ba$.

5.30. Lemma. *Let $(N_{ij})_{i,j}$ be a family of n^2 pairwise commuting square matrices, and N the square matrix of order mn:*

$$N = \begin{bmatrix} N_{11} & \cdots & N_{1n} \\ \vdots & & \vdots \\ N_{n1} & \cdots & N_{nn} \end{bmatrix}.$$

Then: $\det(N) = \det\big(\sum_{\sigma\in \mathrm{S}_n} \varepsilon(\sigma)\, N_{1\sigma_1} N_{2\sigma_2} \ldots N_{n\sigma_n}\big)$.

D Let Δ be the $n\times n$ matrix defined by $\Delta = \sum_{\sigma\in \mathrm{S}_n} \varepsilon(\sigma) N_{1\sigma_1} N_{2\sigma_2} \ldots N_{n\sigma_n}$. Thus we must prove that $\det(N) = \det(\Delta)$.

Let us treat the special cases $n = 2$ then $n = 3$. We replace $\mathbf{A}$ with $\mathbf{A}[Y]$ and N_{ii} by $N_{ii} + Y\mathrm{I}_m$, which has the advantage of making some determinants regular in $\mathbf{A}[Y]$. It suffices to establish the equalities with these new matrices, as we finish by making $Y = 0$.

The key-element of the proof for $n = 2$ resides in the following equality:

$$\begin{bmatrix} N_{11} & N_{12} \\ N_{21} & N_{22} \end{bmatrix} \begin{bmatrix} N_{22} & 0 \\ -N_{21} & \mathrm{I}_m \end{bmatrix} = \begin{bmatrix} N_{11}N_{22} - N_{12}N_{21} & N_{12} \\ 0 & N_{22} \end{bmatrix}.$$

We then consider the LHS and RHS determinants

$$\det(N)\det(N_{22}) = \det(N_{11}N_{22} - N_{12}N_{21})\det(N_{22}),$$

next we simplify by $\det(N_{22})$ (which is regular) to obtain the result.

Case $n = 3$ uses the equality:

$$\begin{bmatrix} N_{11} & N_{12} & N_{13} \\ N_{21} & N_{22} & N_{23} \\ N_{31} & N_{32} & N_{33} \end{bmatrix} \begin{bmatrix} N_{22}N_{33} - N_{23}N_{32} & 0 & 0 \\ N_{31}N_{23} - N_{21}N_{33} & \mathrm{I}_m & 0 \\ N_{21}N_{32} - N_{22}N_{31} & 0 & \mathrm{I}_m \end{bmatrix} = \begin{bmatrix} \Delta & N_{12} & N_{13} \\ 0 & N_{22} & N_{23} \\ 0 & N_{32} & N_{33} \end{bmatrix},$$

which leads to

$$\det(N)\det(N_{22}N_{33} - N_{23}N_{32}) = \det(\Delta)\det\begin{bmatrix} N_{22} & N_{23} \\ N_{32} & N_{33} \end{bmatrix}.$$

Case $n = 2$ provides $\det(N_{22}N_{33} - N_{23}N_{32}) = \det\begin{bmatrix} N_{22} & N_{23} \\ N_{32} & N_{33} \end{bmatrix}$. We simplify by this determinant and obtain $\det(N) = \det(\Delta)$.

The general case is left as an exercise (see Exercise 28). □

5.31. Corollary. *Let* $\mathbf{A} \subseteq \mathbf{B} \subseteq \mathbf{C}$ *be three rings with* $\mathbf{C}$ *free of finite rank over* $\mathbf{B}$ *and* $\mathbf{B}$ *free of finite rank over* $\mathbf{A}$. *We then have:*

$$\mathrm{N}_{\mathbf{C}/\mathbf{A}} = \mathrm{N}_{\mathbf{B}/\mathbf{A}} \circ \mathrm{N}_{\mathbf{C}/\mathbf{B}}, \quad \mathrm{Tr}_{\mathbf{C}/\mathbf{A}} = \mathrm{Tr}_{\mathbf{B}/\mathbf{A}} \circ \mathrm{Tr}_{\mathbf{C}/\mathbf{B}},$$
$$\mathrm{C}_{\mathbf{C}/\mathbf{A}}(c)(X) = \mathrm{N}_{\mathbf{B}[X]/\mathbf{A}[X]}\big(\mathrm{C}_{\mathbf{C}/\mathbf{B}}(c)(X)\big) \quad (c \in \mathbf{C}).$$

Gram determinants and discriminants

5.32. Definition. Let M be an $\mathbf{A}$-module, $\varphi : M \times M \to \mathbf{A}$ be a symmetric bilinear form and $(\underline{x}) = (x_1, \dots, x_k)$ be a list of elements of M. We call the matrix

$$\mathrm{Gram}_{\mathbf{A}}(\varphi, \underline{x}) \overset{\mathrm{def}}{=} \big(\varphi(x_i, x_j)\big)_{i,j \in [\![1..k]\!]}$$

the *Gram matrix of* $(x_1, \dots, x_k)$ *for* φ. Its determinant is called the *Gram determinant of* $(x_1, \dots, x_k)$ *for* φ and is denoted by $\mathrm{gram}_{\mathbf{A}}(\varphi, \underline{x})$.

If $\mathbf{A}y_1 + \cdots + \mathbf{A}y_k \subseteq \mathbf{A}x_1 + \cdots + \mathbf{A}x_k$ we have an equality

$$\mathrm{gram}(\varphi, y_1, \dots, y_k) = \det(A)^2\,\mathrm{gram}(\varphi, x_1, \dots, x_k),$$

where A is a $k \times k$ matrix which expresses the y_j's in terms of the x_i's.

We now introduce an important case of a Gram determinant, the discriminant. Recall that two elements a, b of a ring $\mathbf{A}$ are said to be *associated* if there exists a $u \in \mathbf{A}^{\times}$ such that $a = ub$. In the literature such elements are also referred to as *associates*.

5.33. Proposition and definition. *Let* $\mathbf{C} \supseteq \mathbf{A}$ *be an* $\mathbf{A}$*-algebra which is a free* $\mathbf{A}$*-module of finite rank and* $x_1, \dots, x_k, y_1, \dots, y_k \in \mathbf{C}$.

1. *We call the determinant of the matrix*

$$\big(\mathrm{Tr}_{\mathbf{C}/\mathbf{A}}(x_i x_j)\big)_{i,j \in [\![1..k]\!]}$$

the discriminant *of* $(x_1, \dots, x_k)$. *We denote it by* $\mathrm{disc}_{\mathbf{C}/\mathbf{A}}(x_1, \dots, x_k)$ *or* $\mathrm{disc}(x_1, \dots, x_k)$.

2. *If* $\mathbf{A}y_1 + \cdots + \mathbf{A}y_k \subseteq \mathbf{A}x_1 + \cdots + \mathbf{A}x_k$ *we have*
$$\mathrm{disc}(y_1, \ldots, y_k) = \det(A)^2 \,\mathrm{disc}(x_1, \ldots, x_k),$$
where A *is a* $k \times k$ *matrix which expresses the* y_j*'s in terms of the* x_i*'s.*
3. *In particular, if* $(x_1, \ldots, x_n)$ *and* $(y_1, \ldots, y_n)$ *are two bases of the* $\mathbf{A}$*-algebra* $\mathbf{C}$*, the elements* $\mathrm{disc}(x_1, \ldots, x_n)$ *and* $\mathrm{disc}(y_1, \ldots, y_n)$ *are multiplicatively congruent modulo the squares of* $\mathbf{A}^{\times}$*. We call the corresponding equivalence class the* discriminant of the extension $\mathbf{C}/\mathbf{A}$*. We denote it by* $\mathrm{Disc}_{\mathbf{C}/\mathbf{A}}$*.*
4. *If* $\mathrm{Disc}_{\mathbf{C}/\mathbf{A}}$ *is regular and* $n = [\,\mathbf{C} : \mathbf{A}\,]$*, a system* $u_1, \ldots, u_n$ *in* $\mathbf{C}$ *is an* $\mathbf{A}$*-basis of* $\mathbf{C}$ *if and only if* $\mathrm{disc}(u_1, \ldots, u_n)$ *and* $\mathrm{Disc}_{\mathbf{C}/\mathbf{A}}$ *are associated elements.*

For example when $\mathbf{A} = \mathbb{Z}$ the discriminant of the extension is a well-defined integer, whereas if $\mathbf{A} = \mathbb{Q}$, the discriminant is characterized on the one hand by its sign, and on the other hand by the list of prime numbers contained therein with an odd power.

5.34. Proposition. *Let* $\mathbf{B}$ *and* $\mathbf{C}$ *be two free* $\mathbf{A}$*-algebras of ranks* m *and* n*, respectively, and consider the product algebra* $\mathbf{B} \times \mathbf{C}$*.*

Given a list $(\underline{x}) = (x_1, \ldots, x_m)$ *of elements of* $\mathbf{B}$ *and a list* $(\underline{y}) = (y_1, \ldots, y_n)$ *of elements of* $\mathbf{C}$*, we have:*
$$\mathrm{disc}_{(\mathbf{B}\times\mathbf{C})/\mathbf{A}}(\underline{x}, \underline{y}) = \mathrm{disc}_{\mathbf{B}/\mathbf{A}}(\underline{x}) \times \mathrm{disc}_{\mathbf{C}/\mathbf{A}}(\underline{y}).$$
In particular, $\mathrm{Disc}_{(\mathbf{B}\times\mathbf{C})/\mathbf{A}} = \mathrm{Disc}_{\mathbf{B}/\mathbf{A}} \times \mathrm{Disc}_{\mathbf{C}/\mathbf{A}}$*.*

D The proof is left to the reader. □

5.35. Proposition. *Let* $\mathbf{B} \supseteq \mathbf{A}$ *be a free* $\mathbf{A}$*-algebra of finite rank* p*. We consider*

- *a* $\mathbf{B}$*-module* E*,*
- *a symmetric* $\mathbf{B}$*-bilinear form* $\varphi_{\mathbf{B}} : E \times E \to \mathbf{B}$*,*
- *a basis* $(\underline{b}) = (b_i)_{i\in[\![1..p]\!]}$ *of* $\mathbf{B}$ *over* $\mathbf{A}$*, and*
- *a family* $(\underline{e}) = (e_j)_{j\in[\![1..n]\!]}$ *of* n *elements of* E*.*

Let $(\underline{b} \star \underline{e})$ *be a family* $(b_i e_j)$ *of* np *elements of* E *and* $\varphi_{\mathbf{A}} : E \times E \to \mathbf{A}$ *be the symmetric* $\mathbf{A}$*-bilinear form defined by:*
$$\varphi_{\mathbf{A}}(x, y) = \mathrm{Tr}_{\mathbf{B}/\mathbf{A}}\big(\varphi_{\mathbf{B}}(x, y)\big).$$
We then have the following transitivity formula:
$$\mathrm{gram}(\varphi_{\mathbf{A}}, \underline{b} \star \underline{e}) = \mathrm{disc}_{\mathbf{B}/\mathbf{A}}(\underline{b})^n \times \mathrm{N}_{\mathbf{B}/\mathbf{A}}\big(\mathrm{gram}(\varphi_{\mathbf{B}}, \underline{e})\big).$$

D In the following the indices i, i', k, j, j' satisfy i, i', $k \in [\![1..p]\!]$ and j, $j' \in [\![1..n]\!]$. Let us agree to sort $\underline{b} \star \underline{e}$ in the following order:
$$\underline{b} \star \underline{e} = b_1e_1, \ldots, b_pe_1, b_1e_2, \ldots, b_pe_2, \ldots, b_1e_n, \ldots, b_pe_n.$$

For $x \in \mathbf{B}$, let $\mu_x : \mathbf{B} \to \mathbf{B}$ be the multiplication by x and $m(x)$ be the matrix of μ_x with respect to the basis $(b_i)_{i\in[\![1..p]\!]}$ of $\mathbf{B}$ over $\mathbf{A}$. Thus we define an isomorphism m of the ring $\mathbf{B}$ into a commutative subring of $\mathbb{M}_p(\mathbf{A})$. If we let $m_{ki}(x)$ be the coefficients of the matrix $m(x)$, we then have:

$$\mu_x(b_i) = b_i x = \sum\nolimits_{k=1}^{p} m_{ki}(x) b_k,$$

with $\mathrm{N}_{\mathbf{B}/\mathbf{A}}(x) = \det\big(m(x)\big)$. By letting $\varphi_{jj'} = \varphi_{\mathbf{B}}(e_j, e_{j'}) \in \mathbf{B}$, we have

$$\varphi_{\mathbf{A}}(b_i e_j b_{i'} e_{j'}) = \mathrm{Tr}_{\mathbf{B}/\mathbf{A}}\big(\varphi_{\mathbf{B}}(b_i e_j b_{i'} e_{j'})\big) = \mathrm{Tr}_{\mathbf{B}/\mathbf{A}}(b_i b_{i'} \varphi_{jj'}).$$

By using the equality $b_{i'}\varphi_{jj'} = \sum_{k=1}^{p} m_{ki'}(\varphi_{jj'})\, b_k$, we have with $\mathrm{Tr} = \mathrm{Tr}_{\mathbf{B}/\mathbf{A}}$:

$$\mathrm{Tr}(b_i b_{i'} \varphi_{jj'}) = \mathrm{Tr}\big(\sum\nolimits_{k=1}^{p} b_i\, m_{ki'}(\varphi_{jj'})\, b_k\big) = \sum\nolimits_{k=1}^{p} \mathrm{Tr}(b_i b_k)\, m_{ki'}(\varphi_{jj'}). \quad (*)$$

We define $\beta \in \mathbb{M}_p(\mathbf{A})$ by $\beta_{ik} = \mathrm{Tr}_{\mathbf{B}/\mathbf{A}}(b_i b_k)$. The right-hand sum in $(*)$ is none other than the coefficient of a product of matrices: $\big(\beta \cdot m(\varphi_{jj'})\big)_{ii'}$. The Gram determinant of $\underline{b} \star \underline{e}$ for $\varphi_{\mathbf{A}}$ is therefore an $np \times np$ matrix comprised of n^2 blocks of $p \times p$ matrices. Here is that matrix if we let $\phi_{jj'} = m(\varphi_{jj'})$ to simplify the expression:

$$\begin{bmatrix} \beta\phi_{11} & \beta\phi_{12} & \dots & \beta\phi_{1n} \\ \beta\phi_{21} & \beta\phi_{22} & \dots & \beta\phi_{2n} \\ \vdots & & & \vdots \\ \beta\phi_{n1} & \beta\phi_{n2} & \dots & \beta\phi_{nn} \end{bmatrix} = \begin{bmatrix} \beta & 0 & \dots & 0 \\ 0 & \beta & \dots & \vdots \\ \vdots & & \ddots & 0 \\ 0 & & \dots & \beta \end{bmatrix} \begin{bmatrix} \phi_{11} & \phi_{12} & \dots & \phi_{1n} \\ \phi_{21} & \phi_{22} & \dots & \phi_{2n} \\ \vdots & & & \vdots \\ \phi_{n1} & \phi_{n2} & \dots & \phi_{nn} \end{bmatrix}.$$

By taking the determinants we obtain

$$\mathrm{gram}(\varphi_{\mathbf{A}}, \underline{b} \star \underline{e}) = \det(\beta)^n \cdot \det \begin{bmatrix} \phi_{11} & \phi_{12} & \dots & \phi_{1n} \\ \phi_{21} & \phi_{22} & \dots & \phi_{2n} \\ \vdots & & & \vdots \\ \phi_{n1} & \phi_{n2} & \dots & \phi_{nn} \end{bmatrix}.$$

By using the fact that the matrices ϕ_{jl} pairwise commute, we find that the right-determinant is equal to

$$\det\big(\sum_{\sigma\in\mathrm{S}_n} \varepsilon(\sigma)\phi_{1\sigma_1}\phi_{2\sigma_2}\cdots\phi_{n\sigma_n}\big) = \det m\big(\det(\varphi_{jl})\big) = \mathrm{N}_{\mathbf{B}/\mathbf{A}}\big(\mathrm{gram}(\varphi_{\mathbf{B}}, \underline{e})\big),$$

as required. □

5.36. Theorem. (Transitivity formula for the discriminants)
Let $\mathbf{A} \subseteq \mathbf{B} \subseteq \mathbf{C}$, with $\mathbf{B}$ free over $\mathbf{A}$, $\mathbf{C}$ free over $\mathbf{B}$, $[\,\mathbf{C} : \mathbf{B}\,] = n$ and $[\,\mathbf{B} : \mathbf{A}\,] = m$. Let $(\underline{b}) = (b_i)_{i\in[\![1..m]\!]}$ be a basis of $\mathbf{B}$ over $\mathbf{A}$, $(\underline{c}) = (c_j)_{j\in[\![1..n]\!]}$ be a basis of $\mathbf{C}$ over $\mathbf{B}$ and let $(\underline{b} \star \underline{c})$ be the basis $(b_i c_j)$ of $\mathbf{C}$ over $\mathbf{A}$. Then:

$$\mathrm{disc}_{\mathbf{C}/\mathbf{A}}(\underline{b} \star \underline{c}) \;=\; \mathrm{disc}_{\mathbf{B}/\mathbf{A}}(\underline{b})^{[\,\mathbf{C}:\mathbf{B}\,]}\; \mathrm{N}_{\mathbf{B}/\mathbf{A}}\big(\mathrm{disc}_{\mathbf{C}/\mathbf{B}}(\underline{c})\big),$$

$$\textit{and so}\quad \mathrm{Disc}_{\mathbf{C}/\mathbf{A}} \;=\; \mathrm{Disc}_{\mathbf{B}/\mathbf{A}}^{[\,\mathbf{C}:\mathbf{B}\,]}\; \mathrm{N}_{\mathbf{B}/\mathbf{A}}(\mathrm{Disc}_{\mathbf{C}/\mathbf{B}}).$$

D Direct application of Proposition 5.35. □

6. Basic local-global principle for modules

This section's results will not be used before Chapter V.

We are about to give a slightly more general version of the basic local-global principle 2.3. This new principle concerns arbitrary **A**-modules and linear maps, whilst the basic principle can be considered as the special case where the modules are free and of finite rank. The proof is essentially the same as that of the basic principle.
Beforehand, we start with a brief review of exact sequences and we establish some elementary properties of the localization regarding modules.

Complexes and exact sequences

When we have successive linear maps

$$M \xrightarrow{\alpha} N \xrightarrow{\beta} P \xrightarrow{\gamma} Q \ ,$$

we say that they form a *complex* if the composition of any two successive linear maps is null. We say that the sequence is *exact in* N if $\operatorname{Im}\alpha = \operatorname{Ker}\beta$. The entire sequence is said to be exact if it is exact in N and P. This extends to sequences of arbitrary length.

This "abstract" language has an immediate counterpart in terms of systems of linear equations when we are dealing with free modules of finite rank. For example if $N = \mathbf{A}^n$, $P = \mathbf{A}^m$ and if we have an exact sequence

$$0 \to M \xrightarrow{\alpha} N \xrightarrow{\beta} P \xrightarrow{\gamma} Q \to 0 \ ,$$

The linear map β is represented by a matrix associated with a system of m linear equations with n unknowns, the module M, isomorphic to $\operatorname{Ker}\beta$, represents the defect of injectivity of β and the module Q, isomorphic to $\operatorname{Coker}\beta$, represents its defect of surjectivity of β.

An exact complex of the type

$$0 \quad \to \quad M_m \quad \xrightarrow{u_m} \quad M_{m-1} \quad \longrightarrow \quad \cdots\cdots\cdots \quad \xrightarrow{u_1} \quad M_0 \quad \to \quad 0$$

with $m \geqslant 3$ is called a *long exact sequence (of length m).*

If $m = 2$, we say that we have a *short exact sequence.* In this case M_2 can be identified with a submodule of M_1, and, modulo this identification, M_0 can be identified with M_1/M_2.

An important fact to note is that every long exact sequence of length m "can be decomposed into" $m - 1$ short exact sequences according to the following schema.

$$\begin{array}{ccccccccc}
0 & \to & E_2 & \xrightarrow{\iota_2} & M_1 & \xrightarrow{u_1} & M_0 & \to & 0 \\
0 & \to & E_3 & \xrightarrow{\iota_3} & M_2 & \xrightarrow{v_2} & E_2 & \to & 0 \\
 & \vdots & & & & & & \vdots & \\
0 & \to & E_{m-1} & \xrightarrow{\iota_{m-1}} & M_{m-2} & \xrightarrow{v_{m-2}} & E_{m-2} & \to & 0 \\
0 & \to & M_m & \xrightarrow{u_m} & M_{m-1} & \xrightarrow{v_{m-1}} & E_{m-1} & \to & 0
\end{array}$$

with $E_i = \operatorname{Im} u_{i+1} \subseteq M_i$ for $i \in [\![2..m-1]\!]$, the ι_k's canonical injections, and the v_k's obtained from the u_k's by restricting the range to $\operatorname{Im} u_k$.

An important theme of commutative algebra is provided by the transformations that preserve, or do not preserve, exact sequences.

Here are two basic examples, which use the modules of linear maps.

Let $\mathrm{L}_{\mathbf{A}}(M, P)$ be the $\mathbf{A}$-module of $\mathbf{A}$-linear maps from M to P and $\mathrm{End}_{\mathbf{A}}(M)$ designate $\mathrm{L}_{\mathbf{A}}(M, M)$ (with its ring structure generally noncommutative). The *dual module* of M, $\mathrm{L}_{\mathbf{A}}(M, \mathbf{A})$, will in general be denoted by $M^\star$.

6.1. Fact. *If* $0 \to M \xrightarrow{\alpha} N \xrightarrow{\beta} P$ *is an exact sequence of* $\mathbf{A}$*-modules, and if* F *is an* $\mathbf{A}$*-module, then the sequence*

$$0 \to \mathrm{L}_{\mathbf{A}}(F, M) \longrightarrow \mathrm{L}_{\mathbf{A}}(F, N) \longrightarrow \mathrm{L}_{\mathbf{A}}(F, P)$$

is exact.

D *Exactness in* $\mathrm{L}_{\mathbf{A}}(F, M)$*.* Let $\varphi \in \mathrm{L}_{\mathbf{A}}(F, M)$ such that $\alpha \circ \varphi = 0$. Then, since the first sequence is exact in M, for all $x \in F$, $\varphi(x) = 0$, so $\varphi = 0$.

Exactness in $\mathrm{L}_{\mathbf{A}}(F, N)$*.* Let $\varphi \in \mathrm{L}_{\mathbf{A}}(F, N)$ such that $\beta \circ \varphi = 0$. Then, since the first sequence is exact in N, for all $x \in F$, $\varphi(x) \in \operatorname{Im} \alpha$.
Let $\alpha_1 : \operatorname{Im} \alpha \to M$ be the inverse of the bijection α (regarding the codomain of α as $\operatorname{Im} \alpha$) and $\psi = \alpha_1 \varphi$.
We then obtain the equalities $\mathrm{L}_{\mathbf{A}}(F, \alpha)(\psi) = \alpha\, \alpha_1\, \varphi = \varphi$. □

6.2. Fact. *If* $N \xrightarrow{\beta} P \xrightarrow{\gamma} Q \to 0$ *is an exact sequence of* $\mathbf{A}$*-modules and if* F *is an* $\mathbf{A}$*-module, then the sequence*

$$0 \to \mathrm{L}_{\mathbf{A}}(Q, F) \longrightarrow \mathrm{L}_{\mathbf{A}}(P, F) \longrightarrow \mathrm{L}_{\mathbf{A}}(N, F)$$

is exact.

D *Exactness in* $\mathrm{L}_{\mathbf{A}}(Q, F)$*.* If $\varphi \in \mathrm{L}_{\mathbf{A}}(Q, F)$ satisfies $\varphi \circ \gamma = 0$, then, since γ is surjective, $\varphi = 0$.

Exactness in $\mathrm{L}_{\mathbf{A}}(P, F)$*.* If $\varphi : P \to F$ satisfies $\varphi \circ \beta = 0$, then $\operatorname{Im} \beta \subseteq \operatorname{Ker} \varphi$ and φ is factorized by $P/\operatorname{Im} \beta \simeq Q$, that is $\varphi = \psi \circ \gamma$ for a linear map $\psi : Q \to F$, i.e. $\varphi \in \operatorname{Im} \mathrm{L}_{\mathbf{A}}(\gamma, F)$. □

6.3. Fact. *Let $\beta : N \to P$ be a linear map and $\gamma : P \to \operatorname{Coker}\beta$ be the canonical projection.*

1. *The canonical map ${}^{\mathrm{t}}\gamma : (\operatorname{Coker}\beta)^{\star} \to P^{\star}$ induces an isomorphism of $(\operatorname{Coker}\beta)^{\star}$ on $\operatorname{Ker}{}^{\mathrm{t}}\beta$.*
2. *If the canonical linear maps $N \to N^{\star\star}$ and $P \to P^{\star\star}$ are isomorphisms, then the canonical surjection of $N^{\star}$ in $\operatorname{Coker}{}^{\mathrm{t}}\beta$ provides by duality an isomorphism of $(\operatorname{Coker}{}^{\mathrm{t}}\beta)^{\star}$ on $\operatorname{Ker}\beta$.*

D *1.* We apply Fact 6.2 with $F = \mathbf{A}$.

2. We apply item *1* to the linear map ${}^{\mathrm{t}}\beta$ by identifying N and $N^{\star\star}$, as well as P and $P^{\star\star}$, and thus also β and ${}^{\mathrm{t}}({}^{\mathrm{t}}\beta)$. □

Remark. It is possible to slightly weaken the assumption by requiring that the linear map $P \to P^{\star\star}$ be injective. ■

Localization and exact sequences

6.4. Fact. *Let S be a monoid of a ring $\mathbf{A}$.*

1. *If M is a submodule of N, we have the canonical identification of M_S with a submodule of N_S and of $(N/M)_S$ with N_S/M_S.*
   In particular, for every ideal $\mathfrak{a}$ of $\mathbf{A}$, the $\mathbf{A}$-module $\mathfrak{a}_S$ is canonically identified with the ideal $\mathfrak{a}\mathbf{A}_S$ of $\mathbf{A}_S$.
2. *If $\varphi : M \to N$ is an $\mathbf{A}$-linear map, then:*
   - *a.* $\operatorname{Im}(\varphi_S)$ *is canonically identified with* $\big(\operatorname{Im}(\varphi)\big)_S$,
   - *b.* $\operatorname{Ker}(\varphi_S)$ *is canonically identified with* $\big(\operatorname{Ker}(\varphi)\big)_S$,
   - *c.* $\operatorname{Coker}(\varphi_S)$ *is canonically identified with* $\big(\operatorname{Coker}(\varphi)\big)_S$.
3. *If we have an exact sequence of $\mathbf{A}$-modules*
   $$M \xrightarrow{\varphi} N \xrightarrow{\psi} P\,,$$
   then the sequence of $\mathbf{A}_S$-modules
   $$M_S \xrightarrow{\varphi_S} N_S \xrightarrow{\psi_S} P_S$$
   is also exact.

6.5. Fact. *If $M_1, \ldots, M_r$ are submodules of N and $M = \bigcap_{i=1}^{r} M_i$, then by identifying the modules $(M_i)_S$ and M_S with submodules of N_S we obtain $M_S = \bigcap_{i=1}^{r} (M_i)_S$.*

6.6. Fact. *Let M and N be two submodules of an $\mathbf{A}$-module P,* with N finitely generated. *Then, the conductor ideal $(M_S : N_S)$ is identified with $(M : N)_S$, via the natural maps of $(M : N)$ in $(M_S : N_S)$ and $(M : N)_S$.*

This is particularly applied to the annihilator of a finitely generated ideal.

Local-global principle for exact sequences of modules

6.7. Concrete local-global principle. (For exact sequences)
Let S_1, …, S_n be comaximal monoids of $\mathbf{A}$, M, N, P be $\mathbf{A}$-modules and $\varphi : M \to N$, $\psi : N \to P$ be two linear maps. We write $\mathbf{A}_i$ for $\mathbf{A}_{S_i}$, M_i for M_{S_i} etc. The following properties are equivalent.

1. *The sequence $M \xrightarrow{\varphi} N \xrightarrow{\psi} P$ is exact.*
2. *For each $i \in [\![1..n]\!]$, the sequence $M_i \xrightarrow{\varphi_i} N_i \xrightarrow{\psi_i} P_i$ is exact.*

As a consequence, φ is injective (resp. surjective) if and only if for each $i \in [\![1..n]\!]$, φ_i is injective (resp. surjective)

D We have seen that *1* ⇒ *2* in Fact 6.4.
Assume *2*. Let $\mu_i : M \to M_i$, $\nu_i : N \to N_i$, $\pi_i : P \to P_i$ be the canonical homomorphisms. Let $x \in M$ and $z = \psi\big(\varphi(x)\big)$. We thus have

$$0 = \psi_i\big(\varphi_i(\mu_i(x))\big) = \pi_i\big(\psi(\varphi(x))\big) = \pi_i(z),$$

for some $s_i \in S_i$, $s_i z = 0$ in P. We conclude that $z = 0$ by using the comaximality of the S_i's: $\sum_i u_i s_i = 1$. Now let $y \in N$ such that $\psi(y) = 0$. For each i there exists some $x_i \in M_i$ such that $\varphi_i(x_i) = \nu_i(y)$.
We write $x_i =_{M_i} a_i/s_i$ with $a_i \in M$ and $s_i \in S_i$. The equality $\varphi_i(x_i) = \nu_i(y)$ means that for some $t_i \in S_i$ we have $t_i\varphi(a_i) = t_i s_i y$ in N. If $\sum_i v_i t_i s_i = 1$, we can deduce that $\varphi\big(\sum_i v_i t_i a_i\big) = y$. Thus $\operatorname{Ker}\psi$ is indeed included in $\operatorname{Im}\varphi$. □

6.8. Abstract local-global principle*. (For exact sequences)
Let M, N, P be $\mathbf{A}$-modules, and $\varphi : M \to N$ and $\psi : N \to P$ be two linear maps. The following properties are equivalent.

1. *The sequence $M \xrightarrow{\varphi} N \xrightarrow{\psi} P$ is exact.*
2. *For every maximal ideal $\mathfrak{m}$ the sequence $M_\mathfrak{m} \xrightarrow{\varphi_\mathfrak{m}} N_\mathfrak{m} \xrightarrow{\psi_\mathfrak{m}} P_\mathfrak{m}$ is exact.*

As a consequence, φ is injective (resp. surjective) if and only if for every maximal ideal $\mathfrak{m}$, $\varphi_\mathfrak{m}$ is injective (resp. surjective).

D The property $x = 0$ for an element x of a module is a finite character property. Similarly for the property $y \in \operatorname{Im}\varphi$. Thus, even if the property "the sequence is exact" is not of finite character, it is a conjunction of finite character properties, and we can apply Fact* 2.11 to deduce the abstract local-global principle from the concrete local-global principle. □

Let us finally mention a concrete local-global principle for monoids.

6.9. Concrete local-global principle. (For monoids)
Let S_1, …, S_n be comaximal monoids of $\mathbf{A}$, V be a monoid. The following properties are equivalent.

1. *The monoid V contains* 0.
2. *For $i \in [\![1..n]\!]$, the monoid V seen in $\mathbf{A}_{S_i}$ contains* 0.

D For each i we have some $v_i \in V$ and some $s_i \in S_i$ such that $s_i v_i = 0$. Let $v = \prod_i v_i \in V$. Then, v is zero in the $\mathbf{A}_{S_i}$'s, thus in $\mathbf{A}$. □

Exercises and problems

Exercise 1. We recommend the reader to do the proofs which are not given, are sketched, are left to the reader, etc… In particular, consider the following cases.

- Check Facts 1.2 to 1.4.
- Prove Corollary 2.4.
- In Lemma 2.6 compute suitable exponents for the items *2*, *3* and *4*, by making the proof completely explicit.
- Prove Corollary 3.3. Give a more detailed proof of Theorem 3.4. Check the details in the proof of the local-global principle 3.5. Prove Proposition 3.7.
- Check Facts 6.4 to 6.6. For Fact 6.5 we use the exact sequence $0 \to M \to N \to \bigoplus_{i=1}^{r} N/M_i$ which is preserved by localization.

Exercise 2. (Also see exercise VII-8)

1. *(Invertible elements in $\mathbf{B}[T]$, cf. Lemma 2.6)*
   Let two polynomials $f = \sum_{i=0}^{n} a_i T^i$, $g = \sum_{j=0}^{m} b_j T^j$ with $fg = 1$. Show that the coefficients a_i, $i \geqslant 1$, b_j, $j \geqslant 1$ are nilpotent elements and that $a_n^{m+1} = 0$.
2. *(Characteristic polynomial of a nilpotent matrix)*
   Let $A \in \mathbb{M}_n(\mathbf{B})$ be a nilpotent matrix and $\mathrm{C}_A(T) = T^n + \sum_{k=0}^{n-1} a_k T^k$ be its characteristic polynomial.
   a. Show that the coefficients a_i are nilpotent elements.
   b. Precisely, if $A^e = 0$, then $\mathrm{Tr}(A)^{(e-1)n+1} = 0$ and
   $$a_i^{e_i} = 0 \quad \text{where} \quad e_i = (e-1)\binom{n}{i} + 1 \quad (i = 0, \dots, n-1).$$

Exercise 3. Let $x = (x_1, \dots, x_n) \in \mathbf{A}^n$ be a vector and $s \in \mathbf{A}$.

1. If x is unimodular in $\mathbf{A}/\langle s \rangle$ and in $\mathbf{A}[1/s]$, it is unimodular in $\mathbf{A}$.
2. Let $\mathfrak{b}$ and $\mathfrak{c}$ be two ideals of $\mathbf{A}$. If x is unimodular modulo $\mathfrak{b}$ and modulo $\mathfrak{c}$, then it is also unimodular modulo $\mathfrak{b}\mathfrak{c}$.

Exercise 4. *(A typical application of the basic local-global principle)*
Let $x = (x_1, \ldots, x_n) \in \mathbf{A}^n$ be *unimodular.* For $d \geqslant 1$, we denote by $\mathbf{A}[X_1, \ldots, X_n]_d$ the $\mathbf{A}$-submodule of the homogeneous polynomials of degree d and

$$I_{d,x} = \left\{ f \in \mathbf{A}[\underline{X}]_d \mid f(x) = 0 \right\}, \ \mathbf{A}\text{-submodule of } \mathbf{A}[\underline{X}].$$

1. If $x_1 \in \mathbf{A}^\times$, every $f \in I_{d,x}$ is a linear combination of the $x_1X_j - x_jX_1$ with homogeneous polynomials of degree $d-1$ for coefficients.
2. Generally, every $f \in I_{d,x}$ is a linear combination of the $(x_kX_j - x_jX_k)$ with homogeneous polynomials of degree $d-1$ for coefficients.
3. Let $I_x = \bigoplus_{d \geqslant 1} I_{d,x}$. Show that $I_x = \{ F \mid F(tx) = 0 \}$ (where t is a new indeterminate). Show that I_x is *saturated*, i.e., if $X_j^m F \in I_x$ for some m and for each j, then $F \in I_x$.

Exercise 5. *(Variations of the Gauss-Joyal Lemma 2.6)*
Show that the following statements are equivalent (each statement is universal, i.e., valid for all polynomials and every commutative ring $\mathbf{A}$):

1. $\mathrm{c}(f) = \mathrm{c}(g) = \langle 1 \rangle \ \Rightarrow \ \mathrm{c}(fg) = \langle 1 \rangle$,
2. $(\exists i_0, j_0 \ \ f_{i_0} = g_{j_0} = 1) \ \Rightarrow \ \mathrm{c}(fg) = \langle 1 \rangle$,
3. $\exists p \in \mathbb{N}, \ \left(\mathrm{c}(f)\mathrm{c}(g)\right)^p \subseteq \mathrm{c}(fg)$,
4. *(Gauss-Joyal)* $\mathrm{D}_{\mathbf{A}}\left(\mathrm{c}(f)\mathrm{c}(g)\right) = \mathrm{D}_{\mathbf{A}}\left(\mathrm{c}(fg)\right)$.

Exercise 6. *(Norm of a primitive polynomial through the use of a null ring)*
Let $\mathbf{B}$ be a free $\mathbf{A}$-algebra of finite rank, $\underline{X} = (X_1, \ldots, X_n)$ be indeterminates, $Q \in \mathbf{B}[\underline{X}]$ and $P = \mathrm{N}_{\mathbf{B}[\underline{X}]/\mathbf{A}[\underline{X}]}(Q) \in \mathbf{A}[\underline{X}]$. Show that if Q is primitive, then so is P. *Hint:* check that $\mathbf{A} \cap \mathrm{c}_{\mathbf{B}}(P) = \mathrm{c}_{\mathbf{A}}(P)$, consider the subring $\mathbf{A}' = \mathbf{A}/\mathrm{c}_{\mathbf{A}}(P)$ of $\mathbf{B}' = \mathbf{B}/\mathrm{c}_{\mathbf{B}}(P)$ and the $\mathbf{A}'$-linear map "multiplication by Q," $m_Q : \mathbf{B}'[\underline{X}] \to \mathbf{B}'[\underline{X}]$, $R \mapsto QR$.

Exercise 7. Show that a coherent ring $\mathbf{A}$ is strongly discrete if and only if the test "$1 \in \langle a_1, \ldots, a_n \rangle$?" is explicit for every finite sequence $(a_1, \ldots, a_n)$ in $\mathbf{A}$.

Exercise 8. *(An example of a coherent Noetherian ring with a* non-*coherent quotient.)*
Consider the ring $\mathbb{Z}$ and an ideal $\mathfrak{a}$ generated by an infinite sequence of elements, all zeros besides eventually one, which is then equal to 3 (for example we place a 3 the first time, if it ever occurs, that a zero of the Riemann zeta function[9] has real part not equal to 1/2). If we are able to provide a finite system of generators for the annihilator of 3 in $\mathbb{Z}/\mathfrak{a}$, we are able to say whether the infinite sequence is identically zero or not. This would mean that there exists a sure method to solve conjectures of the Riemann type.

Comment. As every reasonable constructive definition of Noetherianity seems to demand that a Noetherian ring's quotient remains Noetherian, and given the above "counterexample," we cannot hope to have a constructive proof of the theorem of classical mathematics which states that every Noetherian ring is coherent. ■

[9] Here we enumerate the zeros $a_n + ib_n$ with $b_n > 0$ by order of magnitude.

Exercise 9. *(Idempotents of* $\mathbf{A}[X]$*)*
Prove that every idempotent of $\mathbf{A}[X]$ is an idempotent of $\mathbf{A}$.

Exercise 10. Let u and v be two idempotents and x be an element of $\mathbf{A}$.
The element $1-(1-u)(1-v)=u+v-uv$ is denoted by $u \vee v$.

1. Show that $x \in u\mathbf{A} \Leftrightarrow ux = x$. In particular, $u\mathbf{A} = v\mathbf{A} \Leftrightarrow u = v$.
2. The element uv is <u>the</u> least common multiple of u and v amongst the idempotents of $\mathbf{A}$ (i.e., if w is an idempotent, $w \in u\mathbf{A} \cap v\mathbf{A} \Leftrightarrow w \in uv\mathbf{A}$). Actually, we even have $u\mathbf{A} \cap v\mathbf{A} = uv\mathbf{A}$. We write $u \wedge v = uv$.
3. Prove the equality $u\mathbf{A} + v\mathbf{A} = (u \vee v)\mathbf{A}$. Infer that $u \vee v$ is <u>the</u> greatest common divisor of u and v amongst the idempotents of $\mathbf{A}$ (in fact an arbitrary element of $\mathbf{A}$ divides u and v if and only if it divides $u \vee v$).
4. By a sequence of elementary operations, transform the matrix $\mathrm{Diag}(u, v)$ into the matrix $\mathrm{Diag}(u \vee v, u \wedge v)$.
   From it, deduce that the two $\mathbf{A}$-modules $u\mathbf{A} \oplus v\mathbf{A}$ and $(u \vee v)\mathbf{A} \oplus (u \wedge v)\mathbf{A}$ are isomorphic.
5. Show that the two rings $\mathbf{A}/\langle u\rangle \times \mathbf{A}/\langle v\rangle$ and $\mathbf{A}/\langle u \vee v\rangle \times \mathbf{A}/\langle u \wedge v\rangle$ are isomorphic.

Exercise 11. Let $\mathbf{A}$ be a ring and $(e_1, \dots, e_n)$ be a fundamental system of orthogonal idempotents of $\mathrm{Frac}\,\mathbf{A} = \mathbf{K}$. We write $e_i = a_i/d$ with $a_i \in \mathbf{A}$ and $d \in \mathrm{Reg}\,\mathbf{A}$. We then have $a_ia_j = 0$ for $i \neq j$ and $\sum_i a_i$ regular.
1. Establish a converse.
2. Show that $\mathbf{K}[1/e_i] \simeq \mathrm{Frac}\big(\mathbf{A}/\mathrm{Ann}_{\mathbf{A}}(a_i)\big)$ and $\mathbf{K} \simeq \prod_i \mathrm{Frac}\big(\mathbf{A}/\mathrm{Ann}_{\mathbf{A}}(a_i)\big)$.

Exercise 12. *(Separating the irreducible components)*
1. Let $\mathbf{A} = \mathbb{Q}[x, y, z] = \mathbb{Q}[X, Y, Z]/\langle XY, XZ, YZ\rangle$ and $\mathbf{K} = \mathrm{Frac}\,\mathbf{A}$. What are the zeros of $\mathbf{A}$ in $\mathbb{Q}^3$ (i.e. $(x, y, z) \in \mathbb{Q}^3$ such that $xy = yz = zx = 0$)? Give a reduced form of the elements of $\mathbf{A}$. Show that $x + y + z \in \mathrm{Reg}\,\mathbf{A}$. Show that the elements $\dfrac{x}{x+y+z}$, $\dfrac{y}{x+y+z}$ and $\dfrac{z}{x+y+z}$ form a fundamental system of orthogonal idempotents in $\mathbf{K}$. Show that $\mathbf{K} \simeq \mathbb{Q}(X) \times \mathbb{Q}(Y) \times \mathbb{Q}(Z)$.

2. Let $\mathbf{B} = \mathbb{Q}[u, v, w] = \mathbb{Q}[U, V, W]/\langle UVW\rangle$ and $\mathbf{L} = \mathrm{Frac}\,\mathbf{B}$.
What are the zeros of $\mathbf{B}$ in $\mathbb{Q}^3$? Give a reduced form of the elements of $\mathbf{B}$. Show that $\mathbf{L} \simeq \mathbb{Q}(U, V) \times \mathbb{Q}(V, W) \times \mathbb{Q}(W, U)$.

Exercise 13. *(Idempotent and elementary group)*
Let $a \in \mathbf{A}$ be an idempotent. For $b \in \mathbf{A}$, give a matrix $A \in \mathbb{E}_2(\mathbf{A})$ and an element $d \in \mathbf{A}$ such that $A\begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} d \\ 0 \end{bmatrix}$. In particular, explain why $\langle a, b\rangle = \langle d\rangle$.
Moreover, prove that if b is regular (resp. invertible) modulo a, then d is regular (resp. invertible). Finally, if b is idempotent, $d = a \vee b = a + b - ab$.

Exercise 14. Let $(r_1, \ldots, r_m)$ be a finite family of idempotents in a ring $\mathbf{A}$. Let $s_i = 1 - r_i$ and, for a subset I of $[\![1..m]\!]$, let $r_I = \prod_{i \in I} r_i \prod_{i \notin I} s_i$.

1. Show that the diagonal matrix $D = \mathrm{Diag}(r_1, \ldots, r_m)$ is similar to a matrix $D' = \mathrm{Diag}(e_1, \ldots, e_m)$ where the e_i's are idempotents which satisfy: e_i divides e_j if $j > i$. You can start with the $n = 2$ case and use Exercise 10. Show that $\langle e_k \rangle = \mathcal{D}_k(D)$ for all k.

2. Show that we can write $D' = PDP^{-1}$ with P a *generalized permutation matrix*, i.e. a matrix which can be written as $\sum_j f_j P_j$ where the f_j's form a fundamental system of orthogonal idempotents and each P_j is a permutation matrix. generalized permutation — Suggestions:

- The r_I's form a fundamental system of orthogonal idempotents. The diagonal matrix $r_I D$ has the element r_I as its coefficient in position (i, i) if $i \in I$ and 0 otherwise. The matrix P_I then corresponds to a permutation bringing the coefficients r_I to the head of the list. Finally, $P = \sum_I r_I P_I$. Note that the test "$r_I = 0$?" is not necessary!
- We can also treat the $m = 2$ case: find $P = e \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + f \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ with $f = r_2 s_1$, $e = 1 - f$, and $D' = \mathrm{Diag}(r_1 \vee r_2, r_1 \wedge r_2)$.
  Next we treat the $m > 2$ case step by step.

Exercise 15. Recall the proof of the Chinese Remainder Theorem (page 38) and explicitly give the idempotents.

Exercise 16. *(Elementary Group: first steps)* $\mathbb{M}_2(\mathbf{A})$ case.

1. Let $a \in \mathbf{A}$. Determine a matrix $P \in \mathbb{E}_2(\mathbf{A})$ such that $P \begin{bmatrix} a \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ a \end{bmatrix}$. Same for $\begin{bmatrix} \varepsilon a \\ 0 \end{bmatrix} \mapsto \begin{bmatrix} a \\ 0 \end{bmatrix}$ where $\varepsilon \in \mathbf{A}^\times$.

2. Write the matrices $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ and $\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$ as elements of $\mathbb{E}_2(\mathbf{A})$.

3. Show that every triangular matrix of $\mathbb{SL}_2(\mathbf{A})$ is in $\mathbb{E}_2(\mathbf{A})$.

4. Let $u = \begin{bmatrix} x \\ y \end{bmatrix}$, $v = \begin{bmatrix} y \\ x \end{bmatrix}$, $w = \begin{bmatrix} -y \\ x \end{bmatrix}$ with $x, y \in \mathbf{A}$. Show that $v \in \mathbb{GL}_2(\mathbf{A}) \cdot u$ and $w \in \mathbb{E}_2(\mathbf{A}) \cdot u$, but not necessarily $v \in \mathbb{SL}_2(\mathbf{A}) \cdot u$. For example, if x, y are two indeterminates over a ring $\mathbf{k}$, $\mathbf{A} = \mathbf{k}[x, y]$ and $v = Au$, with $A \in \mathbb{GL}_2(\mathbf{A})$, then $\big(\det(A)\big)(0, 0) = -1$. Consequently, we have $\det(A) \in -1 + \mathrm{D}_{\mathbf{k}}(0) \langle x, y \rangle$ (Lemma 2.6), therefore $\det(A) = -1$ if $\mathbf{k}$ is reduced. In addition, if $\det(A) = 1$, then $2 = 0$ in $\mathbf{k}$. As a result, $v \in \mathbb{SL}_2(\mathbf{A}) \cdot u$ if and only if $2 = 0$ in $\mathbf{k}$.

Exercise 17. *(Elementary group: next steps)*
1. Let $A \in \mathbb{M}_{n,m}(\mathbf{A})$ with an invertible coefficient and $(n, m) \neq (1, 1)$. Determine matrices $P \in \mathbb{E}_n(\mathbf{A})$ and $Q \in \mathbb{E}_m(\mathbf{A})$ such that $PAQ = \begin{bmatrix} 1 & 0_{1,m-1} \\ 0_{n-1,1} & A' \end{bmatrix}$.
Example: with $a \in \mathbf{A}^\times$ give P for $P \begin{bmatrix} a \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ (Exercise 16 item *1*).

2. Let $A \in \mathbb{M}_2(\mathbf{A})$ with an invertible coefficient. Compute matrices P and $Q \in \mathbb{E}_2(\mathbf{A})$ such that: $PAQ = \begin{bmatrix} 1 & 0 \\ 0 & \delta \end{bmatrix}$ with $\delta = \det(A)$.

Every matrix $A \in \mathbb{SL}_2(\mathbf{A})$ with an invertible coefficient belongs to $EE_2(\mathbf{A})$. Make the following cases explicit:

$$\begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix}, \quad \begin{bmatrix} 0 & a \\ -a^{-1} & 0 \end{bmatrix}, \qquad \text{with } a \in \mathbf{A}^{\times}.$$

Write the following matrices (with $a \in \mathbf{A}^{\times}$) in $\mathbb{E}_2(\mathbf{A})$:

$$\begin{bmatrix} a & b \\ 0 & a^{-1} \end{bmatrix}, \quad \begin{bmatrix} a & 0 \\ b & a^{-1} \end{bmatrix}, \quad \begin{bmatrix} 0 & a \\ -a^{-1} & b \end{bmatrix}, \quad \begin{bmatrix} b & a \\ -a^{-1} & 0 \end{bmatrix}.$$

3. Prove that if $A = \mathrm{Diag}(a_1, a_2, \ldots, a_n) \in \mathbb{SL}_n(\mathbf{A})$, then $A \in \mathbb{E}_n(\mathbf{A})$.

4. Show that every triangular matrix $A \in \mathbb{SL}_n(\mathbf{A})$ belongs to $\mathbb{E}_n(\mathbf{A})$.

Exercise 18. *(Division matrices D_q of determinant 1)*
A "general division" $a = bq - r$ can be expressed with matrices:

$$\begin{bmatrix} 0 & 1 \\ -1 & q \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} b \\ r \end{bmatrix}.$$

This leads to the introduction of the matrix $D_q = \begin{bmatrix} 0 & 1 \\ -1 & q \end{bmatrix} \in \mathbb{SL}_2(\mathbf{A})$.

Show that $\mathbb{E}_2(\mathbf{A})$ is the monoid generated by the D_q matrices.

Exercise 19. Let $\mathbf{A}$ be a ring and A, $B \in \mathbb{M}_n(\mathbf{A})$. Assume that we have some $i \in \mathbf{A}$ with $i^2 = -1$ and that $2 \in \mathbf{A}^{\times}$. Show that the matrices of $\mathbb{M}_{2n}(\mathbf{A})$

$$M = \begin{bmatrix} A & -B \\ B & A \end{bmatrix} \text{ and } M' = \begin{bmatrix} A + iB & 0 \\ 0 & A - iB \end{bmatrix}$$

are *elementarily similar*, (i.e., $\exists P \in \mathbb{E}_{2n}(\mathbf{A}),\ PMP^{-1} = M'$).
Hint: first treat the $n = 1$ case.

Exercise 20. For $d \in \mathbf{A}^{\times}$ and $\lambda \in \mathbf{A}$ compute the matrix

$$\mathrm{Diag}(1, \ldots, d, \ldots, 1) \cdot \mathrm{E}_{ij}(\lambda) \cdot \mathrm{Diag}(1, \ldots, d^{-1}, \ldots, 1).$$

Show that the subgroup of diagonal matrices of $\mathbb{GL}_n(\mathbf{A})$ normalizes $\mathbb{E}_n(\mathbf{A})$.

Exercise 21. *(A freeness lemma, or a Splitting Off: reader's choice)*
Let $F \in \mathbb{AG}_n(\mathbf{A})$ be a projector with an invertible principal minor of order k. Show that F is similar to a matrix $\begin{bmatrix} \mathrm{I}_k & 0 \\ 0 & F' \end{bmatrix}$ where $F' \in \mathbb{AG}_{n-k}(\mathbf{A})$.

The finitely generated projective module $P \overset{\mathrm{def}}{=} \operatorname{Im} F \subseteq \mathbf{A}^n$ admits a free direct summand with k columns of F for its basis.

Exercise 22. Let $A \in \mathbf{A}^{n \times m}$ be of rank 1. Construct $B \in \mathbf{A}^{m \times n}$ such that $ABA = A$ and verify that AB is a projector of rank 1. Compare your solution with that which would result from the proof of Theorem 5.14.

Exercise 23. *This exercise constitutes an abstraction of the computations that led to Theorem 5.14.* Consider an $\mathbf{A}$-module E “with enough linear forms”, i.e. if $x \in E$ satisfies $\mu(x) = 0$ for all $\mu \in E^\star$, then $x = 0$. This means that the canonical map from E to its bidual, $E \to E^{\star\star}$, is injective. This condition is satisfied if E is a *reflexive* module, i.e. $E \simeq E^{\star\star}$, e.g. a finitely generated projective module, or a free module of finite rank.

For $x_1, \ldots, x_n \in E$, denote by $\bigwedge_r(x_1, \ldots, x_n)$ the ideal of $\mathbf{A}$ generated by the evaluations of every r-multilinear alternating form of E at every r-tuplet of elements of $\{x_1, \ldots, x_n\}$.

Assume that $1 \in \bigwedge_r(x_1, \ldots, x_n)$ *and* $\bigwedge_{r+1}(x_1, \ldots, x_n) = 0$.

We want to prove that the submodule $\sum \mathbf{A}x_i$ is a direct summand in E by explicitly giving a projector $\pi : E \to E$ whose image is this submodule.

1. *(Cramer’s formulas)* Let f be an r-multilinear alternating form over E. Show, for $y_0, \ldots, y_r \in \sum \mathbf{A}x_i$, that
$$\sum\nolimits_{i=0}^{r} (-1)^i f(y_0, \ldots, y_{i-1}, \widehat{y_i}, y_{i+1}, \ldots, y_r)\, y_i = 0.$$
Or, for $y, y_1, \ldots, y_r \in \sum \mathbf{A}x_i$, that
$$f(y_1, \ldots, y_r)\, y = \sum\nolimits_{i=1}^{r} f(y_1, \ldots, y_{i-1}, y, y_{i+1}, \ldots, y_r)\, y_i.$$
2. Give n linear forms $\alpha_i \in E^\star$ such that the linear map
$$\pi : E \to E, \;\; x \mapsto \sum\nolimits_i \alpha_i(x) x_i$$
is a projector onto $\sum \mathbf{A}x_i$. We define $\psi : \mathbf{A}^n \to E$ by $e_i \mapsto x_i$ and $\varphi : E \to \mathbf{A}^n$ by $\varphi(x) = \big(\alpha_1(x), \ldots, \alpha_n(x)\big)$. Arrange for $\pi = \psi \circ \varphi$ and $\pi \circ \psi = \psi$, so that $\psi \circ \varphi \circ \psi = \psi$.
3. *(New proof of Theorem 5.14)* Let $A \in \mathbf{A}^{m \times n}$ be a matrix of rank r. Show that there exists a $B \in \mathbf{A}^{n \times m}$ such that $A\,B\,A = A$.

Exercise 24. Let $A \in \mathbf{A}^{n \times m}$ and $B \in \mathbf{A}^{m \times n}$.

1. We have the following commutativity formula:
$$\det(\mathrm{I}_m + XBA) = \det(\mathrm{I}_n + XAB).$$

First proof. First treat the case where $m = n$, for example by the method of undetermined coefficients. If $m \neq n$, A and B can be completed with rows and columns of 0’s to turn them into square matrices A_1 and B_1 of size $q = \max(m, n)$ as in the proof given page 40. Then check that $\det(\mathrm{I}_m + XBA) = \det(\mathrm{I}_q + XB_1A_1)$ and $\det(\mathrm{I}_n + XAB) = \det(\mathrm{I}_q + XA_1B_1)$.

Second proof. Consider an undetermined X and the matrices
$$B' = \begin{bmatrix} XB & \mathrm{I}_m \\ \mathrm{I}_n & 0_{n,m} \end{bmatrix} \quad \text{and} \quad A' = \begin{bmatrix} A & \mathrm{I}_n \\ \mathrm{I}_m & -XB \end{bmatrix}.$$
Compute $A'B'$ and $B'A'$.

2. What can be deduced about the characteristic polynomials of $A\,B$ and $B\,A$?

Exercise 25. *(Binet-Cauchy formula)*
We use the notations on page 47. For two matrices $A \in \mathbf{A}^{n\times m}$ and $B \in \mathbf{A}^{m\times n}$, prove that we have the Binet-Cauchy formula:

$$\det(BA) = \sum\nolimits_{\alpha\in\mathcal{P}_{m,n}} \det(B_{1..m,\alpha}) \det(A_{\alpha,1..m}).$$

First proof. Use the formula $\det(\mathrm{I}_m + XBA) = \det(\mathrm{I}_n + XAB)$ (Exercise 24). Then consider the coefficient of X^m in each of the polynomials $\det(\mathrm{I}_m + XBA)$ and $\det(\mathrm{I}_n + XAB)$.

Second proof. The matrices A and B represent linear maps $u : \mathbf{A}^m \to \mathbf{A}^n$ and $v : \mathbf{A}^n \to \mathbf{A}^m$.
Then consider the matrices of $\bigwedge^m u$, $\bigwedge^m v$ and $\bigwedge^m(v\circ u)$ with respect to the bases naturally associated with the canonical bases of $\mathbf{A}^n$ and $\mathbf{A}^m$.
Conclude by writing $\bigwedge^m(v\circ u) = \bigwedge^m v \circ \bigwedge^m u$.

Third proof. In the product BA insert between B and A a diagonal matrix D having indeterminates λ_i for coefficients, and see which is the coefficient of $\lambda_{i_1}\cdots\lambda_{i_m}$ in the polynomial $\det(BDA)$ (to do this take $\lambda_{i_1} = \cdots = \lambda_{i_m} = 1$ and let the other be null). Conclude by letting all the λ_i's be equal to 1.

Exercise 26. Let $u \in \mathrm{End}_{\mathbf{A}}(\mathbf{A}^n)$. For $k \in [\![0..n]\!]$, let $u_k = \bigwedge^k(u)$.
Show that $\det(u_k) = \det(u)^{\binom{n-1}{k-1}}$ and that

$$\det(u_k)\det(u_{n-k}) = \det(u)^{\binom{n}{k}} .$$

Exercise 27. For $A \in \mathbf{A}^{n\times r}$ prove that the following properties are equivalent.

1. The matrix A is injective and locally simple.
2. There exists a matrix $B \in \mathbf{A}^{r\times n}$ such that $B\,A = \mathrm{I}_r$.
3. The determinantal ideal $\mathcal{D}_r(A) = \langle 1\rangle$.

Hint: See Theorems 5.14, 5.22 and 5.26.

Exercise 28. Treat the general case in the proof of Lemma 5.30.

Exercise 29. If $\mathrm{gram}_{\mathbf{A}}(\varphi, x_1, \dots, x_n)$ is invertible, the submodule $\mathbf{A}x_1+\cdots+\mathbf{A}x_n$ is free with $(x_1, \dots, x_n)$ as its basis.

Problem 1. *(Gauss' pivot, $A\,B\,A = A$, and linear rationality)*
Let $\mathbf{K}$ be a discrete field. If $x \in \mathbf{K}^n$ is a nonzero vector, its *pivot index* i is the least index i such that $x_i \neq 0$. We say that the coefficient x_i is the *pivot* of x. The *height* $h(x)$ of x is the integer $n - i + 1$ and it is agreed that $h(0) = 0$. For example, for $n = 4$ and $x = \begin{bmatrix} 0 \\ 1 \\ * \\ * \end{bmatrix}$, the pivot index of x is $i = 2$, and $h(x) = 3$.
The following notions of "staggering" are relative to this height h.
We say that a matrix $A \in \mathbb{M}_{n,m}(\mathbf{K})$ *has staggered columns* if the nonzero columns of A have distinct heights; we say that it is *strictly staggered* if, additionally, the

rows at the pivot indices are vectors of the canonical basis of $\mathbf{K}^m$ (these vectors are necessarily distinct). Here is a strictly staggered matrix (0 has been replaced by a dot):

$$\begin{bmatrix} \cdot & \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & a_{24} & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & a_{43} & a_{44} & \cdot & \cdot \\ 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot & \cdot & \cdot \\ a_{71} & a_{72} & a_{73} & a_{74} & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 & \cdot \\ a_{91} & a_{92} & a_{93} & a_{94} & a_{95} & \cdot \end{bmatrix}.$$

1. Let $A \in \mathbb{M}_{n,m}(\mathbf{K})$ be strictly staggered; we define $\overline{A} \in \mathbb{M}_{n,m}(\mathbf{K})$ by annihilating the nonpivot coefficients (the a_{ij}'s in the above exercise) and $B = {}^{\mathrm{t}}\overline{A} \in \mathbb{M}_{m,n}(\mathbf{K})$. Check that $ABA = A$.

Describe the projectors AB, BA and the decomposition $\mathbf{K}^n = \operatorname{Im} AB \oplus \operatorname{Ker} AB$.

2. Let $A \in \mathbb{M}_{n,m}(\mathbf{K})$ be an arbitrary matrix. How do you obtain $Q \in \mathbb{GL}_m(\mathbf{K})$ such that $A' = AQ$ is strictly staggered? How do you compute $B \in \mathbb{M}_{m,n}(\mathbf{K})$ satisfying $ABA = A$?

3. Let $A \in \mathbb{M}_{n,m}(\mathbf{K})$ and $y \in \mathbf{K}^n$. Assume that the system of linear equations $Ax = y$ admits a solution x on an overring of $\mathbf{K}$. Show that it admits a solution on $\mathbf{K}$.

4. Let $\mathbf{K}_0 \subseteq \mathbf{K}$ be a subfield and E, F be two complementary $\mathbf{K}$-linear subspaces of $\mathbf{K}^n$. Assume that E and F are generated by vectors with components in $\mathbf{K}_0$. Show that $\mathbf{K}_0^n = (E \cap \mathbf{K}_0^n) \oplus (F \cap \mathbf{K}_0^n)$.

Let $E \subseteq \mathbf{K}^n$ be a $\mathbf{K}$-linear subspace. We say that E *is* $\mathbf{K}_0$*-rational* if it is generated by vectors with components in $\mathbf{K}_0$.

5. Let F be a complementary subspace of E in $\mathbf{K}^n$ generated by vectors of the canonical basis of $\mathbf{K}^n$: $\mathbf{K}^n = E \oplus F$ and $\pi : \mathbf{K}^n \twoheadrightarrow E$ be the associated projection.

a. Show that E is $\mathbf{K}_0$-rational if and only if $\pi(e_j) \in \mathbf{K}_0^n$ for every vector e_j of the canonical basis.

b. Deduce the existence of a smaller field of rationality for E.

c. What is the field of rationality of the image in $\mathbf{K}^n$ of a strictly staggered matrix?

Problem 2.

1. Partial factorization algorithm. Given two integers a and b prove that we can "efficiently" compute a finite family of pairwise coprime positive integers p_i such that $a = \pm \prod_{i=1}^{n} p_i^{\alpha_i}$ and $b = \pm \prod_{i=1}^{n} p_i^{\beta_i}$.

2. Consider a system of linear equations $AX = B$ in $\mathbb{Z}$ which admits an infinity of solutions in $\mathbb{Q}^m$. To know if it admits a solution in $\mathbb{Z}^m$ we can try a local-global method. Start by determining a solution in $\mathbb{Q}$, which is a vector $X \in \mathbb{Q}^m$. Find an integer d such that $dX \in \mathbb{Z}^m$, such that X has coefficients in $\mathbb{Z}[1/d]$. It then suffices to construct a solution in each localized ring $\mathbb{Z}_{1+p\mathbb{Z}}$ for the prime p's which

divide d and to apply the concrete local-global principle 2.3. To know if there is a solution in $\mathbb{Z}_{1+p\mathbb{Z}}$ and to construct one, we can use the pivot method, provided we take as pivot an element of the matrix (or rather the remaining part of the matrix) which divides every other coefficient, i.e. a coefficient wherein p appears with a minimum exponent.
The drawback of this method is that it requires factorizing d, which can render it unfeasible.
However, we can slightly modify the method in order to avoid having to completely factorize d. We will use the partial factorization algorithm. Start as if d were a prime number. More precisely work with the ring $\mathbb{Z}_{1+d\mathbb{Z}}$. Check whether a coefficient of the matrix is comaximal to d. If one is found, use it as your pivot. Otherwise no coefficient of the matrix is comaximal to d and (by using if necessary the partial factorization algorithm) we have one of the following three cases:

- d divides all the coefficients of the matrix, in which case, either it also divides the coefficients of B and it is reduced to a simpler problem, or it does not divide any coefficient of B and the system of linear equations has no solution,
- d is written as a product of pairwise comaximal factors $d = d_1 \cdots d_k$ with $k \geqslant 2$, in which case we can then work with the localizations at the monoids $(1 + d_1\mathbb{Z})$, …, $(1 + d_k\mathbb{Z})$,
- d is written as a pure power of some d' dividing d, which, with d' in place of d, brings us to a similar but simpler problem.

Check that we can recursively exploit the idea expressed above. Write an algorithm and test it. Examine whether the obtained algorithm runs in a reasonable time.

Some solutions, or sketches of solutions

Exercise 2. *1.* Assume without loss of generality $a_0 = b_0 = 1$. When you write $fg = 1$, you get

$$0 = a_n b_m,\ 0 = a_n b_{m-1} + a_{n-1} b_m,\ 0 = a_n b_{m-2} + a_{n-1} b_{m-1} + a_{n-2} b_m,$$

and so on up to degree 1.
Then prove by induction over j that $\deg(a_n^j g) \leqslant m - j$.
In particular, for $j = m + 1$, we get $\deg(a_n^{m+1} g) \leqslant -1$, i.e. $a_n^{m+1} g = 0$. Whence $a_n^{m+1} = 0$. Finally, by reasoning modulo $\mathrm{D}_{\mathbf{B}}(0)$, we obtain successively nilpotent a_j's for $j = n - 1$, …, 1.

2a. Consider the polynomials over the commutative ring $\mathbf{B}[A]$:

$$f(T) = \det(\mathrm{I}_n - TA) \ \text{ and } \ g(T) = \det(\mathrm{I}_n + TA + T^2A^2 + \cdots + T^{e-1}A^{e-1}).$$

We have $f(T)g(T) = \det(\mathrm{I}_n - T^e A^e) = 1$. The coefficient of degree $n - i$ of f is $\pm a_i$. Apply *1.*

2b. It suffices to prove that $\mathrm{Tr}(A)^{(e-1)n+1} = 0$, because $a_i = \pm \mathrm{Tr}\left(\bigwedge^{n-i}(A)\right)$. Consider the determinant defined with respect to a fixed basis $\mathcal{B}$ of $\mathbf{A}^n$. If we take the canonical basis formed by the e_i's, we have an obvious equality

$$\mathrm{Tr}(f) = \det_{\mathcal{B}}(f(e_1), e_2, \ldots, e_n) + \cdots + \det_{\mathcal{B}}\big(e_1, e_2, \ldots, f(e_n)\big).$$

It can be written in the following form:

$$\mathrm{Tr}(f)\det_{\mathcal{B}}(e_1, \ldots, e_n) = \det_{\mathcal{B}}(f(e_1), e_2, \ldots, e_n) + \cdots + \det_{\mathcal{B}}\big(e_1, e_2, \ldots, f(e_n)\big).$$

In this form we can replace the e_i's by any system of n vectors of $\mathbf{A}^n$: both sides are n-multilinear alternating forms (at the e_i's) over $\mathbf{A}^n$, therefore are equal because they coincide on a basis.

Thus, multiplying a determinant by $\mathrm{Tr}(f)$ reduces to replacing it by a sum of determinants in which f acts on each vector.

One deduces that the expression $\mathrm{Tr}(f)^{n(e-1)+1}\det_{\mathcal{B}}(e_1, \ldots, e_n)$ is equal to a sum of which each term is a determinant of the form

$$\det_{\mathcal{B}}\big(f^{m_1}(e_1), f^{m_2}(e_2), \ldots, , f^{m_n}(e_n)\big),$$

with $\sum_i m_i = n(e-1)+1$, therefore at least one of the exponents m_i is $\geqslant e$.

Remark. This solution for the bound $n(e-1)+1$ is due to Gert Almkvist. See on this matter: ZEILBERGER D. *Gert Almkvist's generalization of a mistake of Bourbaki.* Contemporary Mathematics **143** (1993), p. 609–612. ∎

Exercise 3. *1.* Let $\mathfrak{a} = \langle x_1, \ldots, x_n \rangle$. Obtaining $s^r \in \mathfrak{a}$ (for some r), and $1 - as \in \mathfrak{a}$ (for some a). Write $1 = a^r s^r + (1-as)(1+as+\cdots) \in \mathfrak{a}$.

2. $\mathfrak{a}+\mathfrak{b} = \langle 1 \rangle$, $\mathfrak{a}+\mathfrak{c} = \langle 1 \rangle$ and $(\mathfrak{a}+\mathfrak{b})(\mathfrak{a}+\mathfrak{c}) \subseteq \mathfrak{a}+\mathfrak{b}\mathfrak{c}$, therefore $\mathfrak{a}+\mathfrak{b}\mathfrak{c} = \langle 1 \rangle$.

Exercise 4. *1.* Since f is homogeneous, we have $f(tx) = 0$ for a new indeterminate t. Whence each $U_i \in \mathbf{A}[X_1, \ldots, X_n, t]$ such that $f = \sum_{i=1}^n (X_i - tx_i)U_i$.
By making $t := x_1^{-1}X_1$, we obtain each $v_i \in \mathbf{A}[X_1, \ldots, X_n]$ such that

$$f = \textstyle\sum_{i=2}^n (x_1X_i - x_iX_1)v_i.$$

Finally, since f is homogeneous of degree d, we can replace v_i by its homogeneous component of degree $d-1$.

2. Consider the equality $f = \sum_{k,j}(x_kX_j - x_jX_k)u_{kj}$, where the u_{kj}'s are homogeneous polynomials of degree $d-1$. It is a system of linear equations in the coefficients of the u_{kj}'s. Since this system admits a solution over each localized $\mathbf{A}_{x_i}$ and that the x_i's are comaximal, it admits a solution over $\mathbf{A}$.

3. If $F = \sum_d F_d$ is the decomposition of $F \in \mathbf{A}[X_1, \ldots, X_n]$ into homogeneous components, we have $F(tx) = 0$ if and only if $F_d(x) = 0$ for all d, whence the first item of the question. For the saturation, we prove that if $X_iF \in I_x$ for all i, then $F \in I_x$. But we have $x_iF(tx) = 0$. Therefore, by comaximality of the x_i's, we get $F(tx) = 0$, i.e. $F \in I_x$.

Exercise 6. The polynomial Q, regarded as a polynomial with coefficients in $\mathbf{B}'$, remains primitive and therefore regular (Gauss-Joyal, item *2* of Lemma 2.6). Since m_Q is injective, its determinant $\det(m_Q) = P \in \mathbf{A}'[\underline{X}]$ is regular (Theorem 5.22, item *2*). But P is also null in $\mathbf{A}'[\underline{X}]$. Thus $\mathbf{A}'$ is the null ring, in other words $1 \in \mathrm{c}_{\mathbf{A}}(P)$.

Exercise 9. Let $f(X)$ be an idempotent of $\mathbf{A}[X]$. Clearly $e = f(0)$ is idempotent. We want to prove that $f = e$. For this we can reason separately modulo e and modulo $1-e$.
If $e = 0$, then $f = Xg$. We have $(Xg)(1 - Xg) = 0$, or $1 - Xg$ is regular, thus $g = 0$.
If $e = 1$, consider the idempotent $1 - f$ and we are reduced to the previous case.

Exercise 10. For question *5* first prove the result when $uv = 0$. In the general situation, write $u' = 1 - u$ and $v' = 1 - v$. We then have a fundamental system of orthogonal idempotents $(uv, uv', u'v, u'v')$ and by applying the previous special case we see that the two rings are isomorphic to the product $\mathbf{A}/\langle uv'\rangle \times (\mathbf{A}/\langle uv\rangle)^2 \times \mathbf{A}/\langle u'v\rangle$.

Exercise 11. *2.* We have $\mathbf{K}[1/e_i] \simeq \mathbf{K}/\mathrm{Ann}_{\mathbf{K}}(e_i)$ and $\mathrm{Ann}_{\mathbf{K}}(e_i) = \mathrm{Ann}_{\mathbf{A}}(a_i)\mathbf{K}$. For an element x of $\mathbf{A}$, write $dx = \sum_{i\in[\![1..n]\!]} x_i$ in $\mathbf{K}$, with $x_i = e_i dx = a_i x$. The decomposition is thus entirely in $\mathbf{A}$. Since $dx \equiv x_i \bmod \mathrm{Ann}_{\mathbf{A}}(a_i)$ the component $\mathbf{K}/\mathrm{Ann}_{\mathbf{K}}(e_i)$ of the product, when seen as the ideal $e_i\mathbf{K}$, is formed from the elements of the form $a_i x/y$ with $x \in \mathbf{A}$ and y regular in $\mathbf{A}$. But y is regular in $\mathbf{A}$ if and only if each $y_i = a_i y$ is regular modulo $\mathrm{Ann}_{\mathbf{A}}(a_i)$, so that $\mathbf{K}/\mathrm{Ann}_{\mathbf{K}}(e_i)$ is identified with $\mathrm{Frac}(\mathbf{A}/\mathrm{Ann}_{\mathbf{A}}(a_i))$.

Exercise 12. *1.* The zeros of $\mathbf{A}$ are the three “coordinate axes.”
Every element of $\mathbf{A}$ is uniquely written in the form

$$u = a + xf(x) + yg(y) + zh(z),$$

with f, g, $h \in \mathbb{Q}[T]$. This implies that $x + y + z$ is regular because

$$(x + y + z)u = x\big(a + xf(x)\big) + y\big(a + yg(y)\big) + z\big(a + zh(z)\big).$$

So the elements $\dfrac{x}{x+y+z}$, $\dfrac{y}{x+y+z}$ and $\dfrac{z}{x+y+z}$ form a fundamental system of orthogonal idempotents of $\mathbf{K}$. Conclude with Exercise 11 by noting that $\mathrm{Ann}_{\mathbf{A}}(x) = \langle y, z\rangle$, and thus that

$$\mathbf{A}/\mathrm{Ann}_{\mathbf{A}}(x) \simeq \mathbb{Q}[X].$$

2. The zeros of $\mathbf{B}$ are the three “coordinate planes.” The fundamental system of orthogonal idempotents in $\mathbf{L}$ is given by $\dfrac{uv}{uv+vw+wu}$, $\dfrac{vw}{uv+vw+wu}$ and $\dfrac{wu}{uv+vw+wu}$.

Exercise 13. It suffices to solve the question modulo a and modulo $1-a$.
Modulo a: $\begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} 0 \\ b \end{bmatrix} \mapsto \begin{bmatrix} b \\ b \end{bmatrix} \mapsto \begin{bmatrix} b \\ 0 \end{bmatrix}$.
Modulo $1-a$, $\begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} 1 \\ b \end{bmatrix} \mapsto \begin{bmatrix} 1 \\ 0 \end{bmatrix}$. By patching: $d = (1-a)b + a$ with for example the matrix $A = A_2A_1$, where

$$A_1 = (1-a)\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} + a\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1-a \\ 0 & 1 \end{bmatrix},$$

$$A_2 = (1-a)\begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix} + a\begin{bmatrix} 1 & 0 \\ -b & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ a-ab-1 & 1 \end{bmatrix}$$

and
$$A = \begin{bmatrix} 1 & 1-a \\ a-ab-1 & a \end{bmatrix}.$$

Exercise 18. The matrix $D_0 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ transforms $\begin{bmatrix} x \\ y \end{bmatrix}$ into $\begin{bmatrix} -y \\ x \end{bmatrix}$, so $D_0^2 = -\mathrm{I}_2$ and $D_0^3 = -D_0 = D_0^{-1}$.
We also have $D_0 = \mathrm{E}_{12}(1)\mathrm{E}_{21}(-1)\mathrm{E}_{12}(1)$, $D_0 D_q = -\mathrm{E}_{12}(q)$ and $D_q D_0 = -\mathrm{E}_{21}(q)$.

Exercise 21. Let $(e_1, \ldots, e_n)$ be the canonical basis of $\mathbf{A}^n$ and $(f_1, \ldots, f_n)$ the n columns of F. We can assume that the invertible principal minor is in the north-west position such that $(f_1, \ldots, f_k, e_{k+1}, \ldots, e_n)$ is a basis of $\mathbf{A}^n$.
Since $F(f_j) = f_j$, the matrix of F with respect to this basis is $G \overset{\mathrm{def}}{=} \begin{bmatrix} \mathrm{I}_k & * \\ 0 & * \end{bmatrix}$.
The matrix G is idempotent as well as its transposed G'. Apply to the projector G' the operation that we just subjected to F.
Since $G'(e_j) \in \bigoplus_{i \geqslant k+1} \mathbf{A} e_i$ for $j \geqslant k+1$, the matrix of G' with respect to the new basis is of the form $H = \begin{bmatrix} \mathrm{I}_k & 0 \\ 0 & * \end{bmatrix}$, whence the result because F is similar to ${}^{\mathrm{t}}H$.

Exercise 22. We have each $b_{ji} \in \mathbf{A}$ such that $1 = \sum_{i,j} b_{ji} a_{ij}$. Let $B \in \mathbf{A}^{m \times n}$ be defined by $B = (b_{ji})$. Check that $ABA = A$: $(ABA)_{ij} = \sum_{l,k} a_{il} b_{lk} a_{kj}$.
But $\begin{vmatrix} a_{il} & a_{ij} \\ a_{kl} & a_{kj} \end{vmatrix} = 0$, so $(ABA)_{ij} = \sum_{l,k} a_{ij} a_{kl} b_{lk} = a_{ij} \sum_{l,k} a_{kl} b_{lk} = a_{ij}$.
Consequently, AB is a projector.
Let us prove that AB is of rank 1. We have $\mathrm{Tr}(AB) = \sum_i (AB)_{ii} = \sum_{i,j} a_{ij} b_{ji} = 1$, thus $\mathcal{D}_1(AB) = 1$. Furthermore, $\mathcal{D}_2(AB) \subseteq \mathcal{D}_2(A) = 0$.

Exercise 23. *1.* Fix a linear form μ. The map $E^{r+1} \to \mathbf{A}$ defined by
$$(y_0, \ldots, y_r) \mapsto \textstyle\sum_{i=0}^{r} (-1)^i f(y_0, \ldots, y_{i-1}, \widehat{y_i}, y_{i+1}, \ldots, y_r)\, \mu(y_i),$$
where teh symbol $\widehat{y_i}$ denotes the omission of the element, is an $(r+1)$-multilinear alternating form.

According to the hypothesis $\bigwedge_{r+1}(x_1, \ldots, x_n) = 0$ and the injectivity of $E \mapsto E^{\star\star}$, we obtain
$$\textstyle\sum_{i=0}^{r} (-1)^i f(y_0, \ldots, y_{i-1}, \widehat{y_i}, y_{i+1}, \ldots, y_r)\, y_i = 0.$$
Write y instead of y_0 and execute the following operation: in the expression
$$(-1)^i f(y, \ldots, y_{i-1}, \widehat{y_i}, y_{i+1}, \ldots, y_r),$$
bring y between y_{i-1} and y_i. The permutation thus executed necessitates a multiplication by $(-1)^{i-1}$. We then obtain the second equality in which all the

signs “have disappeared.” For example with $r = 4$, the expression

$$\begin{gathered} f(\widehat{y}, y_1, y_2, y_3, y_4)y - f(y, \widehat{y_1}, y_2, y_3, y_4)y_1 + f(y, y_1, \widehat{y_2}, y_3, y_4)y_2 - \\ f(y, y_1, y_2, \widehat{y_3}, y_4)y_3 + f(y, y_1, y_2, y_3, \widehat{y_4})y_4 = \\ f(y_1, y_2, y_3, y_4)y - f(y, y_2, y_3, y_4)y_1 + f(y, y_1, y_3, y_4)y_2 - \\ f(y, y_1, y_2, y_4)y_3 + f(y, y_1, y_2, y_3)y_4 \end{gathered}$$

is none other than

$$\begin{gathered} f(y_1, y_2, y_3, y_4)y - f(y, y_2, y_3, y_4)y_1 - f(y_1, y, y_3, y_4)y_2 - \\ f(y_1, y_2, y, y_4)y_3 - f(y_1, y_2, y_3, y)y_4. \end{gathered}$$

A faster proof: apply a linear form μ to the last expression above, check that the obtained map $(y, y_1, y_2, y_3, y_4) \mapsto \mu(\ldots)$ is 5-multilinear alternating, and therefore is null by the assumptions.

2. Treat the $r = 3$ case. We have an assumption

$$1 = \sum\nolimits_{ijk} \alpha_{ijk} f_{ijk}(x_i, x_j, x_k), \qquad f_{ijk} \text{ 3-multilinear alternating over } E.$$

Define $\pi : E \to E$ by:

$$\pi(x) = \sum\nolimits_{ijk} \alpha_{ijk}[f_{ijk}(x, x_j, x_k)x_i + f_{ijk}(x_i, x, x_k)x_j + f_{ijk}(x_i, x_j, x)x_k].$$

Clearly, the image of p is contained in the submodule $\sum \mathbf{A}x_i$. In addition, for $x \in \sum \mathbf{A}x_i$, we have

$$f_{ijk}(x, x_j, x_k)x_i + f_{ijk}(x_i, x, x_k)x_j + f_{ijk}(x_i, x_j, x)x_k = f_{ijk}(x_i, x_j, x_k)x.$$

Whence $\pi(x) = x$: the endomorphism $\pi : E \to E$ is a projector onto $\sum \mathbf{A}x_i$. Notice that p is of the form $\pi(x) = \sum_i \alpha_i(x)x_i$ i.e. $\pi = \psi \circ \varphi$ and that $\pi \circ \psi = \psi$.

3. The module E in question is $\mathbf{A}^m$ and the vectors $x_1, \ldots, x_n$ are the columns of A. We have $\psi = A : \mathbf{A}^n \to \mathbf{A}^m$, and if we let $B \in \mathbf{A}^{n \times m}$ be the matrix of $\varphi : \mathbf{A}^m \to \mathbf{A}^n$, we indeed have $ABA = A$. So, the linear map $AB : \mathbf{A}^m \to \mathbf{A}^m$ is a projector having the same image as A.

Exercise 26. Let us first see the case where $u = \mathrm{Diag}(\lambda_1, \ldots, \lambda_n)$. We have a basis (e_I) of $\bigwedge^k(\mathbf{A}^n)$ indexed by the subsets $I \subseteq \{1, \ldots, n\}$ of cardinality k:

$$e_I = e_{i_1} \wedge \cdots \wedge e_{i_k} \qquad I = \{i_1 < \cdots < i_k\}.$$

Then, u_k is diagonal with respect to the basis (e_I): $u_k(e_I) = \lambda_I e_I$ with $\lambda_I = \prod_{i \in I} \lambda_i$. It follows that $\det(u_k) = \prod_{\#I=k} \prod_{i \in I} \lambda_i$. It remains to determine, for some j given in $[\![1..n]\!]$, the number of occurrences of λ_j in the above product. In other words, how many subsets I, of cardinality k, contain j? As many as there are subsets of cardinality $k - 1$ contained in $\{1, \cdots, n\} \setminus \{j\}$, i.e. $\binom{n-1}{k-1}$. The result is proven for a generic matrix. Thus it is true for any matrix. The second point follows from the equalities

$$\binom{n-1}{k-1} + \binom{n-1}{n-k-1} = \binom{n-1}{k-1} + \binom{n-1}{k} = \binom{n}{k}.$$

Exercise 28. The general case is treated by induction on n. Consider the polynomial ring $\mathbb{Z}[(x_{ij})]$ with n^2 indeterminates and the universal matrix $A = (x_{ij})$ with coefficients in this ring. Let $\Delta_{1k} \in \mathbb{Z}[(x_{ij})]$ be the cofactor of x_{1k} in A. These cofactors satisfy the identities:

$$\sum\nolimits_{j=1}^{n} x_{1j}\Delta_{1j} = \det A, \qquad \sum\nolimits_{j=1}^{n} x_{ij}\Delta_{1j} = 0 \quad \text{for } i > 1.$$

Since the N_{kl}'s pairwise commute, the specialization $x_{kl} \mapsto N_{kl}$ is legitimate. Let $N'_{1j} = \Delta_{1j}(x_{kl} \mapsto N_{kl})$, then we have

$$N'_{11} = \sum\nolimits_{\sigma \in \mathrm{S}_{n-1}} \varepsilon(\sigma) N_{2\sigma_2} N_{3\sigma_3} \ldots N_{n\sigma_n}.$$

Let us define N' by:

$$N' = \begin{bmatrix} N'_{11} & 0 & \cdots & 0 \\ N'_{12} & \mathrm{I}_m & & \vdots \\ \vdots & \vdots & \ddots & 0 \\ N'_{1n} & 0 & \cdots & \mathrm{I}_m \end{bmatrix}, \text{ so that } NN' = \begin{bmatrix} \Delta & N_{12} & \cdots & N_{1n} \\ 0 & N_{22} & \cdots & N_{2n} \\ \vdots & & & \vdots \\ 0 & N_{n2} & \cdots & N_{nn} \end{bmatrix}.$$

By taking determinants, we get

$$\det(N)\det(N'_{11}) = \det(\Delta)\det \begin{bmatrix} N_{22} & \cdots & N_{2n} \\ \vdots & & \vdots \\ N_{n2} & \cdots & N_{nn} \end{bmatrix}.$$

The induction hypothesis provides the equalities

$$\det \begin{bmatrix} N_{22} & \cdots & N_{2n} \\ \vdots & & \vdots \\ N_{n2} & \cdots & N_{nn} \end{bmatrix} = \det\Big(\sum_{\sigma \in \mathrm{S}_{n-1}} \varepsilon(\sigma) N_{2\sigma_2} N_{3\sigma_3} \cdots N_{n\sigma_n} \Big) = \det(N'_{11}).$$

Simplification by the regular element $\det(N'_{11})$ gives the equality $\det(N) = \det(\Delta)$.

Problem 1. *1.* If A_j is a nonzero column of A, we have $BA_j = e_j$ and therefore $ABA_j = A_j$; thus AB is the identity over $\operatorname{Im} A$, so $ABA = A$. The matrix AB is lower triangular, and its diagonal coefficients are $0, 1$. The matrix BA is diagonal and its diagonal coefficients are $0, 1$.

$$B = \begin{bmatrix} \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{bmatrix}, \qquad BA = \begin{bmatrix} 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{bmatrix},$$

$$AB = \begin{bmatrix} 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{24} & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{44} & \cdot & a_{43} & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\ a_{74} & \cdot & a_{73} & \cdot & a_{71} & a_{72} & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot \\ a_{94} & \cdot & a_{93} & \cdot & a_{91} & a_{92} & \cdot & a_{95} & \cdot \end{bmatrix}.$$

The complementary subspace $\operatorname{Ker} AB$ of $\operatorname{Im} A = \operatorname{Im} AB$ in $\mathbf{K}^n$ admits as its basis the e_i's for the indices i of the rows that do not contain a pivot index.
In the example, (e_2, e_4, e_7, e_9) is a basis of $\operatorname{Ker} AB$.

2. We obtain (Q, A') by Gauss' (classical) pivot method. If the matrix $B' \in M_{n,m}(\mathbf{K})$ satisfies $A'B'A' = A'$, then $AQB'AQ = AQ$, therefore the matrix $B = QB'$ satisfies $ABA = A$.

3. Consider a matrix $B \in \mathbb{M}_{m,n}(\mathbf{K})$ such that $ABA = A$. Then, if $y = Ax$ for some m-vector with coefficients in an overring of $\mathbf{K}$, we have $A(By) = y$, whence the existence of a solution on $\mathbf{K}$, namely By.

4. Let $(u_1, \ldots, u_r)$ be a generator set of the $\mathbf{K}$-vector space E, constituted of vectors of $\mathbf{K}_0^n$; similarly for $(v_1, \ldots, v_s)$ and F. Let $z \in \mathbf{K}_0^n$, which we want to express in the form $z = x_1u_1 + \cdots + x_ru_r + y_1v_1 + \cdots + y_sv_s$ with each $x_i, y_j \in \mathbf{K}_0$. We thus obtain a $\mathbf{K}_0$-linear system from the unknowns x_i's, y_j's which admits a solution on $\mathbf{K}$, therefore also on $\mathbf{K}_0$.

5.a. If every $\pi(e_j)$ is in $\mathbf{K}_0^n$, then the subspace E, generated by the $\pi(e_j)$'s, is $\mathbf{K}_0$-rational. Conversely, if E is $\mathbf{K}_0$-rational, since F is also $\mathbf{K}_0$-rational, by the previous question we have $\pi(e_j) \in \mathbf{K}_0^n$ for all j.

b. Now trivial: $\mathbf{K}_0$ is the subfield generated by the components of the $\pi(e_j)$ vectors.

c. The field of rationality of a strictly staggered matrix is the subfield generated by the coefficients of the matrix. For example with $E = \operatorname{Im} A \subset \mathbf{K}^5$:

$$A = \begin{array}{c} \\ e_1 \\ e_2 \\ e_3 \\ e_4 \\ e_5 \end{array} \begin{array}{c} \begin{array}{ccc} w_1 & w_2 & w_3 \end{array} \\ \begin{bmatrix} 1 & 0 & 0 \\ a & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ b & c & d \end{bmatrix} \end{array},$$

we get $E = \mathbf{K}w_1 \oplus \mathbf{K}w_2 \oplus \mathbf{K}w_3$ and we have $\mathbf{K}^5 = E \oplus F$ with $F = \mathbf{K}e_2 \oplus \mathbf{K}e_5$. Since

$$e_1 - w_1 \in F, \quad e_3 - w_2 \in F, \quad e_4 - w_3 \in F,$$

we have $\pi(e_1) = w_1$, $\pi(e_3) = w_2$, $\pi(e_4) = w_3$ and $\pi(e_2) = \pi(e_5) = 0$. The field of rationality of E is $\mathbf{K}_0 = \mathbf{k}(a, b, c, d)$, where $\mathbf{k}$ is the prime subfield of $\mathbf{K}$.

Bibliographic comments

The Gauss-Joyal Lemma is in [81], which gives it its name. On the general subject of comparison between the ideals $\mathrm{c}(f)\mathrm{c}(g)$ and $\mathrm{c}(fg)$ see [40, 96, 148] and, in this work, Sections III-2 and III-3 and Proposition XI-3.14.

Regarding the constructive treatment of Noetherianity, see [MRR, 113, 150, 151, 161, 171, 172, 190].

The whole of Section 5 can be more or less found in [Northcott]. For example the formula (12) on page 47 is found in a related form in Theorem 5 on page 10. Likewise, our Cramer-style magic formula (17) on page 48 is very similar to Theorem 6 on page 11: Northcott attaches central importance to the matrix equation $A\,B\,A = A$. On this subject, see also [Rao & Mitra] and [61, Díaz-Toca&al.].

Proposition 5.15 is in [Bhaskara Rao] Theorem 5.5.

Concerning Theorem 5.26: in [Northcott] Theorem 18 on page 122 establishes the equivalence of items *1* and *5* by a method which is not entirely constructive, but Theorem 5 page 10 would allow us to give an explicit formula for the implication *5* $\Rightarrow$ *1*.

Chapter III

The method of undetermined coefficients

Contents

Introduction

Weil Gauss ein echter Prophet der Wissenschaft ist,
deshalb reichen die Begriffe,
die er aus der Tiefe der Wissencshaft schöpft,
weit hinaus über den Zweck,
zu welchem sie aufgestellt wurden.
Kronecker
Vorlesungen Sommersemester 1891. Leçon 11 [18]

Approx. transl.
Because Gauss is a true Prophet of Science,
the concepts that he draws from the depths of Science
go beyond the purpose for which they were established.

In 1816, Gauss published a fundamental article [90] in which he corrects (without citing) the proof of the fundamental theorem of algebra given by Laplace a few years beforehand. Laplace's proof is itself remarkable as it is "purely algebraic:" it claims only two very elementary properties for real numbers: the existence of the square root of a non-negative number and that of a zero for a polynomial of odd degree.

Gauss' goal is to treat this theorem without using a (hypothetical) field of imaginary numbers, over which an arbitrary polynomial would be decomposed into linear factors. Laplace's proof implicitly assumes the existence of such a field $\mathbf{K}$ containing $\mathbb{C} = \mathbb{R}[i]$, and shows that the decomposition into products of linear factors actually takes place in $\mathbb{C}[X]$.

Gauss' proof dispenses with the assumption about the field $\mathbf{K}$ and constitutes a tour de force that shows that you can handle things in a purely formal way. He proves the existence of the gcd of two polynomials by using Euclid's algorithm as well as the corresponding Bézout relation. He shows that every symmetric polynomial is uniquely expressed as a polynomial of elementary symmetric functions (by introducing a lexicographical order on the monomials). He defines the discriminant of a monic polynomial purely formally. He shows (without resorting to roots) that every polynomial can be decomposed into a product of polynomials with a nonzero discriminant. He shows (without resorting to roots) that a polynomial admits a square factor if and only if its discriminant is zero (he works in zero characteristic). Finally, Gauss makes Laplace's proof work in a purely formal way, without resorting to a splitting field, by only using resultants and discriminants.

In short, he establishes a "general method of undetermined coefficients" on a firm basis. This was to be systematically reused, in particular by Leopold Kronecker, Richard Dedekind, Jules Drach, Ernest Vessiot…

In this chapter, we introduce the method of undetermined coefficients and we give some of its applications.

We begin with some generalities about polynomial rings. The Dedekind-Mertens lemma and Kronecker's theorem are two basic tools which provide precise information about the coefficients of a product of two polynomials. These two results will often be used in the remainder of this work.

Here we study the elementary properties of the discriminant and the resultant, and we introduce the fundamental tool that is the universal splitting algebra of a monic polynomial. The latter allows for a simplification of purely formal proofs such as Gauss' by providing a formal substitute for the polynomial's "splitting field."

All of this is very consistent and works with arbitrary commutative rings. The reader will only notice the apparition of fields from Section 6.

The applications that we treat relate to basic Galois theory, the first steps in algebraic number theory, and Hilbert's Nullstellensatz. We have also dedicated a section to Newton's method in algebra.

A few words on finite sets

A set E is said to be *finite* when we explicitly have a bijection between E and an initial segment $\{\, x \in \mathbb{N} \,|\, x < n \,\}$ of $\mathbb{N}$. It is said to be *finitely enumerable* when we explicitly have a surjection of a finite set F onto E.

In general the context is sufficient to distinguish between the two notions. Sometimes, it is advantageous to be very precise. We will make the distinction when necessary by using the notation $\mathrm{P_f}$ or $\mathrm{P_{fe}}$: we will denote by $\mathrm{P_f}(S)$ *the set of finite subsets* of the set S and $\mathrm{P_{fe}}(S)$ *the set of finitely enumerable subsets* of S. In constructive mathematics when S is discrete (resp. finite), we have the equality $\mathrm{P_f}(S) = \mathrm{P_{fe}}(S)$ and it is a discrete set (resp. finite).[1] When S *is not* discrete, $\mathrm{P_f}(S)$ *is not* equal to $\mathrm{P_{fe}}(S)$.

Also note that when S is a finite set every detachable subset (cf. page 33) is finite: the set of finite subsets is then equal to the set of detachable subsets.

The finitely enumerable subsets are omnipresent in the usual mathematical sense. For example when we speak of a finitely generated ideal we mean an ideal generated by a finitely enumerated subset and not by a finite subset. Similarly, when we speak of a *finite family* $(a_i)_{i\in I}$ in the set E, we mean that I is a finite set, therefore the subset $\{\, a_i \,|\, i \in I \,\} \subseteq E$ is finitely enumerated.

Finally, a nonempty set X is said to be *enumerable* if there is a surjective map $x = (x_n) : \mathbb{N} \to X$.

1. Polynomial rings

Partial factorization algorithm

We assume the reader to be familiar with the extended Euclid algorithm which computes the monic gcd of two monic polynomials in $\mathbf{K}[X]$ when $\mathbf{K}$ is a discrete field (see for example Problem 2).

1.1. Lemma. *If* $\mathbf{K}$ *is a discrete field, we have a* partial factorization *algorithm for the finite families of monic polynomials in* $\mathbf{K}[X]$*: a partial factorization for a finite family* $(g_1, \dots, g_r)$ *is given by a finite pairwise comaximal family* $(f_1, \dots, f_s)$ *of monic polynomials and by the expression of each* g_i *in the form*

$$g_i = \prod\nolimits_{k=1}^{s} f_k^{m_{k,i}} \quad (m_{k,i} \in \mathbb{N}).$$

The family $(f_1, \dots, f_s)$ *is called a* partial factorization basis *for the family* $(g_1, \dots, g_r)$*.*

[1] In constructive mathematics we generally refrain from considering the “set of all subsets of a set,” even finite, because it is not a “reasonable” set: it does not seem possible to give a clear definition of its elements (see the discussion page 964). When we used the notation $\mathcal{P}_\ell$ for “the set of subsets of $\{1, \dots, \ell\}$,” on page 47, it was in fact the set of finite subsets of $\{1, \dots, \ell\}$.

D If the g_i's are pairwise comaximal, there is nothing left to prove. Otherwise, assume for example that $\gcd(g_1, g_2) = h_0$, $g_1 = h_0h_1$ and $g_2 = h_0h_2$ with $\deg(h_0) \geqslant 1$. We replace the family $(g_1, \dots, g_r)$ with the family $(h_0, h_1, h_2, g_3, \dots, g_r)$. We note that the sum of the degrees has decreased. We also note that we can delete from the list the polynomials equal to 1, or any repeats of a polynomial. We finish by induction on the sum of the degrees. The details are left to the reader. □

Universal property of polynomial rings

A polynomial ring $\mathbf{A}[X_1, \dots, X_n]$ satisfies the universal property which defines it as *the commutative ring freely generated by* $\mathbf{A}$ *and* n *new elements.* This is the property described by means of the evaluation homomorphism in the following terms.

1.2. Proposition. *Given two commutative rings* $\mathbf{A}$ *and* $\mathbf{B}$*, a homomorphism* $\rho : \mathbf{A} \to \mathbf{B}$ *and* n *elements* $b_1, \dots, b_n \in \mathbf{B}$ *there exists a unique homomorphism* $\varphi : \mathbf{A}[X_1, \dots, X_n] = \mathbf{A}[\underline{X}] \to \mathbf{B}$ *which extends* ρ *and which takes the* X_i*'s to the* b_i*'s.*

$$\begin{tikzcd}
\mathbf{A} \arrow[d, "j"'] \arrow[dr, "\rho"] & \\
\mathbf{A}[\underline{X}] \arrow[r, dashed, "\varphi!"'] & \mathbf{B}
\end{tikzcd} \qquad \varphi(X_i) = b_i,\ i \in [\![1..n]\!].$$

This homomorphism φ is called *the evaluation homomorphism* (of every X_i to b_i). If $P \in \mathbf{A}[\underline{X}]$ has as its image P^ρ in $\mathbf{B}[X_1, \dots, X_n]$, we obtain the equality $\varphi(P) = P^\rho(b_1, \dots, b_n)$. The evaluation homomorphism is also called a *specialization*, and we say that $\varphi(P)$ is obtained by *specializing* each X_i to b_i. When $\mathbf{A} \subseteq \mathbf{B}$, the elements $b_1, \dots, b_n \in \mathbf{B}$ are said to be *algebraically independent over* $\mathbf{A}$ if the corresponding evaluation homomorphism is injective.

By Proposition 1.2 every computation made in $\mathbf{A}[\underline{X}]$ is transferred into $\mathbf{B}$ by means of the evaluation homomorphism.

Clearly, S_n acts as a group of automorphisms of $\mathbf{A}[\underline{X}]$ by permutation of the indeterminates: $(\sigma, Q) \mapsto Q(X_{\sigma 1}, \dots, X_{\sigma n})$.

The following corollary results immediately from Proposition 1.2.

1.3. Corollary. *Given* n *elements* $b_1, \dots, b_n$ *in a commutative ring* $\mathbf{B}$*, there exists a unique homomorphism* $\varphi : \mathbb{Z}[X_1, \dots, X_n] \to \mathbf{B}$ *which takes every* X_i *to* b_i*.*

Algebraic identities

An algebraic identity is an equality between two elements of $\mathbb{Z}[X_1, \ldots, X_n]$ defined differently. It gets automatically transferred into every commutative ring by means of the previous corollary.

Since the ring $\mathbb{Z}[X_1, \ldots, X_n]$ has particular properties, it happens that some algebraic identities are easier to prove in $\mathbb{Z}[X_1, \ldots, X_n]$ than in "an arbitrary ring $\mathbf{B}$." Consequently, if the structure of a theorem reduces to a family of algebraic identities, which is very frequent in commutative algebra, it is often in our interest to use a ring of polynomials with coefficients in $\mathbb{Z}$ by taking as its indeterminates the relevant elements in the statement of the theorem.

The properties of the rings $\mathbb{Z}[\underline{X}]$ which may prove useful are numerous. The first is that it is an integral ring. So it is a subring of its quotient field $\mathbb{Q}(X_1, \ldots, X_n)$ which offers all the facilities of discrete fields.

The second is that it is an infinite and integral ring. Consequently, "all bothersome but rare cases can be ignored." A case is rare when it corresponds to the annihilation of a polynomial Q that evaluates to zero everywhere. It suffices to check the equality corresponding to the algebraic identity when it is evaluated at the points of $\mathbb{Z}^n$ which do not annihilate Q. Indeed, if the algebraic identity we need to prove is $P = 0$, we get that the polynomial PQ defines the function over $\mathbb{Z}^n$ that evaluates to zero everywhere, this implies that $PQ = 0$ and thus $P = 0$ since $Q \neq 0$ and $\mathbb{Z}[\underline{X}]$ is integral. This is sometimes called the "extension principle for algebraic identities."

Other remarkable properties of $\mathbb{Z}[\underline{X}]$ could sometimes be used, like the fact that it is a unique factorization domain (UFD) as well as being a strongly discrete coherent Noetherian ring of finite Krull dimension.

An example of application

1.4. Lemma. *For A, $B \in \mathbb{M}_n(\mathbf{A})$, we have the following results.*

1. $\widetilde{AB} = \widetilde{B}\widetilde{A}$.
2. $\mathrm{C}_{AB} = \mathrm{C}_{BA}$.
3. $\widetilde{PAP^{-1}} = P\widetilde{A}P^{-1}$ *for* $P \in \mathbb{GL}_n(\mathbf{A})$.
4. $\widetilde{\widetilde{A}} = \det(A)^{n-2}A$ *if* $n \geqslant 2$.
5. (The Cayley-Hamilton theorem) $\mathrm{C}_A(A) = 0$.
6. *If* $\Gamma_A(X) = (-1)^{n+1}\big(\mathrm{C}_A(X) - \mathrm{C}_A(0)\big)/X$, *we have* $\widetilde{A} = \Gamma_A(A)$ *(*$n \geqslant 2$*). We also have* $\mathrm{Tr}\,\big(\widetilde{A}\big) = (-1)^{n+1}\Gamma_A(0)$.
7. (Sylvester's identities) *Let* $r \geqslant 1$ *and* $s \geqslant 2$ *such that* $n = r + s$. *Let* $C \in \mathbb{M}_r(\mathbf{A})$, $F \in \mathbb{M}_s(\mathbf{A})$, $D \in \mathbb{M}_{r,s}(\mathbf{A})$, $E \in \mathbb{M}_{s,r}(\mathbf{A})$ *be the matrices*

extracted form A as below

$$A = \begin{array}{|c|c|}\hline C & D \\ \hline E & F \\ \hline\end{array}\ .$$

Let $\alpha_i = \{1, \dots, r, r+i\}$ *and* $\mu_{i,j} = \det(A_{\alpha_i,\alpha_j})$ *for* $i, j \in [\![1..s]\!]$. *Then:*

$$\det(C)^{s-1}\det(A) = \det\big((\mu_{i,j})_{i,j\in[\![1..s]\!]}\big).$$

8. *If* $\det A = 0$*, then* $\bigwedge^2 \widetilde{A} = 0$.

D We can take all the matrices with undetermined coefficients over $\mathbb{Z}$ and localize the ring at $\det P$. In this case A, B, C and P are invertible in the quotient field of the ring $\mathbf{B} = \mathbb{Z}[(a_{ij}), (b_{ij}), (p_{ij})]$. Furthermore, the matrix $\widetilde{A}$ satisfies the equality $\widetilde{A}A = \det(A)\,\mathrm{I}_n$, which characterizes it since $\det A$ is invertible. This provides item *1* via the equality $\det(AB) = \det(A)\det(B)$, items *3* and *4*, and item *6* via item *5* and the equality $\mathrm{C}_A(0) = (-1)^n \det A$. For item *2* we note that $AB = A(BA)A^{-1}$.

For Cayley-Hamilton's theorem, we first treat the case of the *companion matrix of a monic polynomial* $f = T^n - \sum_{k=1}^{n} a_k T^{n-k}$:

$$P = \begin{bmatrix} 0 & \cdots & \cdots & \cdots & 0 & a_n \\ 1 & 0 & & & \vdots & a_{n-1} \\ 0 & \ddots & \ddots & & \vdots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ \vdots & & \ddots & 1 & 0 & a_2 \\ 0 & \cdots & \cdots & 0 & 1 & a_1 \end{bmatrix}.$$

This is the matrix of the "multiplication by t," $\mu_t : y \mapsto ty$ (where t is the class of T) in the quotient ring $\mathbf{A}[T]/\langle f(T)\rangle = \mathbf{A}[t]$, expressed over the basis of the monomials ordered by increasing degrees. Indeed, on the one hand a direct computation shows that $\mathrm{C}_P(T) = f(T)$. On the other hand $f(\mu_t) = \mu_{f(t)} = 0$, thus $f(P) = 0$.

Moreover, in the case of the generic matrix, the determinant of the family $(e_1, Ae_1, \dots, A^{n-1}e_1)$ is necessarily nonzero, therefore the generic matrix is similar to the companion matrix of its characteristic polynomial over the quotient field of $\mathbb{Z}[(a_{ij})]$.

7. Since C is invertible, we can use the generalized Gauss' pivot, by left-multiplication by a matrix $\begin{array}{|c|c|}\hline C^{-1} & 0 \\ \hline E' & \mathrm{I}_s \\ \hline\end{array}$, this reduces to the case where $C = \mathrm{I}_r$ and $E = 0$.

Finally, item *8* results from Sylvester's identity (item *7*) with $s = 2$. □

Remark. Item *3* allows us to define the *cotransposed endomorphism* of an endomorphism of a free module of finite rank, from the cotransposed matrix.

Weights, homogeneous polynomials

We say that we have defined a weight on a polynomial algebra $\mathbf{A}[X_1,\ldots,X_k]$ when we attribute to each indeterminate X_i a weight $w(X_i)\in\mathbb{N}$. We then define the weight of the monomial $\underline{X}^{\underline{m}} = X_1^{m_1}\cdots X_k^{m_k}$ as

$$w(\underline{X}^{\underline{m}}) = \textstyle\sum_i m_i w(X_i),$$

so that $w(\underline{X}^{\underline{m}+\underline{m}'}) = w(\underline{X}^{\underline{m}}) + w(\underline{X}^{\underline{m}'})$. The degree of a polynomial P for this weight, generally denoted by $w(P)$, is the greatest of the weights of the monomials appearing with a nonzero coefficient. This is only well-defined if we have a test of equality to 0 in $\mathbf{A}$ at our disposal. In the opposite case we simply define the statement "$w(P)\leqslant r$."

A polynomial is said to be *homogeneous* (for a weight w) if all of its monomials have the same weight.

When we have an algebraic identity and a weight available, each homogeneous component of the algebraic identity provides a particular algebraic identity.

We can also define weights with values in some monoids with a more complicated order than $(\mathbb{N},0,+,\geqslant)$. We then ask that this monoid be the positive part of a product of totally ordered Abelian groups, or more generally a monoid with gcd (this notion will be introduced in Chapter XI).

Symmetric polynomials

We fix n and $\mathbf{A}$ and we let S_1, …, S_n be the *elementary symmetric polynomials at the X_i's* in $\mathbf{A}[X_1,\ldots,X_n]$. They are defined by the equality

$$T^n + S_1T^{n-1} + S_2T^{n-2} + \cdots + S_n = \textstyle\prod_{i=1}^{n}(T+X_i).$$

We have $S_1 = \sum_i X_i$, $S_n = \prod_i X_i$, $S_k = \sum_{J\in\mathcal{P}_{k,n}}\prod_{i\in J} X_i$. Recall the following well-known theorem (a proof is suggested in Exercise 3).

1.5. Theorem. (Elementary symmetric polynomials)

1. *A polynomial $Q\in\mathbf{A}[X_1,\ldots,X_n]=\mathbf{A}[\underline{X}]$, invariant under permutations of the variables, is uniquely expressible as a polynomial in the elementary symmetric functions S_1, …, S_n. In other words*
   - *the subring of the fixed points of $\mathbf{A}[\underline{X}]$ by the action of the symmetric group S_n is the ring $\mathbf{A}[S_1,\ldots,S_n]$ generated by $\mathbf{A}$ and the S_i's, and*
   - *the S_i's are algebraically independent over $\mathbf{A}$.*

2. *Let us denote by $d(P)$ the total degree of $P \in \mathbf{A}[\underline{X}]$ when each X_i is affected by the weight* 1*, and $d_1(P)$ its degree in X_1. Let $\delta(Q)$ be the total degree of $Q \in \mathbf{A}[S_1, \ldots, S_n]$ when each variable S_i is affected by the weight i and $\delta_1(Q)$ its total degree when each variable S_i is affected by the weight* 1*. Assume that $Q(S_1, \ldots, S_n)$ is evaluated in $P(\underline{X})$.*
   - *a. $d(P) = \delta(Q)$, and if Q is δ-homogeneous, then P is d-homogeneous.*
   - *b. $d_1(P) = \delta_1(Q)$.*
3. $\mathbf{A}[X_1, \ldots, X_n]$ *is a free module of rank $n!$ over* $\mathbf{A}[S_1, \ldots, S_n]$ *and a basis is formed by the monomials $X_1^{k_1} \cdots X_{n-1}^{k_{n-1}}$ such that $k_i \in [\![0..n-i]\!]$ for each i.*

1.6. Corollary. *On a ring* $\mathbf{A}$ *consider the generic polynomial*

$$f = T^n + f_1 T^{n-1} + f_2 T^{n-2} + \cdots + f_n,$$

where the f_i's are the indeterminates. We have an injective homomorphism $j : \mathbf{A}[f_1, \ldots, f_n] \to \mathbf{A}[X_1, \ldots, X_n]$ such that the $(-1)^k j(s_k)$'s are the elementary symmetric polynomials in the X_i's.

In short we can always reduce to the case where $f(T) = \prod_i (T - X_i)$, where the X_i's are other indeterminates.

1.7. Corollary. *On a ring* $\mathbf{A}$ *consider the generic polynomial*

$$f = f_0 T^n + f_1 T^{n-1} + f_2 T^{n-2} + \cdots + f_n,$$

where the f_i's are indeterminates. We have an injective homomorphism $j : \mathbf{A}[f_0, \ldots, f_n] \to \mathbf{B} = \mathbf{A}[F_0, X_1, \ldots, X_n]$, with the following equality in $\mathbf{B}[T]$.

$$j(f_0)\, T^n + j(f_1)\, T^{n-1} + \cdots + j(f_n) = F_0 \prod\nolimits_i (T - X_i)\,.$$

In short, we can always reduce to the case where $f(T) = f_0 \prod_i (T - X_i)$, with indeterminates f_0, X_1, …, X_n.

D It suffices to see that if f_0, g_1, …, $g_n \in \mathbf{B}$ are algebraically independent over $\mathbf{A}$, then the same goes for f_0, $f_0 g_1$, …, $f_0 g_n$. It suffices to verify that $f_0 g_1$, …, $f_0 g_n$ are algebraically independent over $\mathbf{A}[f_0]$. This results from f_0 being regular and from g_1, …, g_n being algebraically independent over $\mathbf{A}[f_0]$. □

2. Dedekind-Mertens lemma

Recall that for a polynomial f of $\mathbf{A}[X_1, \ldots, X_n] = \mathbf{A}[\underline{X}]$, we call the "content of f" and denote by $\mathrm{c}_{\mathbf{A},\underline{X}}(f)$ or $\mathrm{c}(f)$ the ideal generated by the coefficients of f.

Note that we always have $\mathrm{c}(f)\mathrm{c}(g) \supseteq \mathrm{c}(fg)$ and thus $\mathrm{c}(f)^{k+1}\mathrm{c}(g) \supseteq \mathrm{c}(f)^k \mathrm{c}(fg)$ for all $k \geqslant 0$. For k large enough this inclusion becomes an equality.

2.1. Dedekind-Mertens lemma.
For f, $g \in \mathbf{A}[T]$ with $m \geqslant \deg g$ we have $\boxed{\mathrm{c}(f)^{m+1}\mathrm{c}(g) = \mathrm{c}(f)^m\mathrm{c}(fg)}$.

D First of all, notice that the products $f_i g_j$ are the coefficients of the polynomial $f(Y)g(X)$. Similarly, for some indeterminates $Y_0, \ldots, Y_m$, the content of the polynomial $f(Y_0)\cdots f(Y_m)g(X)$ is equal to $\mathrm{c}(f)^{m+1}\mathrm{c}(g)$. Let $h = fg$. Imagine that in the ring $\mathbf{B} = \mathbf{A}[X, Y_0, \ldots, Y_m]$ we are able to show the membership of the polynomial $f(Y_0)\cdots f(Y_m)g(X)$ in the ideal

$$\textstyle\sum_{j=0}^m \big(h(Y_j)\prod_{k,k\neq j}\langle f(Y_k)\rangle\big).$$

We would immediately deduce that $\mathrm{c}(f)^{m+1}\mathrm{c}(g) \subseteq \mathrm{c}(f)^m\mathrm{c}(h)$.
This is more or less what is going to happen. We get rid of the denominators in Lagrange's interpolation formula (we need at least $1 + \deg g$ interpolation points):

$$g(X) = \textstyle\sum_{j=0}^m \;\frac{\prod_{k,k\neq j}(X-Y_k)}{\prod_{k,k\neq j}(Y_j-Y_k)}\; g(Y_j)\,.$$

In the ring $\mathbf{B}$, by letting $\Delta = \prod_{j\neq k}(Y_j - Y_k)$, we get:

$$\Delta \cdot g(X) \;\in\; \textstyle\sum_{j=0}^m \langle g(Y_j)\rangle.$$

Thus by multiplying by $f(Y_0)\cdots f(Y_m)$:

$$\Delta \cdot f(Y_0)\cdots f(Y_m)\cdot g(X) \;\in\; \textstyle\sum_{j=0}^m h(Y_j)\prod_{k,k\neq j}\langle f(Y_k)\rangle.$$

If we show that for any $Q \in \mathbf{B}$ we have $\mathrm{c}(Q) = \mathrm{c}(\Delta\cdot Q)$, the previous membership gives $\mathrm{c}(f)^{m+1}\mathrm{c}(g) \subseteq \mathrm{c}(f)^m\mathrm{c}(h)$.
Note that $\mathrm{c}(Y_i\,Q) = \mathrm{c}(Q)$ and especially that

$$\mathrm{c}\big(Q(Y_0 \pm Y_1, Y_1, \ldots, Y_m)\big) \subseteq \mathrm{c}\big(Q(Y_0, Y_1, \ldots, Y_m)\big).$$

Therefore, by putting $Y_0 = (Y_0 \pm Y_1) \mp Y_1$, $\mathrm{c}\big(Q(Y_0 \pm Y_1, Y_1, \ldots, Y_m)\big) = \mathrm{c}(Q)$.
The following polynomials thus all have the same content:
Q, $Q(Y_0 + Y_1, Y_1, \ldots, Y_m)$, $Y_0\,Q(Y_0 + Y_1, Y_1, \ldots, Y_m)$, $(Y_0 - Y_1)\,Q(Y_0, Y_1, \ldots, Y_m)$.
Whence $\mathrm{c}(Q) = \mathrm{c}(\Delta\cdot Q)$. □

We deduce the following corollaries.

2.2. Corollary. *If f_1, …, f_d are d polynomials (with one indeterminate) of degree $\leqslant \delta$, with $e_i = 1 + (d-i)\delta$ we have*

$$\mathrm{c}(f_1)^{e_1}\mathrm{c}(f_2)^{e_2}\cdots\mathrm{c}(f_d)^{e_d} \subseteq \mathrm{c}(f_1 f_2\cdots f_d).$$

D Let $f = f_1$ and $g = f_2\cdots f_d$. We have $\deg g \leqslant (d-1)\delta$ and $e_1 = 1 + (d-1)\delta$. Dedekind-Mertens lemma thus gives:

$$\mathrm{c}(f)^{e_1}\mathrm{c}(g) = \mathrm{c}(f)^{(d-1)\delta}\mathrm{c}(fg) \subseteq \mathrm{c}(fg), \text{ i.e. } \mathrm{c}(f_1)^{e_1}\mathrm{c}(f_2\cdots f_d) \subseteq \mathrm{c}(f_1 f_2\cdots f_d).$$

We finish by induction on d. □

2.3. Corollary. *Let f and $g \in \mathbf{A}[T]$.*

1. *If* $\mathrm{Ann}_{\mathbf{A}}\big(\mathrm{c}(f)\big) = 0$*, then* $\mathrm{Ann}_{\mathbf{A}[T]}(f) = 0$ (McCoy's Lemma).
2. *If* $\mathbf{A}$ *is reduced, then* $\mathrm{Ann}_{\mathbf{A}[T]}(f) = \mathrm{Ann}_{\mathbf{A}}\big(\mathrm{c}(f)\big)[T]$.
3. *The polynomial f is nilpotent if and only if each of its coefficients is nilpotent.*
4. *If* $\mathrm{c}(f) = 1$*, then* $\mathrm{c}(fg) = \mathrm{c}(g)$.

D Let $g \in \mathrm{Ann}_{\mathbf{A}[T]}(f)$ and $m \geqslant \deg(g)$. Dedekind-Mertens lemma implies:

$$\mathrm{c}(f)^{1+m} g = 0. \tag{$*$}$$

1. So $\mathrm{Ann}_{\mathbf{A}}\mathrm{c}(f) = 0$ implies $g = 0$.
2. Since the ring is reduced, $(*)$ implies $\mathrm{c}(f)g = 0$. Thus every polynomial g annihilated by f is annihilated by $\mathrm{c}(f)$.
Furthermore, $\mathrm{Ann}_{\mathbf{A}}\big(\mathrm{c}(f)\big) = \mathbf{A} \cap \mathrm{Ann}_{\mathbf{A}[T]}(f)$ and thus the inclusion

$$\mathrm{Ann}_{\mathbf{A}[T]}(f) \supseteq \mathrm{Ann}_{\mathbf{A}}\big(\mathrm{c}(f)\big)[T]$$

is always true (whether $\mathbf{A}$ is reduced or not).
3. If $f^2 = 0$, the Dedekind-Mertens lemma implies $\mathrm{c}(f)^{2+\deg f} = 0$.
4. Immediately from $\mathrm{c}(f)^{m+1}\mathrm{c}(g) = \mathrm{c}(f)^m \mathrm{c}(fg)$. □

3. One of Kronecker's theorems

A-algebras and integral elements

We first introduce the terminology of $\mathbf{A}$-algebras. The algebras that we consider in this work are associative, commutative and unitary, unless stated otherwise.

3.1. Definition.

1. An $\mathbf{A}$-*algebra* is a commutative ring $\mathbf{B}$ with a homomorphism of commutative rings $\rho : \mathbf{A} \to \mathbf{B}$. That makes $\mathbf{B}$ an $\mathbf{A}$-module. When $\mathbf{A} \subseteq \mathbf{B}$, or more generally if ρ is injective, we say that $\mathbf{B}$ is an *extension* of $\mathbf{A}$.
2. A *morphism* of the $\mathbf{A}$-algebra $\mathbf{A} \xrightarrow{\rho} \mathbf{B}$ to the $\mathbf{A}$-algebra $\mathbf{A} \xrightarrow{\rho'} \mathbf{B}'$ is a homomorphism of rings $\mathbf{B} \xrightarrow{\varphi} \mathbf{B}'$ satisfying $\varphi \circ \rho = \rho'$. The set of morphisms of $\mathbf{A}$-algebras of $\mathbf{B}$ to $\mathbf{B}'$ is denoted by $\mathrm{Hom}_{\mathbf{A}}(\mathbf{B}, \mathbf{B}')$.

$$\begin{tikzcd}
\mathbf{A} \arrow[d, "\rho"'] \arrow[dr, "\rho'"] & \\
\mathbf{B} \arrow[r, "\varphi"'] & \mathbf{B}'
\end{tikzcd}$$

Remarks.
1) We chose not to reserve the terminology "extension" for the case of fields.

This will require us to use in the cases of fields statements such as "**L** is a field extension of **K**" or "**L** is a field, extending **K**" from this point on.

2) Every ring is uniquely a $\mathbb{Z}$-algebra and every homomorphism of rings is a morphism of the corresponding $\mathbb{Z}$-algebras. The category of commutative rings can be regarded as a special case among the categories of algebras defined above. ∎

Notation. If $b \in \mathbf{B}$ and M is a $\mathbf{B}$-module, we denote by $\mu_{M,b}$ or μ_b the multiplication by b in M: $y \mapsto by$, $M \to M$. This can be regarded as a $\mathbf{B}$-linear map, or, if $\mathbf{B}$ is an $\mathbf{A}$-algebra, as an $\mathbf{A}$-linear map for the $\mathbf{A}$-module structure of M.

3.2. Definition. Let $\mathbf{A} \subseteq \mathbf{B}$ be rings.

1. An element $x \in \mathbf{B}$ is said to be *integral* over $\mathbf{A}$ if there exists some integer $k \geqslant 1$ such that $x^k = a_1x^{k-1} + a_2x^{k-2} + \cdots + a_k$ with each $a_h \in \mathbf{A}$. If $\mathbf{A}$ is a discrete field, we also say that x is *algebraic* over $\mathbf{A}$.
2. In this case, the monic polynomial $P = X^k-(a_1X^{k-1}+a_2X^{k-2}+\cdots+a_k)$ is called an *integral dependence relation* of x over $\mathbf{A}$. In fact, by abuse of language we also say that the equality $P(x) = 0$ is an *integral dependence relation.* If $\mathbf{A}$ is a discrete field, we also speak of an *algebraic dependence relation.*
3. The ring $\mathbf{B}$ is said to be *integral* over $\mathbf{A}$ if every element of $\mathbf{B}$ is integral over $\mathbf{A}$. We will also say that the $\mathbf{A}$-algebra $\mathbf{B}$ is *integral.* If $\mathbf{A}$ and $\mathbf{B}$ are discrete fields, we say that $\mathbf{B}$ is *algebraic* over $\mathbf{A}$.
4. If $\rho : \mathbf{C} \to \mathbf{B}$ is a $\mathbf{C}$-algebra with $\rho(\mathbf{C}) = \mathbf{A}$, we say that the algebra $\mathbf{B}$ is integral over $\mathbf{C}$ if it is integral over $\mathbf{A}$.

The theorem

3.3. Theorem. (Kronecker's Theorem) [122]
In $\mathbf{B}[T]$, consider the polynomials

$$f=\sum_{i=0}^{n}(-1)^i f_iT^{n-i},\ g=\sum_{j=0}^{m}(-1)^j g_jT^{m-j} \text{ and } h=fg=\sum_{r=0}^{p}(-1)^r h_rT^{p-r},$$

where $p = m + n$. Let $\mathbf{A} = \mathbf{Z}[h_0, \dots, h_p]$ be the subring generated by the coefficients of h ($\mathbf{Z}$ is the subring of $\mathbf{B}$ generated by $1_{\mathbf{B}}$).

1. *Each f_ig_j is integral over $\mathbf{A}$.*
2. *In the case where we take indeterminates over the ring $\mathbb{Z}$ for f_i and g_j, we find an integral dependence relation over $\mathbf{A}$ for $z_{i,j} = f_ig_j$ which is homogeneous for different systems of weights attributed to the monomials:*
   a. *the respective weights of $z_{k,\ell}$ and h_r are $k + \ell$ and r.*

b. the respective weights of $z_{k,\ell}$ and h_r are $p-k-\ell$ and $p-r$.

c. the weights of $z_{k,\ell}$ and h_r are $w(z_{k,\ell}) = w(h_r) = 1$.

Naturally these integral dependence relations are then applicable in every ring.

D It suffices to treat item *2*.

Let us first examine an intermediate generic case. We take $f_0 = g_0 = 1$ and indeterminates over $\mathbb{Z}$ for the other f_i's and g_j's. The polynomials f and g are thus monic polynomials in $\mathbf{B}[T]$ with $\mathbf{B} = \mathbb{Z}[f_1, \ldots, f_n, g_1, \ldots, g_m]$, and $\mathbf{A} = \mathbb{Z}[h_1, \ldots, h_p]$.

Assume without loss of generality that $\mathbf{B} \subseteq \mathbf{C} = \mathbb{Z}[x_1, \ldots, x_n, y_1, \ldots, y_m]$, where each x_i and $y_j = x_{n+j}$ are indeterminates, the f_i's are the elementary symmetric polynomials in the x_i's, and the g_j's are the elementary symmetric polynomials in the y_j's (apply Corollary 1.6 twice). If we attribute to x_i and y_j a weight of 1, the $z_{k,\ell}$ and h_r are homogeneous and we obtain the weights described in *2a*. To compute an integral dependence relation for $f_i g_j$ (with eventually i or $j = 0$) over $\mathbf{A}$, consider the subgroup $H_{i,j}$ of S_p formed by the σ's which satisfy $\sigma(f_i g_j) = f_i g_j$ (this subgroup contains at least all the permutations which stabilises $[\![1..n]\!]$). Then consider the polynomial

$$P_{i,j}(T) = \prod\nolimits_{\tau \in \mathrm{S}_p / H_{i,j}} \big(T - \tau(f_i g_j)\big), \tag{$*$}$$

where $\tau \in \mathrm{S}_p / H_{i,j}$ means that we take exactly one τ from each left coset of $H_{i,j}$. Then, $P_{i,j}$ is homogeneous for the weights w_a described in *2a* (i, j being fixed, we denote by w_a the weights *2a*, with $w_a(T) = w_a(z_{i,j})$). Moreover, $P_{i,j}$ is symmetric in the x_k's ($k \in [\![1..p]\!]$). It is therefore uniquely expressible as a polynomial $Q_{i,j}(\underline{h}, T)$ in each h_r and T, and $Q_{i,j}$ is w_a-homogeneous (Theorem 1.5 items *1* and *2a*). The degree in T of $Q_{i,j}$ is $d_{i,j} = (\mathrm{S}_p : H_{i,j})$. For $R \in \mathbf{C}[T]$, denote by $\delta(R)$ the integer $\deg_{x_1}(R) + \deg_T(R)$. We see that δ is a weight, and that $\delta(f_i g_j) = w(f_i g_j) \leqslant 1$, $\delta(h_r) = w(h_r) \leqslant 1$ (with $w(h_r) = 1$ if i, j, $r \geqslant 1$). Moreover, each factor of $P_{i,j}$ in $(*)$ is of weight 1 (but not necessarily homogeneous because we can have $\delta(\sigma(f_i g_j)) = 0$). This gives $\delta(Q_{i,j}) = d_{i,j}$ when the polynomial is evaluated in $\mathbf{C}[T]$. Moreover, by Theorem 1.5 item *2b*, when we write a symmetric polynomial in $(x_1, \ldots, x_p)$, say $S(\underline{x})$, as a polynomial $S_1(\underline{h})$ in the h_i's, we have $\delta(S) = w(S_1)$. Thus $w(Q_{i,j}) = d_{i,j}$.

To treat item *2* itself it suffices to "homogenize." Indeed, if we let $\widetilde{f_i} = f_i / f_0$ and $\widetilde{g_j} = g_j / g_0$, which is legitimized by Corollary 1.7, for $\widetilde{f_i}$ and $\widetilde{g_j}$ we return to the previous situation with regard to the weights *2a*. We obtain a homogeneous integral dependence relation for $\widetilde{z}_{i,j} = \widetilde{f_i}\widetilde{g_j}$ over the subring generated by the $\widetilde{h}_r$

$$Q_{i,j}(\widetilde{h}_1, \ldots, \widetilde{h}_p, \widetilde{z}_{i,j}) = 0,$$

with $\widetilde{z}_{i,j} = f_i g_j / h_0$ and $\widetilde{h}_r = h_r / h_0$.

We multiply the algebraic identity obtained by $h_0^{d_{i,j}}$ so that we obtain a monic polynomial in $z_{i,j}$.

All the denominators have vanished because $w(Q_{i,j}) = d_{i,j}$. We obtain

$$R_{i,j}(h_0, \dots, h_p, f_i g_j) = 0,$$

where $R_{i,j}(h_0, \dots, h_p, T)$ is unitary in T and homogeneous for the weights w_a and w.

What remains is the question of the homogeneity for the weights w_b in *2b*: it suffices to note that we have for all $R \in \mathbf{A}[T]$ the equality $w_a(R) + w_b(R) = pw(R)$. □

Example. In the case where $m = n = 2$, the indicated computation gives the following results.

When $f_0 = g_0 = 1$ the coefficient g_1 annihilates the polynomial

$$\begin{aligned} p_{01}(t) \;=\; & t^6 - 3h_1 t^5 + (3h_1^2 + 2h_2)\, t^4 + (-h_1^3 - 4h_1 h_2)\, t^3 + \\ & (2h_1^2 h_2 + h_1 h_3 + h_2^2 - 4h_4)\, t^2 + (-h_1^2 h_3 - h_1 h_2^2 + 4h_1 h_4)\, t \\ & -h_1^2 h_4 + h_1 h_2 h_3 - h_3^2\,, \end{aligned}$$

so in the general case $f_0 g_1$ annihilates the polynomial

$$\begin{aligned} q_{01}(t) \;=\; & t^6 - 3h_1 t^5 + (3h_1^2 + 2h_0 h_2)\, t^4 + (-h_1^3 - 4h_0 h_1 h_2)\, t^3 + \\ & (2h_0 h_1^2 h_2 + h_0^2 h_1 h_3 + h_0^2 h_2^2 - 4h_0^3 h_4)\, t^2 + \\ & (-h_0^2 h_1^2 h_3 - h_0^2 h_1 h_2^2 + 4h_0^3 h_1 h_4)\, t - h_0^3 h_1^2 h_4 + h_0^3 h_1 h_2 h_3 - h_0^4 h_3^2\,. \end{aligned}$$

When $f_0 = g_0 = 1$ the coefficient g_2 annihilates the polynomial

$$\begin{aligned} p_{02}(t) \;=\; & t^6 - h_2 t^5 + (h_1 h_3 - h_4)\, t^4 + (-h_1^2 h_4 + 2h_2 h_4 - h_3^2)\, t^3 + \\ & (h_1 h_3 h_4 - h_4^2)\, t^2 - h_2 h_4^2\, t + h_4^3\,, \end{aligned}$$

so $f_0 g_2$ annihilates the polynomial

$$\begin{aligned} q_{02}(t) \;=\; & t^6 - h_2 t^5 + (h_1 h_3 - h_0 h_4)\, t^4 + (-h_1^2 h_4 + 2h_0 h_2 h_4 - h_0 h_3^2)\, t^3 + \\ & (h_0 h_1 h_3 h_4 - h_0^2 h_4^2)\, t^2 - h_0^2 h_2 h_4^2\, t + h_0^3 h_4^3\,. \end{aligned}$$

When $f_0 = g_0 = 1$ the coefficient $f_1 g_1$ annihilates the polynomial

$$p_{11}(t) \;=\; t^3 - 2h_2 t^2 + (h_1 h_3 + h_2^2 - 4h_4)\, t + h_1^2 h_4 - h_1 h_2 h_3 + h_3^2\,.$$

When $f_0 = g_0 = 1$ the coefficient $f_1 g_2$ annihilates the polynomial

$$\begin{aligned} p_{12}(t) \;=\; & t^6 - 3h_3 t^5 + (2h_2 h_4 + 3h_3^2)\, t^4 + (-4h_2 h_3 h_4 - h_3^3)\, t^3 + \\ & (h_1 h_3 h_4^2 + h_2^2 h_4^2 + 2h_2 h_3^2 h_4 - 4h_4^3)\, t^2 + \\ & (-h_1 h_3^2 h_4^2 - h_2^2 h_3 h_4^2 + 4h_3 h_4^3)\, t - h_1^2 h_4^4 + h_1 h_2 h_3 h_4^3 - h_3^2 h_4^3\,. \end{aligned}$$

3.4. Corollary. (Multivariate Kronecker's Theorem)
In $\mathbf{B}[X_1, \dots, X_k]$ *consider the polynomials*

$$f = \textstyle\sum_\alpha f_\alpha X^\alpha, \quad g = \sum_\beta b_\beta X^\beta \quad \textit{and} \quad h = fg = \sum_\gamma h_\gamma X^\gamma,$$

(here, α*,* β*,* γ *are multi-indices, and if* $\alpha = (\alpha_1, \dots, \alpha_k)$*,* X^α *is a notation for* $X_1^{\alpha_1} \cdots X_k^{\alpha_k}$*). Let* $\mathbf{A} = \mathbf{Z}[(h_\gamma)]$ *be the subring generated by the coefficients of* h *(*$\mathbf{Z}$ *is the subring of* $\mathbf{B}$ *generated by* $1_\mathbf{B}$*). Then, each* $f_\alpha g_\beta$ *is integral over* $\mathbf{A}$*.*

D We apply what is termed *Kronecker's trick*: let $X_j = T^{n^j}$ with large enough n. This transforms f, g and h into polynomials $F(T)$, $G(T)$, $H(T)$ whose coefficients are those of f, g and h, respectively. □

4. The universal splitting algebra for a monic polynomial over a commutative ring (1)

Disclaimer. In a context where we manipulate algebras, it is sometimes preferable to keep to the intuition that we want to have a field as the base ring, even if it is only a commutative ring. In which case we choose to give a name such as $\mathbf{k}$ to the base ring. This is what we are going to do in this section dedicated to the universal splitting algebra.
When we are truly dealing with a discrete field, we will use $\mathbf{K}$ instead.

We now proceed to the inverse operation to that which passes from the polynomial ring to the subring of symmetric polynomials.
In the presence of a monic polynomial $f = T^n + \sum_{k=1}^n (-1)^k s_k T^{n-k} \in \mathbf{k}[T]$ over a ring $\mathbf{k}$, we want to have at our disposal an extension of $\mathbf{k}$ where the polynomial is decomposed into linear factors. Such an extension can be constructed in a purely formal way. The result is called the universal splitting algebra.

4.1. Definition and notation. Let $f = T^n + \sum_{k=1}^n (-1)^k s_k T^{n-k} \in \mathbf{k}[T]$ be a monic polynomial of degree n. We denote by $\mathrm{Adu}_{\mathbf{k},f}$ the *universal splitting algebra of* f *over* $\mathbf{k}$ defined as follows

$$\mathrm{Adu}_{\mathbf{k},f} = \mathbf{k}[X_1, \dots, X_n]/\mathcal{J}(f) = \mathbf{k}[x_1, \dots, x_n],$$

where $\mathcal{J}(f)$ is the *ideal of symmetric relators* necessary to identify $\prod_{i=1}^n (T - x_i)$ with $f(T)$ in the quotient. Precisely, if S_1, S_2, …, S_n are the elementary symmetric functions of the X_i's, the ideal $\mathcal{J}(f)$ is given by

$$\mathcal{J}(f) = \langle S_1 - s_1,\ S_2 - s_2, \dots,\ S_n - s_n \rangle\,.$$

The universal splitting algebra $\mathbf{A} = \mathrm{Adu}_{\mathbf{k},f}$ can be characterized by the following property.

4.2. Fact. (Universal decomposition algebra, characteristic property)

1. *Let* $\mathbf{C}$ *be a* $\mathbf{k}$*-algebra such that* $f(T)$ *is decomposed into a product of factors* $T - z_i$*. Then, there exists a unique homomorphism of* $\mathbf{k}$*-algebras of* $\mathbf{A}$ *to* $\mathbf{C}$ *which sends the* x_i*'s to the* z_i*'s.*
2. *This characterizes the universal splitting algebra* $\mathbf{A} = \mathrm{Adu}_{\mathbf{k},f}$*, up to unique isomorphism.*
3. *Moreover, if* $\mathbf{C}$ *is generated (as a* $\mathbf{k}$*-algebra) by the* z_i*'s, the universal splitting algebra is isomorphic to a quotient of* $\mathbf{A}$*.*

D For item *1* we use Proposition 1.2, which describes the algebras of polynomials as algebras freely generated by the indeterminates, and Fact II-1.1, which describes the quotient rings as those which allow us to uniquely factorize certain homomorphisms. Item *2* results from the ascertainment that an object that solves a universal problem is alway unique up to unique isomorphism. □

By taking $\mathbf{C} = \mathbf{A}$ we obtain that every permutation of $\{1, \dots, n\}$ produces a (unique) $\mathbf{k}$-automorphism of $\mathbf{A}$.

Stated otherwise: the group S_n of permutations of $\{X_1, \dots, X_n\}$ acts on $\mathbf{k}[X_1, \dots, X_n]$ and fixes the ideal $\mathcal{J}(f)$, thus the action passes to the quotient and this defines S_n as a group of automorphisms of the universal splitting algebra.

To study the universal splitting algebra we introduce *Cauchy modules* which are the following polynomials:

$$\begin{aligned}
f_1(X_1) &= f(X_1)\\
f_2(X_1, X_2) &= \big(f_1(X_1) - f_1(X_2)\big)\big/(X_1 - X_2)\\
&\ \vdots\\
f_{k+1}(X_1, \dots, X_{k+1}) &= \frac{f_k(X_1, \dots, X_{k-1}, X_k) - f_k(X_1, \dots, X_{k-1}, X_{k+1})}{X_k - X_{k+1}}\\
&\ \vdots\\
f_n(X_1, \dots, X_n) &= \frac{f_{n-1}(X_1, \dots, X_{n-2}, X_{n-1}) - f_{n-1}(X_1, \dots, X_{n-2}, X_n)}{X_{n-1} - X_n}.
\end{aligned}$$

The following fact results from the characteristic property of the universal splitting algebras.

4.3. Fact. *With the previous notations for the Cauchy modules, let* $\mathbf{k}_1 = \mathbf{k}[x_1]$ *and* $g_2(T) = f_2(x_1, T)$*. Then, the canonical* $\mathbf{k}_1$*-linear map* $\mathrm{Adu}_{\mathbf{k},f} \to \mathrm{Adu}_{\mathbf{k}_1,g_2}$ *(which sends each* x_i *(*$i \geqslant 2$*) of* $\mathrm{Adu}_{\mathbf{k},f}$ *to the* x_i*'s of* $\mathrm{Adu}_{\mathbf{k}_1,g_2}$*) is an isomorphism.*

Examples. (Cauchy modules)
With $n = 4$,

$$\begin{aligned}
f_1(x) &= x^4 - s_1x^3 + s_2x^2 - s_3x + s_4 \\
f_2(x,y) &= (y^3 + y^2x + yx^2 + x^3) - s_1(y^2 + yx + x^2) + s_2(y + x) - s_3 \\
&= y^3 + y^2(x - s_1) + y(x^2 - s_1x + s_2) + (x^3 - s_1x^2 + s_2x - s_3) \\
f_3(x,y,z) &= (z^2 + y^2 + x^2 + zy + zx + yx) - s_1(z + y + x) + s_2 \\
&= z^2 + z(y + x - s_1) + \big((y^2 + yx + x^2) - s_1(y + x) + s_2\big) \\
f_4(x,y,z,t) &= t + z + y + x - s_1.
\end{aligned}$$

For $f(T) = T^6$,

$$\begin{aligned}
f_2(x,y) &= y^5 + y^4x + y^3x^2 + y^2x^3 + yx^4 + x^5 \\
f_3(x,y,z) &= (z^4 + y^4 + x^4) + (z^2y^2 + z^2x^2 + y^2x^2) + \\
&\quad (zy^3 + zx^3 + yz^3 + yx^3 + xz^3 + xy^3) + \\
&\quad (zyx^2 + zxy^2 + yxz^2) \\
f_4(x,y,z,t) &= (t^3 + z^3 + y^3 + x^3) + (tzy + tyx + tzx + zyx) + \\
&\quad t^2(z + y + x) + z^2(t + y + x) + \\
&\quad y^2(t + z + x) + x^2(t + z + y) \\
f_5(x,y,z,t,u) &= (u^2 + t^2 + z^2 + y^2 + x^2) + \\
&\quad (xu + xt + xz + xy + tu + zu + zt + yu + yt + yz) \\
f_6(x,y,z,t,u,v) &= v + u + t + z + y + x.
\end{aligned}$$

More generally, for $f(T) = T^n$, $f_k(t_1, \dots, t_k)$ is the sum of all the monomials of degree $n + 1 - k$ in $t_1, \dots, t_k$.
By linearity, this allows us to obtain an explicit, precise description of the Cauchy modules for an arbitrary polynomial. ■

By the remark following the last example, the polynomial f_i is symmetric in the variables X_1, …, X_i, monic in X_i, of total degree $n - i + 1$.

Fact 4.2 implies that the ideal $\mathcal{J}(f)$ is equal to the ideal generated by the Cauchy modules. Indeed, the quotient ring by the latter ideal clearly realizes the same universal property as the quotient ring by $\mathcal{J}(f)$.

Thus the universal splitting algebra is a free **k**-module of rank $n!$. More precisely, we obtain the following result.

4.4. Fact. *The* **k**-*module* $\mathbf{A} = \mathrm{Adu}_{\mathbf{k},f}$ *is free and a basis is formed by the "monomials" $x_1^{d_1} \cdots x_{n-1}^{d_{n-1}}$ such that for $k = 1, \dots, n-1$ we have $d_k \leqslant n - k$.*

4.5. Corollary. *Considering the universal splitting algebra of the generic monic polynomial $f(T) = T^n + \sum_{k=1}^{n}(-1)^k S_k T^{n-k}$, where the S_i's are indeterminates, we get an algebra of polynomials $\mathbf{k}[x_1, \dots, x_n]$ with each S_i identifiable with elementary symmetric polynomials in each x_i.*

Comment. (For those who know Gröbner bases)
In the case where **k** is a discrete field, the Cauchy modules can be seen as a Gröbner basis of the ideal $\mathcal{J}(f)$, for the lexicographic monomial order with $X_1 < X_2 < \cdots < X_n$.

In fact, even if $\mathbf{k}$ is not a discrete field, the Cauchy modules still work as a Gröbner basis: Every polynomial in the x_i's can be re-expressed over the previous monomial basis by successive divisions by the Cauchy modules. We first divide by f_n with respect to the variable X_n, which cancels it out. Next we divide by f_{n-1} with respect to the variable X_{n-1}, which brings it to a degree $\leqslant 1$, and so on. ■

5. Discriminant, diagonalization

Definition of the discriminant of a monic polynomial

We define the *discriminant* of a univariate monic polynomial f over a commutative ring $\mathbf{A}$ starting with the case where f is the generic monic polynomial of degree n:

$$f(T)=T^n-S_1T^{n-1}+S_2T^{n-2}+\cdots+(-1)^nS_n\in\mathbb{Z}[S_1,\ldots,S_n][T]=\mathbb{Z}[\underline{S}][T].$$

We can write $f(T)=\prod_i(T-X_i)$ in $\mathbb{Z}[X_1,\ldots,X_n]$ (Corollary 1.6), and we set

$$\operatorname{disc}_T(f)=(-1)^{n(n-1)/2}\prod\nolimits_{i=1}^{n}f'(X_i)=\prod\nolimits_{1\leqslant i<j\leqslant n}(X_i-X_j)^2. \quad (1)$$

As this polynomial in the X_i's is clearly variable permutation invariant, there exists a unique polynomial in the S_i's, $D_n(S_1,\ldots,S_n)\in\mathbb{Z}[\underline{S}]$, which is equal to $\operatorname{disc}_T(f)$. In short, the auxiliary variables X_i can indeed vanish.

Then, for a "concrete" polynomial

$$g(T)=T^n-s_1T^{n-1}+s_2T^{n-2}+\cdots+(-1)^ns_n\in\mathbf{A}[T],$$

we define $\operatorname{disc}_T(g)=D_n(s_1,\ldots,s_n)$.

Naturally, if it happens that $g(T)=\prod_{i=1}^{n}(T-b_i)$ in a ring $\mathbf{B}\supseteq\mathbf{A}$, we would then obtain $\operatorname{disc}_T(g)=\prod_{1\leqslant i<j\leqslant n}(b_i-b_j)^2$ by evaluating the formula (1). In particular, by using the universal splitting algebra we could directly define the discriminant by this formula.

A monic polynomial is said to be *separable* when its discriminant is invertible.

Diagonalization of the matrices on a ring

Let us first recall that if $f\in\mathbf{A}[T]$, a *zero of f in an $\mathbf{A}$-algebra* $\mathbf{B}$ (given by a homomorphism $\varphi:\mathbf{A}\to\mathbf{B}$) is a $y\in\mathbf{B}$ which annihilates the polynomial f^{φ}, the image of f in $\mathbf{B}[T]$.

In addition, the zero y is said to be *simple* if $f'(y)\in\mathbf{B}^{\times}$ (we also say that it is a *simple root* of f).

Here, we are interested in the diagonalizations of matrices on an arbitrary commutative ring, when the characteristic polynomial is *separable*.

First of all, we have the classical “Kernels’ Lemma” II-4.8.
Next is a generalization of the theorem which states (in the discrete field case) that a simple zero of the characteristic polynomial defines a proper subspace of dimension 1.

5.1. Lemma. *Let $n \geqslant 2$, $a \in \mathbf{A}$ and $A \in \mathbb{M}_n(\mathbf{A})$ be a matrix whose characteristic polynomial $f(X) = \mathrm{C}_A(X)$ admits a as simple zero. Let $g = f/(X-a)$, $h = X - a$, $K = \mathrm{Ker}\, h(A)$ and $I = \mathrm{Im}\, h(A)$.*

1. *We have $K = \mathrm{Im}\, g(A)$, $I = \mathrm{Ker}\, g(A)$ and $\mathbf{A}^n = I \oplus K$.*
2. *The matrix $g(A)$ is of rank 1, and $h(A)$ of rank $n-1$.*
3. *If a polynomial $R(X)$ annihilates A, then $R(a) = 0$, i.e. R is a multiple of $X - a$.*
4. *The principal minors of order $n-1$ of $A - a\mathrm{I}_n$ are comaximal. We localize by inverting such a minor, the matrix $g(A)$ becomes simple of rank 1, the modules I and K become free of rank $n-1$ and 1.*

D Suppose without loss of generality that $a = 0$.
Then, $f(X) = Xg(X)$, $h(A) = A$, $g(A) = \pm\widetilde{A}$, $\mathrm{Tr}\,\big(g(A)\big) = g(0)$ (Lemma 1.4 item *6*), and $g(0) = f'(0) \in \mathbf{A}^\times$.

1. We write $g(X) = Xk(X) + g(0)$. This shows that the polynomials $g(X)$ and X are comaximal. Given the Cayley-Hamilton Theorem, the Kernels’ Lemma applies and gives item *1.*

2. Let μ_1, …, μ_n be the principal minors of order $n-1$ of A.
Since $g(A) = \pm\widetilde{A}$, we get $g(0) = \mathrm{Tr}\,\big(g(A)\big) = \pm\,\mathrm{Tr}\,\widetilde{A} = \pm\sum_i \mu_i$. This shows that $\mathrm{rk}\,\big(h(A)\big) = n-1$ and $\mathrm{rk}\,\big(g(A)\big) \geqslant 1$. Finally, we know that $\mathrm{rk}(\widetilde{A}) \leqslant 1$ by Lemma 1.4 item *8.*.

3. Suppose $R(A) = 0$. By multiplying by $\widetilde{A}$, we obtain $R(0)\widetilde{A} = 0$ (since $\widetilde{A}A = 0$). By taking the trace, $R(0)\,\mathrm{Tr}(\widetilde{A}) = 0$ thus $R(0) = 0$.
Note that item *3* also results from item *4*.

4. We have already seen that the μ_i’s are comaximal. After localization at some μ_i, the matrix $g(A)$ becomes simple of rank 1 under the freeness lemma page 45. Therefore I and K become free of rank $n-1$ and 1. □

5.2. Proposition. (Diagonalization of a matrix whose characteristic polynomial is separable) *Let $A \in \mathbb{M}_n(\mathbf{A})$ be a matrix whose characteristic polynomial $\mathrm{C}_A(X)$ is separable, and $\mathbf{A}_1 \supseteq \mathbf{A}$ be a ring on which we can write $\mathrm{C}_A(X) = \prod_{i=1}^n (X - x_i)$ (for example, $\mathbf{A}_1 = \mathrm{Adu}_{\mathbf{A},f}$).*
Let $K_i = \mathrm{Ker}(A - x_i\mathrm{I}_n) \subseteq \mathbf{A}_1^n$.

1. *$\mathbf{A}_1^n = \bigoplus_i K_i$.*
2. *Each K_i is the image of a matrix of rank 1.*
3. *Every polynomial R which annihilates A is a multiple of C_A.*

4. After localization at comaximal elements of $\mathbf{A}_1$ *the matrix is diagonalizable, similar to* $\mathrm{Diag}(x_1, \dots, x_n)$.

NB: if $\alpha \in \mathrm{End}_{\mathbf{A}_1}(\mathbf{A}_1^n)$ has for matrix A, we have $\alpha|_{K_i} = x_i \,\mathrm{Id}_{K_i}$ for each i.

D This is an immediate consequence of the Kernels' Lemma and Lemma 5.1. To render the matrix diagonalizable it suffices to invert some product $\nu_1 \cdots \nu_n$ where each ν_i is a principal minor of order $n-1$ of the matrix $A - x_i \mathrm{I}_n$ (which a priori makes n^n comaximal localizations). □

Remark. An analogous result concerning a matrix that annihilates a separable polynomial $\prod_i (X - x_i)$ is given in Exercise X-4. The proof is elementary. ■

The generic matrix is diagonalizable

Consider n^2 indeterminates $(a_{i,j})_{i,j \in [\![1..n]\!]}$ and let A be the corresponding matrix (it has coefficients in $\mathbf{A} = \mathbb{Z}[(a_{i,j})]$).

5.3. Proposition. *The generic matrix* A *is diagonalizable over a ring* $\mathbf{B}$ *containing* $\mathbb{Z}[(a_{i,j})] = \mathbf{A}$.

D Let $f(T) = T^n - s_1 T^{n-1} + \cdots + (-1)^n s_n$ be the characteristic polynomial of A. Then the coefficients s_i are algebraically independent over $\mathbb{Z}$. To realize this, it suffices to specialize A as the companion matrix of a generic monic polynomial.
In particular, the discriminant $\Delta = \mathrm{disc}(f)$ is nonzero in the integral ring $\mathbf{A}$. Then consider the ring $\mathbf{A}_1 = \mathbf{A}[1/\Delta] \supseteq \mathbf{A}$ and the universal splitting algebra $\mathbf{C} = \mathrm{Adu}_{\mathbf{A}_1,f}$. Let the x_i be the elements of $\mathbf{C}$ such that $f(T) = \prod_i (T - x_i)$. Finally, apply Proposition 5.2. If we want to obtain a diagonalizable matrix, we invert for instance $a = \prod_i \det\big((A - x_i \mathrm{I}_n)_{1..n-1,1..n-1}\big)$. This is an element of $\mathbf{A}$ and it suffices to convince ourselves that it is nonzero by exhibiting a particular matrix, for example the companion matrix of the polynomial $X^n - 1$.
Ultimately, consider $\mathbf{A}_2 = \mathbf{A}[1/(a\Delta)] \supseteq \mathbf{A}$ and take $\mathbf{B} = \mathrm{Adu}_{\mathbf{A}_2,f} \supseteq \mathbf{A}_2$.□

The strength of the previous result, "which makes life considerably easier" is illustrated in the following two subsections.

An identity concerning characteristic polynomials

5.4. Proposition. *Let* A *and* $B \in \mathbb{M}_n(\mathbf{A})$ *be two matrices which have the same characteristic polynomial, and let* $g \in \mathbf{A}[T]$. *Then the matrices* $g(A)$ *and* $g(B)$ *have the same characteristic polynomial.*

5.5. Corollary.

1. *If A is a matrix with characteristic polynomial f, and if we can write $f(T) = \prod_{i=1}^{n}(T - x_i)$ on a ring $\mathbf{A}_1 \supseteq \mathbf{A}$, then the characteristic polynomial of $g(A)$ is equal to the product $\prod_{i=1}^{n} \big(T - g(x_i)\big)$.*

2. *Let $\mathbf{B}$ be a free $\mathbf{A}$-algebra of finite rank n and $x \in \mathbf{B}$. Suppose that in $\mathbf{B}_1 \supseteq \mathbf{B}$, we have $\mathrm{C}_{\mathbf{B}/\mathbf{A}}(x)(T) = \prod_{i=1}^{n}(T - x_i)$. Then, for all $g \in \mathbf{A}[T]$, we have the following equalities.*

$$\mathbf{B}/\mathbf{A}\big(g(x)\big)(T) = \prod\nolimits_{i=1}^{n} \big(T - g(x_i)\big),$$

$$\mathrm{Tr}_{\mathbf{B}/\mathbf{A}}\big(g(x)\big) = \textstyle\sum_{i=1}^{n} g(x_i) \text{ and } \mathrm{N}_{\mathbf{B}/\mathbf{A}}\big(g(x)\big) = \prod_{i=1}^{n} g(x_i).$$

Proof of the proposition and the corollary.
Item *1* of the corollary. Consider the matrix $\mathrm{Diag}(x_1, \ldots, x_n)$ which has the same characteristic polynomial as A and apply the proposition with the ring $\mathbf{A}_1$.
Conversely, if item *1* of the corollary is proven for $\mathbf{A}_1 = \mathrm{Adu}_{\mathbf{A},f}$, it implies Proposition 5.4 since the polynomial $\prod_{i=1}^{n} \big(T - g(x_i)\big)$ computed in $\mathrm{Adu}_{\mathbf{A},f}$ can only depend on f and g.
Now note that the structure of the statement of the corollary, item *1*, when we take $\mathbf{A}_1 = \mathrm{Adu}_{\mathbf{A},f}$, is a family of algebraic identities with the coefficients of the matrix A for indeterminates. It thus suffices to prove it for the generic matrix. However, it is diagonalizable over some overring (Proposition 5.3), and for some diagonalizable matrix the result is clear.
Finally, item *2* of the corollary is an immediate consequence of item *1*. □

An identity concerning exterior powers

The following results, analogous to Proposition 5.4 and to Corollary 5.5, can be proven by following the exact same proof sketch.

5.6. Proposition. *If φ is an endomorphism of a free $\mathbf{A}$-module of finite rank, the characteristic polynomial of $\bigwedge^k \varphi$ only depends on the integer k and on the characteristic polynomial of φ.*

5.7. Corollary. *If $A \in \mathbb{M}_n(\mathbf{A})$ is a matrix with characteristic polynomial f, and if $f(T) = \prod_{i=1}^{n}(T - x_i)$ in an overring of $\mathbf{A}$, then the characteristic polynomial of $\bigwedge^k A$ is equal to the product $\prod_{J \in \mathcal{P}_{k,n}}(T - x_J)$, where $x_J = \prod_{i \in J} x_i$.*

Tschirnhaus transformation

5.8. Definition. Let f and $g \in \mathbf{A}[T]$ with f a monic of degree p. Consider the $\mathbf{A}$-algebra $\mathbf{B} = \mathbf{A}[T]/\langle f \rangle$, which is a free $\mathbf{A}$-module of rank p. We define the *Tschirnhaus transform of f by g*, denoted by $\mathrm{Tsch}_{\mathbf{A},g}(f)$ or $\mathrm{Tsch}_g(f)$, by the equality

$$\mathrm{Tsch}_{\mathbf{A},g}(f) = \mathrm{C}_{\mathbf{B}/\mathbf{A}}(\overline{g}), \quad (\overline{g} \text{ is the class of } g \text{ in } \mathbf{B}).$$

Proposition 5.4 and Corollary 5.5 give the following result.

5.9. Proposition. *Let f and $g \in \mathbf{A}[T]$ with monic f of degree p.*

1. *If A is a matrix such that $f(T) = \mathrm{C}_A(T)$, we have*
$$\mathrm{Tsch}_g(f)(T) = \mathrm{C}_{g(A)}(T).$$
2. *If $f(T) = \prod_i (T - x_i)$ on a ring which contains $\mathbf{A}$, we have*
$$\mathrm{Tsch}_g(f)(T) = \textstyle\prod_i \big(T - g(x_i)\big),$$
in particular, with $\mathbf{B} = \mathbf{A}[T]/\langle f \rangle$ we get
$$\mathrm{N}_{\mathbf{B}/\mathbf{A}}(g) = \textstyle\prod_i g(x_i) \quad \textit{and} \quad \mathrm{Tr}_{\mathbf{B}/\mathbf{A}}(g) = \sum_i g(x_i).$$

Remark. We can also write $\mathrm{Tsch}_{\mathbf{A},g}(f)(T) = \mathrm{N}_{\mathbf{B}[T]/\mathbf{A}[T]}(T - \overline{g})$. In fact for an entirely unambiguous notation we should write $\mathrm{Tsch}(\mathbf{A}, f, g, T)$ instead of $\mathrm{Tsch}_{\mathbf{A},g}(f)$. An analogous ambiguity is also found in the notation $\mathrm{C}_{\mathbf{B}/\mathbf{A}}(g)$. ■

Computation of the Tschirnhaus transform

Recall that the matrix C of the endomorphism μ_t of multiplication by t (the class of T in $\mathbf{B}$) is called the companion matrix of f (see page 87). Then the matrix (over the same basis) of $\mu_{\overline{g}} = g(\mu_t)$ is the matrix $g(C)$. Thus $\mathrm{Tsch}_g(f)$ is the characteristic polynomial[2] of $g(C)$.

New version of the discriminant

Recall (Definition II-5.33) that when $\mathbf{C} \supseteq \mathbf{A}$ is a free $\mathbf{A}$-algebra of finite rank and $x_1, \ldots, x_k \in \mathbf{C}$, we call the determinant of the matrix $\big(\mathrm{Tr}_{\mathbf{C}/\mathbf{A}}(x_i x_j)\big)_{i,j \in [\![1..k]\!]}$ the discriminant of $(x_1, \ldots, x_k)$. We denote it by $\mathrm{disc}_{\mathbf{C}/\mathbf{A}}(x_1, \ldots, x_k)$.
Moreover, if $(x_1, \ldots, x_k)$ is an $\mathbf{A}$-basis of $\mathbf{C}$, we denote by $\mathrm{Disc}_{\mathbf{C}/\mathbf{A}}$ the multiplicative class of $\mathrm{disc}_{\mathbf{C}/\mathbf{A}}(x_1, \ldots, x_k)$ modulo the squares of $\mathbf{A}^\times$. We call it the discriminant of the extension $\mathbf{C}/\mathbf{A}$.

[2] The efficient computation of determinants and characteristic polynomials is of great interest in computer algebra. You can for example consult [Abdeljaoued & Lombardi]. Another formula we can use for the computation of the Tschirnhaus transform is $\mathrm{Tsch}_g(f) = \mathrm{Res}_X\big(f(X), T - g(X)\big)$ (see Lemma 7.3).

In this subsection, we make the link between the discriminant of free algebras of finite rank and the discriminant of monic polynomials.
Let us emphasize the remarkable character of the implication *1a* $\Rightarrow$ *1b* in the following proposition.

5.10. Proposition. (Trace-valued discriminant)
Let $\mathbf{B}$ *be a free* $\mathbf{A}$*-algebra of finite rank* n*,* $x \in \mathbf{B}$ *and* $f = \mathrm{C}_{\mathbf{B}/\mathbf{A}}(x)(T)$*. We have*

$$\mathrm{disc}(1, x, \ldots, x^{n-1}) = \mathrm{disc}(f) = (-1)^{\frac{n(n-1)}{2}} \mathrm{N}_{\mathbf{B}/\mathbf{A}}\big(f'(x)\big).$$

We say that $f'(x)$ *is the* different of x*. The following results ensue.*

1. *The following properties are equivalent.*
   a. $\mathrm{disc}(f) \in \mathbf{A}^\times$.
   b. $\mathrm{Disc}_{\mathbf{B}/\mathbf{A}} \in \mathbf{A}^\times$ *and* $(1, x, \ldots, x^{n-1})$ *is an* $\mathbf{A}$*-basis of* $\mathbf{B}$*.*
   c. $\mathrm{Disc}_{\mathbf{B}/\mathbf{A}} \in \mathbf{A}^\times$ *and* $\mathbf{B} = \mathbf{A}[x]$*.*
2. *If* $\mathrm{Disc}_{\mathbf{B}/\mathbf{A}}$ *is regular, the following properties are equivalent.*
   a. $\mathrm{Disc}_{\mathbf{B}/\mathbf{A}}$ *and* $\mathrm{disc}(f)$ *are associated elements.*
   b. $(1, x, \ldots, x^{n-1})$ *is an* $\mathbf{A}$*-basis of* $\mathbf{B}$*.*
   c. $\mathbf{B} = \mathbf{A}[x]$*.*
3. *The discriminant of a monic polynomial* $g \in \mathbf{A}[T]$ *represents (modulo the squares of* $\mathbf{A}^\times$*) the discriminant of the extension* $\mathbf{A}[T]/\langle g\rangle$ *of* $\mathbf{A}$*. We have* $\mathrm{disc}_T(g) \in \mathbf{A}^\times$ *if and only if* $\langle g(T), g'(T)\rangle = \mathbf{A}$*.*

D In an overring $\mathbf{B}'$ of $\mathbf{B}$, we can write $f(T) = (T - x_1) \cdots (T - x_n)$. For some $g \in \mathbf{A}[T]$, by applying Corollary 5.5, we obtain the equalities

$$\mathrm{Tr}_{\mathbf{B}/\mathbf{A}}\big(g(x)\big) = g(x_1) + \cdots + g(x_n) \text{ and } \mathrm{N}_{\mathbf{B}/\mathbf{A}}\big(g(x)\big) = g(x_1) \cdots g(x_n).$$

Let $M \in \mathbb{M}_n(\mathbf{A})$ be the matrix intervening in the computation of the discriminant of $(1, x, \ldots, x^{n-1})$:

$$M = \big((a_{ij})_{i,j \in [\![0..n-1]\!]}\big), \qquad a_{ij} = \mathrm{Tr}_{\mathbf{B}/\mathbf{A}}(x^{i+j}) = x_1^{i+j} + \cdots + x_n^{i+j}\,.$$

Let $V \in \mathbb{M}_n(\mathbf{B}')$ be the Vandermonde matrix having $[\, x_1^i \; \ldots \; x_n^i \,]$ (where $i \in [\![0..n-1]\!]$) for rows. Then $M = V\,{}^{\mathrm{t}}V$. We deduce

$$\det(M) = \det(V)^2 = \textstyle\prod_{i<j}(x_i - x_j)^2 = \mathrm{disc}(f)\,.$$

This proves the first equality. Since $\mathrm{N}_{\mathbf{B}/\mathbf{A}}\big(f'(x)\big) = f'(x_1) \cdots f'(x_n)$ and $f'(x_i) = \prod_{j \mid j \neq i}(x_i - x_j)$, we get

$$\mathrm{N}_{\mathbf{B}/\mathbf{A}}\big(f'(x)\big) = \textstyle\prod_{(i,j) \mid j \neq i}(x_i - x_j) = (-1)^{\frac{n(n-1)}{2}} \prod_{i<j}(x_i - x_j)^2.$$

The proof of the consequences is left to the reader (use Proposition II-5.33).□

Discriminant of a universal splitting algebra

The equality of the "trace-valued" discriminant and the "polynomial" discriminant, together with the transitivity formula (Theorem II-5.36), allows us to complete the following computation.

5.11. Fact. (Discriminant of a universal splitting algebra)
Let f be a monic polynomial of degree $n \geqslant 2$ of $\mathbf{k}[T]$ and $\mathbf{A} = \mathrm{Adu}_{\mathbf{k},f}$. Then $\mathrm{Disc}_{\mathbf{A}/\mathbf{k}} = \big(\mathrm{disc}_T(f)\big)^{n!/2}$.

D We use the notations of Section 4. We reason by induction on n, the $n = 2$ case being clear. We have $\mathbf{A} = \mathbf{k}_1[x_2, \ldots, x_n]$ with

$$\mathbf{k}_1 = \mathbf{k}[x_1] \simeq \mathbf{k}[X_1]/\langle f(X_1)\rangle\,.$$

Moreover, $\mathbf{A} \simeq \mathrm{Adu}_{\mathbf{k}_1,g_2}$ where

$$g_2(T) = f_2(x_1, T) = \big(f(T) - f(x_1)\big)\big/(T - x_1) \in \mathbf{k}_1[T] \subseteq \mathbf{A}[T].$$

The transitivity formula of the discriminants then gives the following equalities.

$$\mathrm{Disc}_{\mathbf{A}/\mathbf{k}} = \mathrm{Disc}_{\mathbf{k}_1/\mathbf{k}}^{[\mathbf{A}:\mathbf{k}_1]}\ \mathrm{N}_{\mathbf{k}_1/\mathbf{k}}(\mathrm{Disc}_{\mathbf{A}/\mathbf{k}_1}) = (\mathrm{disc}\, f)^{(n-1)!}\ \mathrm{N}_{\mathbf{k}_1/\mathbf{k}}(\mathrm{Disc}_{\mathbf{A}/\mathbf{k}_1}).$$

By using the induction hypothesis we obtain the equality

$$\mathrm{Disc}_{\mathbf{A}/\mathbf{k}_1} = (\mathrm{disc}\, g_2)^{(n-1)!/2} = \big(\textstyle\prod_{2\leqslant i<j\leqslant n}(x_i - x_j)^2\big)^{(n-1)!/2}.$$

For $i \in [\![2..n]\!]$, let τ_i be the transposition $(1, i)$; for $z \in \mathbf{k}_1$, by Corollary 5.5, $\mathrm{N}_{\mathbf{k}_1/\mathbf{k}}(z) = z \prod_{i=2}^{n} \tau_i(z)$. Applied to $z = \prod_{2\leqslant i<j\leqslant n}(x_i - x_j)^2$, this gives

$$\mathrm{N}_{\mathbf{k}_1/\mathbf{k}}(z) = (\mathrm{disc}\, f)^{n-2},\ \text{ whence }\ \mathrm{N}_{\mathbf{k}_1/\mathbf{k}}(\mathrm{Disc}_{\mathbf{A}/\mathbf{k}_1}) = (\mathrm{disc}\, f)^{(n-2)\cdot(n-1)!/2},$$

then

$$\mathrm{Disc}_{\mathbf{A}/\mathbf{k}} = (\mathrm{disc}\, f)^{(n-1)!+(n-2)\cdot(n-1)!/2} = (\mathrm{disc}\, f)^{n!/2}.$$

NB: a detailed examination of the previous computation shows that in fact we have computed the discriminant of the "canonical" basis of the universal splitting algebra described in Fact 4.4. □

5.12. Lemma. *(Same assumptions as for Fact 5.11) Let $z \in \mathbf{A}$.*

$$\mathrm{C}_{\mathbf{A}/\mathbf{k}}(z)(T) = \textstyle\prod_{\sigma\in \mathrm{S}_n} \big(T - \sigma(z)\big).$$

In particular, $\mathrm{Tr}_{\mathbf{A}/\mathbf{k}}(z) = \sum_{\sigma\in\mathrm{S}_n}\sigma(z)$ and $\mathrm{N}_{\mathbf{A}/\mathbf{k}}(z) = \prod_{\sigma\in\mathrm{S}_n}\sigma(z)$.

D It suffices to show the formula for the norm, because we then obtain the one for the characteristic polynomial by replacing $\mathbf{k}$ by $\mathbf{k}[T]$ (which replaces $\mathbf{A}$ by $\mathbf{A}[T]$). The formula for the norm is proven by induction on the number of variables by using Fact 4.3, the transitivity formula for the norms and Corollary 5.5. □

6. Basic Galois theory (1)

In Section 6, **K** designates a nontrivial discrete field.

Factorization and zeros

Recall that a ring is integral if every element is zero or regular.[3] A subring of an integral ring is integral. A discrete field is an integral ring. A ring **A** is integral if and only if its total ring of fractions Frac **A** is a discrete field. We say that Frac **A** is the *field of fractions*, or the *quotient field* of **A**.

6.1. Proposition. *Let* $\mathbf{A} \subseteq \mathbf{B}$ *be rings and* $f \in \mathbf{A}[T]$ *be some monic polynomial of degree* n.

1. *If* z *is a zero of* f *in* **B**, $f(T)$ *is divisible by* $T - z$ *in* $\mathbf{B}[T]$.
2. *Henceforth assume that* **B** *is integral and nontrivial.*[4] *If* $z_1, \ldots, z_k$ *are the pairwise distinct zeros of* f *in* **B**, *the polynomial* $f(T)$ *is divisible by* $\prod_{i=1}^{k}(T - z_i)$ *in* $\mathbf{B}[T]$.
3. *In addition, if* $k = n$, *then* $f(T) = \prod_{i=1}^{n}(T - z_i)$, *and the* z_i*'s are the only zeros of* f *in* **B** *and in every integral extension of* **B**.

D The proof is immediate. Certain more precise results are in Exercise 1, which is dedicated to Lagrange interpolation. □

Strictly finite algebras over a discrete field

6.2. Definition.
A **K**-algebra **A** is said to be *strictly finite* if it is a free **K**-vector space of finite dimension.

In other words, we know of a finite basis of **A** as in a **K**-vector space. In this case, for some $x \in \mathbf{A}$, the trace, the norm, the characteristic polynomial of (multiplication by) x, as well as the minimal polynomial of x over **K**, denoted by $\mathrm{Min}_{\mathbf{K},x}(T)$ or $\mathrm{Min}_x(T)$, can be computed by standard methods of the linear algebra over a discrete field. Similarly, every finite **K**-subalgebra of **A** is strictly finite and the intersection of two strictly finite subalgebras is strictly finite.

[3] The notion is discussed in more detail on page 202.

[4] We could make do without the negative assumption "nontrivial" by reading the assumption that the z_i's are "distinct" as meaning that each $z_i - z_j$ is regular.

6.3. Lemma. *Let* $\mathbf{B} \supseteq \mathbf{K}$ *be a ring integral over* $\mathbf{K}$*. The following properties are equivalent.*

1. $\mathbf{B}$ *is a discrete field.*
2. $\mathbf{B}$ *is without zerodivisors:* $xy = 0 \Rightarrow (x = 0 \text{ or } y = 0)$.
3. $\mathbf{B}$ *is connected and reduced.*

Consequently, if $\mathbf{B}$ *is a discrete field, every finite* $\mathbf{K}$*-subalgebra of* $\mathbf{B}$ *is a discrete field.*

D The implications *1* ⇒ *2* ⇒ *3* are clear.
3 ⇒ *1.* Each element $x \in \mathbf{B}$ annihilates a nonzero polynomial of $\mathbf{K}[X]$ that we can assume is of the form $X^k\big(1 - XR(X)\big)$. Then $x\big(1 - xR(x)\big)$ is nilpotent thus zero. The element $e = xR(x)$ is idempotent and $x = ex$. If $e = 0$, then $x = 0$. If $e = 1$, then x is invertible. □

6.4. Lemma. *Let* $\mathbf{K} \subseteq \mathbf{L} \subseteq \mathbf{A}$ *with* $\mathbf{A}$ *and* $\mathbf{L}$ *strictly finite over* $\mathbf{K}$*. If* $\mathbf{L}$ *is a discrete field, then* $\mathbf{A}$ *is strictly finite over* $\mathbf{L}$*.*

D Proof left to the reader (or see Fact VI-1.3 item *3*). □

If g is an irreducible polynomial of $\mathbf{K}[T]$, the quotient algebra $\mathbf{K}[T]/\langle g\rangle$ is a strictly finite discrete field over $\mathbf{K}$. In fact, as a corollary of the two previous Lemmas we get that every strictly finite extension of discrete fields is obtained by iterating this construction.

6.5. Fact. (Structure of a strictly finite extension of discrete fields)
Let $\mathbf{L} = \mathbf{K}[x_1, \ldots, x_m]$ *be a strictly finite discrete field over* $\mathbf{K}$*.*
For $k \in [\![1..m+1]\!]$*, let* $\mathbf{K}_k = \mathbf{K}[(x_i)_{i<k}]$ *and* $f_k = \mathrm{Min}_{\mathbf{K}_k, x_k}(T)$*, such that* $\mathbf{K}_1 = \mathbf{K}$*, and for* $k \in [\![1..m]\!]$*,* $\mathbf{K}_{k+1} \simeq \mathbf{K}_k[X_k]/\langle f_k(X_k)\rangle$*.*
Then, for $k < \ell$ *in* $[\![1..m+1]\!]$*, the inclusion* $\mathbf{K}_k \to \mathbf{K}_\ell$ *is a strictly finite extension of discrete fields, with*

$$[\,\mathbf{K}_\ell : \mathbf{K}_k\,] = \textstyle\prod_{k \leqslant i < \ell} [\,\mathbf{K}_{i+1} : \mathbf{K}_i\,] = \prod_{k \leqslant i < \ell} \deg_T(f_i).$$

Moreover, if $F_k \in \mathbf{K}[X_1, \ldots, X_k]$ *is a monic polynomial in* X_k *for which we have* $F_k\big((x_i)_{i<k}, X_k\big) = f_k(X_k)$*, we get, by factorization of the evaluation homomorphism, an isomorphism*

$$\mathbf{K}[X_1, \ldots, X_m]/\langle F_1, \ldots, F_m\rangle \xrightarrow{\sim} \mathbf{L}.$$

6.6. Definition. Let $g \in \mathbf{K}[T]$ be a monic polynomial, we call a discrete field $\mathbf{L}$ extension of $\mathbf{K}$ in which g can be completely decomposed and which is generated like $\mathbf{K}$-algebra by the zeros of g a *splitting field of* g *over* $\mathbf{K}$.

Note that $\mathbf{L}$ is finite over $\mathbf{K}$ but that we do not ask that $\mathbf{L}$ be strictly finite over $\mathbf{K}$ (in fact, there is no constructive proof that such a splitting field must be strictly finite over $\mathbf{K}$). This necessitates some subtleties in the following theorem.

6.7. Theorem. (Uniqueness of the splitting field in the strictly finite case) *Let $f \in \mathbf{K}[T]$ be a monic polynomial. Assume that there exists a splitting field $\mathbf{L}$ of f over $\mathbf{K}$.*

1. *Let $\mathbf{M} \supseteq \mathbf{K}$ be a strictly finite discrete field over $\mathbf{K}$, generated by $\mathbf{K}$ and some zeros of f in $\mathbf{M}$. The field $\mathbf{M}$ is isomorphic to a subfield of $\mathbf{L}$.*
2. *Assume that there exists a splitting field of f, strictly finite over $\mathbf{K}$. Then every splitting field of f over $\mathbf{K}$ is isomorphic to $\mathbf{L}$ (which is thus strictly finite over $\mathbf{K}$).*
3. *Let $\mathbf{K}_1$, $\mathbf{K}_2$ be two nontrivial discrete field, $\tau : \mathbf{K}_1 \to \mathbf{K}_2$ be an isomorphism, $f_1 \in \mathbf{K}_1[T]$ be a monic polynomial, $f_2 = f_1^\tau \in \mathbf{K}_2[T]$. If $\mathbf{L}_i$ is a strictly finite field of roots of f_i over $\mathbf{K}_i$ $(i = 1, 2)$, then τ extends to an isomorphism from $\mathbf{L}_1$ to $\mathbf{L}_2$.*

▷ We only prove item *1* in a particular case (sufficiently general). The rest is left to the reader.
We write $f(T) = \prod_{i=1}^n (T - x_i)$ in $\mathbf{L}[T]$. Also suppose that $\mathbf{M} = \mathbf{K}[y, z]$ with $y \neq z$ and $f(y) = f(z) = 0$.
We thus have in $\mathbf{M}[T]$ the equality $f(T) = (T-y)f_1(T) = (T-y)(T-z)f_2(T)$ (Proposition 6.1).
Since $f(y) = 0$, the minimal polynomial $g(Y)$ of y over $\mathbf{K}$ divides $f(Y)$ in $\mathbf{K}[Y]$. Therefore $\prod_{i=1}^n g(x_i) = 0$ in $\mathbf{L}$, which is a discrete field, and one of the x_i's, say x_1, annihilates g. Here we obtain

$$\mathbf{K}[y] \simeq \mathbf{K}[Y]/\langle g(Y) \rangle \simeq \mathbf{K}[x_1] \subseteq \mathbf{L}.$$

The discrete field $\mathbf{K}[y]$ is strictly finite over $\mathbf{K}$ and $\mathbf{M}$ is strictly finite over $\mathbf{K}[y]$ (Lemma 6.4). Then let $h \in \mathbf{K}[Y, Z]$ be a monic polynomial in Z such that $h(y, Z)$ is the minimal polynomial of z over $\mathbf{K}[y]$.
Since $f_1(z) = 0$, the polynomial $h(y, Z)$ divides $f_1(Z) = f(Z)/(Z - y)$ in $\mathbf{K}[y][Z]$, thus its image $h(x_1, Z)$ in $\mathbf{K}[x_1][Z]$ is an irreducible polynomial which divides $f(Z)/(Z - x_1)$. So $h(x_1, Z)$ admits as a zero one of the x_i's for $i \in [\![2..n]\!]$, say x_2, and $h(x_1, Z)$ is the minimal polynomial of x_2 over $\mathbf{K}[x_1]$. We thus obtain the isomorphisms

$$\mathbf{K}[y, z] \simeq \mathbf{K}[y][Z]/\langle h(y, Z) \rangle \simeq \mathbf{K}[x_1][Z]/\langle h(x_1, Z) \rangle \simeq \mathbf{K}[x_1, x_2] \subseteq \mathbf{L}.$$

Note that we also have $\mathbf{K}[y, z] \simeq \mathbf{K}[Y, Z]/\langle g(Y), h(Y, Z) \rangle$. □

Remark. A detailed inspection of the previous proof leads to the conclusion that if $\mathbf{L}$ is a strictly finite splitting field over $\mathbf{K}$, the group of $\mathbf{K}$-automorphisms of $\mathbf{L}$ is a finite group having at most $[\,\mathbf{L} : \mathbf{K}\,]$ elements. If we do not assume that $\mathbf{L}$ is strictly finite over $\mathbf{K}$, we only obtain that it is absurd to assume that this group contains more than $[\,\mathbf{L} : \mathbf{K}\,]$ elements. ■

The elementary case of Galois theory

6.8. Definition and notation. We will use the following notations when a group G operates over a set E.

— For $x \in E$, $\mathrm{St}_G(x) = \mathrm{St}(x) \overset{\mathrm{def}}{=} \{\, \sigma \in G \,|\, \sigma(x) = x \,\}$ designates the *stabilizer* of x.

— $G.x$ designates the orbit of x under G, and we write $G.x = \{x_1, \ldots, x_k\}$ as an abbreviation for: $(x_1, \ldots, x_k)$ *is an enumeration without repetition of* $G.x$*, with* $x_1 = x$.

— For $F \subseteq E$, $\mathrm{Stp}_G(F)$ or $\mathrm{Stp}(F)$ designates the pointwise stabilizer of F.

— If H is a subgroup of G,
  - we denote by $|\, G : H \,|$ the index of H in G,
  - we denote by $\mathrm{Fix}_E(H) = \mathrm{Fix}(H) = E^H$ the subset of elements fixed by H, $\{\, x \in E \,|\, \forall \sigma \in H,\ \sigma(x) = x \,\}$,
  - writing $\sigma \in G/H$ means that we take an element $\sigma \in G$ in each left coset of H in G.

When G is a finite group operating over a ring $\mathbf{B}$, for $b \in \mathbf{B}$, we write

$$\mathrm{Tr}_G(b) = \sum_{\sigma \in G} \sigma(b),\ \mathrm{N}_G(b) = \prod_{\sigma \in G} \sigma(b),\ \text{and}\ \mathrm{C}_G(b)(T) = \prod_{\sigma \in G} \big(T - \sigma(b)\big).$$

If $G.b = \{b_1, \ldots, b_k\}$, (the b_i's pairwise distinct), we write

$$\mathrm{Rv}_{G,b}(T) = \textstyle\prod_{i=1}^{k} (T - b_i).$$

This polynomial is called the *resolvent* of b (relative to G). It is clear that $\big(\mathrm{Rv}_{G,b}\big)^r = \mathrm{C}_G(b)$ with $r = \big|\, G : \mathrm{St}_G(b) \,\big|$.

Given an $\mathbf{A}$-algebra $\mathbf{B}$ we denote by $\mathrm{Aut}_{\mathbf{A}}(\mathbf{B})$ the group of $\mathbf{A}$-automorphisms of $\mathbf{B}$.

6.9. Definition. If $\mathbf{L}$ is a strictly finite extension of $\mathbf{K}$, and a splitting field for a separable monic polynomial over $\mathbf{K}$, we say that $\mathbf{L}$ is a *Galois extension* of $\mathbf{K}$, we then denote $\mathrm{Aut}_{\mathbf{K}}(\mathbf{L})$ by $\mathrm{Gal}(\mathbf{L}/\mathbf{K})$ and we say that it is the *Galois group* of the extension $\mathbf{L}/\mathbf{K}$.

Note well that in the definition of a Galois extension $\mathbf{L}/\mathbf{K}$, the fact that $\mathbf{L}$ is strictly finite (and not only finite) over $\mathbf{K}$ is implied.

6.10. Proposition and definition. (Galois correspondence)
Let $\mathbf{L} \supseteq \mathbf{K}$ *be a strictly finite field over* $\mathbf{K}$.

1. *The group* $\mathrm{Aut}_{\mathbf{K}}(\mathbf{L})$ *is a detachable subgroup of* $\mathbb{GL}_{\mathbf{K}}(\mathbf{L})$. *If* H *is a subgroup of* $\mathrm{Aut}_{\mathbf{K}}(\mathbf{L})$, *the subfield* $\mathbf{L}^H$ *is called the* fixed field of H.
2. *We call the two mappings* Fix *and* Stp *between the two following sets the* Galois correspondence. *On the one hand* $\mathcal{G} = \mathcal{G}_{\mathbf{L}/\mathbf{K}}$ *is the set of finite subgroups of* $\mathrm{Aut}_{\mathbf{K}}(\mathbf{L})$. *On the other hand* $\mathcal{K} = \mathcal{K}_{\mathbf{L}/\mathbf{K}}$ *is the set of strictly finite subextensions of* $\mathbf{L}$.

3. *In the Galois correspondence each of the two mappings is decreasing. In addition,* $H \subseteq \mathrm{Stp}(\mathbf{L}^H)$ *for all* $H \in \mathcal{G}$*,* $\mathbf{M} \subseteq \mathbf{L}^{\mathrm{Stp}(\mathbf{M})}$ *for all* $\mathbf{M} \in \mathcal{K}$*,* $\mathrm{Stp} \circ \mathrm{Fix} \circ \mathrm{Stp} = \mathrm{Stp}$ *and* $\mathrm{Fix} \circ \mathrm{Stp} \circ \mathrm{Fix} = \mathrm{Fix}$*.*

D In item *1* we have to prove that the subgroup is detachable and, in item *2*, that Fix and Stp indeed act on the two sets as described. This is based on finite dimensional linear algebra over the discrete fields. We leave the details to the reader. □

Remark. Even though we can decide if a given element of $\mathbb{GL}_{\mathbf{K}}(\mathbf{L})$ is in $\mathrm{Aut}_{\mathbf{K}}(\mathbf{L})$, and even though it is easy to bound the number of elements of $\mathrm{Aut}_{\mathbf{K}}(\mathbf{L})$, there is no sure general method to compute this number. ■

As a consequence of Theorem 6.7 we have the following corollary.

6.11. Theorem. (Isomorphism extension theorem)
Let $\mathbf{L}/\mathbf{K}$ *be a Galois extension and* $\mathbf{M}$ *be a finite* $\mathbf{K}$*-subextension of* $\mathbf{L}$*. Every* $\mathbf{K}$*-homomorphism* $\tau : \mathbf{M} \to \mathbf{L}$ *extends to an element* $\widetilde{\tau}$ *of* $\mathrm{Gal}(\mathbf{L}/\mathbf{K})$*.*

D $\mathbf{L}$ is the splitting field of a separable polynomial $g \in \mathbf{K}[T]$. We notice that since $\mathbf{L}$ is strictly finite over $\mathbf{K}$, $\mathbf{M}$ is strictly finite over $\mathbf{K}$ and $\mathbf{L}$ strictly finite over $\mathbf{M}$. Let $\mathbf{M}'$ be the image of τ. It is a strictly finite field over $\mathbf{K}$, so $\mathbf{L}$ is strictly finite over $\mathbf{M}'$. Thus $\mathbf{L}$ is a field of roots of g strictly finite over $\mathbf{M}$ and over $\mathbf{M}'$. By Theorem 6.7 (item *3*), we can extend τ to a $\mathbf{K}$-isomorphism $\widetilde{\tau} : \mathbf{L} \to \mathbf{L}$. □

When a separable polynomial over $\mathbf{K}$ has a splitting field $\mathbf{L}$ strictly finite over $\mathbf{K}$, the group $\mathrm{Gal}(\mathbf{L}/\mathbf{K})$ can also be denoted by $\mathrm{Gal}_{\mathbf{K}}(f)$ insofar as Theorem 6.7 gives the uniqueness of $\mathbf{L}$ (up to $\mathbf{K}$-automorphism).

Remark. In constructive mathematics we have the following results (trivial in classical mathematics). For some subgroup H of a finite group the following properties are equivalent.

- H is finite.
- H is finitely generated.
- H is detachable.

Similarly for some $\mathbf{K}$-linear subspace M of a finite dimensional $\mathbf{K}$-vector space the following properties are equivalent.

- M is finite dimensional.
- M is finitely generated (i.e., the image of a matrix).
- M is the kernel of a matrix. ■

6.12. Proposition and definition. (Elementary Galois situation)
Let $\mathbf{A} \subseteq \mathbf{B}$ *be two rings. An* elementary Galois situation *is defined as follows.*

i. We have a separable monic polynomial $Q \in \mathbf{A}[T]$ *of degree* d *and elements* $y_1, y_2, \ldots, y_d$ *of* $\mathbf{B}$ *such that*

$$Q(T) = \textstyle\prod_{i=1}^{d}(T - y_i).$$

ii. Let $y = y_1$. *Assume for each* i *that* $\mathbf{B} = \mathbf{A}[y_i]$ *and that* $\langle Q\rangle$ *is the kernel of the homomorphism of* $\mathbf{A}$*-algebras* $\mathbf{A}[T] \to \mathbf{B}$ *which sends* T *into* y_i *(whence* $\mathbf{B} = \mathbf{A}[y] = \mathbf{A}[y_i] \simeq \mathbf{A}[T]/\langle Q\rangle$*). For each* i *there thus exists a unique* $\mathbf{A}$*-automorphism* σ_i *of* $\mathbf{B}$ *satisfying* $\sigma_i(y) = y_i$.

iii. Assume that these automorphisms form a group, which we denote by G. *In particular,* $|G| = d = [\,\mathbf{B} : \mathbf{A}\,]$.

In the elementary Galois situation we have the following results.

1. a. $\mathrm{Fix}_{\mathbf{B}}(G) = \mathbf{A}$.
b. For all $z \in \mathbf{B}$, $\mathrm{C}_{\mathbf{B}/\mathbf{A}}(z)(T) = \mathrm{C}_G(z)(T)$.

2. Let H *be a detachable subgroup of* G, $\mathbf{A}' = \mathbf{B}^H$ *and*

$$Q_H(T) = \textstyle\prod_{\sigma\in H}\big(T - \sigma(y)\big).$$

Then, we find the elementary Galois situation with $\mathbf{A}'$, $\mathbf{B}$, Q_H *and* $\big(\sigma(y)\big)_{\sigma\in H}$. *In particular,* $\mathbf{B} = \mathbf{A}'[y]$ *is a free* $\mathbf{A}'$*-module of rank* $|H| = [\,\mathbf{B} : \mathbf{A}'\,]$. *In addition,* H *is equal to* $\mathrm{Stp}_G(\mathbf{A}')$.

D *1a.* Consider some $x = \sum_{k=0}^{d-1}\xi_k y^k$ in $\mathbf{B}$ (with each $\xi_k \in \mathbf{A}$) invariant under the action of $G = \{\sigma_1, \ldots, \sigma_d\}$.
We thus have for all $\sigma \in G$, $x = \sum_{k=0}^{d-1}\xi_k\sigma(y)^k$. If $V \in \mathbb{M}_n(\mathbf{B})$ is the Vandermonde matrix

$$V = \begin{bmatrix} 1 & y_1 & y_1^2 & \cdots & y_1^{d-1} \\ \vdots & & & & \vdots \\ \vdots & & & & \vdots \\ 1 & y_d & y_d^2 & \cdots & y_d^{d-1} \end{bmatrix},$$

we get

$$V\begin{bmatrix} \xi_0 \\ \xi_1 \\ \vdots \\ \xi_{d-1} \end{bmatrix} = \begin{bmatrix} x \\ x \\ \vdots \\ x \end{bmatrix} = V\begin{bmatrix} x \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Since $\det({}^{\mathrm{t}}VV) = \mathrm{disc}_T(Q) \in \mathbf{A}^{\times}$, we get $[\,\xi_0\ \xi_1\ \cdots\ \xi_{d-1}\,] = [\,x\ 0\ \cdots\ 0\,]$, and $x = \xi_0 \in \mathbf{A}$.
1b. Since $\mathbf{B} \simeq \mathbf{A}[T]/\langle Q\rangle$, Corollary 5.5 gives, for $g \in \mathbf{A}[Y]$ and $z = g(y_1)$,

the equalities

$$\mathrm{C}_{\mathbf{B}/\mathbf{A}}(z)(T) = \prod_i \big(T - g(y_i)\big) = \prod_{\sigma \in G} \big(T - \sigma(g(y_1))\big) = \mathrm{C}_G(z)(T).$$

2. It is clear that $\mathbf{B} = \mathbf{A}'[\sigma(y)]$ for each $\sigma \in H$ and that Q_H is a separable polynomial of $\mathbf{A}'[T]$. It remains to see that every polynomial $P \in \mathbf{A}'[T]$ which annihilates some $y_i = \sigma_i(y)$ ($\sigma_i \in H$) is a multiple of Q_H. For all $\sigma{\in}H$, since σ is an $\mathbf{A}'$-automorphism of $\mathbf{B}$, we have $P\big(\sigma(y_i)\big){=}\sigma\big(P(y_i)\big){=}0$. Thus P is divisible by each $T - \sigma(y)$, for $\sigma \in H$. As these polynomials are pairwise comaximal, P is a multiple of their product Q_H.

Finally, if $\sigma_j \in G$ is an $\mathbf{A}'$-automorphism of $\mathbf{B}$, $\sigma_j(y) = y_j$ must be a zero of Q_H. However, since Q is separable, the only y_i's that annihilate Q_H are the $\sigma(y)$'s for $\sigma \in H$. Therefore $\sigma_j \in H$. □

Remarks. 1) In the elementary Galois situation nothing states that the y_i's are the only zeros of Q in $\mathbf{B}$, nor that the σ_i's are the only $\mathbf{A}$-automorphisms of $\mathbf{B}$. Take for example $\mathbf{B} = \mathbf{K}^3$, and three distinct elements a, b, c in the discrete field $\mathbf{K}$. The polynomial $Q = (T - a)(T - b)(T - c)$ admits 27 zeros in $\mathbf{B}$, including six which have Q as minimal polynomial, which makes six $\mathbf{K}$-automorphisms of $\mathbf{B}$.

In addition, if we take $z_1 = (a, b, c)$, $z_2 = (b, a, b)$ and $z_3 = (c, c, a)$, we see that $Q = (T - z_1)(T - z_2)(T - z_3)$, which shows that the first condition does not imply the second. However, with $y_1 = (a, b, c)$, $y_2 = (b, c, a)$ and $y_3 = (c, a, b)$, we are in the elementary Galois situation.

2) Concerning condition *iii* in the definition of the elementary Galois situation, we can easily see that it is equivalent to the fact that each σ_i permutes the y_j's. This condition is not a consequence of the first two, as the following example proves. Consider the following 5×5 latin square (in each row and each column, the integers are different), which is not the table of a group

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 5 & 3 \\ 3 & 5 & 4 & 2 & 1 \\ 4 & 1 & 5 & 3 & 2 \\ 5 & 3 & 2 & 1 & 4 \end{bmatrix}.$$

Each row defines a permutation $\sigma_i \in S_5$; thus $\sigma_1 = \mathrm{Id}$, $\sigma_2 = (12453)$, …, $\sigma_5 = (154)(23)$. The σ_i's do not form a group (which would be of order 5) because σ_5 is of order 6. Let $\mathbf{B} = \mathbf{K}^5$ where $\mathbf{K}$ is a field having at least 5 elements a_1, …, a_5, $y = (a_1, \dots, a_5) \in \mathbf{B}$, $y_i = \sigma_i(y)$ and

$$Q(T) = \prod_i (T - y_i) = \prod_i (T - a_i) \in \mathbf{K}[T].$$

Then, in 6.12, the first two conditions *i*, *ii* are satisfied but not condition *iii*. Luckily things are simpler in the field case. ■

6.13. Lemma. *Let $\mathbf{L} = \mathbf{K}[y]$ be a strictly finite discrete field over $\mathbf{K}$. Let Q be the minimal polynomial of y over $\mathbf{K}$. If Q is separable and can be completely factorized in $\mathbf{L}[T]$, we find ourselves in the elementary Galois situation and the corresponding group G is the group $\mathrm{Gal}(\mathbf{L}/\mathbf{K})$ of all the $\mathbf{K}$-automorphisms of $\mathbf{L}$.*

D Let $y = y_1, \ldots, y_d$ be the zeros of Q (of degree d) in $\mathbf{L}$. Each y_i annihilates Q and Q is irreducible in $\mathbf{K}[T]$, so Q is the minimal polynomial of y_i over $\mathbf{K}$ and $\mathbf{K}[y_i]$ is a $\mathbf{K}$-linear subspace of $\mathbf{L}$, free and of same dimension d, therefore equal to $\mathbf{L}$. Finally, since $\mathbf{L}$ is integral, the y_i's are the only zeros of Q in $\mathbf{L}$, thus every $\mathbf{K}$-automorphism of $\mathbf{L}$ is some σ_i, and the σ_i's do indeed form a group: the Galois group $G = \mathrm{Gal}(\mathbf{L}/\mathbf{K})$. □

6.14. Theorem. (Galois correspondence, the elementary case)
Let $\mathbf{L} = \mathbf{K}[y]$ be a strictly finite discrete field over $\mathbf{K}$. Let Q be the minimal polynomial of y over $\mathbf{K}$. Assume that Q is separable and can be completely factorized in $\mathbf{L}[T]$. In particular, $\mathbf{L}$ is a Galois extension of $\mathbf{K}$. We have the following results.

1. *The two maps of the Galois correspondence are two reciprocal bijections.*
2. *For all $\mathbf{M} \in \mathcal{K}_{\mathbf{L}/\mathbf{K}}$, $\mathbf{L}/\mathbf{M}$ is a Galois extension of the Galois group $\mathrm{Fix}(\mathbf{M})$ and $[\,\mathbf{L} : \mathbf{M}\,] = |\mathrm{Fix}(\mathbf{M})|$.*
3. *If $H_1, H_2 \in \mathcal{G}_{\mathbf{L}/\mathbf{K}}$ and $\mathbf{M}_i = \mathrm{Fix}(H_i) \in \mathcal{K}_{\mathbf{L}/\mathbf{K}}$, then*
   - *$H_1 \cap H_2$ corresponds to the $\mathbf{K}$-subalgebra generated by $\mathbf{M}_1 \cup \mathbf{M}_2$,*
   - *$\mathbf{M}_1 \cap \mathbf{M}_2$ corresponds to the subgroup generated by $H_1 \cup H_2$.*
4. *If $H_1 \subseteq H_2$ in $\mathcal{G}_{\mathbf{L}/\mathbf{K}}$ and $\mathbf{M}_i = \mathrm{Fix}(H_i)$, then $\mathbf{M}_1 \supseteq \mathbf{M}_2$ and we have the equality $|\,H_2 : H_1\,| = [\,\mathbf{M}_1 : \mathbf{M}_2\,]$.*
5. *For all $z \in \mathbf{L}$, $\mathrm{C}_{\mathbf{L}/\mathbf{K}}(z)(T) = \mathrm{C}_{\mathrm{Gal}(\mathbf{L}/\mathbf{K})}(z)(T)$.*

D It suffices to prove the first item. By Proposition 6.12 we have the equality $\mathrm{Stp} \circ \mathrm{Fix} = \mathrm{Id}_{\mathcal{G}_{\mathbf{L}/\mathbf{K}}}$.
Now let $\mathbf{M} \in \mathcal{K}_{\mathbf{L}/\mathbf{K}}$. Since $\mathbf{L} = \mathbf{K}[y]$, we have $\mathbf{L} = \mathbf{M}[y]$. As $\mathbf{L}$ is strictly finite over $\mathbf{M}$, we can compute the minimal polynomial P of y over $\mathbf{M}$. It divides Q therefore it is separable. It can be completely factorized in $\mathbf{L}[T]$. Thus, with $\mathbf{M}$, $\mathbf{L} = \mathbf{M}[y]$ and P, we are in the assumptions of Lemma 6.13, so in the elementary Galois situation. The $\mathbf{M}$-automorphisms of $\mathbf{L}$ are $\mathbf{K}$-automorphisms thus they are exactly the elements of the stabilizer $H = \mathrm{Stp}_G(\mathbf{M})$ (where $G = \mathrm{Gal}(\mathbf{L}/\mathbf{K})$). In this situation item *1b* of Proposition 6.12 states that $\mathrm{Fix}(H) = \mathbf{M}$. □

We have just established that the Galois correspondence is bijective, i.e. the fundamental theorem of Galois theory, in the elementary case. However, it will later turn out that this case is in fact the "general" case: each time that we have a Galois extension we can reduce to the elementary situation (Theorems 6.15 and VI-1.9).

Construction of a splitting field by means of a Galois resolvent, basic Galois theory

In this subsection $f \in \mathbf{K}[T]$ is a separable monic polynomial of degree n and $\mathbf{A} = \mathrm{Adu}_{\mathbf{K},f}$ with $f(T) = \prod_i (T - x_i)$ in $\mathbf{A}$.

The aim of the current subsection is to prove the following result: if $\mathbf{K}$ is infinite, and if we know how to factorize the separable monic polynomials in $\mathbf{K}[T]$, then we know how to construct a splitting field for any arbitrary separable monic polynomial, and the obtained extension falls within the elementary framework of Theorem 6.14.

We construct the splitting field by a "uniform" method. Since it is strictly finite, Theorem 6.7 says that this splitting field is isomorphic to any other.

6.15. Theorem. *We introduce indeterminates $u_1, \ldots, u_n$. For $\sigma \in \mathrm{S}_n$ we define $u_\sigma = \sum_i u_i x_{\sigma i}$. We write*

$$R(\underline{u}, T) = \textstyle\prod_{\sigma \in \mathrm{S}_n} (T - u_\sigma) \in \mathbf{K}[\underline{u}, T],$$

and $D(\underline{u}) = \mathrm{disc}_T(R) \in \mathbf{K}[\underline{u}]$.

1. *One of the coefficients of D is equal to $\pm\,\mathrm{disc}(f)^{(n-2)!(n!-1)}$.*

In the following we assume that we specialize the u_i's to elements $a_i \in \mathbf{K}$ and that $D(\underline{a}) \neq 0$ (this is always possible if $\mathbf{K}$ is infinite).

2. *For any arbitrary $\sigma \in \mathrm{S}_n$, the element $a_\sigma = \sum_i a_i x_{\sigma i}$ admits the polynomial $R(\underline{a}, T) \in \mathbf{K}[T]$ for minimal polynomial, such that*
$$\mathbf{A} = \mathbf{K}[a_\sigma] \simeq \mathbf{K}[T]/\langle R(\underline{a}, T)\rangle\,.$$
We write $a = a_{\mathrm{Id}} = \sum_i a_i x_i$.
3. *The only elements of $\mathbf{A}$ fixed by S_n are the elements of $\mathbf{K}$.*
4. *Assume that we know how to decompose $R(\underline{a}, T)$ into a product of irreducible factors in $\mathbf{K}[T]$: $R(\underline{a}, T) = \prod_{j=1}^{\ell} Q_j$.*
   a. *If $\ell = 1$, $\mathbf{A}$ is a field, the extension $\mathbf{A}/\mathbf{K}$ is a splitting field for the polynomial f, as well as for $R(\underline{a}, T)$, and the situation pertains to Theorem 6.14. In particular, $\mathrm{Gal}(\mathbf{A}/\mathbf{K}) \simeq \mathrm{S}_n$.*
   b. *If $\ell > 1$, then $\mathbf{A} \simeq \prod_j \mathbf{K}_j$ where*
   $$\mathbf{K}_j = \mathbf{K}[\pi_j(a)] = \mathbf{A}/\langle Q_j(a)\rangle \simeq \mathbf{K}[T]/\langle Q_j\rangle\,.$$
   ($\pi_j : \mathbf{A} \to \mathbf{K}_j$ is the canonical projection.)
   Let H_j be the subgroup of S_n that stabilizes the ideal $\langle Q_j(a)\rangle_{\mathbf{A}}$. Then
      - *S_n operates transitively over the ideals $\langle Q_j(a)\rangle_{\mathbf{A}}$, so that the Q_j's all have the same degree, $|H_j| = \deg(Q_j) = [\mathbf{K}_j : \mathbf{K}]$, and the $\mathbf{K}_j$'s are pairwise isomorphic discrete fields,*
      - *the extension $\mathbf{K}_1/\mathbf{K}$ is a splitting field for f, as well as for each Q_j, and the situation pertains to Theorem 6.14, in particular, $H_1 = \mathrm{Gal}(\mathbf{K}_1/\mathbf{K})$.*

D *1.* The discriminant D equals (up to sign) the product of the $u_\sigma - u_\tau$ for $\sigma \neq \tau \in \mathrm{S}_n$. Each $u_\sigma - u_\tau$ is a sum of elements $u_i(x_{\sigma i} - x_{\tau i})$: each u_i has coefficient 0 or some $x_j - x_k$ $(j \neq k)$. The first monomial for the lexicographical order that appears in the product D is the monomial

$$u_1^{n!(n!-(n-1)!)}\, u_2^{n!\big((n-1)!-(n-2)!\big)} \cdots u_{n-1}^{n!(2!-1!)},$$

with coefficient a product of elements of the type $x_i - x_j$ $(i \neq j)$. More precisely if $\delta = \mathrm{disc}(f)$, the coefficient in question will be, up to sign,

$$\delta^{(n-2)!(n!-1)}.$$

2. We use Proposition 5.10 since $R(\underline{a}, T)$ is the characteristic polynomial of a (Lemma 5.12).
3. See item *1b* of Proposition 6.12.
4a. This is obvious.
4b. The fact that $\mathbf{A} \simeq \prod_j \mathbf{K}_j$ results from the Chinese remainder theorem. The equality $\prod_j Q_j(T) = \prod_\sigma (T - a_\sigma)$ in $\mathbf{A}[T]$ remains valid in $\mathbf{K}_1[T]$. Thus, there exists for all j some σ_j such that $Q_j\big(\pi_1(a_{\sigma_j})\big) = 0$, in other words, $Q_j(a_{\sigma_j}) \in \langle Q_1(a) \rangle_{\mathbf{A}}$. Furthermore, in $\mathbf{A}$ we have $Q_j(a_{\sigma_j}) = \sigma_j\big(Q_j(a)\big)$ because $Q_j \in \mathbf{K}[T]$. So $\sigma_j\big(\,\langle Q_j(a) \rangle_{\mathbf{A}}\,\big) \subseteq \langle Q_1(a) \rangle_{\mathbf{A}}$.
This gives us a surjection $\sigma_j : \mathbf{A}/\langle Q_j(a) \rangle \to \mathbf{A}/\langle Q_1(a) \rangle$, i.e. a surjection $\mathbf{K}[T]/\langle Q_j \rangle \to \mathbf{K}[T]/\langle Q_1 \rangle$. This results in $\deg Q_1 \leqslant \deg Q_j$, and by symmetry $\deg Q_j = \deg Q_1$, whence $\sigma_j\big(\,\langle Q_j(a) \rangle_{\mathbf{A}}\,\big) = \langle Q_1(a) \rangle_{\mathbf{A}}$.
Thus S_n operates transitively over the ideals $\langle Q_j(a) \rangle_{\mathbf{A}}$ and the $\mathbf{K}_j$'s are pairwise isomorphic. □

Remark. The construction of the splitting field suggested here is in fact more or less impractical as soon as the degree n of f is equal to or greater than 7, as it necessitates a factorization of a polynomial of degree $n!$. We propose in Chapter VII a less brutal dynamic method that has the additional advantage of not demanding to know how to factorize the separable polynomials of $\mathbf{K}[T]$. The counterpart of this absence of factorization will be that, despite knowing how to compute in "some" splitting field, a priori we will never be able to determine it in its entirety (in the sense of knowing its dimension as a $\mathbf{K}$-vector space). The same lack of precision also applies to the Galois group. ■

Example. Consider the polynomial `p(T)`$\in \mathbb{Q}[T]$ below. We ask `Magma` to randomly take some linear combination `z` from the `xi` (the zeros of `p(T)` in the universal splitting algebra $\mathbf{A} = \mathrm{Adu}_{\mathbb{Q},p}$), to compute $\mathrm{Min}_{\mathbb{Q},z}(T)$, and then to factorize it. The software efficiently gives the minimal polynomial `pm` of degree 720 and decomposes it into a product of 30 factors of degree 24 (the totality in one or two minutes). One of these factors is the polynomial `q`. As `q` is very cumbersome, we ask `Magma` to compute a Gröbner basis of the ideal generated by the Cauchy modules on the one hand, and by q(z) on the other, which provides a clearer description of the splitting field $\mathbf{A}/\langle q(z)\rangle$: x6 is annihilated by p, x5 is annihilated by a polynomial of degree 4 with coefficients in $\mathbb{Q}[x_6]$, x1, …, x4 are expressed in terms of x5 and x6. The computation of the Gröbner basis takes several hours. Magma can then compute the Galois group, which is given by two generators. Here are the results:

```
p:=T^6 - 3*T^5 + 6*T^4 - 7*T^3 + 2*T^2 + T - 1;
z:=x1 + 2*x2 + 13*x3 - 24*x4 + 35*x5 - 436*x6;
pm:=T^720 + 147240*T^719 + 10877951340*T^718 + 537614218119000*T^717 +
    19994843992714365210*T^716 + 596880113924932859498208*T^715 +
    14896247531385087685472255280*T^714 + ...
q:= T^24 + 4908*T^23 + 13278966*T^22 + 25122595960*T^21 +
    36160999067785*T^20 + 41348091425849608*T^19 +
    38304456918334801182*T^18 + 28901611463650323108996*T^17 +...
//we annihilate q(z): description of the field of roots;
Affine Algebra of rank 6 over Rational Field
Variables: x1, x2, x3, x4, x5, x6
Quotient relations:
x1 + 18/37*x5^3*x6^5 - 45/37*x5^3*x6^4 + 104/37*x5^3*x6^3 - 3*x5^3*x6^2
    + 36/37*x5^3*x6 - 1/37*x5^3 - 27/37*x5^2*x6^5 + 135/74*x5^2*x6^4 -
    156/37*x5^2*x6^3 + 9/2*x5^2*x6^2 - 54/37*x5^2*x6 + 3/74*x5^2 +
    91/37*x5*x6^5 - 455/74*x5*x6^4 + 460/37*x5*x6^3 - 25/2*x5*x6^2 +
    108/37*x5*x6 + 31/74*x5 - 41/37*x6^5 + 205/74*x6^4 - 204/37*x6^3 +
    11/2*x6^2 - 45/37*x6 - 53/74,
x2 + x6 - 1,
x3 + x5 - 1,
x4 - 18/37*x5^3*x6^5 + 45/37*x5^3*x6^4 - 104/37*x5^3*x6^3 + 3*x5^3*x6^2
    - 36/37*x5^3*x6 + 1/37*x5^3 + 27/37*x5^2*x6^5 - 135/74*x5^2*x6^4 +
    156/37*x5^2*x6^3 - 9/2*x5^2*x6^2 + 54/37*x5^2*x6 - 3/74*x5^2 -
    91/37*x5*x6^5 + 455/74*x5*x6^4 - 460/37*x5*x6^3 + 25/2*x5*x6^2 -
    108/37*x5*x6 - 31/74*x5 + 41/37*x6^5 - 205/74*x6^4 + 204/37*x6^3 -
    11/2*x6^2 + 45/37*x6 - 21/74,
x5^4 - 2*x5^3 + x5^2*x6^2 - x5^2*x6 + 4*x5^2 - x5*x6^2 + x5*x6 - 3*x5 +
     x6^4 - 2*x6^3 + 4*x6^2 - 3*x6 - 1,
x6^6 - 3*x6^5 + 6*x6^4 - 7*x6^3 + 2*x6^2 + x6 - 1
// the Galois group;
Permutation group acting on a set of cardinality 6
Order = 24 = 2^3 * 3
    (1, 4)(2, 5)(3, 6)
    (1, 2, 4, 6)
```

Note that $\mathrm{disc}_T(p) = 2^4 \times 37^3$, which is not unrelated to the denominators appearing in the Gröbner basis. We will return to this example on page 429 when discussing the dynamic method. ■

Remark. Here we interrupt our treatment of basic Galois theory. We shall resume the current thread in Sections VI-1 and VI-2, which the reader can refer to directly from here (the results of the intermediate chapters will not be used). In Chapter VII we will address a more sophisticated theory which proves to be necessary when we do not have at our disposal a factorization algorithm for the separable polynomials over the base field. ■

7. The resultant

The resultant is the basic tool of Elimination theory. This is based on the basic Elimination lemma on page 121, which is applied to arbitrary rings, and on its Corollary 7.7 for the geometric case.

Elimination theory

Elimination theory concerns the systems of polynomial equations (or *polynomial systems*).

Such a system $(f_1, \ldots, f_s)$ in $\mathbf{k}[X_1, \ldots, X_n] = \mathbf{k}[\underline{X}]$, where $\mathbf{k}$ is a discrete field, can admit some zeros in $\mathbf{k}^n$, or in $\mathbf{L}^n$, where $\mathbf{L}$ is an overfield of $\mathbf{k}$, or even an arbitrary $\mathbf{k}$-algebra. The zeros depend only on the ideal $\mathfrak{a} = \langle f_1, \ldots, f_s \rangle$ of $\mathbf{k}[\underline{X}]$ generated by the f_i's. We also call them *the zeros of the ideal* $\mathfrak{a}$.

Let $\pi : \mathbf{L}^n \to \mathbf{L}^r$ be the projection which forgets the last $n - r$ coordinates. If $V \subseteq \mathbf{L}^n$ is the set of zeros of $\mathfrak{a}$ on $\mathbf{L}$, we are interested in as precise a description as possible of the projection $W = \pi(V)$, if possible as zeros of a polynomial system in the variables $(X_1, \ldots, X_r)$.

Here intervenes in a natural way the *elimination ideal* (elimination of the variables X_{r+1}, …, X_n for the considered polynomial system), which is defined by $\mathfrak{b} = \mathfrak{a} \cap \mathbf{k}[X_1, \ldots, X_r]$. Indeed every element of W is clearly a zero of $\mathfrak{b}$.

The converse is not always true (and in any case not at all obvious), but it is true in some good cases: if $\mathbf{L}$ is an algebraically closed field and if the ideal is in a Noether position (Theorem 9.5).

A reassuring fact, and easy to establish by the considerations of linear algebra over discrete fields, is that the elimination ideal $\mathfrak{b}$ "does not depend on" the considered base field $\mathbf{k}$. More precisely, if $\mathbf{k}_1$ is an overfield of $\mathbf{k}$, we have the following results.

- The ideal $\langle f_1, \ldots, f_s \rangle_{\mathbf{k}_1[X_1,\ldots,X_n]}$ only depends on the ideal $\mathfrak{a}$: it is the ideal $\mathfrak{a}_1$ of $\mathbf{k}_1[X_1, \ldots, X_n]$ generated by $\mathfrak{a}$.
- The ideal of elimination $\mathfrak{b}_1 = \mathfrak{a}_1 \cap \mathbf{k}_1[X_1, \ldots, X_r]$ only depends on $\mathfrak{b}$: it is the ideal of $\mathbf{k}_1[X_1, \ldots, X_r]$ generated by $\mathfrak{b}$.

Elementary Elimination theory faces two obstacles.

The first is the difficulty of computing $\mathfrak{b}$ from $\mathfrak{a}$, i.e. of computing some finite generator set of $\mathfrak{b}$ from the polynomial system $(f_1, \dots, f_s)$. This computation is rendered possible by the theory of the Gröbner bases, which we do not address in this work. In addition this computation is not uniform, unlike the computations linked to resultant theory.

The second obstacle is that one only obtains truly satisfactory results for homogeneous polynomial systems. The basic example that shows this is the determinant. Consider a generic system of linear equations $(f_1, \dots, f_n)$ of $\mathbf{k}[\underline{a}][\underline{X}]$, where the variables a_{ij} in $\underline{a}$ represent the n^2 coefficients of the n linear forms f_i, and the X_j's are the unknowns. Then the ideal $\langle \det(\underline{a}) \rangle$ of $\mathbf{k}[\underline{a}]$ is indeed the elimination ideal of the variables X_j for the system $(f_1, \dots, f_n)$, provided we only take into account the zeros of the system distinct from $\underline{0} = (0, \dots, 0)$.
The simplicity of this result should be contrasted with the discussion, in the non-homogeneous framework, of systems where the f_i's are affine forms.
Furthermore, even though the zeros of the ideal $\langle \det(\underline{a}) \rangle$ correspond effectively to the systems that admit some zero $\neq \underline{0}$, this ideal is not exactly equal to $\langle f_1, \dots, f_n \rangle \cap \mathbf{k}[\underline{a}]$, we first need to *saturate* the ideal $\mathfrak{a} = \langle f_1, \dots, f_n \rangle$ w.r.t. the homogeneous variables X_j; i.e. add every g to it such that, for each $j \in [\![1..n]\!]$, $gX_j^N \in \mathfrak{a}$ for some large enough N. In the current case, this saturated ideal is the ideal $\mathfrak{a} + \det(\underline{a})\mathbf{k}[\underline{a}][\underline{X}]$, each $\det(\underline{a})X_j$ is in $\mathfrak{a}$, and the intersection of the saturation with $\mathbf{k}[\underline{a}]$ is indeed $\langle \det(\underline{a}) \rangle$.

What will be retained from this little introduction to Elimination theory is a definition: let $\mathbf{k}$ be a commutative ring, $\mathfrak{a}$ be an ideal of $\mathbf{k}[X_1, \dots, X_n]$ and $r \in [\![0..n-1]\!]$, we then define the *elimination ideal of the variables* X_{r+1}*, …,* X_n *for the ideal* $\mathfrak{a}$ as being the ideal $\mathfrak{b} = \mathfrak{a} \cap \mathbf{k}[X_1, \dots, X_r]$.

We will remain wary of the fact that if $\mathbf{k}$ is an arbitrary ring, the ideal $\mathfrak{a}$ can very well be finitely generated even if $\mathfrak{b}$ is not finitely generated.

The Sylvester matrix

In what follows, we do not assume the ring $\mathbf{A}$ to be discrete, so much so that the degree of a polynomial of $\mathbf{A}[X]$ is not necessarily exactly known. From the point of view of computation, in general we have to take the polynomials in $\mathbf{A}[X]$ in the form of *formal polynomials*, i.e. pairs (f, p) where f is a polynomial and p is the upper bound of its degree. This notion is also useful when changing the base ring because a polynomial can for instance have its degree decrease without us knowing how to test it (e.g. upon passage to the quotient ring).

Recall the definition of the Sylvester matrix and of the resultant of two polynomials (formal polynomials of degrees p and $q \geqslant 0$):

$$\begin{aligned} f &= a_p X^p + a_{p-1} X^{p-1} + \cdots + a_0, \\ g &= b_q X^q + b_{q-1} X^{q-1} + \cdots + b_0. \end{aligned}$$

The *Sylvester matrix* of f and g (in degrees p and q) is the following matrix

$$\mathrm{Syl}_X(f,p,g,q) = \underbrace{\begin{bmatrix} a_p & \cdots & \cdots & \cdots & \cdots & a_0 & & \\ & \ddots & & & & & \ddots & \\ & & a_p & \cdots & \cdots & \cdots & \cdots & a_0 \\ b_q & \cdots & \cdots & b_0 & & & & \\ & \ddots & & & \ddots & & & \\ & & & & & & & \\ & & & \ddots & & & \ddots & \\ & & & & b_q & \cdots & \cdots & b_0 \end{bmatrix}}_{p+q} \begin{array}{l} \left.\vphantom{\begin{matrix}a\\a\\a\end{matrix}}\right\} q \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\\a\end{matrix}}\right\} p \end{array}$$

This matrix can be regarded as the matrix whose rows are the coordinates of the polynomials $(X^{q-1}f, \ldots, Xf, f, X^{p-1}g, \ldots, Xg, g)$ over the basis $(X^{p+q-1}, X^{p+q-2}, \ldots, X, 1)$.

The *resultant of f and g (in degrees p and q)*, denoted by $\mathrm{Res}_X(f,p,g,q)$, is the determinant of this Sylvester matrix

$$\mathrm{Res}_X(f,p,g,q) \overset{\mathrm{def}}{=} \det\big(\mathrm{Syl}_X(f,p,g,q)\big). \tag{2}$$

If the context is clear, we also denote it by $\mathrm{Res}_X(f,g)$ or $\mathrm{Res}(f,g)$. We have

$$\mathrm{Res}_X(f,p,g,q) = (-1)^{pq}\mathrm{Res}_X(g,q,f,p), \tag{3}$$

and also, for $a, b \in \mathbf{A}$,

$$\mathrm{Res}_X(af,p,bg,q) = a^q b^p \mathrm{Res}_X(f,p,g,q). \tag{4}$$

If $p = q = 0$, we obtain the determinant of an empty matrix, i.e. 1.

7.1. Fact. *If $p \geqslant 1$ or $q \geqslant 1$, then* $\mathrm{Res}_X(f,p,g,q) \in \langle f,g\rangle_{\mathbf{A}[X]} \cap \mathbf{A}$. *More precisely, for each $n \in [\![0..p+q-1]\!]$, there exist u_n and $v_n \in \mathbf{A}[X]$ such that* $\deg u_n < q$, $\deg v_n < p$ *and*

$$X^n \,\mathrm{Res}_X(f,g) = u_n(X)f(X) + v_n(X)g(X). \tag{5}$$

▷ Let S be the transpose of $\mathrm{Syl}_X(f,p,g,q)$. The columns of S express polynomials $X^k f$ or $X^\ell g$ over the basis of the monomials of degree $< p+q$. By using Cramer's formula

$$S\,\widetilde{S} = \det S \cdot \mathrm{I}_{p+q}\ ,$$

we see that each $X^n\mathrm{Res}(f,g)$ (which corresponds to one of the columns of the right-hand side matrix) is a linear combination of the columns of S. □

Remark. We can also view Equality (5) in the $n = 0$ case as expressing the determinant of the matrix below developed according to the last column (this is in fact the Sylvester matrix in which we have replaced each coefficient in the last column by the "name" of its row):

$$\begin{bmatrix}
a_p & \cdots & \cdots & \cdots & \cdots & a_0 & & X^{q-1}f \\
 & \ddots & & & & & \ddots & \\
 & & a_p & \cdots & \cdots & \cdots & \cdots & f \\
b_q & \cdots & \cdots & b_0 & & & & X^{p-1}g \\
 & \ddots & & & \ddots & & & \\
 & & & & & & & \\
 & & & b_q & \cdots & \cdots & b_0 & Xg \\
 & & & & b_q & \cdots & \cdots & g
\end{bmatrix}.$$

■

7.2. Corollary. *Let f, $g \in \mathbf{A}[X]$ and $a \in \mathbf{B} \supseteq \mathbf{A}$, with $f(a) = g(a) = 0$, and $p \geqslant 1$ or $q \geqslant 1$, then $\mathrm{Res}_X(f, p, g, q) = 0$.*

Note that if the two degrees are over-evaluated the resultant is annihilated, and the intuitive interpretation is that the two polynomials have a common zero "at infinity." Whilst if $a_p = 1$, the resultant (for f in degree p) is the same regardless of the formal degree chosen for g. This then allows for an unambiguous switch to the notation $\mathrm{Res}(f, g)$, as in the following lemma.

7.3. Lemma. *Let f and $g \in \mathbf{A}[X]$ with f monic of degree p.*

1. *We write $\mathbf{B} = \mathbf{A}[X]/\langle f\rangle$ and denote by μ_g multiplication by (the class of) g in $\mathbf{B}$, which is a free $\mathbf{A}$-module of rank p. Then*
$$\mathrm{N}_{\mathbf{B}/\mathbf{A}}(g) = \det \mu_g = \mathrm{Res}(f, g). \tag{6}$$
2. *Therefore*
$$\mathrm{Res}(f, gh) = \mathrm{Res}(f, g)\,\mathrm{Res}(f, h), \tag{7}$$
$$\mathrm{Res}(f, g + fh) = \mathrm{Res}(f, g). \tag{8}$$
3. *For every square matrix $A \in \mathbb{M}_p(\mathbf{A})$ for which the characteristic polynomial is equal to f, we have*
$$\mathrm{Res}(f, g) = \det\big(g(A)\big). \tag{9}$$
4. *If we write $f = \prod_{i=1}^{p}(X - x_i)$ in an extension of $\mathbf{A}$, we obtain*
$$\mathrm{Res}(f, g) = \prod\nolimits_{i=1}^{p} g(x_i). \tag{10}$$

D *1.* By elementary manipulations of rows, the Sylvester matrix

$$\mathrm{Syl}_X(f,p,g,q) = \begin{bmatrix} 1 & a_{p-1} & \cdots & \cdots & \cdots & a_0 & & \\ & \ddots & \ddots & & & & \ddots & \\ & & 1 & a_{p-1} & \cdots & \cdots & \cdots & a_0 \\ b_q & \cdots & \cdots & b_0 & & & & \\ & \ddots & & & \ddots & & & \\ & & & & & & & \\ & & & \ddots & & & \ddots & \\ & & & & b_q & \cdots & \cdots & b_0 \end{bmatrix}$$

is transformed into the matrix visualized below, in which the rows $q+1$, …, $q+p$ now contain the remainders of the division by f of the polynomials $X^{p-1}g$, …, Xg, g. Thus the $p \times p$ matrix in the south-east corner is exactly the transpose of the matrix of the endomorphism μ_g of $\mathbf{B}$ over the basis of the monomials and its determinant is equal to that of the Sylvester matrix.

$$\begin{bmatrix} 1 & a_{p-1} & \cdots & \cdots & \cdots & a_0 & & \\ & \ddots & \ddots & & & & \ddots & \\ & & 1 & a_{p-1} & \cdots & \cdots & \cdots & a_0 \\ 0 & \cdots & 0 & \times & \cdots & \cdots & \cdots & \times \\ \vdots & & \vdots & \vdots & & & & \vdots \\ \vdots & & \vdots & \vdots & & & & \vdots \\ 0 & \cdots & 0 & \times & \cdots & \cdots & \cdots & \times \end{bmatrix}$$

2. Results from item *1.*

3 and *4.* Result from Proposition 5.9 via item *1.*

We can also give the following direct proofs.

4. First of all, from Equation (7) we deduce the symmetrical formula

$$\mathrm{Res}(f_1 f_2, g) = \mathrm{Res}(f_1, g)\ \mathrm{Res}(f_2, g)$$

for f_1 and f_2 monic (use the equations (3) and (4) and the fact that in the case where the coefficients of g are indeterminates we can assume $g = b_q g_1$ with g_1 monic). Next, a direct computation gives $\mathrm{Res}(X - a, g) = g(a)$.

3. We must prove $\mathrm{Res}(\mathrm{C}_A, g) = \det\big(g(A)\big)$ for some polynomial g and an arbitrary matrix A. This is an algebraic identity concerning the coefficients of A and of g. We can thus restrict ourselves to the case where the matrix A is the generic matrix. Then, it is diagonalized in an overring and we conclude by applying item *4.* □

Remark. Item *4* offers a non-negligible converse to Corollary 7.2: if $\mathbf{A}$ is integral and if f and g are two monic polynomials of $\mathbf{A}[T]$ that are completely factorized in an integral ring containing $\mathbf{A}$, they have a common zero if and only if their resultant is null. ■

In the case of a nontrivial discrete field $\mathbf{K}$ we can do a little better.

7.4. Fact. *Let f and $g \in \mathbf{K}[X]$ of degrees p and $q \geqslant 1$, with $\mathrm{Res}(f, g) = 0$. Then, f and g have a gcd of degree $\geqslant 1$.*

D The $\mathbf{K}$-linear map $(u, v) \mapsto uf + vg$ where $\deg u < q$ and $\deg v < p$ admits as matrix over the bases of monomials the transpose of the Sylvester matrix. Thus let $(u, v) \neq (0, 0)$ in the kernel. The polynomial $uf = -vg$ is of degree $< p + q$. So $\deg\big(\mathrm{lcm}(f, g)\big) < p + q$, which implies $\deg\big(\gcd(f, g)\big) > 0$. □

Comment. The above proof assumes that we know the elementary theory of divisibility (via Euclid's algorithm) in the rings of type $\mathbf{K}[X]$. This theory shows the existence of a gcd and of a lcm with the relation

$$\mathrm{lcm}(f, g)\ \gcd(f, g) = \alpha f g, \qquad (\alpha \in \mathbf{K}^{\times}).$$

Another proof would consist in saying that in a discrete field $\mathbf{L}$, which is an extension of $\mathbf{K}$, the polynomials f and g are split (i.e., are decomposed into factors of degree 1) which implies, given the previous remark, that f and g have a common zero and thus a common factor of degree > 0. One must then finish by stating that the gcd is computed by Euclid's algorithm and thus does not depend on the chosen base field (which must only contain the coefficients of f and g). Nevertheless this second proof, which somewhat gives "the true motivation for the theorem," assumes the existence of $\mathbf{L}$ (which is not guaranteed from a constructive point of view) and does not avoid the theory of divisibility in $\mathbf{K}[X]$ via Euclid's algorithm. ■

7.5. Basic elimination lemma.
Let f and $g \in \mathbf{A}[X]$ with f monic of degree p. Then, $R = \mathrm{Res}_X(f, g)$ is well defined and the elimination ideal $\mathfrak{a} = \langle f, g\rangle_{\mathbf{A}[X]} \cap \mathbf{A}$ satisfies

$$\mathfrak{a}^p \ \subseteq\ \mathrm{Res}_X(f, g)\mathbf{A} \ \subseteq\ \mathfrak{a}.$$

In particular

1. *R is invertible if and only if $1 \in \langle f, g\rangle$,*
2. *R is regular if and only if $\mathfrak{a}$ is faithful, and*
3. *R is nilpotent if and only if $\mathfrak{a}$ is nilpotent.*

D We already know that $\mathrm{Res}_X(f, g) \in \langle f, g\rangle_{\mathbf{A}[X]}$.
We use the notations of Lemma 7.3, item *1.* We denote by x the class of X in $\mathbf{B} = \mathbf{A}[X]/\langle f\rangle$. A basis of $\mathbf{B}$ over $\mathbf{A}$ is $(1, x, \ldots, x^{p-1})$. Let $(\gamma_i)_{i \in [\![1..p]\!]}$ be elements of $\mathfrak{a}$. The elements γ_1, $\gamma_2 x$, …, $\gamma_p x^{p-1}$ are in $\mathrm{Im}\,\mu_g$, so the matrix $D = \mathrm{Diag}(\gamma_1, \ldots, \gamma_p)$ can be written in the form GB, where G is

the matrix of μ_g over the basis of the monomials. It follows that

$$\prod_{k=1}^{p} \gamma_k \;=\; \det D \;=\; \det G \,\det B \;=\; \mathrm{Res}(f,g)\,\det B.$$

Thus the element $\prod_{k=1}^{p} \gamma_k$ of $\mathfrak{a}^p$ belongs to $\langle \mathrm{Res}(f,g)\rangle_{\mathbf{A}}$. □

The basic elimination lemma will be generalized later (Lemmas 9.2 and IV-10.1). The term "elimination ideal" comes from the following facts which result from the previous lemma and from Lemma 7.3.

7.6. Corollary. *Let* $\mathbf{A}$ *be an integral ring and* f, $g \in \mathbf{A}[X]$. *If* f *is monic and can be completely factorized, the following properties are equivalent.*

1. *The elimination ideal* $\langle f,g\rangle_{\mathbf{A}[X]} \cap \mathbf{A}$ *is null.*
2. *The resultant* $\mathrm{Res}_X(f,g) = 0$.
3. *The polynomials* f *and* g *have a common root.*

A discrete field $\mathbf{K}$ is said to be *algebraically closed* if every monic polynomial of $\mathbf{K}[X]$ can be decomposed into a product of factors $X - x_i$ ($x_i \in \mathbf{K}$).

7.7. Corollary. *Let* $\mathbf{K}$ *be a algebraically closed discrete field.*
Write $\mathbf{A} = \mathbf{K}[Y_1,\dots,Y_m]$. *Let* f *and* $g \in \mathbf{A}[X]$ *with* f *monic in* X. *For some arbitrary element* $\underline{\zeta} = (\zeta_1,\dots,\zeta_m)$ *of* $\mathbf{K}^m$, *the following properties are equivalent.*

1. $\underline{\zeta}$ *annihilates all the polynomials of the elimination ideal* $\langle f,g\rangle \cap \mathbf{A}$.
2. $\mathrm{Res}_X\big(f(\underline{\zeta},X), g(\underline{\zeta},X)\big) = 0$.
3. $f(\underline{\zeta},X)$ *and* $g(\underline{\zeta},X)$ *have a common root.*

Consequently if V *is the set of zeros common to* f *and* g *in* $\mathbf{K}^{m+1}$, *and if* $\pi : \mathbf{K}^{m+1} \to \mathbf{K}^m$ *is the projection that forgets the last coordinate, then* $\pi(V)$ *is the set of zeros of* $\mathrm{Res}_X(f,g) \in \mathbf{K}[Y_1,\dots,Y_m]$.

Revisiting the discriminant

When $g = \prod_{i=1}^{n}(X - y_i)$, Lemma 7.3 gives $\mathrm{Res}_X(g,g') = \prod_{i=1}^{n} g'(y_i)$ and thus

$$\mathrm{disc}(g) = (-1)^{n(n-1)/2}\mathrm{Res}_X(g,g'). \tag{11}$$

Since the equality $g(X) = \prod_{i=1}^{n}(X - y_i)$ can always be performed in the universal splitting algebra if g is monic, we obtain that Equality (11) is valid for every monic polynomial, over every commutative ring.

The following fact results therefore from the basic elimination lemma.

7.8. Fact. *Consider some monic polynomial* $g \in \mathbf{A}[X]$.

- $\langle g(X), g'(X)\rangle = \langle 1\rangle$ *if and only if* $\mathrm{disc}\, g$ *is invertible.*
- *The ideal* $\langle g(X), g'(X)\rangle \cap \mathbf{A}$ *is faithful if and only if* $\mathrm{disc}\, g$ *is a regular element of* $\mathbf{A}$.

7.9. Fact. *If $f = gh \in \mathbf{A}[X]$ with g, h monic, we have the following equality*

$$\operatorname{disc}(f) = \operatorname{disc}(g)\operatorname{disc}(h)\operatorname{Res}(g,h)^2 \tag{12}$$

D This immediately results from Equations (7), (8) page 119 and (11). □

7.10. Corollary. *Let $f \in \mathbf{A}[X]$ be monic and $\mathbf{B} = \mathbf{A}[x] = \mathbf{A}[X]/\langle f\rangle$.*

1. *If f possesses a square factor,* $\operatorname{disc} f = 0$. *Conversely, if* $\operatorname{disc} f = 0$ *and if $f(X) = \prod(X - x_i)$ in some integral ring containing $\mathbf{A}$, two of the zeros x_i are equal.*
2. *Assume f is separable and $f = gh$ (g and h monic).*
   a. *The polynomials g and h are separable and comaximal.*
   b. *There exists some idempotent e of $\mathbf{B}$ such that $\langle e\rangle = \langle \pi(g)\rangle$.*
   We have $\mathbf{B} \simeq \mathbf{B}/\langle g\rangle \times \mathbf{B}/\langle h\rangle$.
3. *Assume* $\operatorname{disc} f$ *is regular and $f = gh$ (g and h monic).*
   Then, the elements $\operatorname{disc} g$, $\operatorname{disc} h$ *and* $\operatorname{Res}(g,h)$ *are regular.*

D All this results from Fact 7.9, except maybe the idempotent e in item *2*. If $gu + hv = 1$, then $e = \overline{gu}$ is required. □

7.11. Corollary. *Let $\mathbf{K}$ be a discrete field, $f \in \mathbf{K}[X]$ a separable monic polynomial and $\mathbf{B} = \mathbf{K}[X]/\langle f\rangle$. In item 2 of the previous corollary, we associate with every divisor g of f the idempotent e such that $\langle \overline{g}\rangle = \langle e\rangle$. This establishes a bijection between the monic divisors of f and the idempotents of $\mathbf{B}$. This bijection respects divisibility.*

D The reciprocal bijection is given by $e = \overline{v} \mapsto \gcd(v, f)$. □

We now introduce the notions of prime subfields and of characteristic of a discrete field.

More generally, if $\mathbf{A}$ is an arbitrary ring, we denote by $\mathbb{Z}_\mathbf{A}$ the *prime subring of* $\mathbf{A}$ defined as follows:

$$\mathbb{Z}_\mathbf{A} = \left\{\, n \cdot (m \cdot 1_A)^{-1} \,|\, n, m \in \mathbb{Z},\ m \cdot 1_\mathbf{A} \in \mathbf{A}^\times \,\right\}.$$

If $\rho : \mathbb{Z} \to \mathbf{A}$ is the unique homomorphism of rings of $\mathbb{Z}$ in $\mathbf{A}$, the prime subring is therefore isomorphic to $S^{-1}\mathbb{Z}/\operatorname{Ker}\rho$, where $S = \rho^{-1}(\mathbf{A}^\times)$. A ring can be called prime if it is equal to its prime subring. Actually the terminology is only common in the case of fields.

When $\mathbf{K}$ is a discrete field, the prime subring is a subfield, called the *prime subfield of* $\mathbf{K}$. For some $m > 0$ we will say that $\mathbf{K}$ *is of characteristic* $> m$, and we write "$\operatorname{char}(\mathbf{K}) > m$" if for every $n \in [\![1..m]\!]$, the element $n \cdot 1_\mathbf{K}$ is invertible.

When $\mathbf{K}$ is nontrivial, if there exists some $m > 0$ such that $m \cdot 1_\mathbf{K} = 0$, then there is a minimum number of them, which is a prime number p, and we say that the field *is of characteristic p*. When the prime subfield of $\mathbf{K}$ is isomorphic to $\mathbb{Q}$, the convention is to speak of a *null characteristic*, but we will also use the terminology *infinite characteristic* in the contexts where it is useful to remain consistent with the previous notation, for instance in Fact 7.12.

We can conceive[5] some nontrivial discrete fields whose characteristic is not well defined from a constructive point of view. However, for a discrete field the statement "$\mathrm{char}(\mathbf{K}) > m$" is always decidable.

7.12. Fact. *Let $\mathbf{K}$ be a discrete field and $f \in \mathbf{K}[X]$ be a monic polynomial. If $\operatorname{disc} f = 0$ and $\mathrm{char}(\mathbf{K}) > \deg f$, f possesses a square factor of degree $\geqslant 1$.*

D Let $n = \deg f$. The polynomial f' is of degree $n-1$. Let $g = \gcd(f, f')$. We have $\deg g \in [\![1..n-1]\!]$ (Fact 7.4). We write $f = gh$ therefore

$$\operatorname{disc}(f) = \operatorname{Res}(g,h)^2 \operatorname{disc}(g) \operatorname{disc}(h).$$

Thus, $\operatorname{Res}(g,h) = 0$, or $\operatorname{disc}(g) = 0$, or $\operatorname{disc}(h) = 0$. In the first case, the polynomials g and h have a gcd k of degree $\geqslant 1$ and k^2 divides f. In the two other cases, since $\deg g < \deg f$ and $\deg h < \deg f$, we can finish by induction on the degree, by noting that if $\deg f = 1$, then $\operatorname{disc} f \neq 0$, which assures the initialization. □

8. Algebraic number theory, first steps

Here we give some general applications, in elementary number theory, of the results previously obtained in this chapter. For a glimpse of the many fascinating facets of number theory, the reader should consult the wonderful book [Ireland & Rosen].

Integral algebras

We give a few precisions relating to Definition 3.2.

8.1. Definition.

1. An $\mathbf{A}$-algebra $\mathbf{B}$ is said to be *finite* if $\mathbf{B}$ is a finitely generated $\mathbf{A}$-module. We also say that $\mathbf{B}$ *is finite over* $\mathbf{A}$. In the case of an extension, we speak of a *finite extension* of $\mathbf{A}$.
2. Assume $\mathbf{A} \subseteq \mathbf{B}$. The ring $\mathbf{A}$ is said to be *integrally closed* in $\mathbf{B}$ if every element of $\mathbf{B}$ integral over $\mathbf{A}$ is in $\mathbf{A}$.

[5] We can also be presented with such cases resulting from a complicated construction in a subtle proof.

8.2. Fact. *Let* $\mathbf{A} \subseteq \mathbf{B}$ *and* $x \in \mathbf{B}$. *The following properties are equivalent.*

1. *The element* x *is integral over* $\mathbf{A}$.
2. *The subalgebra* $\mathbf{A}[x]$ *of* $\mathbf{B}$ *is finite.*
3. *There exists a faithful and finitely generated* $\mathbf{A}$*-module* $M \subseteq \mathbf{B}$ *such that* $xM \subseteq M$.

D *3* ⇒ *1* (a fortiori *2* ⇒ *1*.) Consider a matrix A with coefficients in $\mathbf{A}$ which represents $\mu_{x,M}$ (the multiplication by x in M) on a finite generator set of M. If f is the characteristic polynomial of A, we have by the Cayley-Hamilton theorem $0 = f(\mu_{x,M}) = \mu_{f(x),M}$ and since the module is faithful, $f(x) = 0$.
The rest is left to the reader. □

We also easily obtain the following fact.

8.3. Fact. *Let* $\mathbf{B}$ *be an* $\mathbf{A}$*-algebra and* $\mathbf{C}$ *be a* $\mathbf{B}$*-algebra.*

1. *If* $\mathbf{C}$ *is finite over* $\mathbf{B}$ *and* $\mathbf{B}$ *finite over* $\mathbf{A}$*, then* $\mathbf{C}$ *is finite over* $\mathbf{A}$.
2. *An* $\mathbf{A}$*-algebra generated by a finite number of integral elements over* $\mathbf{A}$ *is finite.*
3. *The elements of* $\mathbf{B}$ *that are integral over* $\mathbf{A}$ *form a ring integrally closed in* $\mathbf{B}$. *We call it the* integral closure of $\mathbf{A}$ in $\mathbf{B}$.

8.4. Lemma. *Let* $\mathbf{A} \subseteq \mathbf{B}$ *and* $f \in \mathbf{B}[\underline{X}]$. *The polynomial* f *is integral over* $\mathbf{A}[\underline{X}]$ *if and only if each coefficient of* f *is integral over* $\mathbf{A}$.

D The condition is sufficient, by item *3* of the previous lemma. In the other direction consider an integral dependence relation $P(f) = 0$ for f (with $P \in \mathbf{A}[\underline{X}][T]$, monic). We have in $\mathbf{B}[\underline{X}, T]$ an equality

$$P(\underline{X}, T) = \big(T - f(\underline{X})\big)\,\big(T^n + u_{n-1}(\underline{X})T^{n-1} + \cdots + u_0(\underline{X})\big).$$

Since the coefficient of T^n in the second factor is 1, the multivariate Kronecker's theorem implies that each coefficient of f is integral over $\mathbf{A}$. □

8.5. Lemma. *Let* $\mathbf{A} \subseteq \mathbf{B}$*,* L *be a free* $\mathbf{B}$*-module of finite rank and* $u \in \mathrm{End}_{\mathbf{B}}(L)$ *be integral over* $\mathbf{A}$. *Then, the coefficients of the characteristic polynomial of* u *are integral over* $\mathbf{A}$. *In particular,* $\det(u)$ *and* $\mathrm{Tr}(u)$ *are integral over* $\mathbf{A}$.

D Let us first prove that $\det(u)$ is integral over $\mathbf{A}$. Let $\mathcal{E} = (e_1, \ldots, e_n)$ be a fixed basis of L. The $\mathbf{A}$-module $\mathbf{A}[u]$ is a finitely generated $\mathbf{A}$-module, and so the module

$$E = \textstyle\sum_{i\in[\![1..n]\!],k\geqslant 0} \mathbf{A}u^k(e_i) \subseteq L$$

is a finitely generated $\mathbf{A}$-module, with $u(E) \subseteq E$. Let us introduce the module

$$D = \textstyle\sum_{\underline{x}\in E^n} \mathbf{A}\det_{\mathcal{E}}(\underline{x}) \subseteq \mathbf{B}.$$

Since E is a finitely generated $\mathbf{A}$-module, D is a finitely generated $\mathbf{A}$-module, and it is faithful, we have $1 \in D$ as $\det_{\mathcal{E}}(\mathcal{E}) = 1$. Finally, the equality

$$\det(u)\det_{\mathcal{E}}(x_1,\dots,x_n) = \det_{\mathcal{E}}\big(u(x_1),\dots,u(x_n)\big)$$

and the fact that $u(E) \subseteq E$ show that $\det(u)D \subseteq D$.
Next consider $\mathbf{A}[X] \subseteq \mathbf{B}[X]$ and the $\mathbf{B}[X]$-module $L[X]$.
We have $X\mathrm{Id}_{L[X]} - u \in \mathrm{End}_{\mathbf{B}[X]}(L[X])$. If u is integral over $\mathbf{A}$, $X\mathrm{Id}_{L[X]} - u$ is integral over $\mathbf{A}[X]$ therefore $\mathrm{C}_u(X) = \det(X\mathrm{Id}_{L[X]} - u)$ is integral over $\mathbf{A}[X]$. We conclude with Lemma 8.4. □

8.6. Corollary. *Let* $\mathbf{A} \subseteq \mathbf{B} \subseteq \mathbf{C}$ *where* $\mathbf{C}$ *is a finite free* $\mathbf{B}$*-module. Let* $x \in \mathbf{C}$ *be integral over* $\mathbf{A}$*. Then,* $\mathrm{Tr}_{\mathbf{C}/\mathbf{B}}(x)$*,* $\mathrm{N}_{\mathbf{C}/\mathbf{B}}(x)$ *and all the coefficients of* $\mathrm{C}_{\mathbf{C}/\mathbf{B}}(x)$ *are integral over* $\mathbf{A}$*. If in addition* $\mathbf{B}$ *is a discrete field, the coefficients of the minimal polynomial* $\mathrm{Min}_{\mathbf{B},x}$ *are integral over* $\mathbf{A}$*.*

▷ We apply the previous lemma with $L = \mathbf{C}$ and $u = \mu_x$. For the final statement, we use Kronecker's theorem and the fact that the minimal polynomial divides the characteristic polynomial. □

Integrally closed rings

8.7. Definition. An integral ring $\mathbf{A}$ is said to be *integrally closed* if it is integrally closed in its quotient field.

8.8. Fact. *Let* $\mathbf{A} \subseteq \mathbf{B}$*,* S *be a monoid of* $\mathbf{A}$*,* $x \in \mathbf{B}$ *and* $s \in S$*.*

1. *The element* $x/s \in \mathbf{B}_S$ *is integral over* $\mathbf{A}_S$ *if and only if there exists a* $u \in S$ *such that* xu *is integral over* $\mathbf{A}$*.*
2. *If* $\mathbf{C}$ *is the integral closure of* $\mathbf{A}$ *in* $\mathbf{B}$*, then* $\mathbf{C}_S$ *is the integral closure of* $\mathbf{A}_S$ *in* $\mathbf{B}_S$*.*
3. *If* $\mathbf{A}$ *is integrally closed, then so is* $\mathbf{A}_S$*.*

▷ It suffices to prove item *1.* First assume x/s integral over $\mathbf{A}_S$. We have for example an equality in $\mathbf{B}$

$$u(x^3 + a_2sx^2 + a_1s^2x + a_0s^3) = 0,$$

with $u \in S$ and each $a_i \in \mathbf{A}$. By multiplying by u^2 we obtain

$$(ux)^3 + a_2us(ux)^2 + a_1u^2s^2(ux) + a_0u^3s^3 = 0$$

in $\mathbf{B}$. Conversely suppose xu is integral over $\mathbf{A}$ with $u \in S$. We have for example an equality

$$(ux)^3 + a_2(ux)^2 + a_1(ux) + a_0 = 0$$

in $\mathbf{B}$, therefore in $\mathbf{B}_S$ we have

$$x^3 + (a_2/u)x^2 + (a_1/u^2)x + (a_0/u^3) = 0.$$

□

8.9. Concrete local-global principle. (Integral elements)
Let S_1, …, S_n be comaximal monoids of a ring $\mathbf{A} \subseteq \mathbf{B}$ and $x \in \mathbf{B}$. We have the following equivalences.

1. *The element x is integral over $\mathbf{A}$ if and only if it is integral over each $\mathbf{A}_{S_i}$.*
2. *Assume $\mathbf{A}$ is integral, then $\mathbf{A}$ is integrally closed if and only if each $\mathbf{A}_{S_i}$ is integrally closed.*

D In item *1* we need to prove that if the condition is locally achieved, then it is globally achieved. Consider then some $x \in \mathbf{B}$ which satisfies for each i a relation $(s_i x)^k = a_{i,1}(s_i x)^{k-1} + a_{i,2}(s_i x)^{k-2} + \cdots + a_{i,k}$ with $a_{i,h} \in \mathbf{A}$ and $s_i \in S_i$ (we can assume without loss of generality that the degrees are the same). We then use a relation $\sum s_i^k u_i = 1$ to obtain an integral dependence relation of x over $\mathbf{A}$. □

Kronecker's theorem easily implies the following lemma.

8.10. Lemma. (Kronecker's theorem, case of an integral ring)
Let $\mathbf{A}$ be integrally closed, and $\mathbf{K}$ be its quotient field. If we have $f = gh$ in $\mathbf{K}[T]$ with g, h monic and $f \in \mathbf{A}[T]$, then g and h are also in $\mathbf{A}[T]$.

8.11. Lemma. *The ring $\mathbb{Z}$ as well as the ring $\mathbf{K}[X]$ when $\mathbf{K}$ is a discrete field are integrally closed.*

D In fact this holds for every ring with an integral gcd $\mathbf{A}$ (see Section XI-2). Let $f(T) = T^n - \sum_{k=0}^{n-1} f_k T^k$ and a/b be a reduced fraction in the quotient field of $\mathbf{A}$ with $f(a/b) = 0$. By multiplying by b^n we obtain

$$a^n = b\ \textstyle\sum_{k=0}^{n-1} f_k a^k b^{n-1-k}.$$

Since $\gcd(a, b) = 1$, $\gcd(a^n, b) = 1$. But b divides a^n, therefore b is invertible, and $a/b \in \mathbf{A}$. □

8.12. Theorem. *If $\mathbf{A}$ is integrally closed, the same goes for $\mathbf{A}[X]$.*

D Let $\mathbf{K} = \operatorname{Frac}\mathbf{A}$. If some element f of $\mathbf{K}(X)$ is integral over $\mathbf{A}[X]$, it is integral over $\mathbf{K}[X]$, therefore in $\mathbf{K}[X]$ because $\mathbf{K}[X]$ is integrally closed. The result follows by Lemma 8.4; all the coefficients of the polynomial f are integral over $\mathbf{A}$, therefore in $\mathbf{A}$. □

An interesting corollary of Kronecker's theorem is the following property (with the same notation as in Theorem 3.3).

8.13. Proposition. *Let $f, g \in \mathbf{A}[\underline{X}]$. Assume that $\mathbf{A}$ is integrally closed, and that $a \in \mathbf{A}$ divides all the coefficients of $h = fg$, then a divides all the $f_\alpha\, g_\beta$. In other words*

$$\mathrm{c}(fg) \equiv 0 \mod a \quad \Longleftrightarrow \quad \mathrm{c}(f)\mathrm{c}(g) \equiv 0 \mod a.$$

D Indeed, when considering the polynomials f/a and g with coefficients in the quotient field of $\mathbf{A}$, Kronecker's theorem implies that $f_\alpha\, g_\beta/a$ is integral over $\mathbf{A}$ because every h_γ/a is in $\mathbf{A}$. □

Decomposition of polynomials into products of irreducible factors

8.14. Lemma. *Let $\mathbf{K}$ be a discrete field. The polynomials of $\mathbf{K}[X]$ can be decomposed into products of irreducible factors if and only if we have an algorithm to compute the zeros in $\mathbf{K}$ of an arbitrary polynomial of $\mathbf{K}[X]$.*

D The second condition is a priori weaker since it amounts to determining the factors of degree 1 for some polynomial of $\mathbf{K}[X]$. Assume this condition is satisfied. To know whether there exists a decomposition $f = gh$ with g and h monic of fixed degrees > 0, we apply Kronecker's theorem. We obtain for each coefficient of g and h a finite number of possibilities (they are the zeros of monic polynomials that we can explicitly express according to the coefficients of f). □

8.15. Proposition. *In $\mathbb{Z}[X]$ and $\mathbb{Q}[X]$ the polynomials can be decomposed into products of irreducible factors. A nonconstant polynomial of $\mathbb{Z}[X]$ is irreducible in $\mathbb{Z}[X]$ if and only if it is primitive and irreducible in $\mathbb{Q}[X]$.*

D For $\mathbb{Q}[X]$ we apply Lemma 8.14. We must therefore show that we know how to determine the rational zeros of a monic polynomial f with rational coefficients. We can even assume that the coefficients of f are integral. The elementary theory of divisibility in $\mathbb{Z}$ shows then that if a/b is a zero of f, a must divide the leading coefficient and b the constant coefficient of f; there is therefore only a finite number of tests to execute.

For $\mathbb{Z}[X]$, a primitive polynomial f being given, we want to know if there exists a decomposition $f = gh$ with g and h of fixed degrees > 0. We can assume $f(0) \neq 0$. We apply Kronecker's theorem. A product $g_0 h_j$ for instance must be a zero in $\mathbb{Z}$ of a monic polynomial $q_{0,j}$ of $\mathbb{Z}[T]$ that we can compute. In particular, $g_0 h_j$ must divide $q_{0,j}(0)$, which only leaves a finite number of possibilities for h_j.

Finally, for the last item, if some primitive polynomial f in $\mathbb{Z}[X]$ can be decomposed in the form $f = gh$ in $\mathbb{Q}[X]$ we can assume that g is primitive in $\mathbb{Z}[X]$. Let a be a coefficient of h, then every ag_j is in $\mathbb{Z}$ (Kronecker's theorem), and the Bézout relation $\sum_j g_j u_j = 1$ shows that $a \in \mathbb{Z}$. □

Number fields

We call a discrete field $\mathbf{K}$ a *number field* if it is strictly finite over $\mathbb{Q}$.

Galois closure

8.16. Theorem. (Splitting field, primitive element theorem)

1. *If f is a separable monic polynomial of $\mathbb{Q}[X]$ there exists a number field $\mathbf{L}$ over which we can write $f(X) = \prod_i (X - x_i)$. In addition, with some $\alpha \in \mathbf{L}$ we have*
$$\mathbf{L} = \mathbb{Q}[x_1, \ldots, x_n] = \mathbb{Q}[\alpha] \simeq \mathbb{Q}[T]/\langle Q \rangle\,,$$
where $Q(\alpha) = 0$ and the monic polynomial Q is irreducible in $\mathbb{Q}[T]$ and is completely decomposable in $\mathbf{L}[T]$.
In particular, the extension $\mathbf{L}/\mathbb{Q}$ is Galoisian and Theorem 6.14 applies.
2. *Every number field $\mathbf{K}$ is contained in a Galois extension of the above type. In addition, there exists some $x \in \mathbf{K}$ such that $\mathbf{K} = \mathbb{Q}[x]$.*

D *1.* This results from Theorem 6.15 and from Proposition 8.15.
2. A number field is generated by a finite number of elements that are algebraic over $\mathbb{Q}$. Each of these elements admits a minimal polynomial that is irreducible over $\mathbb{Q}$ and therefore separable (Fact 7.12). By taking the lcm f of these polynomials we obtain a separable polynomial. By applying item *1* to f and by using Theorem 6.7, we see that $\mathbf{K}$ is isomorphic to a subfield of $\mathbf{L}$. Finally, as the Galois correspondence is bijective and as the Galois group $\mathrm{Gal}(\mathbf{L}/\mathbb{Q})$ is finite, the field $\mathbf{K}$ only contains an explicit finite number of subfields $\mathbf{K}_i$ strictly finite over $\mathbb{Q}$. If we choose $x \in \mathbf{K}$ outside of the union of these subfields (which are strict $\mathbb{Q}$-vector subspaces), we necessarily have $\mathbb{Q}[x] = \mathbf{K}$; it is a subfield of $\mathbf{K}$ strictly finite over $\mathbb{Q}$ and distinct from all the $\mathbf{K}_i$'s. □

Cotransposed element

If $\mathbf{B}$ is a free $\mathbf{A}$-algebra of finite rank, we can identify $\mathbf{B}$ with a commutative subalgebra of $\mathrm{End}_{\mathbf{A}}(B)$, where B designates the $\mathbf{A}$-module $\mathbf{B}$ deprived of its multiplicative structure, by means of the homomorphism $x \mapsto \mu_{\mathbf{B},x}$, where $\mu_{\mathbf{B},x} = \mu_x$ is the multiplication by x in $\mathbf{B}$. Then, since $\widetilde{\mu}_x = G(\mu_x)$ for some polynomial G of $\mathbf{A}[T]$ (Lemma 1.4 item *6*), we can define $\widetilde{x}$ by the equality $\widetilde{x} = G(x)$, or equivalently $\widetilde{\mu_x} = \mu_{\widetilde{x}}$. If more precision is necessary, we will use the notation $\mathrm{Adj}_{\mathbf{B}/\mathbf{A}}(x)$. This element $\widetilde{x}$ is called *the cotransposed element of* x. We then have the important equality

$$x\,\widetilde{x} = x\ \mathrm{Adj}_{\mathbf{B}/\mathbf{A}}(x) = \mathrm{N}_{\mathbf{B}/\mathbf{A}}(x). \tag{13}$$

Remark. Let us also note that the applications "norm of" and "cotransposed element of" enjoy some properties of "$\mathbf{A}$-rationality," which directly result

from their definitions: if $P \in \mathbf{B}[X_1, \dots, X_k]$, then by taking the x_i's in $\mathbf{A}$, $\mathrm{N}_{\mathbf{B}/\mathbf{A}}\big(P(x_1, \dots, x_k)\big)$ and $\mathrm{Adj}_{\mathbf{B}/\mathbf{A}}\,\big(P(x_1, \dots, x_k)\big)$ are given by polynomials of $\mathbf{A}[X_1, \dots, X_k]$.
In fact $\mathbf{B}[\underline{X}]$ is free over $\mathbf{A}[\underline{X}]$ with the same basis as that of $\mathbf{B}$ over $\mathbf{A}$ and $\mathrm{N}_{\mathbf{B}/\mathbf{A}}\big(P(\underline{x})\big)$ is given by the evaluation at $\underline{x}$ of $\mathrm{N}_{\mathbf{B}[\underline{X}]/\mathbf{A}[\underline{X}]}\big(P(\underline{X})\big)$ (likewise for the cotransposed element). We will use by abuse of notation $\mathrm{N}_{\mathbf{B}/\mathbf{A}}\big(P(\underline{X})\big)$.
Furthermore, if $[\,\mathbf{B} : \mathbf{A}\,] = n$ and if P is homogeneous of degree d, then $\mathrm{N}_{\mathbf{B}/\mathbf{A}}\big(P(\underline{X})\big)$ is homogeneous of degree nd and $\mathrm{Adj}_{\mathbf{B}/\mathbf{A}}\big(P(\underline{X})\big)$ is homogeneous of degree $(n-1)\,d$. ■

Ring of integers of a number field

If $\mathbf{K}$ is a number field its *ring of integers* is the integral closure of $\mathbb{Z}$ in $\mathbf{K}$.

8.17. Proposition and definition. (Discriminant of a number field)
Let $\mathbf{K}$ be a number field and $\mathbf{Z}$ its ring of integers.

1. *An element y of $\mathbf{K}$ is in $\mathbf{Z}$ if and only if $\mathrm{Min}_{\mathbb{Q},y}(X) \in \mathbb{Z}[X]$.*
2. *We have $\mathbf{K} = (\mathbb{N}^*)^{-1}\mathbf{Z}$.*
3. *Assume that $\mathbf{K} = \mathbb{Q}[x]$ with $x \in \mathbf{Z}$. Let $f(X) = \mathrm{Min}_{\mathbb{Q},x}(X)$ be in $\mathbb{Z}[X]$ and Δ^2 be the greatest square factor of $\mathrm{disc}_X\, f$.*
   Then, $\mathbb{Z}[x] \subseteq \mathbf{Z} \subseteq \frac{1}{\Delta}\mathbb{Z}[x]$.
4. *The ring $\mathbf{Z}$ is a free $\mathbb{Z}$-module of rank $[\,\mathbf{K} : \mathbf{Q}\,]$.*
5. *The integer* $\mathrm{Disc}_{\mathbf{Z}/\mathbb{Z}}$ *is well-defined. We call it the* discriminant of the number field $\mathbf{K}$.

D *1.* Results from Lemma 8.10 (Kronecker's theorem).

2. Let $y \in \mathbf{K}$ and $g(X) \in \mathbb{Z}[X]$ be a nonzero polynomial that annihilates y. If a is the leading coefficient of g, ay is integral over $\mathbb{Z}$.

3. Let $\mathbf{A} = \mathbb{Z}[x]$ and $n = [\,\mathbf{K} : \mathbf{Q}\,]$. Let $z \in \mathbf{Z}$, which we as $h(x)/\delta$ with $\delta \in \mathbb{N}^*$, $\langle \delta \rangle + \mathrm{c}(h) = \langle 1 \rangle$ and $\deg h < n$. We have $\mathbf{A} + \mathbb{Z}z \subseteq \frac{1}{\delta}\mathbf{A}$ and it thus suffices to prove that δ^2 divides $\mathrm{disc}_X(f)$. The ring $\mathbf{A}$ is a free $\mathbb{Z}$-module of rank n, with the basis $\mathcal{B}_0 = (1, x, \dots, x^{n-1})$. Proposition 5.10 gives

$$\mathrm{Disc}_{\mathbf{A}/\mathbb{Z}} = \mathrm{disc}_{\mathbf{A}/\mathbb{Z}}(\mathcal{B}_0) = \mathrm{disc}_{\mathbf{K}/\mathbb{Q}}(\mathcal{B}_0) = \mathrm{disc}_X\, f.$$

The $\mathbb{Z}$-module $M = \mathbf{A} + \mathbb{Z}z$ is also free, of rank n with a basis $\mathcal{B}_1$, and we obtain the equalities

$$\mathrm{disc}_X\, f = \mathrm{disc}_{\mathbf{K}/\mathbb{Q}}(\mathcal{B}_0) = \mathrm{disc}_{\mathbf{K}/\mathbb{Q}}(\mathcal{B}_1) \times d^2,$$

where d is the determinant of the matrix of $\mathcal{B}_0$ over $\mathcal{B}_1$ (Proposition II-5.33 *2*). Finally, $d = \pm\delta$ by the following Lemma 8.18, as required.

4. Without loss of generality we use the setup of item *3.* There is only a finite number of finitely generated $\mathbb{Z}$-modules between $\mathbb{Z}[x]$ and $\frac{1}{\Delta}\mathbb{Z}[x]$, and for each of them we can test whether it is contained in $\mathbf{Z}$. The largest is necessarily equal to $\mathbf{Z}$. □

Remarks.
1) As a corollary, we see that in the context of item *3*, if $\mathrm{disc}_X(f)$ has no square factors, then $\mathbf{Z} = \mathbb{Z}[x]$.

2) The proof of item *4* does not provide the practical means to compute a $\mathbb{Z}$-basis of $\mathbf{Z}$. For some more precise information see Problem 9. Actually we do not know of a general *polynomial time* algorithm to compute a $\mathbb{Z}$-basis of $\mathbf{Z}$. ■

One says that an ideal $\mathfrak{a}$ of a ring $\mathbf{A}$ is *principal* when it is generated by a single element.

8.18. Lemma. *Let $N \subseteq M$ be two free $\mathbf{A}$-modules of the same rank n with $M = N + \mathbf{A}z$. Assume that for some regular element $\delta \in \mathbf{A}$, we have $\delta z \in N$ and $\delta z = a_1 e_1 + \cdots + a_n e_n$, where $(e_1, \dots, e_n)$ is a basis of N. Then, the determinant d of a matrix of a basis of N over a basis M satisfies*

$$d \,\langle \delta, a_1, \dots, a_n \rangle = \langle \delta \rangle \tag{14}$$

In particular, $\langle \delta, a_1, \dots, a_n \rangle$ is a principal ideal, and if δ, a_1, …, a_n are comaximal, then $\langle d \rangle = \langle \delta \rangle$. Moreover, $M/N \simeq \mathbf{A}/\langle d \rangle$.

D Equality (14) is left to the reader (see Exercise 20).
It remains to prove that $M/N \simeq \mathbf{A}/\langle d \rangle$. By letting $\overline{z}$ be the class of z in M/N, since $M/N \simeq \mathbf{A}\overline{z}$, we must prove that $\mathrm{Ann}_{\mathbf{A}}(\overline{z}) = \langle d \rangle$, i.e. that $bz \in N \Leftrightarrow b \in \langle d \rangle$. It is clear that $dz \in N$.
If $bz \in N$, then $b\delta z \in \delta N$, therefore by writing $\delta z = a_1 e_1 + \cdots + a_n e_n$, we get $ba_i \in \langle \delta \rangle$, then $b \,\langle \delta, a_1, \dots, a_n \rangle \subseteq \langle \delta \rangle$. By multiplying by d and by simplifying by δ, we obtain $b \in \langle d \rangle$. □

The multiplicative theory of the ideals of a number field

8.19. Definition. An ideal $\mathfrak{a}$ of a ring $\mathbf{A}$ is said to be *invertible* if there exist an ideal $\mathfrak{b}$ and a regular element a such that $\mathfrak{a}\,\mathfrak{b} = \langle a \rangle$.

8.20. Fact. *Let $\mathfrak{a}$ be an invertible ideal of a ring $\mathbf{A}$.*

1. *The ideal $\mathfrak{a}$ is finitely generated.*
2. *If $\mathfrak{a}$ is generated by k elements and if $\mathfrak{a}\,\mathfrak{b} = \langle a \rangle$ with a regular, then $\mathfrak{b}$ is generated by k elements. Furthermore $\mathfrak{b} = (\langle a \rangle : \mathfrak{a})$.*
3. *We have the rule $\mathfrak{a}\,\mathfrak{c} \subseteq \mathfrak{a}\,\mathfrak{d} \;\Rightarrow\; \mathfrak{c} \subseteq \mathfrak{d}$ for all ideals $\mathfrak{c}$ and $\mathfrak{d}$.*
4. *If $\mathfrak{c} \subseteq \mathfrak{a}$ there exists a unique $\mathfrak{d}$ such that $\mathfrak{d}\,\mathfrak{a} = \mathfrak{c}$, namely $\mathfrak{d} = (\mathfrak{c} : \mathfrak{a})$, and if $\mathfrak{c}$ is finitely generated, so is $\mathfrak{d}$.*

$\mathbb{D}$ *3.* If $\mathfrak{a}\,\mathfrak{c} \subseteq \mathfrak{a}\,\mathfrak{d}$ by multiplying by $\mathfrak{b}$ we obtain $a\,\mathfrak{c} \subseteq a\,\mathfrak{d}$, and since a is regular, this implies $\mathfrak{c} \subseteq \mathfrak{d}$.

1. If $\mathfrak{a}\,\mathfrak{b} = \langle a \rangle$, we find two finitely generated ideals $\mathfrak{a}_1 \subseteq \mathfrak{a}$ and $\mathfrak{b}_1 \subseteq \mathfrak{b}$ such that $a \in \mathfrak{a}_1\,\mathfrak{b}_1$ and thus $\mathfrak{a}\,\mathfrak{b} = \langle a \rangle \subseteq \mathfrak{a}_1\,\mathfrak{b}_1 \subseteq \mathfrak{a}\,\mathfrak{b}_1 \subseteq \mathfrak{a}\,\mathfrak{b}$. From the above, we deduce the equalities $\mathfrak{a}_1\,\mathfrak{b}_1 = \mathfrak{a}\,\mathfrak{b}_1 = \mathfrak{a}\,\mathfrak{b}$. Whence $\mathfrak{b} = \mathfrak{b}_1$ by item *3.* Similarly, $\mathfrak{a} = \mathfrak{a}_1$.

2. If $\mathfrak{a} = \langle a_1, \dots, a_k \rangle$, we find $b_1, \dots, b_k \in \mathfrak{b}$ such that $\sum_i a_i b_i = a$.

By reasoning as in item *1* with $\mathfrak{a}_1 = \mathfrak{a}$ and $\mathfrak{b}_1 = \langle b_1, \dots, b_k \rangle$ we obtain the equality $\mathfrak{b} = \langle b_1, \dots, b_k \rangle$. Since $\mathfrak{a}\,\mathfrak{b} = \langle a \rangle$, we have $\mathfrak{b} \subseteq (\langle a \rangle : \mathfrak{a})$. Conversely, if $x\mathfrak{a} \subseteq \langle a \rangle$, then $x\,\langle a \rangle = x\,\mathfrak{a}\,\mathfrak{b} \subseteq a\,\mathfrak{b}$, thus $ax = ab$ for some $b \in \mathfrak{b}$ and $x \in \mathfrak{b}$ because a is regular.

4. From $\mathfrak{a}\,\mathfrak{b} = \langle a \rangle$ we deduce $\mathfrak{c}\,\mathfrak{b} \subseteq \langle a \rangle$. All the elements of $\mathfrak{c}\,\mathfrak{b}$ being multiples of a, by dividing them by a we get an ideal $\mathfrak{d}$, that we denote by $\frac{1}{a}\,\mathfrak{c}\,\mathfrak{b}$, and with which we obtain the equality $\mathfrak{a}\,\mathfrak{d} = \frac{1}{a}\,\mathfrak{c}\,\mathfrak{b}\,\mathfrak{a} = \frac{1}{a}\,\mathfrak{c}\,\langle a \rangle = \mathfrak{c}$ because a is regular.

If $\mathfrak{c}$ is finitely generated, $\mathfrak{d}$ is generated by the elements obtained by dividing each generator of $\mathfrak{c}\,\mathfrak{b}$ by a.

The uniqueness of $\mathfrak{d}$ results from item *3.*

All is left to prove is that $\mathfrak{d} = (\mathfrak{c} : \mathfrak{a})$. The inclusion $\mathfrak{d} \subseteq (\mathfrak{c} : \mathfrak{a})$ is immediate. Conversely, if $x\mathfrak{a} \subseteq \mathfrak{c}$, then $x\,\langle a \rangle \subseteq \mathfrak{c}\,\mathfrak{b}$, therefore $x \in \frac{1}{a}\,\mathfrak{c}\,\mathfrak{b} = \mathfrak{d}$. □

The following theorem is the key theorem in the multiplicative theory of the ideals of number fields. We provide two proofs. Beforehand we invite the readers to acquaint themselves with Problem 3 which gives Kummer's little theorem, which solves with minimal costs the question for "almost all" the finitely generated ideals of the number fields. Problem 5 is also instructive as it gives a direct proof of the invertibility of all the nonzero finitely generated ideals as well as of their unique decomposition into a product of "prime factors" for the ring $\mathbb{Z}[\sqrt[n]{1}\,]$.

8.21. Theorem. (Invertibility of the ideals of a number field)
Every nonzero finitely generated ideal of the ring of integers $\mathbf{Z}$ *of a number field* $\mathbf{K}$ *is invertible.*

$\mathbb{D}$ *First proof (à la Kronecker.*[6]*)*

Take for example $\mathfrak{a} = \langle \alpha, \beta, \gamma \rangle$. Let $\mathbf{A} = \mathbb{Q}[X]$ and $\mathbf{B} = \mathbf{K}[X]$. The algebra $\mathbf{B}$ is free over $\mathbf{A}$ with the same basis as that of $\mathbf{K}$ over $\mathbb{Q}$. Consider the polynomial $g = \alpha + \beta X + \gamma X^2$ which satisfies $\mathrm{c}_{\mathbf{Z}}(g) = \mathfrak{a}$. Since α, β, γ are integral over $\mathbb{Z}$, g is integral over $\mathbb{Z}[X]$. Let $h(X) = \mathrm{Adj}_{\mathbf{B}/\mathbf{A}}(g)$ be the cotransposed element of g. We know that h is expressed as a polynomial in g and in the coefficients of the characteristic polynomial of g. By applying

[6] Actually Kronecker does not use the *cotransposed element* of $\alpha + \beta X + \gamma X^2$ (as stated in the definition we have given), but the product of all the conjugates of $\alpha X + \beta Y + \gamma Z$ in a Galois extension. This introduces a slight variation in the proof.

Corollary 8.6 we deduce that h has coefficients in $\mathbf{Z}$. Let $\mathfrak{b}$ be the finitely generated ideal of $\mathbf{Z}$ generated by the coefficients of h.
We have $gh = \mathrm{N}_{\mathbf{B}/\mathbf{A}}(g) \in \mathbf{Z}[X] \cap \mathbb{Q}[X] = \mathbb{Z}[X]$. Let d be the gcd of the coefficients of gh. Proposition 8.13 tells us that an arbitrary element of $\mathbf{Z}$ divides d if and only if it divides all the elements of $\mathfrak{a}\,\mathfrak{b}$.
In particular, $d\mathbf{Z} \supseteq \mathfrak{a}\,\mathfrak{b}$. Given the Bézout relation that expresses d according to the coefficients of gh we also have $d \in \mathfrak{a}\,\mathfrak{b}$. Therefore $d\mathbf{Z} = \mathfrak{a}\,\mathfrak{b}$.

Second proof (à la Dedekind.)
First of all we notice that it suffices to know how to invert the ideals with two generators by virtue of the following remark. For three arbitrary ideals $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ in a ring we always have the equality

$$(\mathfrak{a}+\mathfrak{b})(\mathfrak{b}+\mathfrak{c})(\mathfrak{c}+\mathfrak{a}) = (\mathfrak{a}+\mathfrak{b}+\mathfrak{c})(\mathfrak{a}\mathfrak{b}+\mathfrak{b}\mathfrak{c}+\mathfrak{a}\mathfrak{c}),$$

therefore, if we know how to invert the ideals with k generators ($k \geqslant 2$), we also know how to invert the ideals with $k+1$ generators.
We thus consider an ideal $\langle \alpha, \beta \rangle$ with $\alpha \neq 0$. As α is integral over $\mathbb{Z}$, we can find $\overline{\alpha} \in \mathbf{Z}$ such that $\overline{\alpha}\alpha \in \mathbb{Z} \setminus \{0\}$. Thus, even if it means replacing (α, β) with $(\overline{\alpha}\alpha, \overline{\alpha}\beta)$, we restrict ourselves to the study of an ideal $\langle a, \beta \rangle$ with $(a, \beta) \in \mathbb{Z} \times \mathbf{Z}$.
Let $f \in \mathbb{Z}[X]$ be a monic polynomial which is annihilated in β. We write

$$f(X) = (X - \beta)h(X), \text{ where } h \in \mathbf{Z}[X]\,.$$

We thus have $f(aX) = (aX - \beta)h(aX)$, which we rewrite as $f_1 = g_1 h_1$. Let then d be the gcd of the coefficients of f_1 in $\mathbb{Z}$. With $\mathfrak{b} = \mathrm{c}_{\mathbf{Z}}(h_1)$ and $\mathfrak{a} = \mathrm{c}_{\mathbf{Z}}(g_1) = \langle a, \beta \rangle$, we clearly have $d \in \mathfrak{a}\mathfrak{b}$. Moreover, Proposition 8.13 tells us that an arbitrary element of $\mathbf{Z}$ divides all the elements of $\mathrm{c}_{\mathbf{Z}}(f_1) = \langle d \rangle$ if and only if it divides all the elements of the ideal $\mathfrak{a}\,\mathfrak{b}$. In particular, d divides all the elements of $\mathfrak{a}\,\mathfrak{b}$. Thus $\mathfrak{a}\mathfrak{b} = \langle d \rangle$. □

The following theorem shows that the finitely generated ideals of a number field with regard to the elementary operations (sum, intersection, product, exact division) behave essentially equivalently to the principal ideals of $\mathbb{Z}$. The latter translate the theory of divisibility for the natural numbers very precisely.
Recall that in the bijection $n \mapsto n\mathbb{Z}$ ($n \in \mathbb{N}$, $n\mathbb{Z}$ a finitely generated ideal of $\mathbb{Z}$): the product corresponds to the product, divisibility corresponds to inclusion; the gcd to the sum; the lcm to the intersection; and the exact division to the conductor.

8.22. Theorem. (The finitely generated ideals of a number field)
Let $\mathbf{K}$ be a number field and $\mathbf{Z}$ its ring of integers.

1. *If $\mathfrak{b}$ and $\mathfrak{c}$ are two arbitrary ideals, and if $\mathfrak{a}$ is some nonzero finitely generated ideal of $\mathbf{Z}$, we have the implication*

$$\mathfrak{a}\,\mathfrak{b} \subseteq \mathfrak{a}\,\mathfrak{c} \quad\Rightarrow\quad \mathfrak{b} \subseteq \mathfrak{c}\,.$$

2. If $\mathfrak{b} \subseteq \mathfrak{c}$ *are two finitely generated ideals, there exists some finitely generated ideal* $\mathfrak{a}$ *such that* $\mathfrak{a}\,\mathfrak{c} = \mathfrak{b}$*.*

3. The set of finitely generated ideals of $\mathbf{Z}$ *is stable by finite intersections and we have the following equalities (where* $\mathfrak{a}$*,* $\mathfrak{b}$*,* $\mathfrak{c}$ *designates finitely generated ideals of* $\mathbf{Z}$*):*

$$\begin{aligned}
&a. & (\mathfrak{a} \cap \mathfrak{b})(\mathfrak{a} + \mathfrak{b}) &= \mathfrak{a}\mathfrak{b}\,, \\
&b. & \mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c}) &= (\mathfrak{a} \cap \mathfrak{b}) + (\mathfrak{a} \cap \mathfrak{c})\,, \\
&c. & \mathfrak{a} + (\mathfrak{b} \cap \mathfrak{c}) &= (\mathfrak{a} + \mathfrak{b}) \cap (\mathfrak{a} + \mathfrak{c})\,, \\
&d. & \mathfrak{a}(\mathfrak{b} \cap \mathfrak{c}) &= (\mathfrak{a}\mathfrak{b}) \cap (\mathfrak{a}\mathfrak{c})\,, \\
&e. & (\mathfrak{a} + \mathfrak{b})^n &= \mathfrak{a}^n + \mathfrak{b}^n \quad (n \in \mathbb{N})\,.
\end{aligned}$$

4. If $\mathfrak{a}$ *is some nonzero finitely generated ideal of* $\mathbf{Z}$ *the ring* $\mathbf{Z}/\mathfrak{a}$ *is finite. In particular, we have tests to decide:*

- *if some* $x \in \mathbf{Z}$ *is in* $\mathfrak{a}$*,*
- *if some* $x \in \mathbf{Z}$ *is invertible modulo* $\mathfrak{a}$*,*
- *if* $\mathfrak{a}$ *is contained in another finitely generated ideal* $\mathfrak{b}$*,*
- *if* $\mathbf{Z}/\mathfrak{a}$ *is a discrete field (we then say that* $\mathfrak{a}$ *is a detachable maximal ideal).*

5. Every distinct finitely generated ideal of $\langle 0 \rangle$ *and* $\langle 1 \rangle$ *is equal to a product of detachable invertible maximal ideals, and this decomposition is unique up to order of the factors.*

D *1* and *2.* By Fact 8.20.

3. If one of the finitely generated ideals is zero everything is clear. We assume they are nonzero in the remainder of the proof.

3a. Let $\mathfrak{c}$ such that $\mathfrak{c}(\mathfrak{a} + \mathfrak{b}) = \mathfrak{a}\mathfrak{b}$. Since $(\mathfrak{a} \cap \mathfrak{b})(\mathfrak{a} + \mathfrak{b}) \subseteq \mathfrak{a}\mathfrak{b}$, we obtain the inclusion $\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{c}$ (simplification by $\mathfrak{a} + \mathfrak{b}$). Conversely, $\mathfrak{c}\mathfrak{a} \subseteq \mathfrak{a}\mathfrak{b}$, thus $\mathfrak{c} \subseteq \mathfrak{b}$ (simplification by $\mathfrak{a}$). Similarly $\mathfrak{c} \subseteq \mathfrak{a}$.

3c. We multiply both sides by $\mathfrak{a} + \mathfrak{b} + \mathfrak{c} = (\mathfrak{a} + \mathfrak{b}) + (\mathfrak{a} + \mathfrak{c})$.
The right-hand side gives $(\mathfrak{a} + \mathfrak{b})(\mathfrak{a} + \mathfrak{c})$.
The left-hand side gives $\mathfrak{a}(\mathfrak{a} + \mathfrak{b} + \mathfrak{c}) + \mathfrak{a}(\mathfrak{b} \cap \mathfrak{c}) + (\mathfrak{b} + \mathfrak{c})(\mathfrak{b} \cap \mathfrak{c})$.
Both cases result in $\mathfrak{a}(\mathfrak{a} + \mathfrak{b} + \mathfrak{c}) + \mathfrak{b}\mathfrak{c}$.

3b. For the inclusion, the finitely generated ideals form a lattice (the supremum is the sum and the infimum is the intersection). We come to see that one of the laws is distributive with respect to the other. Classically, in a lattice this implies the other distributivity (see page 620).

3d. The map $\mathfrak{x} \mapsto \mathfrak{a}\,\mathfrak{x}$ (of the set of finitely generated ideals to the set of finitely generated ideals which are multiples of $\mathfrak{a}$) is an isomorphism of the order structure by item *1.* This implies that the map transforms $\mathfrak{b} \cap \mathfrak{c}$ into the infimum of $\mathfrak{a}\mathfrak{b}$ and $\mathfrak{a}\mathfrak{c}$ inside the set of finitely generated ideals that are multiples of $\mathfrak{a}$. It thus suffices to establish that $\mathfrak{a}\mathfrak{b} \cap \mathfrak{a}\mathfrak{c}$ is a multiple of $\mathfrak{a}$. This results from item *2.*

3e. For example with $n = 3$, $(\mathfrak{a}+\mathfrak{b})^3 = \mathfrak{a}^3 + \mathfrak{a}^2\mathfrak{b} + \mathfrak{a}\mathfrak{b}^2 + \mathfrak{b}^3$.
By multiplying $(\mathfrak{a}+\mathfrak{b})^3$ and $\mathfrak{a}^3 + \mathfrak{b}^3$ by $(\mathfrak{a}+\mathfrak{b})^2$ we find in both cases

$$\mathfrak{a}^5 + \mathfrak{a}^4\mathfrak{b} + \cdots + \mathfrak{a}\mathfrak{b}^4 + \mathfrak{b}^5.$$

4. View $\mathbf{Z}$ as a free $\mathbb{Z}$-module of rank $n = [\,\mathbf{K} : \mathbb{Q}\,]$. It is obvious that a finitely generated ideal $\mathfrak{a}$ containing the integer $m \neq 0$ can be explicitly expressed as a finitely generated $\mathbb{Z}$-submodule of $\mathbb{Z}^n$ containing $m\mathbb{Z}^n$.

5. Let $\mathfrak{a}$ be a finitely generated ideal $\neq \langle 0\rangle, \langle 1\rangle$. The finitely generated maximal ideals of $\mathbf{Z}$ containing $\mathfrak{a}$ are obtained by determining the finitely generated maximal ideals of $\mathbf{Z}/\mathfrak{a}$ (which is possible because the ring $\mathbf{Z}/\mathfrak{a}$ is finite). If $\mathfrak{p}$ is a finitely generated maximal ideal containing $\mathfrak{a}$, we can write $\mathfrak{a} = \mathfrak{b}\,\mathfrak{p}$. Furthermore, we have the equality $|\,\mathbf{Z} : \mathfrak{a}\,| = |\,\mathbf{Z} : \mathfrak{b}\,|\,|\,\mathfrak{b} : \mathfrak{a}\,|$. We then obtain the decomposition into products of finitely generated maximal ideals by induction on $|\,\mathbf{Z} : \mathfrak{a}\,|$. The uniqueness results from the fact that if a finitely generated maximal ideal $\mathfrak{p}$ contains a product of finitely generated maximal ideals, it is necessarily equal to one of them, otherwise it would be comaximal with the product. □

We end this section with a few generalities concerning *the ideals that avoid the conductor*. The situation in number theory is the following. We have a number field $\mathbf{K} = \mathbb{Q}[\alpha]$ with α integral over $\mathbb{Z}$. We denote by $\mathbf{Z}$ the ring of integers of $\mathbf{K}$, i.e. the integral closure of $\mathbb{Z}$ in $\mathbf{K}$. Even though it is possible in principle, it is not easy to obtain a basis of $\mathbf{Z}$ as a $\mathbb{Z}$-module, nor is it easy to study the structure of the monoid of the finitely generated ideals of $\mathbf{Z}$.

Assume that we have a ring $\mathbf{Z}'$ which constitutes an approximation of $\mathbf{Z}$ in the sense that $\mathbb{Z}[\alpha] \subseteq \mathbf{Z}' \subseteq \mathbf{Z}$. For example let $\mathbf{Z}' = \mathbb{Z}[\alpha]$ initially. We are interested in the multiplicative structure of the group of fractional ideals of $\mathbf{Z}$,[7] and we want to rely on that of $\mathbf{Z}'$ to study it in detail.

The following theorem states that "this works very well for most ideals, i.e. for every one that avoids the conductor of $\mathbf{Z}$ into $\mathbf{Z}'$."

8.23. Definition.

Let $\mathbf{A}$, $\mathbf{B}$ be two rings such that $\mathbf{A} \subseteq \mathbf{B}$, and let $\mathfrak{a}$ and $\mathfrak{b}$ be respective ideals of $\mathbf{A}$ and $\mathbf{B}$.

1. The *conductor of* $\mathbf{B}$ *into* $\mathbf{A}$ is $(\mathbf{A} : \mathbf{B}) = \{\, x \in \mathbf{B} \,|\, x\mathbf{B} \subseteq \mathbf{A} \,\}$.
2. The *extension of* $\mathfrak{a}$ is the ideal $\mathfrak{a}\mathbf{B}$ of $\mathbf{B}$.
3. The *contraction of* $\mathfrak{b}$ is the ideal $\mathbf{A} \cap \mathfrak{b}$ of $\mathbf{A}$.

[7] A fractional ideal of $\mathbf{Z}$ is a $\mathbf{Z}$-submodule of $\mathbf{K}$ equal to $\frac{1}{m}\,\mathfrak{a}$ for some $m \in \mathbb{Z}^\star$ and a finitely generated ideal $\mathfrak{a}$ of $\mathbf{Z}$, cf. page 573.

8.24. Theorem. (Dedekind's theorem, ideals that avoid the conductor) *Let $\mathbf{A}$, $\mathbf{B}$ be two rings such that $\mathbf{A} \subseteq \mathbf{B}$ and $\mathfrak{f}$ be the conductor of $\mathbf{B}$ into $\mathbf{A}$.*

1. *The ideal $\mathfrak{f}$ is the annihilator of the $\mathbf{A}$-module $\mathbf{B}/\mathbf{A}$. It is simultaneously an ideal of $\mathbf{A}$ and an ideal of $\mathbf{B}$, and it is the greatest ideal with this property.*

We denote by $\mathcal{A}$ (resp. $\mathcal{B}$) the class of ideals of $\mathbf{A}$ (resp. of $\mathbf{B}$) comaximal to $\mathfrak{f}$.

2. *For $\mathfrak{a} \in \mathcal{A}$, we have $\mathbf{A}/\mathfrak{a} \simeq \mathbf{B}/\mathfrak{a}\mathbf{B}$ and for $\mathfrak{b} \in \mathcal{B}$, we have $\mathbf{B}/\mathfrak{b} \simeq \mathbf{A}/\mathbf{A} \cap \mathfrak{b}$.*
3. *$\mathcal{A}$ is stable under multiplication, sum, intersection and satisfies*
$$\mathfrak{a} \in \mathcal{A},\, \mathfrak{a}' \supseteq \mathfrak{a} \quad \Longrightarrow \quad \mathfrak{a}' \in \mathcal{A}.$$
In particular, $\mathfrak{a}_1\mathfrak{a}_2 \in \mathcal{A}$ if and only if $\mathfrak{a}_1$ and $\mathfrak{a}_2 \in \mathcal{A}$. The same properties are valid for $\mathcal{B}$.
4. *The extension and the contraction, restricted respectively to $\mathcal{A}$ and $\mathcal{B}$, are inverses of each other. They preserve multiplication, inclusion, intersection and the finitely generated character.*
5. *Assume that $\mathbf{B}$ is integral. Then, an ideal $\mathfrak{a} \in \mathcal{A}$ is invertible in $\mathbf{A}$ if and only if $\mathfrak{a}\mathbf{B}$ is invertible in $\mathbf{B}$. Similarly, an ideal $\mathfrak{b} \in \mathcal{B}$ is invertible in $\mathbf{B}$ if and only if $\mathbf{A} \cap \mathfrak{b}$ is invertible in $\mathbf{A}$.*

D We only prove a few properties. Notice that we always have the inclusions $\mathfrak{a} \subseteq \mathbf{A} \cap \mathfrak{a}\mathbf{B}$ and $(\mathbf{A} \cap \mathfrak{b})\mathbf{B} \subseteq \mathfrak{b}$.

Let $\mathfrak{a} \in \mathcal{A}$, so $1 = a + f$ with $a \in \mathfrak{a}$ and $f \in \mathfrak{f}$; a fortiori, $1 \in \mathfrak{a}\mathbf{B} + \mathfrak{f}$. Let us prove that $\mathbf{A} \cap \mathfrak{a}\mathbf{B} = \mathfrak{a}$. We take $x \in \mathbf{A} \cap \mathfrak{a}\mathbf{B}$ and we write

$$x = xf + xa \in \mathfrak{a}\mathbf{B}\mathfrak{f} + \mathfrak{a} \subseteq \mathfrak{a}\mathbf{A} + \mathfrak{a} = \mathfrak{a}\,.$$

Hence the result. We also see that $\mathbf{B} = \mathbf{A} + \mathfrak{a}\mathbf{B}$, so the composed morphism $\mathbf{A} \to \mathbf{B}/\mathfrak{a}\mathbf{B}$ is surjective with kernel $\mathfrak{a}$, which gives an isomorphism $\mathbf{A}/\mathfrak{a} \simeq \mathbf{B}/\mathfrak{a}\mathbf{B}$.

Let $\mathfrak{b} \in \mathcal{B}$, so $1 = b + f$ with $b \in \mathfrak{b}$, $f \in \mathfrak{f}$. Since $\mathfrak{f} \subseteq \mathbf{A}$, we have $b \in \mathbf{A} \cap \mathfrak{b}$ therefore $1 \in \mathbf{A} \cap \mathfrak{b} + \mathfrak{f}$. Let us prove that $(\mathbf{A} \cap \mathfrak{b})\mathbf{B} = \mathfrak{b}$. If $x \in \mathfrak{b}$, then

$$x = (b + f)x = bx + xf \in (\mathbf{A} \cap \mathfrak{b})\mathbf{B} + \mathfrak{b}\mathfrak{f} \subseteq (\mathbf{A} \cap \mathfrak{b})\mathbf{B} + \mathbf{A} \cap \mathfrak{b} \subseteq (\mathbf{A} \cap \mathfrak{b})\mathbf{B}.$$

Thus $\mathfrak{b} \subseteq (\mathbf{A} \cap \mathfrak{b})\mathbf{B}$ then $\mathfrak{b} = (\mathbf{A} \cap \mathfrak{b})\mathbf{B}$. In addition, since $\mathbf{B} = \mathfrak{b} + \mathfrak{f} \subseteq \mathfrak{b} + \mathbf{A}$, the composed morphism $\mathbf{A} \to \mathbf{B}/\mathfrak{b}$ is surjective, with kernel $\mathbf{A} \cap \mathfrak{b}$, which gives an isomorphism $\mathbf{A}/\mathbf{A} \cap \mathfrak{b} \simeq \mathbf{B}/\mathfrak{b}$.

The extension is multiplicative, so the contraction (restricted to $\mathcal{B}$) which is its inverse, is also multiplicative. The contraction is compatible with the intersection, so the extension (restricted to $\mathcal{A}$) which is its inverse, is also compatible with the intersection.

Let $\mathfrak{b} = \langle b_1, \ldots, b_n \rangle_{\mathbf{B}} \in \mathcal{B}$. Let us prove that $\mathbf{A} \cap \mathfrak{b}$ is finitely generated. We write $1 = a + f^2$ with $a \in \mathfrak{b}$, $f \in \mathfrak{f}$. Since $f \in \mathbf{A}$, we have $a \in \mathbf{A} \cap \mathfrak{b}$. We prove that $(a, fb_1, \ldots, fb_n)$ is a generator set of $\mathbf{A} \cap \mathfrak{b}$.

Let $x \in \mathbf{A} \cap \mathfrak{b}$ which we write as $x = \sum_i y_i b_i$ with $y_i \in \mathbf{B}$, then

$$x = \textstyle\sum_i (y_i a + y_i f^2) b_i = xa + \sum_i (y_i f) f b_i \in \langle a, fb_1, \ldots, fb_n \rangle_{\mathbf{A}} \,.$$

For an ideal $\mathfrak{b} \in \mathcal{B}$ (not necessarily finitely generated), we have in fact proved the following result: if $1 = a + f^2$ with $a \in \mathfrak{b}$ and $f \in \mathfrak{f}$, then $\mathbf{A} \cap \mathfrak{b} = \mathbf{A}a + f(f\mathfrak{b})$ (and $f\mathfrak{b}$ is an ideal of $\mathbf{A}$).

Let $\mathfrak{b} \in \mathcal{B}$ be an invertible ideal, let us prove that $\mathfrak{a} = \mathbf{A} \cap \mathfrak{b}$ is an invertible ideal. We write $1 = a + f$ with $a \in \mathfrak{b}$ and $f \in \mathfrak{f}$, such that $a \in \mathfrak{a}$.

If $a = 0$, then $1 = f \in \mathfrak{f}$, so $\mathbf{A} = \mathbf{B}$ and there is nothing left to prove. Otherwise, a is regular and there exists an ideal $\mathfrak{b}'$ of $\mathbf{B}$ such that $\mathfrak{b}\mathfrak{b}' = a\mathbf{B}$. Since the ideals $a\mathbf{B}$, $\mathfrak{b}$ and $\mathfrak{b}'$ are comaximal to $\mathfrak{f}$, we can apply the multiplicative character of the contraction to the equality $\mathfrak{b}\mathfrak{b}' = a\mathbf{B}$ to obtain the equality $\mathfrak{a}\mathfrak{a}' = a\mathbf{A}$ with $\mathfrak{a}' = \mathbf{A} \cap \mathfrak{b}'$. □

9. Hilbert's Nullstellensatz

In this section we illustrate the importance of the resultant by showing how Hilbert's Nullstellensatz can be deducted from it. We will use a generalization of the basic elimination lemma 7.5.

The algebraic closure of $\mathbb{Q}$ and of finite fields

Let $\mathbf{K} \subseteq \mathbf{L}$ be discrete fields. We say that $\mathbf{L}$ *is an algebraic closure of* $\mathbf{K}$ if $\mathbf{L}$ is algebraic over $\mathbf{K}$ and algebraically closed.

The reader will concede that $\mathbb{Q}$ and the fields $\mathbb{F}_p$ possess an algebraic closure. This will be discussed in further detail in Section VI-1, especially with Theorem VI-1.18.

The classical Nullstellensatz (algebraically closed case)

The Nullstellensatz is a theorem which concerns the systems of polynomial equations over a discrete field. Very informally, its meaning can be described as follows: a geometric statement necessarily possesses an algebraic certificate. Or even: a proof in commutative algebra can (almost) always be summarized by simple algebraic identities if it is sufficiently general.

If we have discrete fields $\mathbf{K} \subseteq \mathbf{L}$, and if $(\underline{f}) = (f_1, \ldots, f_s)$ is a system of polynomials in $\mathbf{K}[X_1, \ldots, X_n] = \mathbf{K}[\underline{X}]$, we say that $(\xi_1, \ldots, \xi_n) = (\underline{\xi})$ is a *zero of* $(\underline{f})$ *in* $\mathbf{L}^n$, or a *zero of* $(\underline{f})$ *with coordinates in* $\mathbf{L}$, if the equations $f_i(\underline{\xi}) = 0$ are satisfied. Let $\mathfrak{f} = \langle f_1, \ldots, f_s \rangle_{\mathbf{K}[\underline{X}]}$. Then, all the polynomials $g \in \mathfrak{f}$ are annihilated in such a $(\underline{\xi})$. We therefore equally refer to $(\underline{\xi})$ as a *zero of the ideal* $\mathfrak{f}$ *in* $\mathbf{L}^n$ or as *having coordinates in* $\mathbf{L}$.

We begin with an almost obvious fact.

9.1. Fact. *Let $\mathbf{k}$ be a commutative ring and $h \in \mathbf{k}[X]$ a monic polynomial of degree $\geqslant 1$.*

- *If some multiple of h is in $\mathbf{k}$, this multiple is null.*
- *Let f and $g \in \mathbf{k}[X]$ of respective formal degrees p and q. If h divides f and g, then $\mathrm{Res}_X(f, p, g, q) = 0$.*

We now present a generalization of the basic elimination lemma 7.5.

9.2. Lemma. (Elimination of a variable between several polynomials)
Let f, g_1, …, $g_r \in \mathbf{k}[X]$ ($r \geqslant 1$), with f monic of degree d.
Let $\mathfrak{f} = \langle f, g_1, \ldots, g_r\rangle$ and $\mathfrak{a} = \mathfrak{f} \cap \mathbf{k}$ (this is the elimination ideal of the variable X in $\mathfrak{f}$). Also let

$$g(T, X) = g_1 + Tg_2 + \cdots + T^{r-1}g_r \in \mathbf{k}[T, X],$$
$$R(T) = R(f, g_1, \ldots, g_r)(T) = \mathrm{Res}_X\big(f, g(T, X)\big) \in \mathbf{k}[T],$$
$$\mathfrak{b} = \mathfrak{R}(f, g_1, \ldots, g_r) \overset{\mathrm{def}}{=} \mathrm{c}_{\mathbf{k},T}\big(R(f, g_1, \ldots, g_r)(T)\big) \subseteq \mathbf{k}.$$

1. *The ideal $\mathfrak{b}$ is generated by $d(r-1)+1$ elements and we have the inclusions*
$$\mathfrak{b} \subseteq \mathfrak{a} \subseteq \sqrt{\mathfrak{b}} = \sqrt{\mathfrak{a}}\,. \tag{15}$$
More precisely, let $e_i = 1 + (d-i)(r-1)$, $i \in [\![1..d]\!]$, then for arbitrary elements a_1, …, $a_d \in \mathfrak{a}$, we have
$$a_1^{e_1}a_2^{e_2}\cdots a_d^{e_d} \in \mathfrak{R}(f, g_1, \ldots, g_r)\,.$$
In particular, we have the following equivalences
$$1 \in \mathfrak{b} \iff 1 \in \mathfrak{a} \iff 1 \in \mathfrak{f}\,. \tag{16}$$
2. *If $\mathbf{k}$ is a discrete field contained in a discrete algebraically closed field $\mathbf{L}$, let h be the monic gcd of f, g_1, …, g_r and V be the set of zeros of $\mathfrak{f}$ in $\mathbf{L}^n$. Then, we have the following equivalences*
$$1 \in \mathfrak{b} \iff 1 \in \mathfrak{a} \iff 1 \in \mathfrak{f} \iff h = 1 \iff V = \emptyset \tag{17}$$

D *1.* We know that $R(T)$ is of the form
$$u(T, X)f(X) + v(T, X)g(T, X),$$
so each coefficient of $R(T)$ is a linear combination of f and the g_i's in $\mathbf{k}[X]$. This gives the inclusion $\mathfrak{b} \subseteq \mathfrak{a}$. The inequality $\deg_T(R) \leqslant d(r-1)$ gives the majoration $d(r-1)+1$ for the number of generators of $\mathfrak{b}$.
If f_1, …, f_d are d polynomials (with one indeterminate) of degree $< r$, we deduce from the Dedekind-Mertens lemma (see Corollary 2.2) the following inclusion.
$$\mathrm{c}(f_1)^{e_1}\mathrm{c}(f_2)^{e_2}\cdots\mathrm{c}(f_d)^{e_d} \subseteq \mathrm{c}(f_1f_2\cdots f_d). \tag{$\star$}$$
Assume $f(X) = (X-x_1)\cdots(X-x_d)$. Then let for $i \in [\![1..d]\!]$
$$f_i(T) = g_1(x_i) + g_2(x_i)T + \cdots + g_r(x_i)T^{r-1},$$
such that $f_1f_2\cdots f_d = \mathrm{Res}_X(f, g_1 + g_2T + \cdots + g_rT^{r-1})$.
Thus, for $a_j \in \mathfrak{a} = \langle f, g_1, \ldots, g_r\rangle_{\mathbf{k}[X]} \cap \mathbf{k}$, by evaluating at x_i, we obtain $a_j \in \langle g_1(x_i), \ldots, g_r(x_i)\rangle = \mathrm{c}(f_i)$. By applying the inclusion ($\star$) we

obtain the membership $a_1^{e_1}a_2^{e_2}\cdots a_d^{e_d}\in\mathfrak{b}$.
Let us move on to the general case. Consider the universal splitting algebra $\mathbf{k}'=\mathrm{Adu}_{\mathbf{k},f}$. The previous computation is valid for $\mathbf{k}'$. Since $\mathbf{k}'=\mathbf{k}\oplus E$ as a $\mathbf{k}$-module, we have the equality $(\mathfrak{b}\mathbf{k}')\cap\mathbf{k}=\mathfrak{b}$. For some $a_j\in\mathfrak{a}$, this allows us to conclude that $a_1^{e_1}a_2^{e_2}\cdots a_d^{e_d}\in\mathfrak{b}$, because the product is in $(\mathfrak{b}\mathbf{k}')\cap\mathbf{k}$.

2. By definition of the gcd, we have $\mathfrak{f}=\langle h\rangle$. Moreover, $h=1\Leftrightarrow V=\emptyset$. So the rest clearly follows by item *1.*
Here is however a more direct proof for this particular case, which gives the point of origin of the magical proof of 1.
Assume that h is equal to 1; then in this case $1\in\mathfrak{f}$ and $1\in\mathfrak{a}$. Assume next that h is of degree $\geqslant 1$; then $\mathfrak{a}=\langle 0\rangle$. We therefore have obtained the equivalences $1\in\mathfrak{a}\iff 1\in\mathfrak{f}\iff\deg(h)=0$ and $\mathfrak{a}=\langle 0\rangle\iff\deg(h)\geqslant 1$.
Let us now prove the equivalence $\deg(h)\geqslant 1\iff\mathfrak{b}=\langle 0\rangle$.
If $\deg(h)\geqslant 1$, then $h(X)$ divides $g(T,X)$, so $R(f,g_1,\ldots,g_r)(T)=0$ (Fact 9.1), i.e. $\mathfrak{b}=\langle 0\rangle$.
Conversely, assume $\mathfrak{b}=\langle 0\rangle$. Then, for all values of the parameter $t\in\mathbf{L}$, the polynomials $f(X)$ and $g(t,X)$ have a common zero in $\mathbf{L}$ (f is monic and the resultant of both polynomials is null).
Consider the zeros $\xi_1,\ldots,\xi_d\in\mathbf{L}$ of f. By taking $d(r-1)+1$ distinct values of t, we find some ξ_ℓ such that $g(t,\xi_\ell)=0$ for at least r values of t. This implies that $g(T,\xi_\ell)$ is zero everywhere, i.e. that ξ_ℓ annihilates all the g_i's, and that h is a multiple of $X-\xi_\ell$, therefore $\deg(h)\geqslant 1$. □

Item *2* of Lemma 9.2 gives the following corollary.

9.3. Corollary. *Let $\mathbf{K}$ be a nontrivial discrete field contained in an algebraically closed field $\mathbf{L}$. Given the hypotheses of Lemma 9.2, with the ring $\mathbf{k}=\mathbf{K}[X_1,\ldots,X_{n-1}]$, then, for $\alpha=(\alpha_1,\ldots,\alpha_{n-1})\in\mathbf{L}^{n-1}$ the following properties are equivalent.*

1. *There exists a $\xi\in\mathbf{L}$ such that (α,ξ) annihilates $(f,g_1,\ldots,g_r)$.*
2. *α is a zero of the ideal $\mathfrak{b}=\mathfrak{R}(f,g_1,\ldots,g_r)\subseteq\mathbf{k}$.*

Note: if the total degree of the generators of $\mathfrak{f}$ is bounded above by d, we obtain as generators of $\mathfrak{b}$, $d(r-1)+1$ polynomials of total degree bounded by $2d^2$.

Remark. The above corollary has the desired structure to step through an induction which allows for a description of the zeros of $\mathfrak{f}$ in $\mathbf{L}^n$.
Indeed, by starting from the finitely generated ideal $\mathfrak{f}\subseteq\mathbf{K}[X_1,\ldots,X_n]$ we produce a finitely generated ideal $\mathfrak{b}\subseteq\mathbf{k}$ with the following property: *the zeros of $\mathfrak{f}$ in $\mathbf{L}^n$ are exactly projected onto the zeros of $\mathfrak{b}$ in $\mathbf{L}^{n-1}$.* More precisely, above each zero of $\mathfrak{b}$ in $\mathbf{L}^{n-1}$ there is a finite, nonzero number of zeros of $\mathfrak{f}$ in $\mathbf{L}^n$, bounded by $\deg_{X_n}(f)$.

So either all the generators of $\mathfrak{b}$ are zero and the process describing the zeros of $\mathfrak{f}$ is complete, or one of the generators of $\mathfrak{b}$ is nonzero and we are ready to do to $\mathfrak{b} \subseteq \mathbf{K}[X_1, \ldots, X_{n-1}]$ what we did to $\mathfrak{f} \subseteq \mathbf{K}[X_1, \ldots, X_n]$ *on the condition however that we find* a monic polynomial in X_{n-1} in the ideal $\mathfrak{b}$. This final question is resolved by the following change of variables lemma. ■

9.4. Lemma. (Change of variables lemma)
Let $\mathbf{K}$ *be an infinite discrete field and* $g \neq 0$ *in* $\mathbf{K}[\underline{X}] = \mathbf{K}[X_1, \ldots, X_n]$ *of degree* d*. There exists* $(a_1, \ldots, a_{n-1}) \in \mathbf{K}^{n-1}$ *such that the polynomial*

$$g(X_1 + a_1 X_n, \ldots, X_{n-1} + a_{n-1} X_n, X_n)$$

is of the form $aX_n^d + h$ *with* $a \in \mathbf{K}^\times$ *and* $\deg_{X_n} h < d$*.*

D Let g_d be the homogeneous components of degree d of g. Then

$$g(X_1 + a_1 X_n, \ldots, X_{n-1} + a_{n-1} X_n, X_n) = g_d(a_1, \ldots, a_{n-1}, 1) X_n^d + h,$$

with $\deg_{X_n} h < d$. Since $g_d(X_1, \ldots, X_n)$ is nonzero and homogeneous, the polynomial $g_d(X_1, \ldots, X_{n-1}, 1)$ is nonzero.
There thus exists $(a_1, \ldots, a_{n-1}) \in \mathbf{K}^{n-1}$ such that $g_d(a_1, \ldots, a_{n-1}, 1) \neq 0$.□

We now obtain a "weak Nullstellensatz" (i.e. the equivalence between $V = \emptyset$ and $\langle f_1, \ldots, f_s \rangle = \langle 1 \rangle$ in the theorem) and a "Noether position" which gives a description of V in the nonempty case.

9.5. Theorem. (Weak Nullstellensatz and Noether position)
Let $\mathbf{K}$ *be an infinite discrete field contained in an algebraically closed field* $\mathbf{L}$ *and* $(f_1, \ldots, f_s)$ *a polynomial system in* $\mathbf{K}[X_1, \ldots, X_n]$*.*
Let $\mathfrak{f} = \langle f_1, \ldots, f_s \rangle_{\mathbf{K}[\underline{X}]}$ *and* V *be the variety of the zeros of* $(f_1, \ldots, f_s)$ *in* $\mathbf{L}^n$*.*

1. *Either* $\langle f_1, \ldots, f_s \rangle = \langle 1 \rangle$*, and* $V = \emptyset$*.*
2. *Or* $V \neq \emptyset$*. Then there exist an integer* $r \in [\![0..n]\!]$*, a* $\mathbf{K}$*-linear change of variables (the new variables are denoted by* $Y_1, \ldots, Y_n$*), and finitely generated ideals* $\mathfrak{f}_j \subseteq \mathbf{K}[Y_1, \ldots, Y_j]$ $(j \in [\![r..n]\!])$*, which satisfy the following properties.*
   - *We have* $\mathfrak{f} \cap \mathbf{K}[Y_1, \ldots, Y_r] = 0$*. In other words, the ring* $\mathbf{K}[Y_1, \ldots, Y_r]$ *is identified with a subring of the quotient ring* $\mathbf{K}[\underline{X}]/\mathfrak{f}$*.*
   - *Each* Y_j $(j \in [\![r+1..n]\!])$ *is integral over* $\mathbf{K}[Y_1, \ldots, Y_r]$ *modulo* $\mathfrak{f}$*. In other words the ring* $\mathbf{K}[\underline{X}]/\mathfrak{f}$ *is integral over the subring* $\mathbf{K}[Y_1, \ldots, Y_r]$*.*
   - *We have the inclusions* $\langle 0 \rangle = \mathfrak{f}_r \subseteq \mathfrak{f}_{r+1} \subseteq \ldots \subseteq \mathfrak{f}_{n-1} \subseteq \mathfrak{f}$ *and for each* $j \in [\![r..n]\!]$ *we have the equality* $\sqrt{\mathfrak{f}} \cap \mathbf{K}[Y_1, \ldots, Y_j] = \sqrt{\mathfrak{f}_j}$*.*
   - *For the new coordinates corresponding to the* Y_i*'s, let* π_j *be the projection* $\mathbf{L}^n \to \mathbf{L}^j$ *which forgets the last coordinates* $(j \in [\![1..n]\!])$*. For each* $j \in [\![r..n-1]\!]$ *the projection of the variety* $V \subseteq \mathbf{L}^n$ *over* $\mathbf{L}^j$ *is exactly the variety* V_j *of the zeros of* $\mathfrak{f}_j$*. In addition, for each element* α *of* V_j*, the fiber* $\pi_j^{-1}(\alpha)$ *is finite, nonempty, with a uniformly bounded number of elements.*

In particular

- *Either V is empty (and we can concede that $r = -1$).*
- *Or V is finite and nonempty, $r = 0$ and the coordinates of the points of V are algebraic over* $\mathbf{K}$.
- *Or $r \geqslant 1$ and the projection π_r surjectively sends V onto $\mathbf{L}^r$ (so V is infinite). In this case, if $\alpha \in \mathbf{K}^r$, the coordinates of the points of $\pi_r^{-1}(\alpha)$ are algebraic over* $\mathbf{K}$.

D We reason as stated in the remark preceding the change of variables lemma. Note that the first step of the process only takes place if the initial polynomial system is nonzero, in which case the first operation consists in a linear change of variables which makes one of the f_i's monic in Y_n. □

Remarks.

1) The number r above corresponds to the maximum number of indeterminates for a polynomial ring $\mathbf{K}[Z_1, \dots, Z_r]$ which is isomorphic to a $\mathbf{K}$-subalgebra of $\mathbf{K}[\underline{X}]/\langle f_1, \dots, f_s \rangle$. This is related to Krull dimension theory which will be presented in Chapter XIII (see especially Theorem XIII-5.4).

2) Assume that the degrees of the f_j's are bounded above by d.
By basing ourselves on the result stated at the end of Corollary 9.3, we can give some bounds in the previous theorem by computing a priori, solely according to the integers n, s, j and d,

- on the one hand an upper bound for the number of generators for each ideal $\mathfrak{f}_j$,
- on the other hand an upper bound for the degrees of these generators.

3) The computation of the ideals $\mathfrak{f}_j$ as well as all the statements of the theorem which do not concern the variety V are valid even when we do not know of some algebraically closed field $\mathbf{L}$ containing $\mathbf{K}$. To do this, we only use Lemmas 9.2 and 9.4. We will look at this in more detail in Theorems VII-1.1 and VII-1.5. ■

The restriction introduced by the hypothesis "$\mathbf{K}$ is infinite" will vanish in the classical Nullstellensatz because of the following fact.

9.6. Fact. *Let $\mathbf{K} \subseteq \mathbf{L}$ be discrete fields and h, f_1, ..., $f_s \in \mathbf{K}[X_1, \dots, X_n]$, then $h \in \langle f_1, \dots, f_s \rangle_{\mathbf{K}[X_1,\dots,X_n]} \iff h \in \langle f_1, \dots, f_s \rangle_{\mathbf{L}[X_1,\dots,X_n]}$.*

D Indeed, an equality $h = \sum_i a_i f_i$, once the degrees of the a_i's are fixed, can be seen as a system of linear equations whose unknowns are the coefficients of the a_i's. The fact that a system of linear equations admits a solution does not depend on the field in which we look for the solution, so long as it contains the coefficients of the system of linear equations; the pivot method is a completely rational process. □

As a corollary of the weak Nullstellensatz and from the previous fact we obtain the classical Nullstellensatz.

9.7. Theorem. (Classical Nullstellensatz)
Let $\mathbf{K}$ *be a discrete field contained in an algebraically closed field* $\mathbf{L}$ *and* g, f_1, $\dots$, f_s *be some polynomials in* $\mathbf{K}[X_1,\dots,X_n]$. *Let* V *be the variety of the zeros of* $(f_1,\dots,f_s)$ *in* $\mathbf{L}^n$. *Then either 1. there exists a point* ξ *of* V *such that* $g(\xi)\neq 0$, *or 2. there exists an integer* N *such that* $g^N\in\langle f_1,\dots,f_s\rangle_{\mathbf{K}[\underline{X}]}$.

D The $g=0$ case is clear, so we suppose $g\neq 0$. We apply the *Rabinovitch trick*, i.e. we introduce an additional indeterminate T and we notice that g is annihilated at the zeros of $(f_1,\dots,f_s)$ if and only if the system $(1-gT,f_1,\dots,f_s)$ admits no solution. Then we apply the weak Nullstellensatz to this new polynomial system, with $\mathbf{L}$ (which is infinite) instead of $\mathbf{K}$. We obtain in $\mathbf{K}[\underline{X}][T]$ (thanks to Fact 9.6) an equality

$$\big(1-g(\underline{X})T\big)a(\underline{X},T)+f_1(\underline{X})b_1(\underline{X},T)+\cdots+f_s(\underline{X})b_s(\underline{X},T)=1.$$

In the localized ring $\mathbf{K}[\underline{X}][1/g]$, we perform the substitution $T=1/g$. More precisely, by remaining in $\mathbf{K}[\underline{X},T]$, if N is the greatest of the degrees in T of the b_i's, we multiply the previous equality by g^N and we replace in $g^Nb_i(\underline{X},T)$ each g^NT^k by g^{N-k} modulo $(1-gT)$. We then obtain an equality

$$\big(1-g(\underline{X})T\big)a_1(\underline{X},T)+f_1(\underline{X})c_1(\underline{X})+\cdots+f_s(\underline{X})c_s(\underline{X})=g^N,$$

in which $a_1=0$ necessarily, since if we look at a_1 in $\mathbf{K}[\underline{X}][T]$, its formally leading coefficient in T is zero. □

Remark. Note that the separation of the different cases in Theorems 9.5 and 9.7 is explicit. ■

9.8. Corollary. *Let* $\mathbf{K}$ *be a discrete field contained in an algebraically closed field* $\mathbf{L}$ *and* $\mathfrak{a}=\langle f_1,\dots,f_s\rangle$, $\mathfrak{b}$ *be two finitely generated ideals of* $\mathbf{K}[X_1,\dots,X_n]$. *Let* $\mathbf{K}_0$ *be the subfield of* $\mathbf{K}$ *generated by the coefficients of the* f_i*'s.*
The following properties are equivalent.

1. $\mathfrak{b}\subseteq \mathrm{D}_{\mathbf{K}[\underline{X}]}(\mathfrak{a})$.
2. $\mathfrak{b}\subseteq \mathrm{D}_{\mathbf{L}[\underline{X}]}(\mathfrak{a})$.
3. *Every zero of* $\mathfrak{a}$ *in* $\mathbf{L}^n$ *is a zero of* $\mathfrak{b}$.
4. *For every subfield* $\mathbf{K}_1$ *of* $\mathbf{L}$ *finite over* $\mathbf{K}_0$, *every zero of* $\mathfrak{a}$ *in* $\mathbf{K}_1^n$ *is a zero of* $\mathfrak{b}$.

In particular, $\mathrm{D}_{\mathbf{K}[\underline{X}]}(\mathfrak{a})=\mathrm{D}_{\mathbf{K}[\underline{X}]}(\mathfrak{b})$ *if and only if* $\mathfrak{a}$ *and* $\mathfrak{b}$ *have the same zeros in* $\mathbf{L}^n$.

D Immediate consequence of the Nullstellensatz. □

The formal Nullstellensatz

We now move onto a *formal Nullstellensatz*, formal in the sense that it applies (in classical mathematics) to an arbitrary ideal over an arbitrary ring. Nevertheless to have a constructive statement we will be content with a polynomial ring $\mathbb{Z}[\underline{X}]$ for our arbitrary ring and a finitely generated ideal for our arbitrary ideal.

Although this may seem very restrictive, practice shows that this is not the case because we can (almost) always apply the method of undetermined coefficients to a commutative algebra problem; a method which reduces the problem to a polynomial problem over $\mathbb{Z}$. An illustration of this will be given next.

Note that to read the statement, when we speak of a zero of some $f_i \in \mathbb{Z}[\underline{X}]$ over a ring $\mathbf{A}$, one must first consider f_i modulo $\operatorname{Ker}\varphi$, where φ is the unique homomorphism $\mathbb{Z} \to \mathbf{A}$, with $\mathbf{A}_1 \simeq \mathbb{Z}/\operatorname{Ker}\varphi$ as its image. This thus reduces to a polynomial $\overline{f_i}$ of $\mathbf{A}_1[\underline{X}] \subseteq \mathbf{A}[\underline{X}]$.

9.9. Theorem. (Nullstellensatz over $\mathbb{Z}$, formal Nullstellensatz)
Let $\mathbb{Z}[\underline{X}] = \mathbb{Z}[X_1, \ldots, X_n]$*. Consider* g, f_1, $\ldots$, f_s *in* $\mathbb{Z}[\underline{X}]$

1. *For the system* $(f_1, \ldots, f_s)$ *the following properties are equivalent.*
   - *a.* $1 \in \langle f_1, \ldots, f_s \rangle$.
   - *b. The system does not admit a zero on any nontrivial discrete field.*
   - *c. The system does not admit a zero on any finite field or on any finite extension of* $\mathbb{Q}$.
   - *d. The system does not admit a zero on any finite field.*
2. *The following properties are equivalent.*
   - *a.* $\exists N \in \mathbb{N},\ g^N \in \langle f_1, \ldots, f_s \rangle$.
   - *b. The polynomial* g *is annihilated at the zeros of the system* $(f_1, \ldots, f_s)$ *on any discrete field.*
   - *c. The polynomial* g *is annihilated at the zeros of the system* $(f_1, \ldots, f_s)$ *on every finite field and on every finite extension of* $\mathbb{Q}$.
   - *d. The polynomial* g *is annihilated at the zeros of the system* $(f_1, \ldots, f_s)$ *on every finite field.*

D It suffices to prove the weak version *1*, as we can then get the general version *2* by applying the Rabinovitch trick. Regarding the weak version, the difficult task is the implication $d \Rightarrow a$.

Let us first deal with $c \Rightarrow a$. Apply the weak Nullstellensatz by considering $\mathbb{Z} \subseteq \mathbb{Q}$. This gives the membership

$$m \in \langle f_1, \dots, f_s \rangle_{\mathbb{Z}[\underline{X}]} \quad \text{with } m \in \mathbb{Z} \setminus \{0\} \qquad (\star_{\mathbb{Q}}).$$

By applying the weak Nullstellensatz with an algebraic closure $\mathbf{L}_p$ of $\mathbb{F}_p$ we also obtain for each prime number $p \mid m$ a membership

$$1 \in \langle f_1, \dots, f_s \rangle_{\mathbb{Z}[\underline{X}]} + p\mathbb{Z}[\underline{X}] \qquad (\star_{\mathbb{F}_p}).$$

However, in any ring, for three arbitrary ideals $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$, we have the inclusion $(\mathfrak{a} + \mathfrak{b})(\mathfrak{a} + \mathfrak{c}) \subseteq \mathfrak{a} + \mathfrak{b}\mathfrak{c}$. By expressing the above m in $(\star_{\mathbb{Q}})$ in the form $\prod_j p_j^{k_j}$ with prime p_j's, we therefore obtain

$$1 \in \langle f_1, \dots, f_s \rangle_{\mathbb{Z}[\underline{X}]} + m\mathbb{Z}[\underline{X}].$$

This membership, joint with $(\star_{\mathbb{Q}})$, provides $1 \in \langle f_1, \dots, f_s \rangle_{\mathbb{Z}[\underline{X}]}$.

d $\Rightarrow$ *c*. We show that a zero $(\underline{\xi})$ of the system $(f_1, \dots, f_s)$ in a finite extension of $\mathbb{Q}$ leads to a zero of $(f_1, \dots, f_s)$ in a finite extension of $\mathbb{F}_p$ for all the prime numbers, except for a finite number of them.

Indeed, let $\mathbf{Q} = \mathbb{Q}[\alpha] \simeq \mathbb{Q}[X]/\langle h(X) \rangle$ (with h irreducible and monic in $\mathbb{Z}[X]$) be a finite extension of $\mathbb{Q}$ and $(\underline{\xi}) \in \mathbf{Q}^n$ be a zero of $(f_1, \dots, f_s)$. If $\xi_j = q_j(\alpha)$ with $q_j \in \mathbb{Q}[X]$ for $j \in [\![1..n]\!]$, this means that

$$f_i(q_1, \dots, q_n) \equiv 0 \bmod h \quad \text{in } \mathbb{Q}[X],\ i \in [\![1..s]\!].$$

This remains true in $\mathbb{F}_p[X]$ as soon as none of the denominators appearing in the q_j's is a multiple of p, provided one takes the fractions from $\mathbb{F}_p$

$$\overline{f_i}(\overline{q_1}, \dots, \overline{q_n}) \equiv 0 \bmod \overline{h} \quad \text{in } \mathbb{F}_p[X],\ i \in [\![1..s]\!].$$

For such a p, we take an irreducible monic divisor $h_p(X)$ of $\overline{h}(X)$ in $\mathbb{F}_p[X]$ and consider the finite field $\mathbf{F} = \mathbb{F}_p[X]/\langle h_p(X) \rangle$ with α_p the class of X. Then, $\big(q_1(\alpha_p), \dots, q_n(\alpha_p)\big)$ is a zero of $(f_1, \dots, f_s)$ in $\mathbf{F}^n$. □

We have the following immediate corollary, with finitely generated ideals.

9.10. Corollary. (Nullstellensatz over $\mathbb{Z}$, formal Nullstellensatz, 2)
Write $\mathbb{Z}[\underline{X}] = \mathbb{Z}[X_1, \dots, X_n]$. For two finitely generated ideals $\mathfrak{a}$, $\mathfrak{b}$ of $\mathbb{Z}[\underline{X}]$ the following properties are equivalent.

1. $\mathrm{D}_{\mathbb{Z}[\underline{X}]}(\mathfrak{a}) \subseteq \mathrm{D}_{\mathbb{Z}[\underline{X}]}(\mathfrak{b})$.
2. $\mathrm{D}_{\mathbf{K}}\big(\varphi(\mathfrak{a})\big) \subseteq \mathrm{D}_{\mathbf{K}}\big(\varphi(\mathfrak{b})\big)$ *for every discrete field* $\mathbf{K}$ *and every homomorphism* $\varphi : \mathbb{Z}[\underline{X}] \to \mathbf{K}$.
3. *Idem but restricted to algebraic extensions of* $\mathbb{Q}$ *and to finite fields.*
4. *Idem but restricted to finite fields.*

An application example

Consider the following result, already proven in Lemma II-2.6: *An element f of $\mathbf{A}[\underline{X}]$ is invertible if and only if $f(\underline{0})$ is invertible and $f - f(\underline{0})$ is nilpotent. In other words $\mathbf{A}[\underline{X}]^\times = \mathbf{A}^\times + \mathrm{D}_{\mathbf{A}}(0)[\underline{X}]$.*

We can assume that $fg = 1$ with $f = 1 + Xf_1$ and $g = 1 + Xg_1$. Consider the coefficients of f_1 and g_1 as being indeterminates. We are brought to prove the following result.

An equality $f_1 + g_1 + Xf_1g_1 = 0$ $(*)$ *implies that the coefficients of* f_1 *are nilpotent.*

However, since the indeterminates are evaluated in a field, the coefficients of f_1 are annihilated at the zeros of the polynomial system in the indeterminates given by the equality $(*)$. We conclude with the formal Nullstellensatz.

When compared with the proof given for item *4* of Lemma II-2.6, we can assert that the one given here is both simpler (no need to find a more subtle computation) and cleverer (usage of the formal Nullstellensatz).

Note. Another example is given in the solution to Problem XV-1. ∎

10. Newton's method in algebra

Let $\mathbf{k}$ be a ring and f_1, …, $f_s \in \mathbf{k}[\underline{X}] = \mathbf{k}[X_1, \dots, X_n]$. The *Jacobian matrix* of the system is the matrix

$$\mathrm{JAC}_{X_1,\dots,X_n}(f_1, \dots, f_s) = \left(\frac{\partial f_i}{\partial X_j}\right)_{i\in[\![1..s]\!],j\in[\![1..n]\!]} \in \mathbf{k}[\underline{X}]^{s\times n}.$$

It is also denoted by $\mathrm{JAC}_{\underline{X}}(\underline{f})$ or $\mathrm{JAC}(\underline{f})$. It is visualized as follows

$$\begin{array}{c|cccc|}
 & X_1 & X_2 & \cdots & X_n \\
f_1 & \frac{\partial f_1}{\partial X_1} & \frac{\partial f_1}{\partial X_2} & \cdots & \frac{\partial f_1}{\partial X_n} \\
f_2 & \frac{\partial f_2}{\partial X_1} & \frac{\partial f_2}{\partial X_2} & \cdots & \frac{\partial f_2}{\partial X_n} \\
f_i & \vdots & & & \vdots \\
 & \vdots & & & \vdots \\
f_s & \frac{\partial f_s}{\partial X_1} & \frac{\partial f_s}{\partial X_2} & \cdots & \frac{\partial f_s}{\partial X_n}
\end{array}.$$

If $s = n$, we denote by $\mathrm{Jac}_{\underline{X}}(\underline{f})$ or $\mathrm{Jac}_{X_1,\dots,X_n}(f_1, \dots, f_n)$ or $\mathrm{Jac}(\underline{f})$ the *Jacobian* of the system $(\underline{f})$, i.e. the determinant of the Jacobian matrix.

In analysis Newton's method to approximate a root of a differentiable function $f : \mathbb{R} \to \mathbb{R}$ is the following. Starting from a point x_0 "near a root," at which the derivative is "far from 0", we construct a series $(x_m)_{m\in\mathbb{N}}$ by induction by letting

$$x_{m+1} = x_m - \frac{f(x_m)}{f'(x_m)}.$$

The method can be generalized for a system of p equations with p unknowns. A solution of such a system is a zero of a function $f : \mathbb{R}^p \to \mathbb{R}^p$. We apply "the same formula" as above

$$x_{m+1} = x_m - f'(x_m)^{-1} \cdot f(x_m),$$

where $f'(x)$ is the differential (the Jacobian matrix) of f at the point $x \in \mathbb{R}^p$, which must be invertible in a neighborhood of x_0.

This method, and other methods of the infinitesimal calculus, can also be applied in certain cases in algebra, by replacing the Leibnizian infinitesimals by the nilpotent elements.

If for instance $\mathbf{A}$ is a $\mathbb{Q}$-algebra and $x \in \mathbf{A}$ is nilpotent, the formal series

$$1 + x + x^2/2 + x^3/6 + \dots$$

which defines $\exp(x)$ only has a finite number of nonzero terms in $\mathbf{A}$ and therefore defines an element $1 + y$ with y nilpotent. Since the equality

$$\exp(x + x') = \exp(x)\exp(x'),$$

holds in analysis, it is also valid with regard to formal series over $\mathbb{Q}$. So when x and x' are nilpotents in $\mathbf{A}$ we will obtain the same equality in $\mathbf{A}$. Similarly the formal series

$$y - y^2/2 + y^3/3 - \dots$$

which defines $\log(1 + y)$, only has a finite number of terms in $\mathbf{A}$ when y is nilpotent and allows for a definition of $\log(1 + y)$ as a nilpotent element of $\mathbf{A}$. Furthermore, for nilpotent x and y, we obtain the equalities

$$\log\big(\exp(x)\big) = x \text{ and } \exp\big(\log(1 + y)\big) = 1 + y$$

as consequences of the corresponding equalities for the formal series.

In a similar style we easily obtain, by using the inverse formal series of $1 - x$, the following result.

10.1. Lemma. (Residually invertible elements lemma)

1. *If $ef \equiv 1$ modulo the nilradical, then e is invertible and*
$$e^{-1} = f \textstyle\sum_{k\geqslant 0}(1 - ef)^k.$$
2. *A square matrix $E \in \mathbb{M}_n(\mathbf{A})$ invertible modulo the nilradical is invertible. Assume that $d\det(E) \equiv 1$ modulo the nilradical.*
Let $F = d\widetilde{E}$ (where $\widetilde{E}$ is the cotransposed matrix of E). Then, E^{-1} is in the subring of $\mathbb{M}_n(\mathbf{A})$ generated by the coefficients of the characteristic polynomial of E, d and E.
More precisely, the matrix $\mathrm{I}_n - EF = \big(1 - d\det(E)\big)\mathrm{I}_n$ is nilpotent and
$$E^{-1} = F \textstyle\sum_{k\geqslant 0}\big(1 - d\det(E)\big)^k.$$

Let us move on to Newton's method.

10.2. Theorem. (Newton's linear method)
Let $\mathfrak{N}$ be an ideal of $\mathbf{A}$, $\underline{f} = {}^{\mathrm{t}}[\, f_1 \ \cdots \ f_n \,]$ be a vector whose coordinates are polynomials in $\mathbf{A}[X_1, \ldots, X_n]$, and $\underline{a} = {}^{\mathrm{t}}(a_1, \ldots, a_n)$ in $\mathbf{A}^n$ be a approximated simple zero *of the system in the following sense.*

- *The Jacobian matrix $J(\underline{a})$ of $\underline{f}$ at point $\underline{a}$ is invertible modulo $\mathfrak{N}$; let $U \in \mathbb{M}_n(\mathbf{A})$ be such an inverse.*
- *The vector $\underline{f}(\underline{a})$ is null modulo $\mathfrak{N}$.*

Consider the sequence $(\underline{a}^{(m)})_{m \geqslant 1} \in \mathbf{A}^n$ defined by Newton's linear iteration

$$\underline{a}^{(1)} = \underline{a}, \quad \underline{a}^{(m+1)} = \underline{a}^{(m)} - U \cdot \underline{f}(\underline{a}^{(m)}).$$

a. *This sequence satisfies the following $\mathfrak{N}$-adic requirements:*
$$\underline{a}^{(1)} \equiv \underline{a} \mod \mathfrak{N}, \text{ and} \forall m, \ \underline{a}^{(m+1)} \equiv \underline{a}^{(m)} \text{ and } \underline{f}(\underline{a}^{(m)}) \equiv 0 \mod \mathfrak{N}^m.$$

b. *This sequence is unique in the following sense, if $\underline{b}^{(m)}$ is another sequence satisfying the requirements of a., then for all m, $\underline{a}^{(m)} \equiv \underline{b}^{(m)} \mod \mathfrak{N}^m$.*

c. *Let $\mathbf{A}_1$ be the subring generated by the coefficients of the f_i's, by those of U and by the coordinates of $\underline{a}$. In this ring let $\mathfrak{N}_1$ be the ideal generated by the coefficients of $\mathrm{I}_n - UJ(\underline{a})$ and the coordinates of $\underline{a}$. If the generators of $\mathfrak{N}_1$ are nilpotent, the sequence converges in a finite number of steps towards a zero of the system $\underline{f}$, and it is the unique zero of the system congruent to $\underline{a}$ modulo $\mathfrak{N}_1$.*

Under the same assumptions, we have the following quadratic method.

10.3. Theorem. (Newton's quadratic method)
Let us define the sequences $(\underline{a}^{(m)})_{m \geqslant 0}$ in $\mathbf{A}^n$ and $(U^{(m)})_{m \geqslant 0}$ in $\mathbb{M}_n(\mathbf{A})$ by the following Newton quadratic iteration

$$\begin{array}{ll} \underline{a}^{(0)} = \underline{a}, & \underline{a}^{(m+1)} = \underline{a}^{(m)} - U^{(m)} \cdot \underline{f}(\underline{a}^{(m)}), \\ U^{(0)} = U, & U^{(m+1)} = U^{(m)} \left(2\mathrm{I}_n - J(\underline{a}^{(m+1)}) U^{(m)}\right). \end{array}$$

Then, we obtain for all m the following congruences:

$$\begin{array}{llll} \underline{a}^{(m+1)} \equiv \underline{a}^{(m)} & \text{and} & U^{(m+1)} \equiv U^{(m)} & \mod \mathfrak{N}^{2^m} \\ \underline{f}(\underline{a}^{(m)}) \equiv 0 & \text{and} & U^{(m)} J(\underline{a}^{(m)}) \equiv \mathrm{I}_n & \mod \mathfrak{N}^{2^m}. \end{array}$$

The proofs are left to the reader (cf. [98]) by observing that the iteration concerning the inverse of the Jacobian matrix can be justified by Newton's linear method or by the following computation in a not necessarily commutative ring

$$(1 - ab)^2 = 1 - ab' \quad \text{with} \quad b' = b(2 - ab).$$

10.4. Corollary. (Residual idempotents lemma)

1. *For every commutative ring* $\mathbf{A}$*:*
   a. *two equal idempotents modulo* $\mathrm{D}_{\mathbf{A}}(0) = \sqrt{\langle 0 \rangle}$ *are equal;*
   b. *every idempotent* e *modulo an ideal* $\mathfrak{N}$ *is uniquely lifted to an idempotent* e' *modulo* $\mathfrak{N}^2$*; Newton's quadratic iteration is given by* $e \mapsto 3e^2 - 2e^3$*.*
2. *Similarly every matrix* $E \in \mathbb{M}_n(\mathbf{A})$ *idempotent modulo* $\mathfrak{N}$ *is lifted to a matrix* F *idempotent modulo* $\mathfrak{N}^2$*. The "lifting"* F *is unique provided that* $F \in \mathbf{A}[E]$*. Newton's quadratic iteration is given by* $E \mapsto 3E^2 - 2E^3$*.*

D *1a.* Left to the reader. A stronger version is proven in Lemma IX-5.1.
1b. Consider the polynomial $T^2 - T$, and note that $2e - 1$ is invertible modulo $\mathfrak{N}$ since $(2e-1)^2 = 1$ modulo $\mathfrak{N}$.
2. Apply item *1* with the commutative ring $\mathbf{A}[E] \subseteq \mathrm{End}(\mathbf{A}^n)$. □

Exercises and problems

Exercise 1. *(Lagrange interpolation)* Let $\mathbf{A}$ be a commutative ring. Prove the following statements.

1. Let f, $g \in \mathbf{A}[X]$ and $a_1, \ldots, a_k$ be elements of $\mathbf{A}$ such that $a_i - a_j \in \mathrm{Reg}\,\mathbf{A}$ for $i \neq j$.
   a. If the a_i's are zeros of f, f is a multiple of $(X - a_1) \cdots (X - a_k)$.
   b. If $f(a_i) = g(a_i)$ for $i \in [\![1..k]\!]$ and if $\deg(f - g) < k$, then $f = g$.
2. If $\mathbf{A}$ is integral and infinite, the element f of $\mathbf{A}[X]$ is characterized by the polynomial function that f defines over $\mathbf{A}$.
3. *(Lagrange interpolation polynomial)* Let $(x_0, \ldots, x_n)$ be in $\mathbf{A}$ such that each $x_i - x_j \in \mathbf{A}^\times$ (for $i \neq j$). Then, for $(y_0, \ldots, y_n)$ in $\mathbf{A}$ there exists exactly one polynomial f of degree $\leqslant n$ such that for each $j \in [\![0..n]\!]$ we have $f(x_j) = y_j$. More precisely, the polynomial f_i of degree $\leqslant n$ such that $f_i(x_i) = 1$ and $f_i(x_j) = 0$ for $j \neq i$ is equal to
$$f_i = \frac{\prod_{j \in [\![0..n]\!], j \neq i} (X - x_j)}{\prod_{j \in [\![0..n]\!], j \neq i} (x_i - x_j)},$$
and the interpolation polynomial f above is equal to $\sum_{i \in [\![0..n]\!]} y_i f_i$.
4. With the same assumptions, letting $h = (X - x_0) \cdots (X - x_n)$, we obtain an isomorphism of $\mathbf{A}$-algebras: $\mathbf{A}[X]/\langle h \rangle \to \mathbf{A}^{n+1}$, $\overline{g} \mapsto \big(g(x_0), \ldots, g(x_n)\big)$.
5. Interpret the previous results with linear algebra (Vandermonde matrix and determinant) and with the Chinese remainder theorem (use the pairwise comaximal ideals $\langle X - x_i \rangle$).

Exercise 2. *(Generators of the ideal of a finite set)* See also Exercise XIV-4. Let $\mathbf{K}$ be a discrete field and $V \subset \mathbf{K}^n$ be a finite set. Following the steps below show that the ideal $\mathfrak{a}(V) = \{\, f \in \mathbf{K}[\underline{x}] \mid \forall\, w \in V,\ f(w) = 0 \,\}$ is generated by n elements (note that this bound does not depend on $\#V$ and that the result is clear for $n = 1$). We denote by $\pi_n : \mathbf{K}^n \to \mathbf{K}$ the n^{th} projection and for each $\xi \in \pi_n(V)$,

$$V_\xi = \left\{\, (\xi_1, \dots, \xi_{n-1}) \in \mathbf{K}^{n-1} \mid (\xi_1, \dots, \xi_{n-1}, \xi) \in V \,\right\}.$$

1. Let $U \subset \mathbf{K}$ be a finite subset and to each $\xi \in U$, associate a polynomial
$$Q_\xi \in \mathbf{K}[x_1, \dots, x_{n-1}].$$
Find a polynomial $Q \in \mathbf{K}[\underline{x}]$ satisfying $Q(x_1, \dots, x_{n-1}, \xi) = Q_\xi$ for all $\xi \in U$.
2. Let $V \subset \mathbf{K}^n$ be a set such that $\pi_n(V)$ is finite. Suppose that for each $\xi \in \pi_n(V)$, the ideal $\mathfrak{a}(V_\xi)$ is generated by m polynomials. Show that $\mathfrak{a}(V)$ is generated by $m + 1$ polynomials. Conclude the result.

Exercise 3. *(Detailed proof of Theorem 1.5)*
Consider the ring $\mathbf{A}[X_1, \dots, X_n] = \mathbf{A}[\underline{X}]$ and let $S_1, \dots, S_n$ be the elementary symmetric functions of $\underline{X}$. All the considered polynomials are formal polynomials, because we do not assume that $\mathbf{A}$ is discrete. We introduce another system of indeterminates, $(\underline{s}) = (s_1, \dots, s_n)$, and on the ring $\mathbf{A}[\underline{s}]$ we define the weight δ by $\delta(s_i) = i$ (a formally nonzero polynomial has a well-defined formal weight).
Denote by $\varphi : \mathbf{A}[\underline{s}] \to \mathbf{A}[\underline{X}]$ the evaluation homomorphism defined by $\varphi(s_i) = S_i$. Consider on the monomials of $\mathbf{A}[\underline{X}] = \mathbf{A}[X_1, \dots, X_n]$ the `deglex` order for which two monomials are first compared according to their total degree, then according to the lexicographical order with $X_1 > \cdots > X_n$. This provides for some $f \in \mathbf{A}[\underline{X}]$ (formally nonzero) a notion of a *formally leading monomial* that we denote by $\operatorname{lm}(f)$. This "monomial order" is clearly isomorphic to $(\mathbb{N}, \leqslant)$.

0. Check that every symmetric polynomial (i.e. invariant under the action of S_n) of $\mathbf{A}[\underline{X}]$ is equal to some formally symmetric polynomial, i.e. invariant under the action of S_n as a formal polynomial.

1. (Injectivity of φ)
Let $\alpha = (\alpha_1, \dots, \alpha_n)$ be a decreasing exponent sequence ($\alpha_1 \geqslant \cdots \geqslant \alpha_n$).
Let $\beta_i = \alpha_i - \alpha_{i+1}$ ($i \in [\![1..n-1]\!]$). Show that

$$\operatorname{lm}(S_1^{\beta_1} S_2^{\beta_2} \cdots S_{n-1}^{\beta_{n-1}} S_n^{\alpha_n}) = X_1^{\alpha_1} X_2^{\alpha_2} \cdots X_n^{\alpha_n}.$$

Deduce that φ is injective.

2. (End of the proof of items 1 and 2 of Theorem 1.5) Let $f \in \mathbf{A}[\underline{X}]$ be a formally symmetric, formally nonzero polynomial, and $\underline{X}^\alpha = \operatorname{lm}(f)$.

- Show that α is decreasing. Deduce an algorithm to express every symmetric polynomial of $\mathbf{A}[\underline{X}]$ as a polynomial in $(S_1, \dots, S_n)$ with coefficients in $\mathbf{A}$, i.e. in the image of φ. The halting of the algorithm can be proven by induction on the monomial order, isomorphic to $\mathbb{N}$.
- As an example, write the symmetrized polynomial of the monomial $X_1^4 X_2^2 X_3$ in $\mathbf{A}[X_1, \dots, X_4]$ as a polynomial in the S_i's.

3. (Proof of item 3 of the theorem)

- Let $g(T) \in \mathbf{B}[T]$ be a monic polynomial of degree $n \geqslant 1$. Show that $\mathbf{B}[T]$ is a free $\mathbf{B}[g]$-module with basis $(1, T, \dots, T^{n-1})$.
  Deduce that $\mathbf{A}[S_1, \dots, S_{n-1}][X_n]$ is a free module over $\mathbf{A}[S_1, \dots, S_{n-1}][S_n]$, with basis $(1, X_n, \dots, X_n^{n-1})$.
- Denote by $\underline{S}' = (S'_1, \dots, S'_{n-1})$ the elementary symmetric functions of the variables $(X_1, \dots, X_{n-1})$. Show that $\mathbf{A}[\underline{S}', X_n] = \mathbf{A}[S_1, \dots, S_{n-1}, X_n]$.
- Deduce from the two previous items that $\mathbf{A}[\underline{S}', X_n]$ is a free $\mathbf{A}[\underline{S}]$-module with basis $(1, X_n, \dots, X_n^{n-1})$.
- Conclude by induction on n that the family
  $$\{\, X^\alpha \mid \alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n,\ \forall k \in [\![1..n]\!],\ \alpha_k < k \,\}$$
  forms a basis of $\mathbf{A}[\underline{X}]$ over $\mathbf{A}[\underline{S}]$.

4. (Another proof of item 3 of the theorem, and even more, after reading Section 4)
Prove that $\mathbf{A}[\underline{X}]$ is canonically isomorphic to the universal splitting algebra of the polynomial $t^n + \sum_{k=1}^{n} (-1)^k s_k t^{n-k}$ over the ring $\mathbf{A}[s_1, \dots, s_n]$.

Exercise 4. Let $S_1, \dots, S_n \in \mathbf{A}[\underline{X}] = \mathbf{A}[X_1, \dots, X_n]$ be the n elementary symmetric functions.

1. For $n = 3$, check that $X_1^3 + X_2^3 + X_3^3 = S_1^3 - 3S_1S_2 + 3S_3$. Deduce that for all n, $\sum_{i=1}^{n} X_i^3 = S_1^3 - 3S_1S_2 + 3S_3$.
2. By using a method analogous to the previous question, express the polynomials $\sum_{i \neq j} X_i^2 X_j$, $\sum_{i \neq j} X_i^3 X_j$, $\sum_{i<j} X_i^2 X_j^2$ in terms of the elementary symmetric functions.
3. State a general result.

Exercise 5. *(The Newton sums and the complete symmetric functions)*
Let $S_i \in \mathbf{A}[\underline{X}] = \mathbf{A}[X_1, \dots, X_n]$ be the elementary symmetric functions by agreeing to take $S_i = 0$ for $i > n$ and $S_0 = 1$.
For $r \geqslant 1$, define the *Newton sums* by $P_r = X_1^r + \cdots + X_n^r$. Work in the ring of formal series $\mathbf{A}[\underline{X}][[t]]$ and introduce the series

$$P(t) = \textstyle\sum_{r \geqslant 1} P_r\, t^r \quad \text{and} \quad E(t) = \sum_{r \geqslant 0} S_r\, t^r.$$

1. Check the equality $P(t) = \sum_{i=1}^{n} \frac{X_i}{1 - X_i t}$.
2. When $u \in \mathbf{B}[[t]]$ is invertible, considering the logarithmic derivative
   $$D_{\log}(u) = u' u^{-1},$$
   show that we get a morphism of groups $D_{\log} : (\mathbf{B}[[t]]^\times, \times) \to (\mathbf{B}[[t]], +)$.
3. By using the logarithmic derivation, prove *Newton's relation*
   $$P(-t) = \tfrac{E'(t)}{E(t)}, \quad \text{or } P(-t)E(t) = E'(t).$$
4. For $d \geqslant 1$, deduce Newton's formula
   $$\textstyle\sum_{r=1}^{d} (-1)^{r-1} P_r\, S_{d-r} = d\, S_d.$$

For $r \geqslant 0$, we define the *complete symmetric function of degree r* by

$$H_r = \sum\nolimits_{|\alpha|=r} \underline{X}^{\alpha}.$$

Thus $H_1 = S_1$, $H_2 = \sum_{i \leqslant j} X_i X_j$, $H_3 = \sum_{i \leqslant j \leqslant k} X_i X_j X_k$. We define the series

$$H(t) = \sum\nolimits_{r \geqslant 1} H_r \, t^r.$$

5. Show the equality $H(t) = \sum_{i=1}^{n} \frac{1}{1-X_i\,t}$.
6. Deduce the equality $H(t)\,E(-t) = 1$, then for $d \in [\![1..n]\!]$,
   $$\sum\nolimits_{r=0}^{d} (-1)^r S_r \, H_{d-r} = 0, \quad H_d \in \mathbf{A}[S_1, \ldots, S_d], \quad S_d \in \mathbf{A}[H_1, \ldots, H_d].$$
7. Consider the homomorphism $\varphi : \mathbf{A}[S_1, \ldots, S_n] \to \mathbf{A}[S_1, \ldots, S_n]$ defined by $\varphi(S_i) = H_i$. Show that $\varphi(H_d) = S_d$ for $d \in [\![1..n]\!]$. Thus
   - $\varphi \circ \varphi = \mathrm{I}_{\mathbf{A}[\underline{S}]}$,
   - $H_1, \ldots, H_n$ are algebraically independent over $\mathbf{A}$,
   - $\mathbf{A}[\underline{S}] = \mathbf{A}[\underline{H}]$, and expressing S_d in terms of $H_1, \ldots, H_d$ is the same as expressing H_d in terms of $S_1, \ldots, S_d$.

Exercise 6. *(Equivalent forms of the Dedekind-Mertens lemma)*
Prove that the following assertions are equivalent (each of the assertions is universal, i.e. valid for all polynomials and all commutative rings):

1. $\mathrm{c}(f) = \langle 1 \rangle \implies \mathrm{c}(g) = \mathrm{c}(fg)$.

2. $\exists p \in \mathbb{N}\ \ \mathrm{c}(f)^p \mathrm{c}(g) \subseteq \mathrm{c}(fg)$.

3. (Dedekind-Mertens, weak form) $\quad \exists p \in \mathbb{N}\ \ \mathrm{c}(f)^{p+1}\mathrm{c}(g) = \mathrm{c}(f)^p \mathrm{c}(fg)$.

4. $\mathrm{Ann}\big(\mathrm{c}(f)\big) = 0 \implies \mathrm{Ann}\big(\mathrm{c}(fg)\big) = \mathrm{Ann}\big(\mathrm{c}(g)\big)$.

5. (McCoy) $\quad \big(\mathrm{Ann}(\mathrm{c}(f)\big) = 0,\ fg = 0) \implies g = 0$.

6. $(\mathrm{c}(f) = \langle 1 \rangle\,,\ fg = 0) \implies g = 0$.

Exercise 7. Let $\mathfrak{c} = \mathrm{c}(f)$ be the content of $f \in \mathbf{A}[T]$. Dedekind-Mertens lemma gives $\mathrm{Ann}_{\mathbf{A}}(\mathfrak{c})[T] \subseteq \mathrm{Ann}_{\mathbf{A}[T]}(f) \subseteq \mathrm{D}_{\mathbf{A}}(\mathrm{Ann}_{\mathbf{A}}\big(\mathfrak{c})\big)[T]$. Give an example for which there is no equality.

Exercise 8. Deduce Kronecker's theorem (page 92) from the Dedekind-Mertens lemma.

Exercise 9. *(Cauchy modules)* We can give a very precise explanation for the fact that the ideal $\mathcal{J}(f)$ (Definition 4.1) is equal to the ideal generated by the Cauchy modules. This works with a beautiful formula. Let us introduce a new variable T. Prove the following results.

1. In $\mathbf{A}[X_1, \ldots, X_n, T] = \mathbf{A}[\underline{X}, T]$, we have
   $$\begin{aligned} f(T) \;=\; & f_1(X_1) + (T - X_1) f_2(X_1, X_2) + \\ & (T - X_1)(T - X_2) f_3(X_1, X_2, X_3) + \cdots + \\ & (T - X_1) \cdots (T - X_{n-1}) f_n(X_1, \ldots, X_n) + \\ & (T - X_1) \cdots (T - X_n) \end{aligned} \tag{18}$$

2. In the $\mathbf{A}[\underline{X}]$-submodule of $\mathbf{A}[\underline{X},T]$ formed by the polynomials of degree $\leqslant n$ in T, the polynomial $f(T)-(T-X_1)\cdots(T-X_n)$ possesses two different expressions.
   - On the one hand, over the basis $(1,T,T^2,\ldots,T^n)$, its coordinates are
   $$\big((-1)^n(s_n-S_n),\ldots,(s_2-S_2),-(s_1-S_1),0\big).$$
   - On the other hand, over the basis
   $$\big(1,(T-X_1),(T-X_1)(T-X_2),\ldots,(T-X_1)\cdots(T-X_n)\big),$$
   its coordinates are $(f_1,f_2,\ldots,f_n,0)$.

   Consequently over the ring $\mathbf{A}[X_1,\ldots,X_n]$, each of the two vectors
   $$\big((-1)^n(s_n-S_n),\ldots,(s_2-S_2),-(s_1-S_1)\big) \quad\text{and}\quad (f_1,\ldots,f_{n-1},f_n)$$
   are expressed in terms of the other by means of an unipotent matrix (triangular with 1's along the diagonal).

Exercise 10. *(The polynomial X^p-a)* Let $a\in\mathbf{A}^\times$ and p be a prime number. Suppose that the polynomial X^p-a has in $\mathbf{A}[X]$ a nontrivial monic divisor. Show that a is a p^{th} power in $\mathbf{A}$.

Exercise 11. *(With the extension principle of algebraic identities)*
Let $S_n(\mathbf{A})$ be the submodule of $\mathbb{M}_n(\mathbf{A})$ consisting of the symmetric matrices. For $A\in S_n(\mathbf{A})$, let φ_A be the endomorphism of $S_n(\mathbf{A})$ defined by $S\mapsto {}^{\mathrm{t}}ASA$. Compute $\det(\varphi_A)$ in terms of $\det(A)$. Show that C_{φ_A} only depends on C_A.

Exercise 12. Let $\mathbf{B}\supseteq\mathbf{A}$ be an integral $\mathbf{A}$-algebra which is a free $\mathbf{A}$-module of rank n, $\mathbf{K}=\mathrm{Frac}(\mathbf{A})$ and $\mathbf{L}=\mathrm{Frac}(\mathbf{B})$. Show that every basis of $\mathbf{B}/\mathbf{A}$ is a basis of $\mathbf{L}/\mathbf{K}$.

Exercise 13. Let $f\in\mathbf{A}[X]$, $g\in\mathbf{A}[Y]$, $h\in\mathbf{A}[X,Y]$. Prove that
$$\mathrm{Res}_Y\big(g,\mathrm{Res}_X(f,h)\big)=\mathrm{Res}_X\big(f,\mathrm{Res}_Y(g,h)\big).$$

Exercise 14. *(Newton sums and* $\mathrm{Tr}(A^k)$*)* Let $A\in\mathbb{M}_n(\mathbf{B})$ be a matrix.
Let $\mathrm{C}_A(X)=X^n+\sum_{j=1}^n(-1)^js_jX^{n-j}$, $s_0=1$ and $p_k=\mathrm{Tr}(A^k)$.

1. Show that the p_k's and s_j's are linked by Newton's formulas for the sums of the k^{th} powers (Exercise 5): $\sum_{r=1}^d(-1)^{r-1}p_rs_{d-r}=ds_d$ ($d\in[\![1..n]\!]$).

2. If $\mathrm{Tr}(A^k)=0$ for $k\in[\![1..n]\!]$, and if $n!$ is regular in $\mathbf{B}$, then $\mathrm{C}_A(X)=X^n$.

NB: this exercise can be considered as a variation on the theme of Proposition 5.9.

Exercise 15. Let $\mathbf{K}\subseteq\mathbf{L}$ be two finite fields, $q=\#\mathbf{K}$ and $n=[\,\mathbf{L}:\mathbf{K}\,]$. The subring of $\mathbf{K}$ generated by 1 is a field $\mathbb{F}_p$ where p is a prime number, and $q=p^r$ for an integer $r>0$. *Frobenius' automorphism* of (the $\mathbf{K}$-extension) $\mathbf{L}$ is given by $\sigma:\mathbf{L}\to\mathbf{L}$, $\sigma(x)=x^q$.

1. Let R be the union of the roots in $\mathbf{L}$ of the polynomials $X^{q^d}-X$ with $1\leqslant d<n$. Show that $\#R<q^n$ and that for $x\in\mathbf{L}\setminus R$, $\mathbf{L}=\mathbf{K}[x]$.

2. Here $\mathbf{K}=\mathbb{F}_2$ and $\mathbf{L}=\mathbb{F}_2[X]/\langle\Phi_5(X)\rangle=\mathbb{F}_2[x]$ where $\Phi_5(X)$ is the cyclotomic polynomial $X^4+X^3+X^2+X+1$. Check that $\mathbf{L}$ is indeed a field; x is a primitive element of $\mathbf{L}$ over $\mathbf{K}$ but it is not a generator of the multiplicative group $\mathbf{L}^\times$.

3. For $x \in \mathbf{L}^\times$, let $o(x)$ be its order in the multiplicative group $\mathbf{L}^\times$.
Show that $\mathbf{L} = \mathbf{K}[x]$ if and only if the order of q in the group $(\mathbb{Z}/\langle o(x)\rangle)^\times$ is n.

Exercise 16. The aim of the exercise is to prove that in a discrete field the group of n^{th} roots of unity is cyclic. Consequently the multiplicative group of a finite field is cyclic. We prove a result that is barely more general.
Show that in a nontrivial commutative ring $\mathbf{A}$, if elements $(x_i)_{i\in[\![1..n]\!]}$ form a group G for the multiplication, and if $x_i - x_j$ is regular for every pair i, j $(i \neq j)$, then G is cyclic.
Hint: by the structure theorem of finite Abelian groups, a finite Abelian group, additively denoted, in which every equation $dx = 0$ admits at most d solutions is cyclic. Also use Exercise 1.

Exercise 17. *(Structure of finite fields, Frobenius' automorphism)*

1. Prove that two finite fields which have the same order are isomorphic.

2. If $\mathbf{F} \supseteq \mathbb{F}_p$ is a finite field of order p^r, prove that $\tau : x \mapsto x^p$ defines an automorphism of $\mathbf{F}$. This is called *Frobenius' automorphism.* Show that the group of automorphisms of $\mathbf{F}$ is a cyclic group of order r generated by τ.

3. In the previous case, $\mathbf{F}$ is a Galois extension of $\mathbb{F}_p$. Describe the Galois correspondence.

NB: We often denote by $\mathbb{F}_q$ a finite field of order q, knowing that it is a slightly ambiguous notation if q is not prime.

Exercise 18. *(Algebraic closure of* $\mathbb{F}_p$*)*

1. For each integer $r > 0$ construct a field $\mathbb{F}_{p^{r!}}$ of order $p^{r!}$. By proceeding by induction we have an inclusion $\imath_r : \mathbb{F}_{p^{r!}} \hookrightarrow \mathbb{F}_{p^{(r+1)!}}$.

2. Construct a field $\mathbb{F}_{p^\infty}$ by taking the union of the $\mathbb{F}_{p^{r!}}$ via the inclusions $\imath_r$. Show that $\mathbb{F}_{p^\infty}$ is an algebraically closed field that contains a (unique) copy of each finite field of characteristic p.

Exercise 19. *(Lcm of separable polynomials)*

1. Let x, x', y, $y' \in \mathbf{B}$. Show that $\langle x, x'\rangle \langle y, y'\rangle \langle x, y\rangle^2 \subseteq \langle xy, x'y + y'x\rangle$.
Deduce that the product of two separable and comaximal monic polynomials in $\mathbf{A}[T]$ is a separable polynomial.

2. If $\mathbf{A}$ is a discrete field, the lcm of several separable polynomials is separable.

Exercise 20. *(Index of a finitely generated submodule in a free module)*

1. Let $A \in \mathbf{A}^{m\times n}$ and $E = \text{Im}(A) \subseteq \mathbf{A}^m$. Show that $\mathcal{D}_m(A)$ only depends on E. We call this ideal the *index of E in $L = \mathbf{A}^m$*, and we denote it by $|\,L : E\,|_{\mathbf{A}}$ (or $|\,L : E\,|$). Note that this index is null as soon as E is not sufficiently close to L, for example if $n < m$.
Check that in the case where $\mathbf{A} = \mathbb{Z}$ we find the usual index of the subgroup of a group for two free Abelian groups of the same rank.

2. If $E \subseteq F$ are finitely generated submodules of $L \simeq \mathbf{A}^m$, we have $|\,L : E\,| \subseteq |\,L : F\,|$.

3. In addition, if F is free and of rank m, we have the transitivity formula

$$|\,L:E\,| = |\,L:F\,|\,|\,F:E\,|.$$

4. If δ is a regular element of $\mathbf{A}$, we have $|\,\delta L : \delta E\,| = |\,L : E\,|$. Deduce the equality (14) (page 131) stated in Lemma 8.18.

Exercise 21. *(Remark on Fact 8.20)* Let $\mathfrak{a}$ and $\mathfrak{b}$ be two ideals in a ring $\mathbf{A}$ such that $\mathfrak{a}\,\mathfrak{b} = \langle a \rangle$ with a regular. Show that if $\mathfrak{a}$ is generated by k elements, we can find in $\mathfrak{b}$ a generator set of k elements.

Exercise 22. *(Decomposition of an ideal into a product of invertible maximal ideals)* Consider a nontrivial integral ring *with explicit divisibility*[8] $\mathbf{A}$.

1. If $\mathfrak{a}$ is an invertible ideal and if $\mathfrak{b}$ is a finitely generated ideal, prove that there is a test for $\mathfrak{b} \subseteq \mathfrak{a}$.

Let $\mathfrak{q}_1$, …, $\mathfrak{q}_n$ be maximal ideals (in the sense that the quotient rings $\mathbf{A}/\mathfrak{q}_k$ are nontrivial discrete fields), $\mathfrak{b}$ be a finitely generated ideal and a be a regular element of $\mathbf{A}$ satisfying $a\mathbf{A} = \mathfrak{q}_1 \cdots \mathfrak{q}_n \subseteq \mathfrak{b}$.

2. Show that the $\mathfrak{q}_i$'s are invertible and $\mathfrak{b}$ is the product of some of the $\mathfrak{q}_i$'s (and thus it is invertible). Furthermore, this decomposition of $\mathfrak{b}$ into a product of finitely generated maximal ideals is unique up to order of the factors.

Exercise 23. *(Legendre symbol)*
Let $\mathbf{k}$ be a finite field of odd cardinality q; we define the *Legendre symbol*

$$\left(\frac{\bullet}{\mathbf{k}}\right) : \mathbf{k}^\times \longrightarrow \{\pm 1\},\ x \longmapsto \begin{cases} \ \ 1 \text{ if } x \text{ is a square in } \mathbf{k}^\times, \\ -1 \text{ otherwise.} \end{cases}$$

Show that $\left(\frac{\cdot}{\mathbf{k}}\right)$ is a group morphism and that $\left(\frac{x}{\mathbf{k}}\right) = x^{\frac{q-1}{2}}$.
In particular, -1 is a square in $\mathbf{k}^\times$ if and only if $q \equiv 1 \bmod 4$.

NB: if p is an odd prime number and x is an integer comaximal to p we find Legendre's symbol $\left(\frac{x}{p}\right)$ in the form $\left(\frac{\overline{x}}{\mathbb{F}_p}\right)$.

Exercise 24. *(Rabinovitch's trick)*
Let $\mathfrak{a} \subseteq \mathbf{A}$ be an ideal and $x \in \mathbf{A}$. Consider the following ideal of $\mathbf{A}[T]$:

$$\mathfrak{b} = \langle \mathfrak{a}, 1 - xT \rangle = \mathfrak{a}[T] + \langle 1 - xT \rangle_{\mathbf{A}[T]}\,.$$

Show the equivalence $x \in \sqrt{\mathfrak{a}} \iff 1 \in \mathfrak{b}$.

Exercise 25. *(Jordan-Chevalley-Dunford decomposition)*
Let $M \in \mathbb{M}_n(\mathbf{A})$. Suppose that the characteristic polynomial of M divides a power of a separable polynomial f.

1. Show that there exist D, $N \in \mathbb{M}_n(\mathbf{A})$ such that:

- D and N are polynomials in M (with coefficients in $\mathbf{A}$).
- $M = D + N$.

[8] We say that an arbitrary ring is with explicit divisibility if we have an algorithm that tests, for a and $b \in \mathbf{A}$, if $\exists x$, $a = bx$, and in case of a positive answer, gives a suitable x.

- $f(D) = 0$.
- N is nilpotent.

2. Prove the uniqueness of the above decomposition, including by weakening the first constraint, by only requiring that $DN = ND$.

Exercise 26. *(Separably integral elements)*
Let $\mathbf{A} \subseteq \mathbf{B}$. We say that $z \in \mathbf{B}$ is *separably integral* over $\mathbf{A}$ if z is a root of a separable monic polynomial of $\mathbf{A}[T]$. Here we are looking for an example for which the sum of two separably integral elements is a nonzero nilpotent and nonseparably integral element.
Let $\mathbf{B} = \mathbf{A}[x] = \mathbf{A}[X]\big/\big\langle X^2 + bX + c\big\rangle$. Suppose that $\Delta = b^2 - 4c$ is a unit of $\mathbf{A}$. For $a \in \mathbf{A}$, compute the characteristic polynomial of ax over $\mathbf{A}$ and its discriminant. Deduce an example as stated when $\mathrm{D}_{\mathbf{A}}(0) \neq 0$.

Problem 1. *(Some useful resultants and discriminants)*
1. Show that $\operatorname{disc}(X^n + c) = (-1)^{\frac{n(n-1)}{2}} n^n c^{n-1}$. More generally, prove for $n \geqslant 2$ the equality

$$\operatorname{disc}(X^n + bX + c) = (-1)^{\frac{n(n-1)}{2}} \big(n^n c^{n-1} + (1-n)^{n-1} b^n\big).$$

2. For $n, m \in \mathbb{N}^*$, by letting $d = \gcd(n, m)$, $n_1 = \dfrac{n}{d}$ and $m_1 = \dfrac{m}{d}$ prove the equality

$$\operatorname{Res}(X^n - a, X^m - b) = (-1)^n (b^{n_1} - a^{m_1})^d.$$

More generally

$$\operatorname{Res}(\alpha X^n - a, n, \beta X^m - b, m) = (-1)^n (\alpha^{m_1} b^{n_1} - \beta^{n_1} a^{m_1})^d.$$

3. Notations as in item *2*, with $1 \leqslant m \leqslant n-1$. Then prove

$$\operatorname{disc}(X^n + bX^m + c) = (-1)^{\frac{n(n-1)}{2}} c^{m-1} \big(n^{n_1} c^{n_1 - m_1} - (n-m)^{n_1 - m_1} m^{m_1} (-b)^{n_1}\big)^d.$$

4. For $n \in \mathbb{N}^*$, denote by Φ_n the cyclotomic polynomial of level n (see Problem 4). Then, for prime $p \geqslant 3$ prove

$$\operatorname{disc}(\Phi_p) = (-1)^{\frac{p-1}{2}} p^{p-2}.$$

5. Let p be prime and $k \geqslant 1$. Then prove that $\Phi_{p^k}(X) = \Phi_p(X^{p^{k-1}})$ and

$$\operatorname{disc}(\Phi_{p^k}) = (-1)^{\frac{\varphi(p^k)}{2}} p^{(k(p-1)-1)p^{k-1}} \qquad (p, k) \neq (2, 1),$$

with for $p \neq 2$, $(-1)^{\frac{\varphi(p^k)}{2}} = (-1)^{\frac{p-1}{2}}$. For $p = 2$, prove that we obtain $\operatorname{disc}(\Phi_4) = -4$ and $\operatorname{disc}(\Phi_{2^k}) = 2^{(k-1)2^{k-1}}$ for $k \geqslant 3$. In addition, prove that $\operatorname{disc}(\Phi_2) = 1$.

6. Let $n \geqslant 1$ and ζ_n be an n^{th} primitive root of the unit.
If n is not the power of a prime number, then prove that $\Phi_n(1) = 1$, and $1 - \zeta_n$ is invertible in $\mathbb{Z}[\zeta_n]$.
If $n = p^k$ with p prime, $k \geqslant 1$, then prove that $\Phi_n(1) = p$. Finally, prove that $\Phi_1(1) = 0$.

7. Let $\Delta_n = \operatorname{disc}(\Phi_n)$. For coprime n, m, prove that we have the multiplicativity formula $\Delta_{nm} = \Delta_n^{\varphi(m)} \Delta_m^{\varphi(n)}$ and the equality

$$\Delta_n = (-1)^{\frac{\varphi(n)}{2}} \frac{n^{\varphi(n)}}{\prod_{p \mid n} p^{\frac{\varphi(n)}{p-1}}} \qquad \text{for } n \geqslant 3.$$

Problem 2. *(Euclidean rings, the $\mathbb{Z}[i]$ example)*
A *Euclidean stathm* is a map $\varphi : \mathbf{A} \to \mathbb{N}$ that satisfies the following properties[9] (roughly speaking, we copy the Euclidean division in $\mathbb{N}$)

- $\varphi(a) = 0 \iff a = 0$.
- $\forall a, b \neq 0,\ \exists q, r, \quad a = bq + r$ and $\varphi(r) < \varphi(b)$.

A *Euclidean ring* is a nontrivial integral ring given with a Euclidean stathm. Note that the ring is discrete. We can then do with the "division" given by the stathm the same thing we do in $\mathbb{Z}$ with Euclidean division.
The most renowed examples are the following.

- $\mathbb{Z}$, with $\varphi(x) = |x|$,
- $\mathbf{K}[X]$ ($\mathbf{K}$ a discrete field), with $\varphi(P) = 1 + \deg(P)$ for $P \neq 0$,
- $\mathbb{Z}[i] \simeq \mathbb{Z}[X]\big/\big\langle X^2 + 1\big\rangle$, with $\varphi(m + in) = m^2 + n^2$,
- $\mathbb{Z}[i\sqrt{2}] \simeq \mathbb{Z}[X]\big/\big\langle X^2 + 2\big\rangle$, with $\varphi(m + i\sqrt{2}n) = m^2 + 2n^2$.

In addition, in these examples we have the equivalence $x \in \mathbf{A}^\times \iff \varphi(x) = 1$.

1. *(Extended Euclidean algorithm)* For all a, b, there exist u, v, a_1, b_1, g such that
$$\begin{bmatrix} g \\ 0 \end{bmatrix} = \begin{bmatrix} u & v \\ -b_1 & a_1 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} \quad \text{and} \quad ua_1 + vb_1 = 1.$$
In particular, $\langle a, b\rangle = \langle g\rangle$ and g is a gcd of a and b. If $(a, b) \neq (0, 0)$, $\dfrac{ab}{g}$ is a lcm of a and b.
2. a. Show that the ring $\mathbf{A}$ is principal.
   b. Let us make the following assumptions.
      - $\mathbf{A}^\times$ is a detachable subset of $\mathbf{A}$.
      - We have a primality test at our disposal for the elements of $\mathbf{A} \setminus \mathbf{A}^\times$ in the following sense: given $a \in \mathbf{A} \setminus \mathbf{A}^\times$ we know how to decide if a is irreducible, and in case of a negative response, write a in the form bc with b, $c \in \mathbf{A} \setminus \mathbf{A}^\times$.

   Show then that $\mathbf{A}$ satisfies the "fundamental theorem of arithmetic" (unique decomposition into prime factors, up to association).

The $\mathbb{Z}[i]$ example. Recall that $z = m + in \mapsto \overline{z} = m - in$ is an automorphism of $\mathbb{Z}[i]$ and that the norm $\mathrm{N} = \mathrm{N}_{\mathbb{Z}[i]/\mathbb{Z}}$ ($\mathrm{N}(z) = z\overline{z}$) is a Euclidean stathm. Take an element of $\mathbb{Z}[i]$ close to $a/b \in \mathbb{Q}[i]$ for the above q and check that $\mathrm{N}(r) \leqslant \mathrm{N}(b)/2$. To know which are the irreducible elements of $\mathbb{Z}[i]$, it suffices to know how to decompose in $\mathbb{Z}[i]$ each prime number p of $\mathbb{N}$.
This amounts to determining the ideals containing $p\mathbb{Z}[i]$, i.e. the ideals of $\mathbf{Z}_p := \mathbb{Z}[i]/\langle p\rangle$. But $\mathbf{Z}_p \simeq \mathbb{F}_p[X]\big/\big\langle X^2 + 1\big\rangle$. We are thus reduced to finding the divisors of $X^2 + 1$, therefore to factorizing $X^2 + 1$, in $\mathbb{F}_p[X]$.

[9] In the literature we sometimes find a "Euclidean stathm" defined as a map $\varphi : \mathbf{A} \to \mathbb{N} \cup \{-\infty\}$, or $\varphi : \mathbf{A} \to \mathbb{N} \cup \{-1\}$ (the minimum value being always equal to $\varphi(0)$).

3. Show that a priori three cases can arise.
   - $X^2 + 1$ is irreducible in $\mathbb{F}_p[X]$, and p is irreducible in $\mathbb{Z}[i]$.
   - $X^2 + 1 = (X + u)(X - u)$ in $\mathbb{F}_p[X]$ with $u \neq -u$, and then
     $$\langle p \rangle = \langle i + u, p \rangle \, \langle i - u, p \rangle = \langle m + in \rangle \, \langle m - in \rangle \text{ and } p = m^2 + n^2.$$
   - $X^2 + 1 = (X + u)^2$ in $\mathbb{F}_p[X]$, and then $\langle p \rangle = \langle i + u \rangle^2$. This only happens for $p = 2$, with $2 = (-i)(1 + i)^2$ (where $-i \in \mathbb{Z}[i]^\times$).
4. If $p \equiv 3 \bmod 4$, then -1 is not a square in $\mathbb{F}_p$. If $p \equiv 1 \bmod 4$, then -1 is a square in $\mathbb{F}_p$. In this case give an efficient algorithm to write p in the form $m^2 + n^2$ in $\mathbb{N}$.
5. Let $z \in \mathbb{Z}[i]$. We can write $z = m(n + qi)$ with $m, n, q \in \mathbb{N}$ $\gcd(n, q) = 1$. Give an efficient algorithm to decompose z into prime factors in $\mathbb{Z}[i]$ knowing a decomposition into prime factors of $\mathrm{N}(z) = m^2(n^2 + q^2)$ in $\mathbb{N}$.
   Given a decomposition into prime factors of $s \in \mathbb{N}$, describe under which condition s is a sum of two squares, as well as the number of expressions $s = a^2 + b^2$ with $0 < a \leqslant b$ in $\mathbb{N}$.
6. Say in which (relatively rare) cases we can generalize the previous procedure to decompose into prime factors the finitely generated ideals of a ring $\mathbb{Z}[\alpha]$, when α is an algebraic integer.

Problem 3. *(Kummer's little theorem)*
Problem 2 can be generalized for rings of principal integers of the form $\mathbb{Z}[\alpha]$, but this case is relatively rare. On the contrary, Kummer's little theorem gives the decomposition of a prime number (in $\mathbb{N}$) into products of 2-generated maximal ideals for almost all the prime numbers, in all the rings of integers. This shows the intrinsic superiority of the "ideal numbers" introduced by Kummer. Furthermore, the argument is extremely simple and only requires the Chinese remainder theorem. However, the prime numbers that do not fall under the scope of Kummer's little theorem constitute in fact the heart of algebraic number theory. Those are the ones that required a fine tuning of the theory (according to two distinct methods due to Kronecker and Dedekind), without which all decisive progress would not have been possible.

Consider a zero α of an irreducible monic polynomial $f(T) \in \mathbb{Z}[T]$, such that $\mathbb{Z}[\alpha] \simeq \mathbb{Z}[T]/\langle f(T) \rangle$. Let $\Delta = \mathrm{disc}(f)$.

1. Let p be a prime number which does not divide Δ.
   - Show that $f(T)$ is separable in $\mathbb{F}_p[T]$.
   - Decompose $f(T)$ in $\mathbb{F}_p[T]$ in the form $\prod_{k=1}^{\ell} Q_k(T)$ with distinct monic irreducible Q_k's. Let $q_k = Q_k(\alpha)$ (in fact it is only defined modulo p, but we can lift Q_k in $\mathbb{Z}[T]$). Show that in $\mathbb{Z}[\alpha]$ we have $\langle p \rangle = \prod_{k=1}^{\ell} \langle p, q_k \rangle$ and that the ideals $\langle p, q_k \rangle$ are maximal, distinct and invertible. In particular, if $\ell = 1$, $\langle p \rangle$ is maximal.
   - Show that this decomposition remains valid in every ring $\mathbf{A}$ such that $\mathbb{Z}[\alpha] \subseteq \mathbf{A} \subseteq \mathbf{Z}$, where $\mathbf{Z}$ is the ring of integers of $\mathbb{Q}[\alpha]$.

2. Let $a \in \mathbb{Z}[\alpha]$ such that $A = \mathrm{N}_{\mathbb{Z}[\alpha]/\mathbb{Z}}(a)$ is comaximal to Δ. Let $\mathfrak{a} = \langle b_1, \ldots, b_r \rangle$ be a finitely generated ideal of $\mathbb{Z}[\alpha]$ containing a. Show that in $\mathbb{Z}[\alpha]$ the ideal $\mathfrak{a}$ is invertible and can be decomposed into products of maximal ideals that divide the prime factors of A. Finally, this decomposition is unique up to order of the factors and all of this remains valid in every ring $\mathbf{A}$ as above.

Problem 4. *(The cyclotomic polynomial Φ_n)*
In $\mathbf{A}[X]$, the polynomial $X^n - 1$ is separable if and only if $n \in \mathbf{A}^\times$.
Let $\mathbf{Q}_n$ be a splitting field over $\mathbb{Q}$ for this polynomial. Let $\mathbb{U}_n$ be the group of n^{th} roots of the unit in $\mathbf{Q}_n$. It is a cyclic group of order n, which therefore has $\varphi(n)$ generators (n^{th} primitive roots of the unit). We define $\Phi_n(X) \in \mathbf{Q}_n[X]$ by $\Phi_n(X) = \prod_{o(\xi)=n}(X - \xi)$. It is a monic polynomial of degree $\varphi(n)$. We have the fundamental equality

$$X^n - 1 = \prod\nolimits_{d|n} \Phi_d(X),$$

which allows us to prove by induction on n that $\Phi_n(X) \in \mathbb{Z}[X]$.

1. Following the steps below, prove that $\Phi_n(X)$ is irreducible in $\mathbb{Z}[X]$ (therefore in $\mathbb{Q}[X]$, Proposition 8.15). Let f, g be two monic polynomials of $\mathbb{Z}[X]$ with $\Phi_n = fg$ and $\deg f \geqslant 1$; you must prove that $g = 1$.

   a. It suffices to prove that $f(\xi^p) = 0$ for every prime $p \not| n$ and for every zero ξ of f in $\mathbf{Q}_n$.

   b. Suppose that $g(\xi^p) = 0$ for some zero ξ of f in $\mathbf{Q}_n$. Examine what happens in $\mathbb{F}_p[X]$ and conclude the result.

2. Let us fix a root ξ_n of Φ_n in $\mathbf{Q}_n$.
   Show that $\mathbf{Q}_n = \mathbb{Q}(\xi_n)$ and that with $(\mathbb{Q}, \mathbf{Q}_n, \Phi_n)$, we are in the elementary Galois situation of Lemma 6.13.
   Describe the explicit isomorphisms of the groups

$$\mathrm{Aut}(\mathbb{U}_n) \simeq (\mathbb{Z}/n\mathbb{Z})^\times \simeq \mathrm{Gal}(\mathbf{Q}_n/\mathbb{Q}).$$

3. Let $\mathbf{K}$ be a field of characteristic 0. What can be said of a splitting field $\mathbf{L}$ of $X^n - 1$ over $\mathbf{K}$?

Problem 5. *(The ring $\mathbb{Z}[\sqrt[n]{1}]$: Prüfer domain, factorization of ideals)*
Let $\Phi_n(X) \in \mathbb{Z}[X]$ be the cyclotomic polynomial of order n, irreducible over $\mathbb{Q}$. Let $\mathbf{Q}_n = \mathbb{Q}(\zeta_n) \simeq \mathbb{Q}[X]/\langle\Phi_n\rangle$. The multiplicative group $\mathbb{U}_n$ generated by ζ_n (n^{th} primitive root of the unit) is cyclic of order n.
Among other things we will prove that the ring $\mathbf{A} = \mathbb{Z}[\mathbb{U}_n] = \mathbb{Z}[\zeta_n] \simeq \mathbb{Z}[X]/\langle\Phi_n\rangle$ is a *Prüfer domain*: an integral ring whose nonzero finitely generated ideals are invertible (cf. Section VIII-4 and Chapiter XII).

1. Let $p \in \mathbb{N}$ be a prime number. The steps below show that $\sqrt{p\mathbf{A}}$ is a principal ideal and express it as a finite product of 2-generated invertible maximal ideals. Consider the distinct irreducible factors of Φ_n modulo p that we lift to the monic polynomials $f_1, \dots, f_k \in \mathbb{Z}[X]$. Let $g = f_1 \cdots f_k$ (such that $\overline{g}$ is the subset without a square factor of Φ_n modulo p) and $\mathfrak{p}_i = \langle p, f_i(\zeta_n)\rangle$ for $i \in [\![1..k]\!]$.

a. Show that $\mathfrak{p}_i$ is a maximal ideal and that
$$\sqrt{p\mathbf{A}} = \langle p, g(\zeta_n)\rangle = \mathfrak{p}_1 \dots \mathfrak{p}_k$$

b. If p does not divide n, prove that $\overline{g} = \overline{\Phi_n}$, thus $\sqrt{p\mathbf{A}} = \langle p\rangle$ is a principal ideal.

c. Suppose that p divides n and write $n = mp^k$ with $k \geqslant 1$, $\gcd(m, p) = 1$.
By studying the factorization of Φ_n modulo p, prove that $\overline{g} = \overline{\Phi_m}$. Deduce that $\sqrt{p\mathbf{A}} = \langle p, \Phi_m(\zeta_n)\rangle$. Then prove that $p \in \langle\Phi_m(\zeta_n)\rangle$, and therefore that $\sqrt{p\mathbf{A}} = \langle\Phi_m(\zeta_n)\rangle$ is a principal ideal.

d. Deduce that $p\mathbf{A}$ is a product of the form $\mathfrak{p}_1^{e_1} \dots \mathfrak{p}_k^{e_k}$.

2. Let $a \in \mathbb{Z} \setminus \{0\}$; prove that $a\mathbf{A}$ is a product of invertible maximal ideals with two generators. Deduce that in $\mathbf{A}$ every nonzero finitely generated ideal can be decomposed into a product of 2-generated invertible maximal ideals and that the decomposition is unique up to factor order.

Problem 6. *(An elementary property of Gauss sums)*
Let $\mathbf{k}$ be a finite field of cardinality q and $\mathbf{A}$ be an integral ring. Consider

- a "multiplicative character" $\chi : \mathbf{k}^\times \to \mathbf{A}^\times$, i.e. a morphism of multiplicative groups,
- an "additive character" $\psi : \mathbf{k} \to \mathbf{A}^\times$, i.e. a morphism of groups
$$\psi : (\mathbf{k}, +) \to (\mathbf{A}^\times, \times).$$

Suppose that neither χ nor ψ are trivial and that χ is extended to the whole of $\mathbf{k}$ via $\chi(0) = 0$. Finally, the Gauss sum of χ is defined, with respect to ψ, by
$$G_\psi(\chi) = \textstyle\sum_{x\in\mathbf{k}} \chi(x)\psi(x) = \sum_{x\in\mathbf{k}^\times} \chi(x)\psi(x).$$
We aim to prove that
$$G_\psi(\chi)G_\psi(\chi^{-1}) = q\chi(-1),$$
and give arithmetic applications of this result (Question *4*).

1. Let G be a finite group and $\varphi : G \to \mathbf{A}^\times$ be a nontrivial homomorphism. Show that $\sum_{x\in G} \varphi(x) = 0$.

2. Show that

$$\sum_{x+y=z} \chi(x)\chi^{-1}(y) = \begin{cases} -\chi(-1) & \text{if } z \neq 0, \\ (q-1)\chi(-1) & \text{otherwise.} \end{cases}$$

3. Deduce that $G_\psi(\chi)G_\psi(\chi^{-1}) = q\chi(-1)$.

4. Consider $\mathbf{k} = \mathbb{F}_p$ where p is an odd prime number, $\mathbf{A} = \mathbb{Q}(\sqrt[p]{1})$, and ζ a p^{th} primitive root of the unit in $\mathbf{A}$. The characters ψ and χ are defined by

$$\psi(i \bmod p) = \zeta^i, \qquad \chi(i \bmod p) = \left(\tfrac{i}{p}\right) \quad \text{(Legendre symbol).}$$

a. Then, $\chi = \chi^{-1}$, the Gauss sums $G_\psi(\chi)$, $G_\psi(\chi^{-1})$ are equal to

$$\tau \overset{\text{def}}{=} \sum_{i\in\mathbb{F}_p^*} \left(\tfrac{i}{p}\right)\zeta^i,$$

and by letting $p^* = (-1)^{\frac{p-1}{2}}p$ (such that $p^* \equiv 1 \bmod 4$), we obtain

$$\tau^2 = p^*, \quad \text{in particular,} \quad \mathbb{Q}(\sqrt{p^*}) \subseteq \mathbb{Q}(\sqrt[p]{1}).$$

b. Define $\tau_0 = \sum_{i\in\mathbb{F}_p^{\times 2}} \zeta^i$, $\tau_1 = \sum_{i\in\mathbb{F}_p^{\times}\setminus\mathbb{F}_p^{\times 2}} \zeta^i$ such that $\tau = \tau_0 - \tau_1$. Show that τ_0 and τ_1 are the roots of $X^2 + X + \frac{1-p^*}{4}$ and that the ring $\mathbb{Z}[\tau_0] = \mathbb{Z}[\tau_1]$ is the ring of integers of $\mathbb{Q}(\sqrt{p^*})$.

Problem 7. *(The Dedekind polynomial $f(X) = X^3 + X^2 - 2X + 8$)*
The aim of this problem is to provide an example of a ring $\mathbf{A}$ of integers of a number field which is not a monogenic $\mathbb{Z}$-algebra.[10]

1. Show that f is irreducible in $\mathbb{Z}[X]$ and that $\operatorname{disc}(f) = -2\,012 = -2^2 \times 503$.
2. Let α be a root of $f(X)$. Show that $\beta = 4\alpha^{-1}$ is integral over $\mathbb{Z}$, that
$$\mathbf{A} = \mathbb{Z} \oplus \mathbb{Z}\alpha \oplus \mathbb{Z}\beta$$
is the ring of integers of $\mathbb{Q}(\alpha)$ and that $\operatorname{Disc}_{\mathbf{A}/\mathbb{Z}} = -503$.
3. Show that the prime number $p = 2$ is completely decomposed in $\mathbf{A}$, in other words that $\mathbf{A}/2\mathbf{A} \simeq \mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2$. Deduce that $\mathbf{A}$ is not a monogenic $\mathbb{Z}$-algebra.
4. *(Avoiding the conductor, Dedekind)* Let $\mathbf{B} \subseteq \mathbf{B}'$ be two rings, $\mathfrak{f}$ be an ideal of $\mathbf{B}$ satisfying $\mathfrak{f}\mathbf{B}' \subseteq \mathbf{B}$; a fortiori $\mathfrak{f}\mathbf{B}' \subseteq \mathbf{B}'$ and $\mathfrak{f}$ is also an ideal of $\mathbf{B}'$. Then, for every ideal $\mathfrak{b}$ of $\mathbf{B}$ such that $1 \in \mathfrak{b} + \mathfrak{f}$, by letting $\mathfrak{b}' = \mathfrak{b}\mathbf{B}'$, the canonical morphism $\mathbf{B}/\mathfrak{b} \to \mathbf{B}'/\mathfrak{b}'$ is an isomorphism.
5. Deduce that 2 is an *essential divisor* of $\mathbf{A}$; by that we mean that 2 divides the index $|\,\mathbf{A} : \mathbb{Z}[x]\,|$ for any primitive element x of $\mathbb{Q}(\alpha)/\mathbb{Q}$ integral over $\mathbb{Z}$.

Problem 8. *(Norm of an ideal in quasi-Galoisian context)*
Let $(\mathbf{B}, \mathbf{A}, G)$ where $G \subseteq \operatorname{Aut}(\mathbf{B})$ is a finite group, and $\mathbf{A} = \mathbf{B}^G = \operatorname{Fix}_{\mathbf{B}}(G)$. If $\mathfrak{b}$ is an ideal of $\mathbf{B}$, let $\mathrm{N}'_G(\mathfrak{b}) = \prod_{\sigma\in G} \sigma(\mathfrak{b})$ (ideal of $\mathbf{B}$) and $\mathrm{N}_G(\mathfrak{b}) = \mathbf{A} \cap \mathrm{N}'_G(\mathfrak{b})$ (ideal of $\mathbf{A}$).

1. Show that $\mathbf{B}$ is integral over $\mathbf{A}$.

[10] An $\mathbf{A}$-algebra $\mathbf{B}$ is said to be *monogenic* when it is generated, as an $\mathbf{A}$-algebra, by a unique element x. So $\mathbf{B} = \mathbf{A}_1[x]$ where $\mathbf{A}_1$ is the image of $\mathbf{A}$ in $\mathbf{B}$.

2. Let $\mathbf{B} = \mathbb{Z}[\sqrt{d}]$ where $d \in \mathbb{Z}$ is not a square, τ be the automorphism (also denoted by $z \mapsto \overline{z}$) defined by $\sqrt{d} \mapsto -\sqrt{d}$, and $G = \langle \tau \rangle$. Therefore $\mathbf{A} = \mathbb{Z}$. Suppose that $d \equiv 1 \bmod 4$ and let $\mathfrak{m} = \left\langle 1 + \sqrt{d}, 1 - \sqrt{d} \right\rangle$.

    a. We have $\mathfrak{m} = \overline{\mathfrak{m}}$, $\mathrm{N}'_G(\mathfrak{m}) = \mathfrak{m}^2 = 2\mathfrak{m}$ and $\mathrm{N}_G(\mathfrak{m}) = 2\mathbb{Z}$. Deduce that $\mathfrak{m}$ is not invertible and that we do not have $\mathrm{N}'_G(\mathfrak{m}) = \mathrm{N}_G(\mathfrak{m})\mathbf{B}$.

    b. Show that $\mathbb{Z}[\sqrt{d}]/\mathfrak{m} \simeq \mathbb{F}_2$; thus $\mathfrak{m}$ is of index 2 in $\mathbb{Z}[\sqrt{d}]$ but 2 is not the gcd of the $\mathrm{N}_G(z)$'s, $z \in \mathfrak{m}$. Also check that $\mathfrak{b} \mapsto |\,\mathbf{B} : \mathfrak{b}\,|$ is not multiplicative over the nonzero ideals of $\mathbf{B}$.

3. Suppose that $\mathbf{B}$ is integrally closed and that $\mathbf{A}$ is a Bézout domain.
   Let $\mathfrak{b} \subseteq \mathbf{B}$ be a finitely generated ideal.

    a. Give a $d \in \mathbf{A}$ such that $\mathrm{N}'_G(\mathfrak{b}) = d\mathbf{B}$. In particular, if $\mathfrak{b}$ is nonzero, it is invertible. Thus, $\mathbf{B}$ is a Prüfer domain.

    b. Show that $\mathrm{N}_G(\mathfrak{b}) = d\mathbf{A}$, therefore $\mathrm{N}'_G(\mathfrak{b}) = \mathrm{N}_G(\mathfrak{b})\mathbf{B}$.

    c. Suppose that $\mathbf{B}/\mathfrak{b}$ is isomorphic as an $\mathbf{A}$-module to $\mathbf{A}/\langle a_1 \rangle \times \cdots \times \mathbf{A}/\langle a_k \rangle$. Show that $\mathrm{N}_G(\mathfrak{b}) = \langle a_1 \cdots a_k \rangle_{\mathbf{A}}$.

    d. Suppose $\#G = 2$. Express, in terms of a finite generator set of $\mathfrak{b}$, elements $z_1, \ldots, z_m \in \mathfrak{b}$ such that $\mathrm{N}_G(\mathfrak{b}) = \langle \mathrm{N}(z_i), i \in [\![1..m]\!] \rangle_{\mathbf{A}}$.

Problem 9. *(Forking lemma)*

1. Let $\mathbf{A}$ be an integrally closed ring with quotient field $\mathbf{k}$, $\mathbf{K}$ be a separable finite extension of $\mathbf{k}$ of degree n, $\mathbf{B}$ be the integral closure of $\mathbf{A}$ in $\mathbf{K}$. Show that there exists a basis $(\underline{e}) = (e_1, \ldots, e_n)$ of $\mathbf{L}/\mathbf{K}$ contained in $\mathbf{B}$. Let $\Delta = \mathrm{disc}(\underline{e})$ and $(\underline{e}') = (e'_1, \ldots, e'_n)$ be the trace-dual basis of $(\underline{e})$. Show the inclusions
$$\textstyle\bigoplus_{i=1}^n \mathbf{A}e_i \ \subseteq\ \mathbf{B}\ \subseteq\ \bigoplus_{i=1}^n \mathbf{A}e'_i\ \subseteq\ \Delta^{-1} \bigoplus_{i=1}^n \mathbf{A}e_i.$$

In the following $\mathbf{A} = \mathbb{Z}$ and $\mathbf{k} = \mathbb{Q}$; $\mathbf{K}$ is thus a number field and $\mathbf{B} = \mathbf{Z}$ is its ring of integers. Consider some $x \in \mathbf{Z}$ such that $\mathbf{K} = \mathbb{Q}[x]$.
Let $f(X) = \mathrm{Min}_{\mathbb{Q},x}(X) \in \mathbb{Z}[X]$ and δ^2 be the greatest square factor of $\mathrm{disc}_X(f)$. By Proposition 8.17, $\mathbf{Z}$ is a free $\mathbb{Z}$-module of rank $n = [\mathbf{L} : \mathbb{Q}]$, and we have $\mathbb{Z}[x] \subseteq \mathbf{Z} \subseteq \frac{1}{\delta}\mathbb{Z}[x]$. This is slightly more precise than the result from item *1.*
Consider a finitely generated $\mathbb{Z}$-algebra $\mathbf{B}$ intermediate between $\mathbb{Z}[x]$ and $\mathbf{Z}$. As it is a finitely generated $\mathbb{Z}$-module, $\mathbf{B}$ is also a free $\mathbb{Z}$-module of rank n. The most important case is that where $\mathbf{B} = \mathbf{Z}$.
The aim of the problem is to find a $\mathbb{Z}$-basis of $\mathbf{B}$ of the form
$$\mathcal{B} = \left(\tfrac{g_0}{d_0}, \tfrac{g_1(x)}{d_1}, \tfrac{g_2(x)}{d_2}, \ldots, \tfrac{g_{n-1}(x)}{d_{n-1}}\right)$$
with $g_k \in \mathbb{Z}[X]$ of degree k for all k, and each $d_k > 0$ ass mall as possible. Establish this result with monic polynomials g_k and $1 = d_0 \mid d_1 \mid d_2 \mid \cdots \mid d_{n-1}$.
The field $\mathbf{K}$ is a $\mathbb{Q}$-vector space with basis $(1, x, \ldots, x^{n-1})$ and for $k \in [\![0..n-1]\!]$, let $\pi_k : \mathbf{K} \to \mathbb{Q}$ be the linear component form over x^k and
$$Q_k = \textstyle\bigoplus_{i=0}^k \mathbb{Q}\,x^i,\ Z_k = \dfrac{1}{\delta}\textstyle\bigoplus_{i=0}^k \mathbb{Z}\,x^i, \quad \text{and } F_k = Q_k \cap \mathbf{B} = Z_k \cap \mathbf{B}.$$
It is clear that $Q_0 = \mathbb{Q}$, $Q_{n-1} = \mathbf{K}$, $F_0 = \mathbb{Z}$ and $F_{n-1} = \mathbf{B}$.

2. Show that the $\mathbb{Z}$-module F_k is free and of rank $k+1$.
   The $\mathbb{Z}$-module $\pi_k(F_k)$ is a finitely generated $\mathbb{Z}$-submodule of $\frac{1}{\delta}\mathbb{Z}$. Show that it is of the form $\frac{1}{d_k}\mathbb{Z}$ for some d_k that divides δ. NB: $d_0 = 1$.
3. Let y_k be an element of F_k such that $\pi_k(y_k) = \frac{1}{d_k}$.
   Write y_k in the form $f_k(x)/d_k$, with $f_k \in \mathbb{Q}[X]$ monic and of degree k. Clearly $y_0 = 1$. However, the other y_i's are not uniquely determined. Show that $(1, y_1, \ldots, y_k)$ is a $\mathbb{Z}$-basis of F_k.
4. Show that if $i + j \leqslant n - 1$, we have $d_i d_j \mid d_{i+j}$. In particular d_i divides d_k if $1 \leqslant i < k \leqslant n-1$. Also deduce that $d_1^{n(n-1)/2}$ divides δ.
5. Show that $d_k y_k \in \mathbb{Z}[x]$ for each $k \in [\![0..n-1]\!]$. Deduce that $f_k \in \mathbb{Z}[X]$ and that $\big(1, f_1(x), \ldots, f_{n-1}(x)\big)$ is a $\mathbb{Z}$-basis of $\mathbb{Z}[x]$.
6. Show that $\mathcal{B} = \big(1, \frac{1}{d_1} f_1(x), \ldots, \frac{1}{d_{n-1}} f_{n-1}(x)\big)$ is a $\mathbb{Z}$-basis of $\mathbf{B}$ adapted to the inclusion $\mathbb{Z}[x] \subseteq \mathbf{B}$. The d_i's are therefore the invariant factors of this inclusion, and $\prod_{i=1}^{n-1} d_i$ is equal to the index $\big|\, \mathbf{B} : \mathbb{Z}[x] \,\big|$ that divides δ.

Problem 10. *(Changing variables, polynomial automorphisms and Newton's method)*
Let $F = (F_1, \ldots, F_n)$ with $F_i \in \mathbf{A}[X] = \mathbf{A}[X_1, \ldots, X_n]$ and $\theta_F : \mathbf{A}[X] \to \mathbf{A}[X]$ be the morphism of $\mathbf{A}$-algebras performing $X_i \mapsto F_i$; we therefore have $\theta_F(g) = g(F)$. Assume that $\mathbf{A}[X] = \mathbf{A}[F]$: there thus exists a $G_i \in \mathbf{A}[X]$ satisfying $X_i = G_i(F)$, which is classically written (with some slight abuses) as $X = G(F)$ and at times $X = G \circ F$ (in the sense of maps of $\mathbf{A}[X]^n$ to $\mathbf{A}[X]^n$).
Note the converse as $\theta_F \circ \theta_G = \mathrm{I}_{\mathbf{A}[X]}$.
Here we will prove that $\theta_G \circ \theta_F = \mathrm{I}_{\mathbf{A}[X]}$, or $X = F(G)$.
Consequently (cf. Question 1) G is uniquely determined, θ_F is an automorphism of $\mathbf{A}[X]$ and $F_1, \ldots, F_n$ are algebraically independent over $\mathbf{A}$.
The idea consists in using the ring of formal series $\mathbf{A}[[X]]$ or at least the quotient rings $\mathbf{A}[X]/\mathfrak{m}^d$ where $\mathfrak{m} = \langle X_1, \ldots, X_n \rangle$. Let $F = (F_1, \ldots, F_n) \in \mathbf{A}[[X]]^n$. Study for which condition there exists a $G = (G_1, \ldots, G_n)$, $G_i \in \mathbf{A}[[X]]$ without a constant term, satisfying $F(G) = X$. We then have $F(0) = 0$, and by letting $J_0 = \mathrm{JAC}(F)(0)$, we obtain $J_0 \in \mathbb{GL}_n(\mathbf{A})$ (since $\mathrm{JAC}(F)(0) \circ \mathrm{JAC}(G)(0) = \mathrm{I}_{\mathbf{A}^n}$). We will prove the converse: in the case where $F(0) = 0$ and $J_0 \in \mathbb{GL}_n(\mathbf{A})$, there exists a $G = (G_1, \ldots, G_n)$, with $G_i \in \mathbf{A}[[X]]$, $G_i(0) = 0$, and $F(G) = X$.

1. By assuming this converse, prove that G is unique and that $G(F) = X$.
2. Let $\mathbf{S} \subset \mathbf{A}[[X]]$ be the set of formal series without a constant term; $\mathbf{S}^n$ is, with respect to the composition law, a monoid whose neutral element is X. Recall Newton's method for solving an equation $P(z) = 0$ in z: introduce the iterator $\Phi : z \mapsto z - P'(z)^{-1} P(z)$ and the sequence $z_{d+1} = \Phi(z_d)$ with an adequate z_0; or a variant $\Phi : z \mapsto z - P'(z_0)^{-1} P(z)$. To solve $F(G) - X = 0$ in G, check that this leads to the iterator over $\mathbf{S}^n$
$$\Phi : G \mapsto G - J_0^{-1} \cdot (F(G) - X)$$

3. Introduce $\mathrm{val} : \mathbf{A}[[X]] \to \mathbb{N} \cup \{\infty\}$: $\mathrm{val}(g) = d$ means that d is the (total) minimum degree of the monomials of g, agreeing that $\mathrm{val}(0) = +\infty$. We therefore have $\mathrm{val}(g) \geqslant d$ if and only if $g \in \mathfrak{m}^d$. For g, let $h \in \mathbf{A}[[X]]$ and G, $H \in \mathbf{A}[[X]]^n$
$$d(f,g) = \tfrac{1}{2^{\mathrm{val}(f-g)}}, \qquad d(F,G) = \max_i d(F_i, G_i).$$
Show that Φ is a contracting map: $d\big(\Phi(G), \Phi(H)\big) \leqslant d(G,H)/2$. Deduce that Φ admits a unique fixed point $G \in \mathbf{S}^n$, the unique solution of $F(G) = X$.
4. Solve the initial problem with respect to polynomials.
5. Check that the following systems are changes of variables and make their inverses explicit (in $\mathbb{Z}[X,Y,Z]$ then in $\mathbb{Z}[X_1, X_2, X_3, X_4, X_5]$):
$$(X - 2fY - f^2Z,\ Y + fZ,\ Z) \text{ with } f = XZ + Y^2,$$
$$(X_1 + 3X_2X_4^2 - 2X_3X_4X_5,\ X_2 + X_4^2X_5,\ X_3 + X_4^3,\ X_4 + X_5^3,\ X_5).$$

Some solutions, or sketches of solutions

Exercise 2. *1.* Lagrange interpolation: $Q = \sum_{\xi \in U} \left(\prod_{\zeta \in U \setminus \{\xi\}} \frac{x_n - \zeta}{\xi - \zeta} \right) Q_\xi$.

2. Assume that each $\mathfrak{a}(V_\xi) \subset \mathbf{K}[x_1, \dots, x_{n-1}]$ (for $\xi \in \pi_n(V)$) is generated by m polynomials
$$\mathfrak{a}(V_\xi) = \left\langle f_j^\xi, j \in [\![1..m]\!] \right\rangle, \quad f_j^\xi \in \mathbf{K}[x_1, \dots, x_{n-1}].$$
By item *1*, there exists an $f_j \in \mathbf{K}[\underline{x}]$ satisfying $f_j(x_1, \dots, x_{n-1}, \xi) = f_j^\xi$ for all $\xi \in \pi_n(V)$. Then prove, based on item *1*, that
$$\mathfrak{a}(V) = \langle P, f_1, \dots, f_m \rangle \qquad \text{with } P = \prod_{\xi \in \pi_n(V)} (x_n - \xi).$$
Conclude by induction on n.

Exercise 3. *4.* Consider the polynomial ring $\mathbf{B} = \mathbf{A}[s_1, \dots, s_n]$ where the s_i's are indeterminates, then the polynomial $f(t) = t^n + \sum_{k=1}^n (-1)^k s_k t^{n-k} \in \mathbf{B}[t]$. Consider also the universal splitting algebra
$$\mathbf{C} = \mathrm{Adu}_{\mathbf{B},f} = \mathbf{B}[x_1, \dots, x_n] = \mathbf{A}[x_1, \dots, x_n],$$
with, in $\mathbf{C}[t]$, the equality $f(t) = \prod_{i=1}^n (t - x_i)$.
Let $\rho : \mathbf{A}[X_1, \dots, X_n] \to \mathbf{A}[x_1, \dots, x_n]$ and $\varphi : \mathbf{A}[s_1, \dots, s_n] \to \mathbf{A}[S_1, \dots, S_n]$ be the evaluation homomorphisms $X_i \mapsto x_i$ and $s_i \mapsto S_i$.

We clearly have $\rho(S_i) = s_i$. Therefore, by letting ρ_1 be the restriction of ρ to $\mathbf{A}[\underline{S}]$ and $\mathbf{A}[\underline{s}]$, we have $\varphi \circ \rho_1 = \mathrm{Id}_{\mathbf{A}[\underline{S}]}$ and $\rho_1 \circ \varphi = \mathrm{Id}_{\mathbf{A}[\underline{s}]}$. This shows that the S_i's are algebraically independent over $\mathbf{A}$ and we can identify $\mathbf{A}[\underline{S}]$ and $\mathbf{A}[\underline{s}] = \mathbf{B}$.

$$\begin{tikzcd}
\mathbf{A}[\underline{X}] \arrow[r, shift left, "\rho"] & \mathbf{A}[\underline{x}] \arrow[l, shift left, "\psi"] \\
\mathbf{A}[\underline{S}] \arrow[u, hook] \arrow[r, shift left, "\rho_1"] & \mathbf{A}[\underline{s}] \arrow[u, hook] \arrow[l, shift left, "\varphi"]
\end{tikzcd}$$

By the universal property of the universal splitting algebra, there exists a (unique) $\mathbf{B}$-homomorphism $\psi : \mathbf{C} \to \mathbf{A}[\underline{X}]$ which sends x_i onto X_i. It follows that ρ and ψ are two mutually reciprocal isomorphisms. Thus the x_i's are algebraically independent over $\mathbf{A}$ and $\mathbf{A}[\underline{X}]$ is free and of rank $n!$ over $\mathbf{A}[\underline{S}] = \mathbf{B}$, with the prescribed basis.

NB: this proof does not seem to simply give the fact that the symmetric polynomials of $\mathbf{A}[\underline{X}]$ are in $\mathbf{A}[\underline{S}]$.

Exercise 4. *1.* Let $f = (X_1^3 + X_2^3 + \cdots + X_n^3) - (S_1^3 - 3S_2S_2 + 3S_3)$. It is a homogeneous symmetric polynomial, therefore $f = g(S_1, \ldots, S_n)$ where $g = g(Y_1, \ldots, Y_n)$ is homogeneous in weight, of weight 3 with respect to the weight $\alpha_1 + 2\alpha_2 + \cdots + n\alpha_n$.

The equality $\alpha_1 + 2\alpha_2 + \cdots + n\alpha_n = 3$ implies $\alpha_i = 0$ for $i > 3$, so g only depends on Y_1, Y_2, Y_3, say $g = g(Y_1, Y_2, Y_3)$. In the equality

$$(X_1^3 + X_2^3 + \cdots + X_n^3) - (S_1^3 - 3S_2S_2 + 3S_3) = g(S_1, S_2, S_3),$$

put $X_i := 0$ for $i > 3$; we obtain $g(S_1', S_2', S_3') = 0$ where S_1', S_2', S_3' are the elementary symmetric functions of X_1, X_2, X_3. Deduce that $g = 0$ then $f = 0$.

2. For the first, we can assume $n = 3$; we find $S_1S_2 - 3S_3$. For the other two which are homogeneous, symmetric, of degree 4 we work with 4 indeterminates and we obtain $S_1^2S_2 - 2S_2^2 - S_1S_3 + 4S_4$ and $S_2^2 - 2S_1S_3 + 2S_4$.

3. Let $n > d$ and $f(X_1, \ldots, X_n)$ be a homogeneous symmetric polynomial of degree d. Let $h \in \mathbf{A}[X_1, \ldots, X_d] = f(X_1, \ldots, X_d, 0, \ldots, 0)$. If $h = 0$, then $f = 0$. We can translate this result by saying that we have isomorphisms of $\mathbf{A}$-modules at the level of the homogeneous symmetric components of degree d:

$$\cdots \to \mathbf{A}[X_1, \ldots, X_{d+2}]_d^{\text{sym.}} \xrightarrow{X_{d+2}:=0} \mathbf{A}[X_1, \ldots, X_{d+1}]_d^{\text{sym.}} \xrightarrow{X_{d+1}:=0} \mathbf{A}[X_1, \ldots, X_d]_d^{\text{sym.}} .$$

Exercise 7. Let $\mathbf{A} = \mathbb{Z}[U, V]/\left\langle U^2, V^2 \right\rangle = \mathbb{Z}[u, v] = \mathbb{Z} \oplus \mathbb{Z}u \oplus \mathbb{Z}v \oplus \mathbb{Z}uv$.
a. We take $f = uT + v$ so $\mathfrak{c} = \langle u, v \rangle$. We then have

$$\mathrm{Ann}(u) = \mathbf{A}u,\ \mathrm{Ann}(v) = \mathbf{A}v,\ \mathrm{Ann}(\mathfrak{c}) = \mathrm{Ann}(u) \cap \mathrm{Ann}(v) = \mathbf{A}uv \text{ and } \mathrm{D}\big(\mathrm{Ann}(\mathfrak{c})\big) = \mathfrak{c}.$$

b. Let $g = uT - v$. We have $fg = 0$ but $g \notin \mathrm{Ann}(\mathfrak{c})[T]$; we have $u \in \mathrm{D}\big(\mathrm{Ann}(\mathfrak{c})\big)$ but $u \notin \mathrm{Ann}_{\mathbf{A}[T]}(f)$ (idem for v).

Exercise 9. It suffices to prove item *1.* We have

$$f(T) = f(X_1) + (T - X_1)f_2(X_1, T)$$

by definition of $f_1 = f$ and f_2. Similarly

$$f_2(X_1, T) = f_2(X_1, X_2) + (T - X_2)f_3(X_1, X_2, T)$$

by definition of f_3. So

$$f(T) = f(X_1) + (T - X_1)f_2(X_1, X_2) + (T - X_1)(T - X_2)f_3(X_1, X_2, T).$$

Continue until

$$\begin{aligned} f_{n-1}(X_1, \ldots, X_{n-2}, T) \ = \ & f_{n-1}(X_1, \ldots, X_{n-2}, X_{n-1}) + \\ & (T - X_{n-1})f_n(X_1, \ldots, X_{n-1}, T), \end{aligned}$$

which gives

$$\begin{aligned} f(T) \ = \ & f_1(X_1) + (T - X_1)f_2(X_1, X_2) + (T - X_1)(T - X_2)f_3(X_1, X_2, X_3) \\ & + \ \cdots \ + \ (T - X_1) \cdots (T - X_{n-1})f_n(X_1, \ldots, X_{n-1}, T). \end{aligned}$$

Finally, $f_n(X_1, \ldots, X_{n-1}, T)$ is monic of degree 1 in T so

$$f_n(X_1, \ldots, X_{n-1}, T) = f_n(X_1, \ldots, X_{n-1}, X_n) + (T - X_n).$$

Note that this proves in particular that $f_n = S_1 - s_1$.

Exercise 10. Let $f \in \mathbf{A}[X]$ be monic of degree d, with $f \mid X^p - a$ and $1 \leqslant d \leqslant p-1$. In a ring $\mathbf{B} \supseteq \mathbf{A}$, we write $f(X) = \prod_{i=1}^{d}(X - \alpha_i)$, therefore $\alpha_i^p = a$ and $\prod_i \alpha_i = b$ with $b = (-1)^d f(0) \in \mathbf{A}$. By lifting to the power p, $a^d = b^p$. However, $\gcd(d, p) = 1$, so $1 = ud + vp$, then $a = a^{ud} a^{vp} = (b^u a^v)^p$.

Exercise 11. Let e_{ij} be the matrix of $\mathbb{M}_n(\mathbf{A})$ having a single nonzero coefficient, the coefficient in position (i, j), equal to 1. The module $S_n(\mathbf{A})$ is free and a basis is formed by the e_{ii}'s for $i \in [\![1..n]\!]$ and the $e_{ij} + e_{ji}$ for $1 \leqslant i < j < n$. It suffices to treat the case where $A = \mathrm{Diag}(\lambda_1, \ldots, \lambda_n)$. Then, $\varphi_A = \mathrm{Diag}(\lambda_1^2, \ldots, \lambda_n^2)$, and $\varphi_A(e_{ij} + e_{ji}) = \lambda_i \lambda_j (e_{ij} + e_{ji})$. Whence $\det(\varphi_A) = (\det A)^{n+1}$.

Exercise 12. Let $\underline{e} = (e_1, \ldots, e_n)$ be a basis of $\mathbf{B}/\mathbf{A}$. Clearly $\underline{e}$ is a $\mathbf{K}$-free family. Let $x = b/b' \in \mathbf{L}$ with $b \in \mathbf{B}$, $b' \in \mathbf{B} \setminus \{0\}$; we write

$$x = (b\widetilde{b'})/(b'\widetilde{b'}) = b\widetilde{b'}/\mathrm{N}_{\mathbf{B}/\mathbf{A}}(b') \in \mathbf{K}e_1 + \cdots + \mathbf{K}e_n.$$

Exercise 14. *1.* It suffices to prove it for the generic matrix $(a_{ij})_{i,j \in [\![1..n]\!]}$ with coefficients in $\mathbf{A} = \mathbb{Z}[(a_{ij})_{i,j \in [\![1..n]\!]}]$. This matrix is diagonalizable in an overring of $\mathbf{A}$.

2. Follows immediately from *1.*

Exercise 15. *1.* We have $\#R \leqslant \sum_{d=1}^{n-1} q^d < 1 + q + \cdots + q^{n-1} = \frac{q^n - 1}{q - 1}$.
A fortiori, $\#R < q^n - 1 < q^n$. Let $x \in \mathbf{L} \setminus R$ and $d = [\mathbf{K}[x] : \mathbf{K}]$. We have $x^{q^d} = x$, and since $x \notin R$, then $d = n$.

2. The cyclotomic polynomial is irreducible in $\mathbb{F}_2[X]$. Indeed, the only irreducible polynomial of degree 2 of $\mathbb{F}_2[X]$ is $X^2 + X + 1$, Φ_5 has no root in $\mathbb{F}_2$, and $\Phi_5 \neq (X^2 + X + 1)^2$. We have $\#\mathbf{L} = 2^4 = 16$, $\#\mathbf{L}^\times = 15$, but $x^5 = 1$.

3. Let $\sigma : \mathbf{L} \to \mathbf{L}$ be the Frobenius automorphism of $\mathbf{L}/\mathbf{K}$, i.e. $\sigma(x) = x^q$. We can easily check that $\mathbf{L} = \mathbf{K}[x]$ if and only if the $\sigma^i(x)$'s, $i \in [\![0..n-1]\!]$, are pairwise distinct. This condition is equivalent to $\sigma^k(x) = x \Rightarrow k \equiv 0 \bmod n$, i.e. $x^{q^k} = x \Rightarrow k \equiv 0 \bmod n$. But

$$x^{q^k} = x \iff x^{q^k - 1} = 1 \iff o(x) \mid q^k - 1 \iff q^k \equiv 1 \bmod o(x).$$

We then deduce, for $x \in \mathbf{L}^\times$, that $\mathbf{L} = \mathbf{K}[x]$ if and only if the order of q in the group of invertible elements modulo $o(x)$ is exactly n.

Exercise 19. *1.* We have $\langle g, g' \rangle \langle g, h \rangle \subseteq \langle g, g'h \rangle = \langle g, g'h + gh' \rangle$.
Similarly, $\langle h, h' \rangle \langle g, h \rangle \subseteq \langle h, g'h + gh' \rangle$. By evaluating the product we get

$$\langle g, g' \rangle \langle h, h' \rangle \langle g, h \rangle^2 \subseteq \langle g, g'h + h'g \rangle \langle h, g'h + h'g \rangle \subseteq \langle gh, g'h + h'g \rangle.$$

For the second item of the question we apply the result established above and Fact 7.8. NB: this also results from Equation (12), Fact 7.9.

2. It suffices to treat the case of two separable polynomials f, $g \in \mathbf{A}[T]$.
Let $h = \gcd(f, g)$. We have $f = hf_1$, $g = hg_1$, with $\gcd(f_1, g_1) = 1$.
Since g is separable, $\gcd(h, g_1) = 1$, so $\gcd(hf_1, g_1) = 1 = \gcd(f, g_1)$.
The polynomials f, g_1 are separable, comaximal, therefore their product $\mathrm{lcm}(f, g)$ is separable.

Exercise 20. *1* and *2.* These are special cases of what is stated in Fact II-5.5.

3. Suppose $L = \mathbf{A}^m$. If $A \in \mathbb{M}_m(\mathbf{A})$ is a matrix whose columns form a basis of F, it is injective and its determinant is regular. If B is a matrix corresponding to the inclusion $F \subseteq E$, we have

$$|\,L : F\,| = \langle \det A \rangle, \;\; |\,F : E\,| = \mathcal{D}_m(B) \;\text{ and }\; |\,L : E\,| = \mathcal{D}_m(AB),$$

hence the desired equality.

4. We have $|\,N : \delta N\,| = \langle \delta^n \rangle$. We also have $|\,N : \delta M\,| = \delta^{n-1}\,\langle \delta, a_1, \ldots, a_n \rangle$: take for the generator set of δM the family $\delta e_1, \ldots, \delta e_n, \delta z$ where $e_1, \ldots, e_n$ is a basis of N (we use $M = N + \mathbf{A}z$), and compute the determinantal ideal of order n of a matrix of the following type (for $n = 3$) $\begin{bmatrix} \delta & 0 & 0 & a_1 \\ 0 & \delta & 0 & a_2 \\ 0 & 0 & \delta & a_3 \end{bmatrix}$.

Then

$$idgN : \delta N \;=\; |\,N : \delta M\,|\,|\,\delta M : \delta N\,| \;=\; |\,N : \delta M\,|\,|\,M : N\,|,$$

i.e. $\langle \delta^n \rangle = |\,M : N\,|\,\delta^{n-1}\,\langle \delta, a_1, \ldots, a_n \rangle$.

By simplifying by δ^{n-1} we obtain the equality $\langle \delta \rangle = d\,\langle \delta, a_1, \ldots, a_n \rangle$.

Exercise 22. *1.* If $\mathfrak{a}\mathfrak{a}' = a\mathbf{A}$ with a regular, then $\mathfrak{b} \subseteq \mathfrak{a}$ is equivalent to $\mathfrak{b}\mathfrak{a}' \subseteq a\mathbf{A}$. Note that the test provides a finitely generated ideal $\mathfrak{c} = \mathfrak{b}\mathfrak{a}'/a$ such that $\mathfrak{a}\mathfrak{c} = \mathfrak{b}$ in case of a positive response, and an element $b \notin \mathfrak{a}$ among the generators of $\mathfrak{b}$ in case of a negative response.

2. It is clear that the $\mathfrak{q}_i$'s are invertible (and thus finitely generated).

Perform the tests $\mathfrak{b} \subseteq \mathfrak{q}_i$. If a response is positive, for instance $\mathfrak{b} \subseteq \mathfrak{q}_1$, write $\mathfrak{c}\mathfrak{q}_1 = \mathfrak{b}$, whence $\mathfrak{q}_2 \cdots \mathfrak{q}_n \subseteq \mathfrak{c}$, and finish by induction.

If all the tests are negative, we have some $x_i \in \mathfrak{b}$ and $y_i \in \mathbf{A}$ such that $1 - x_i y_i \in \mathfrak{q}_i$ (here suppose that the quotient rings $\mathbf{A}/\mathfrak{q}_i$ are discrete fields), whence, by evaluating the product, $1 - b \in \mathfrak{q}_1 \cdots \mathfrak{q}_n \subseteq \mathfrak{b}$ with $b \in \mathfrak{b}$, so $1 \in \mathfrak{b}$.

Finally, we address the uniqueness question. Assume that $\mathfrak{b} = \mathfrak{q}_1 \cdots \mathfrak{q}_k$.

It suffices to prove that if a finitely generated maximal ideal $\mathfrak{q}$ contains $\mathfrak{b}$, it is equal to one of the $\mathfrak{q}_i$'s ($i \in [\![1..k]\!]$).

Since we can test $\mathfrak{q} \subseteq \mathfrak{q}_i$, if each of the tests are negative we explicitly have $1 \in \mathfrak{q} + \mathfrak{q}_i$ for each i and so $1 \in \mathfrak{q} + \mathfrak{b}$.

NB: if we do not assume that $\mathfrak{b}$ is finitely generated and $\mathbf{A}$ has explicit divisibility, the proof of Kummer's little theorem would require that we at least know how to test $\mathfrak{q} \subseteq \mathfrak{b}$ for every "subproduct" $\mathfrak{q}$ of $\mathfrak{q}_1 \cdots \mathfrak{q}_n$.

Exercise 24. Assume $x \in \sqrt{\mathfrak{a}}$; as $\mathfrak{a} \subseteq \mathfrak{b}$, in $\mathbf{A}[T]/\mathfrak{b}$, $\overline{x}$ is nilpotent and invertible (since $\overline{xT} = 1$), therefore $\mathbf{A}[T]/\mathfrak{b}$ is the null ring, i.e. $1 \in \mathfrak{b}$.

Conversely, suppose $1 \in \mathfrak{b}$ and reason in the ring $\mathbf{A}[T]/\mathfrak{a}[T] = (\mathbf{A}/\mathfrak{a})[T]$. Since $1 \in \mathfrak{b}$, $1 - xT$ is invertible in this ring, therefore x is nilpotent in $\mathbf{A}/\mathfrak{a}$, i.e. $x \in \sqrt{\mathfrak{a}}$.

Exercise 25. *(Decomposition of Jordan-Chevalley-Dunford)*

Existence. Look for a zero D of f, a "neighbor of M," (i.e., with $M - D$ nilpotent), in the commutative ring $\mathbf{K}[M]$. We have by hypothesis $f(M)^k = 0$ for some $k \leqslant n$, and if $uf^k + vf' = 1$, we obtain $v(M)f'(M) = \mathrm{I}_n$.

Consequently, the Newton method, starting with $x_0 = M$, gives the solution in $\mathbf{K}[M]$ in $\lceil \log_2(k) \rceil$ iterations.

Uniqueness. The solution is unique, under the condition $f(D) = 0$, in every commutative ring containing $\mathbf{K}[M]$, for example in $\mathbf{K}[M, N]$ if the pair (D, N) solves the given problem.

When we only assume that the minimal polynomial of D is separable, the uniqueness is more delicate.

A solution would be to directly prove that the characteristic polynomial of D is necessarily equal to that of M, but it is not that simple.[11]

Let us call (D_1, N_1) the solution in $\mathbf{K}[M]$ given by Newton's method. Since D and N commute, they commute with $M = D+N$ and so with D_1 and N_1 because they belong to $\mathbf{K}[M]$. From this we deduce that $D - D_1$ is nilpotent because it is equal to $N_1 - N$ with N and N_1 being nilpotents that commute. But the algebra $\mathbf{K}[D, D_1]$ is étale by Theorem VI-1.7, so it is reduced, and $D = D_1$.

Exercise 26. We have $\mathbf{B} = \mathbf{A}[x] = \mathbf{A} \oplus \mathbf{A}x$ with x separably integral over $\mathbf{A}$. Let $z \mapsto \widetilde{z}$ be the automorphism of the $\mathbf{A}$-algebra $\mathbf{B}$ which swaps x and $-b-x$. For $z \in \mathbf{B}$, we have $\mathrm{C}_{\mathbf{B}/\mathbf{A}}(z)(T) = (T-z)(T-\widetilde{z})$.

Thus $\mathrm{C}_{\mathbf{B}/\mathbf{A}}(ax)(T) = T^2 + abT + a^2c$, and its discriminant is equal to $a^2\Delta$.

Let $\varepsilon \in \mathbf{A}$ be nonzero nilpotent and let $y = (\varepsilon - 1)x$. Then, y is separably integral over $\mathbf{A}$ because $(\varepsilon-1)^2\Delta$ is invertible. Furthermore, the element $z = x + y = \varepsilon x$ is nonzero nilpotent. Assume that $\varepsilon^2 = 0$ and let $g \in \mathbf{A}[X]$ be a monic polynomial that annihilates z, we will prove that g is not separable.

Let us write $g(X) = u + vX + X^2h(X)$, then $z^2 = 0$, so $u + vz = 0$.

Since $\mathbf{B} = \mathbf{A} \oplus \mathbf{A}x$, we obtain $u = v\varepsilon = 0$, then $g(X) = X\ell(X)$ with $\ell(0) = v$ non-invertible (otherwise, $\varepsilon = 0$). Finally, $\mathrm{disc}(g) = \mathrm{disc}(\ell)\ \mathrm{Res}(X,\ell)^2 = \mathrm{disc}(\ell)\ v^2$ is non-invertible.

Problem 1.

1. Let $f(X) = X^n + c = (X - x_1)\cdots(X - x_n)$. Then, $f' = nX^{n-1}$ and

$$\mathrm{Res}(f, f') = f'(x_1)\cdots f'(x_n) = n^n(x_1\cdots x_n)^{n-1} = n^n\big((-1)^n c\big)^{n-1} = n^n c^{n-1}.$$

Variant:

$$\mathrm{Res}(f', f) = n^n \mathrm{Res}(X^{n-1}, f) = n^n \textstyle\prod_{i=1}^{n-1} f(0) = n^n c^{n-1}.$$

2. Let $f(X) = X^n + bX + c = (X - x_1)\cdots(X - x_n)$;

$$\mathrm{disc}(f) = (-1)^{\frac{n(n-1)}{2}} \textstyle\prod_{i=1}^n y_i \quad \text{with} \quad y_i = f'(x_i) = nx_i^{n-1} + b\,.$$

To compute the product of the y_i's, we compute the product P of the x_iy_i's (that of the x_i's is equal to $(-1)^n c$). We have $x_iy_i = nx_i^n + bx_i = ux_i + v$, with $u = (1-n)b$, $v = -nc$. We use the elementary symmetric functions $S_j(x_1, \ldots, x_n)$ (almost all null)

$$\textstyle\prod_{i=1}^n (ux_i + v) = \sum_{j=0}^n u^j S_j(x_1, \ldots, x_n)v^{n-j}.$$

We get

$$P = v^n + u^n S_n + u^{n-1}S_{n-1}v = v^n + u^n(-1)^n c + u^{n-1}(-1)^{n-1}bv\,,$$

[11] In zero characteristic, one trick consists in retrieving the characteristic polynomial of a matrix A from the $\mathrm{Tr}(A^k)$ by following Le Verrier's method.

i.e., by replacing u and v by their values

$$\begin{aligned} P &= (-1)^n n^n c^n + (n-1)^n b^n c - n(n-1)^{n-1} b^n c \\ &= (-1)^n n^n c^n + b^n c\big((n-1)^n - n(n-1)^{n-1}\big) \\ &= (-1)^n n^n c^n - b^n c(n-1)^{n-1}. \end{aligned}$$

By dividing by $(-1)^n c$, we obtain the product of the y_i's then the stated formula.

3. Left to the sagacity of the reader who can consult [186].

4. By letting $\Delta_p = \operatorname{disc}(\Phi_p)$, we have the equality

$$\operatorname{disc}(X^p - 1) = \operatorname{Res}(X-1, \Phi_p)^2 \operatorname{disc}(X-1)\Delta_p = \Phi_p(1)^2\Delta_p = p^2\Delta_p.$$

By using $\operatorname{disc}(X^n - 1) = (-1)^{\frac{n(n-1)}{2}} n^n (-1)^{n-1}$, we obtain

$$\Delta_2 = 1, \qquad \Delta_p = (-1)^{\frac{p-1}{2}} p^{p-2} \quad \text{for } p \geqslant 3.$$

5. Let $q = p^{k-1}$; let us first prove that $r := \operatorname{Res}(X^q - 1, \Phi_{p^k}) = p^q$.
With $X^q - 1 = \prod_{i=1}^q (X - \zeta_i)$, we have $r = \prod_{i=1}^q \Phi_{p^k}(\zeta_i)$. In addition

$$\Phi_{p^k}(X) = \tfrac{Y^p - 1}{Y-1} = Y^{p-1} + \cdots + Y + 1 \quad \text{with} \quad Y = X^q.$$

By making $X := \zeta_i$, we must make $Y := 1$, we obtain $\Phi_{p^k}(\zeta_i) = p$, then $r = p^q$.
Let $D_k = \operatorname{disc}(X^{p^k} - 1)$. Since $X^{p^k} - 1 = (X^q - 1)\Phi_{p^k}(X)$, we have

$$D_k = \operatorname{Res}(X^q - 1, \Phi_{p^k})^2 D_{k-1} \operatorname{disc}(\Phi_{p^k}) = p^{2q} D_{k-1} \operatorname{disc}(\Phi_{p^k}).$$

We use $\operatorname{disc}(X^n - 1) = (-1)^{\frac{n(n-1)}{2}} n^n (-1)^{n-1}$ for $n = p^k$ and q

$$D_k / D_{k-1} = \varepsilon\, p^N, \quad \varepsilon = \pm 1, \quad N = kp^k - (k-1)q = \big(k(p-1)+1\big)\, q\,.$$

For $\operatorname{disc}(\Phi_{p^k})$ to be obtained, D_k/D_{k-1} must be divided by p^{2q}, which replaces the exponent N with $N - 2q = (k(p-1)-1)q$. As for the sign ε, for odd p,

$$\varepsilon = (-1)^{\frac{p^k - 1}{2}} (-1)^{\frac{q-1}{2}} = (-1)^{\frac{p^k - q}{2}} = (-1)^{\frac{p-1}{2}}.$$

For $p = 2$, $\varepsilon = 1$ for $k \geqslant 3$ or $k = 1$ and $\varepsilon = -1$ for $k = 2$.

6. If n is not the power of a prime, we can write $n = mp^k$ with p prime, $\gcd(m,p) = 1$, $k \geqslant 1$ and $m \geqslant 2$. Then, $\Phi_n(X) = \Phi_m(X^{p^k})/\Phi_m(X^{p^{k-1}})$, an equality in which we put $X = 1$ to obtain $\Phi_n(1) = 1$. The other items are easy.

7. Let f, g be two monic polynomials, with $d = \deg f$, $e = \deg g$ and $d, e \geqslant 1$. Let $\mathbf{A}[x] = \mathbf{A}[X]/\langle f(X)\rangle$, $\mathbf{A}[y] = \mathbf{A}[Y]/\langle g(Y)\rangle$. Let $f \otimes g$ be the characteristic polynomial of $x \otimes y$ in $\mathbf{A}[x] \otimes_{\mathbf{A}} \mathbf{A}[y] = \mathbf{A}[X,Y]/\langle f(X), g(Y)\rangle$. It is a monic polynomial of degree de. Since $f(X) = \prod_i (X - x_i)$, $g(Y) = \prod_j (Y - y_j)$, we obtain $(f \otimes g)(T) = \prod_{i,j}(T - x_i y_j)$. We easily see that

$$\operatorname{disc}(f \otimes g) = \prod\nolimits_{(i,j)<(i',j')} (x_i y_j - x_{i'} y_{j'})^2 = \operatorname{disc}(f)^e \operatorname{disc}(g)^d f(0)^e g(0)^d \pi\,,$$

where $\pi \in \mathbf{A}$ is the product $\prod_{i \neq i',\, j \neq j'} (x_i y_j - x_{i'} y_{j'})$.
Let n, $m \geqslant 2$ with $\gcd(n,m) = 1$ and ζ_n, ζ_m, ζ_{nm} be the roots of the unit of respective orders n, m, nm. By the Chinese remainder theorem, we obtain the equality $\Phi_{nm} = \Phi_n \otimes \Phi_m$. As $\Phi_n(0) = \Phi_m(0) = 1$ (since $n, m \geqslant 2$), we have the

equality

$$\Delta_{nm} = \Delta_n^{\varphi(m)} \Delta_m^{\varphi(n)}\, \pi\,,$$

where $\pi \in \mathbb{Z}$ is the following product.

$$\textstyle\prod_{i\neq i',\, j\neq j'} (\zeta_n^i \zeta_m^j - \zeta_n^{i'} \zeta_m^{j'}), \text{ for } i, i' \in (\mathbb{Z}/n\mathbb{Z})^\times \text{ and } j, j' \in (\mathbb{Z}/m\mathbb{Z})^\times.$$

Let $C \subset (\mathbb{Z}/nm\mathbb{Z})^\times \times (\mathbb{Z}/nm\mathbb{Z})^\times$ be the set of pairs (a, b) with a, b invertible modulo nm, $a \not\equiv b \bmod n$, $a \not\equiv b \bmod m$. The Chinese remainder theorem gives us

$$\pi = \textstyle\prod_{(a,b)\in C} (\zeta_{nm}^a - \zeta_{nm}^b).$$

Let $z \mapsto \overline{z}$ be complex conjugation. Then, π is of the form $z\overline{z}$, therefore $\pi \in \mathbb{N}^*$. Indeed, $(a, b) \in C \Rightarrow (-a, -b) \in C$ with $(a, b) \neq (-a, -b)$.

Furthermore, for $c \in \mathbb{Z}$ a non-multiple of n or m, consider the element ζ_{nm}^c which is of order $nm/\gcd(c, nm) = n'm'$ with $n' = n/\gcd(c, n) > 1$, $m' > 1$ and $\gcd(n', m') = 1$. Therefore $n'm'$ is not a power of a prime number, and, by the previous question, $1 - \zeta_{nm}^c$ is invertible in $\mathbb{Z}[\zeta_{nm}^c]$, a fortiori in $\mathbb{Z}[\zeta_{nm}]$. We deduce that π is invertible in $\mathbb{Z}[\zeta_{nm}]$, therefore in $\mathbb{Z}$.

Recap: $\pi = 1$, and $\Delta_{nm} = \Delta_n^{\varphi(m)} \Delta_m^{\varphi(n)}$.

Finally, if the formula that gives the cyclotomic discriminant is satisfied for two pairwise comaximal integers n and m, it is satisfied for the product nm (use the first item). However, it is true for integers which are powers of a prime by Question *5*, therefore it is true for every integer $\geqslant 3$.

Problem 2. *4.* Consider $p \equiv 1 \bmod 4$. The polynomial $Y^{\frac{p-1}{2}} - 1 \in \mathbb{F}_p[Y]$ is of degree $< \#\mathbb{F}_p^\times$. There thus exists a non-root $y \in \mathbb{F}_p^\times$ of this polynomial; let $x = y^{\frac{p-1}{4}}$ so that $x^2 = y^{\frac{p-1}{2}} \neq 1$; but $x^4 = 1$ thus $x^2 = -1$. Actually, for half of the $y \in \mathbb{F}_p^\times$, we have $y^{\frac{p-1}{2}} = 1$ (the squares), and for the other half (the non-squares), we have $y^{\frac{p-1}{2}} = -1$.

Let us address the question of the efficient algorithm. What we mean by this is that the execution time has a small power of the number of digits of p as its order of magnitude.

We first determine some $x \in \mathbb{F}_p$ such that $x^2 = -1$. For that we randomly draw integers y over $[\![2..(p-1)/2]\!]$ and we compute $y^{\frac{p-1}{4}}$ in $\mathbb{F}_p$ (for that we use an efficient algorithm of exponentiation modulo p). The probability of failure (when the result is ± 1) is of $1/2$ at each draw.

Once such an x is found, it remains to compute $\gcd(x + i, p)$ with the Euclidean algorithm. As the norm is divided by at least 2 at each step, the algorithm is efficient.

NB: the brute force method which would consist in saying “since $p \equiv 1 \bmod 4$, it possesses a factor of the form $m + in$, and all that is left to do is try out every $m < p$” quickly proves to be impractical as soon as p is large enough.

5. The decomposition of the prime divisors of m is treated in the previous item. It remains to decompose $n + qi$.

Regarding the decomposition of $n^2 + q^2$, we already know that the only prime numbers therein are 2 (with the exponent 1) or some $p \equiv 1 \bmod 4$.

If $u + vi$ is the factor of some p that divides $n^2 + q^2$, then $u + vi$ or $u - vi$ divides $n + qi$. If p appears with the exponent k in $n^2 + q^2$, and if $u + vi$ divides

$n+qi$, then $u+vi$ appears with the exponent k in $n+qi$.
If $s=2^k\prod_i p_i^{m_i}\prod_j q_j^{n_j}$ with every $p_i \equiv 3 \bmod 4$ and every $q_j \equiv 1 \bmod 4$, then the condition insuring that s is the sum of two squares is that every m_i be even. Note that an expression $s=a^2+b^2$ with $0<a\leqslant b$ corresponds to two conjugated elements $a \pm ib$ defined up to association (for example multiplying by i comes down to permuting a and b). It follows that in the case where s is the sum of two squares, the number of expressions of s as a sum of the squares is equal to $(1/2)\prod_j(1+n_j)$ unless the n_j's are all even, in which case we add or subtract $1/2$ depending on whether we consider that an expression a^2+0^2 is or is not legitimate as a sum of two squares.
For example with $5=\mathrm{N}(a)$, $a=2+i$ and $13=\mathrm{N}(b)$, $b=3+2i$ we obtain

$$\begin{array}{rll} 5=\mathrm{N}(a) & \text{gives} & 5=2^2+1^2, \\ 10=\mathrm{N}\big(a(1+i)\big)=\mathrm{N}(1+3i) & \text{gives} & 10=1^2+3^2, \\ 5^3=\mathrm{N}(a^3)=\mathrm{N}(5a) & \text{gives} & 125=2^2+11^2=10^2+5^2, \\ 5^4=\mathrm{N}(a^4)=\mathrm{N}(5a^2)=\mathrm{N}(25) & \text{gives} & 625=7^2+24^2=15^2+20^2=25^2+0, \\ 5^2\times 13=\mathrm{N}(a^2b)=\mathrm{N}(a^2\overline{b})=\mathrm{N}(5b) & \text{gives} & 325=18^2+1=17^2+6^2=15^2+10^2. \end{array}$$

Similarly $5^3\times 13=\mathrm{N}(a^3b)=\mathrm{N}(a^3\overline{b})=\mathrm{N}(5ab)=\mathrm{N}(5a\overline{b})$ gives

$$1625=16^2+37^2=28^2+29^2=20^2+35^2=40^2+5^2.$$

An analogous computation gives

$$1105=5\times 13\times 17=9^2+32^2=33^2+4^2=23^2+24^2=31^2+12^2.$$

Problem 3. *1.* The discriminant can be specialized and Δ is invertible modulo p. Next note that $\mathbb{Z}[\alpha]/\langle p\rangle \simeq \mathbb{F}_p[t] := \mathbb{F}_p[T]/\langle f(T)\rangle$. This already implies that the ideals $\langle q_k, p\rangle$ are maximal in $\mathbb{Z}[\alpha]$. For $j \neq k$, $\langle Q_j(t)\rangle+\langle Q_k(t)\rangle=\langle 1\rangle$ in $\mathbb{F}_p[t]$, so $\langle q_j\rangle+\langle q_k\rangle+\langle p\rangle=\langle 1\rangle$ in $\mathbb{Z}[\alpha]$. Whence $\langle q_j,p\rangle+\langle q_k,p\rangle=\langle 1\rangle$.
By the Chinese remainder theorem, the product of the $\langle q_k,p\rangle$ is therefore equal to their intersection, which is equal to $\langle p\rangle$ because the intersection of the $\langle Q_j(t)\rangle$ in $\mathbb{F}_p[t]$ is equal to their product, which is null.
Note that the equality $\langle p\rangle=\prod_{k=1}^{\ell}\langle p, Q_k(\alpha)\rangle$ is maintained in every ring containing $\mathbb{Z}[\alpha]$. Similarly for the comaximal character of the ideals.
If we move from $\mathbb{Z}[\alpha]$ to $\mathbf{A}$, then the only thing left to check is that the $\langle p,q_k\rangle$'s remain as maximal ideals. This is indeed the case and the quotient fields are isomorphic. Indeed, every element of $\mathbf{A}$ is of the form a/m where $a\in\mathbb{Z}[\alpha]$ and m^2 divides Δ (Proposition 8.17). Since m is comaximal to p the natural homomorphism $\mathbb{Z}[\alpha]/\langle p,q_k\rangle \to \mathbf{A}/\langle p,q_k\rangle$ is an isomorphism.

2. Apply Exercise 22.

Problem 4. *1a.* For primes p_1, p_2, … that do not divide n, we deduce that $f(\xi^{p_1p_2\cdots})=0$, i.e. $f(\xi^m)=0$ for every m such that $\gcd(n,m)=1$, or even that $f(\xi')=0$ for every ξ', n^{th} primitive root of the unit. So $f=\Phi_n$.
1b. Let $h(X)=\gcd_{\mathbb{Q}[X]}\big(f(X),g(X^p)\big)$. By Kronecker's theorem $h\in\mathbb{Z}[X]$. We have $h(\xi)=0$, therefore $\deg h\geqslant 1$. Let us reason modulo p. We have $g(X^p)=g(X)^p$, so $\overline{h}\mid\overline{f}$ and $\overline{h}\mid\overline{g}^p$. If π is an irreducible factor of $\overline{h}$, π^2 is a square factor of $X^n-\overline{1}$, but $X^n-\overline{1}$ is separable in $\mathbb{F}_p[X]$.

Note: the discriminant of the polynomial $X^n + c$ is $(-1)^{\frac{n(n-1)}{2}} n^n c^{n-1}$, in particular that of $X^n - 1$ is $(-1)^{\frac{(n+2)(n+3)}{2}} n^n$.

2. If G a cyclic group of order n, we have the classical isomorphisms

$$\mathrm{End}(G) \simeq \mathbb{Z}/n\mathbb{Z} \text{ (as rings) and } \mathrm{Aut}(G) \simeq \big((\mathbb{Z}/n\mathbb{Z})^\times, \times\big) \text{ (as groups).}$$

Whence canonical isomorphisms $\mathrm{Aut}(\mathbb{U}_n) \simeq (\mathbb{Z}/n\mathbb{Z})^\times \simeq \mathrm{Gal}(\mathbf{Q}_n/\mathbb{Q})$.
If $m \in (\mathbb{Z}/n\mathbb{Z})^\times$, we obtain the automorphism σ_m of $\mathbf{Q}_n$ defined by $\sigma_m(\zeta) = \zeta^m$ for $\zeta \in \mathbb{U}_n$.

3. Assume know a field of roots $\mathbf{L}$ as a strictly finite extension of $\mathbf{K}$. The map $\sigma \mapsto \sigma|_{\mathbb{U}_n}$ is an injective morphism of $\mathrm{Aut}_{\mathbf{K}}(\mathbf{L})$ into $\mathrm{Aut}(\mathbb{U}_n)$. In particular, $\mathrm{Aut}_{\mathbf{K}}(\mathbf{L})$ is isomorphic to a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$. Moreover, for every n^{th} primitive root of the unit ξ in $\mathbf{L}$, we have $\mathbf{L} = \mathbf{K}(\xi)$. So, every irreducible factor of $\Phi_n(X)$ in $\mathbf{K}[X]$ has the same degree $[\,\mathbf{L} : \mathbf{K}\,]$. However, it is not a priori obvious to determine what type of operation on $\mathbf{K}$ is necessary to factorize $\Phi_n(X)$ in $\mathbf{K}[X]$. We now give an example where we can determine with certainty $[\,\mathbf{L} : \mathbf{K}\,]$: let $p \geqslant 3$ be a prime, $p^* = (-1)^{\frac{p-1}{2}} p$ and $\mathbf{K} = \mathbb{Q}(\sqrt{p^*})$. Then $\mathbf{K} \subseteq \mathbf{Q}_p$ (Gauss), the only p^{th} root of the unit contained in $\mathbf{K}$ is 1 and $\Phi_p(X)$ can be factorized in $\mathbf{K}[X]$ as a product of two irreducible polynomials of the same degree $\frac{p-1}{2}$.

Problem 5. *1a.* On the one hand we have $\mathbf{A}/\mathfrak{p}_i \simeq \mathbb{F}_p[X]\big/\big\langle\overline{f_i}\big\rangle$ so $\mathfrak{p}_i$ is maximal. On the other hand, let $\overline{\mathbf{A}} = \mathbf{A}/p\mathbf{A} \simeq \mathbb{F}_p[X]\big/\big\langle\overline{\Phi_n}\big\rangle$ and $\pi : \mathbf{A} \twoheadrightarrow \overline{\mathbf{A}}$ be the canonical surjection; then $\sqrt{p\mathbf{A}} = \pi^{-1}\big(\mathrm{D}_{\overline{\mathbf{A}}}(0)\big)$ and

$$\mathrm{D}_{\overline{\mathbf{A}}}(0) = \langle\overline{g}\rangle\big/\big\langle\overline{\Phi_n}\big\rangle \simeq \big\langle\overline{f_1}\big\rangle\big/\big\langle\overline{\Phi_n}\big\rangle \times \cdots \times \big\langle\overline{f_k}\big\rangle\big/\big\langle\overline{\Phi_n}\big\rangle,$$

hence the result.

1b. Results from the fact that Φ_n is separable modulo p.

1c. We easily check the following equalities in $\mathbb{Z}[X]$

$$\Phi_n(X) = \Phi_{mp}(X^{p^{k-1}}) = \frac{\Phi_m(X^{p^k})}{\Phi_m(X^{p^{k-1}})},$$

and thus in $\mathbb{F}_p[X]$, by letting φ be the Euler's indicator function

$$\Phi_n(X) = \frac{\Phi_m(X)^{p^k}}{\Phi_m(X)^{p^{k-1}}} = \Phi_m(X)^{\varphi(p^k)} \qquad \bmod p.$$

The polynomial Φ_m is separable modulo p so the subset without a square factor of Φ_n modulo p is $\overline{g} = \overline{\Phi_m}$; whence $\sqrt{p\mathbf{A}} = \langle p, \Phi_m(\zeta_n)\rangle$.
Let us prove that $p \in \langle\Phi_m(\zeta_n)\rangle$. If $\zeta_p \in \mathbb{U}_n$ is a p^{th} primitive root of the unit, we have the equality

$$\Phi_p(X) = \textstyle\sum_{i=0}^{p-1} X^i = \prod_{j=1}^{p-1}(X - \zeta_p^j),$$

hence, by making $X := 1$

$$p = \textstyle\prod_{j=1}^{p-1}(1 - \zeta_p^j) \in \langle 1 - \zeta_p\rangle\,.$$

By applying this to $\zeta_p = \zeta_n^{mp^{k-1}}$, we obtain $p \in \big\langle 1 - \zeta_n^{mp^{k-1}}\big\rangle$.
However, $X^{mp^{k-1}} - 1$ is a multiple of Φ_m in $\mathbb{Z}[X]$, therefore $\zeta_n^{mp^{k-1}} - 1$ is a multiple of $\Phi_m(\zeta_n)$ in $\mathbf{A}$, whence $p \in \langle\Phi_m(\zeta_n)\rangle$.

1d. As $\sqrt{p\mathbf{A}} = \mathfrak{p}_1 \cdots \mathfrak{p}_k = \langle \Phi_m(\zeta_n) \rangle$ is finitely generated, there is an exponent e such that $(\mathfrak{p}_1 \cdots \mathfrak{p}_k)^e \subseteq p\mathbf{A}$ and we apply Exercise 22.
Note: we can take $e = \varphi(p^k) = p^k - p^{k-1}$.

2. The first item is immediate. Next, if $\mathfrak{a}$ is a nonzero finitely generated ideal of $\mathbf{A}$, it contains a nonzero element z. Then, $a = \mathrm{N}_{\mathbf{Q}_n/\mathbb{Q}}(z) = z\widetilde{z}$ is a nonzero integer belonging to $\mathfrak{a}$. We write $a\mathbf{A} \subseteq \mathfrak{a}$ as a product of invertible maximal ideals and we again apply Exercise 22 to the ideal $\mathfrak{a}$.

Problem 6. *1.* Let $x_0 \in G$ such that $\varphi(x_0) \neq 1$.
We write $\sum_{x\in G} \varphi(x) = \sum_{x\in G} \varphi(xx_0)$, therefore $S\varphi(x_0) = S$ with $S = \sum_{x\in G} \varphi(x)$, i.e. $\big(1 - \varphi(x_0)\big)S = 0$, whence $S = 0$.
2. First note that $\chi^{-1}(-1) = \chi(-1)$ since $\chi(-1)^2 = \chi\big((-1)^2\big) = 1$. We write

$$\textstyle\sum_{x+y=z} \chi(x)\chi^{-1}(y) = \sum_{x\neq 0,z} \chi\left(\frac{x}{z-x}\right).$$

If $z \neq 0$, the map $x \mapsto \frac{x}{z-x}$ is a bijection of $\mathbf{k}\cup\{\infty\}$ onto $\mathbf{k}\cup\{\infty\}$ which transforms z into ∞, ∞ into -1, 0 into 0, which gives a bijection of $\mathbf{k}^\times \setminus \{z\}$ onto $\mathbf{k}^\times \setminus \{-1\}$. We can therefore write

$$\textstyle\sum_{x+y=z} \chi(x)\chi^{-1}(y) = \sum_{v\in\mathbf{k}^\times\setminus\{-1\}} \chi(v) = \sum_{v\in\mathbf{k}^\times} \chi(v) - \chi(-1) = 0 - \chi(-1).$$

If $z = 0$ we have the equality

$$\textstyle\sum_{x+y=z} \chi(x)\chi^{-1}(y) = \sum_{x\neq 0} \chi(-1) = (q-1)\chi(-1).$$

3. We write

$$\textstyle G_\psi(\chi)G_\psi(\chi^{-1}) = \sum_{x,y} \chi(x)\chi^{-1}(y)\psi(x+y) = \sum_{z\in\mathbf{k}} S(z)\psi(z),$$

with $S(z) = \sum_{x+y=z} \chi(x)\chi^{-1}(y)$. Whence

$$\begin{aligned} G_\psi(\chi)G_\psi(\chi^{-1}) &= (q-1)\chi(-1) - \chi(-1)\textstyle\sum_{z\neq 0} \psi(z) \\ &= q\chi(-1) - \chi(-1)\textstyle\sum_{z\in\mathbf{k}} \psi(z) = q\chi(-1). \end{aligned}$$

4. The first item is immediate. We easily have $\tau_0\tau_1 = \frac{1-p^*}{4}$. The rest follows.

Problem 7. *1.* If $g(x) = 0$, with $x \in \mathbb{Z}$ and $g(X) \in \mathbb{Z}[X]$ monic, then $x \mid g(0)$. Here $\pm 1, \pm 2, \pm 4, \pm 8$ are not roots of $f(X)$, therefore this polynomial is irreducible. The discriminant of the polynomial $X^3 + aX^2 + bX + c$ is

$$18abc - 4a^3c + a^2b^2 - 4b^3 - 27c^2, \quad \text{hence the result for } a = 1,\ b = -2,\ c = 8.$$

2. The element $\beta = 4\alpha^{-1} \in \mathbb{Q}(\alpha)$ is integral over $\mathbb{Z}$ since

$$\alpha^3 + \alpha^2 - 2\alpha + 8 = 0 \overset{/\alpha^3}{\Longrightarrow} 1 + \alpha^{-1} - 2\alpha^{-2} + 8\alpha^{-3} = 0 \overset{\times 8}{\Longrightarrow} 8 + 2\beta - \beta^2 + \beta^3 = 0.$$

To check that $\mathbf{A} = \mathbb{Z} \oplus \mathbb{Z}\alpha \oplus \mathbb{Z}\beta$ is a ring, it suffices to see that $\alpha^2, \alpha\beta, \beta^2 \in \mathbf{A}$. It is clear for $\alpha\beta = 4$. We have $\alpha^2 + \alpha - 2 + 2\beta = 0$, so $\alpha^2 = 2 - \alpha - 2\beta$, and since $\beta^3 - \beta^2 + 2\beta + 8 = 0$, $\beta^2 = \beta - 2 - 8\beta^{-1} = \beta - 2 - 2\alpha$.
The expression of $(1, \alpha, \alpha^2)$ over the basis $(1, \alpha, \beta)$ is provided by the matrix

$$\begin{array}{c} \\ 1 \\ \alpha \\ \beta \end{array} \begin{array}{c} \begin{array}{ccc} 1 & \alpha & \alpha^2 \end{array} \\ \left[\begin{array}{ccc} 1 & 0 & 2 \\ 0 & 1 & -1 \\ 0 & 0 & -2 \end{array}\right] \end{array}.$$

The ring $\mathbb{Z}[\alpha]$ is therefore of index 2 in $\mathbf{A}$; but

$$\mathrm{Disc}_{\mathbb{Z}[\alpha]/\mathbb{Z}} = |\,\mathbf{A} : \mathbb{Z}[\alpha]\,|^2 \cdot \mathrm{Disc}_{\mathbf{A}/\mathbb{Z}} \quad \text{so} \quad \mathrm{Disc}_{\mathbf{A}/\mathbb{Z}} = -503.$$

Since the discriminant of $\mathbf{A}$ is squarefree, $\mathbf{A}$ is the ring of integers of $\mathbb{Q}(\alpha)$.

3. Let us prove that α, β and $\gamma := 1 + \alpha + \beta$ form, modulo 2, a fundamental system of orthogonal idempotents

$$\alpha + \alpha^2 = 2 - 2\beta, \quad \beta^2 - \beta = 2 - 2\alpha, \quad \alpha\beta = 4,$$

hence modulo 2

$$\alpha \equiv \alpha^2, \quad \beta \equiv \beta^2, \quad \gamma^2 \equiv \gamma, \quad \alpha + \beta + \gamma \equiv 1, \quad \alpha\beta \equiv 0, \quad \alpha\gamma \equiv 0, \quad \beta\gamma \equiv 0.$$

We therefore have $\mathbf{A}/2\mathbf{A} = \mathbb{F}_2\overline{\alpha} \oplus \mathbb{F}_2\overline{\beta} \oplus \mathbb{F}_2\overline{\gamma}$. If we want to compute the factorization of 2 in $\mathbf{A}$, we notice that (α, β, γ) is a $\mathbb{Z}$-basis of $\mathbf{A}$ and by denoting by π the morphism of reduction modulo 2, $\pi : \mathbf{A} \to \mathbf{A}/2\mathbf{A}$, the prime ideals of $\mathbf{A}$ over 2 are the inverse images of the prime ideals of $\mathbf{A}/2\mathbf{A}$. For example $\mathfrak{a} = \pi^{-1}(\{0\} \oplus \mathbb{F}_2\overline{\beta} \oplus \mathbb{F}_2\overline{\gamma}) = \langle 2\alpha, \beta, \gamma \rangle$. Thus by letting $\mathfrak{b} = \langle \alpha, 2\beta, \gamma \rangle$ and $\mathfrak{c} = \langle \alpha, \beta, 2\gamma \rangle$, we have $\mathbf{A}/\mathfrak{a} \simeq \mathbf{A}/\mathfrak{b} \simeq \mathbf{A}/\mathfrak{c} \simeq \mathbb{F}_2$ and $2\mathbf{A} = \mathfrak{abc} = \mathfrak{a} \cap \mathfrak{b} \cap \mathfrak{c}$.

In general, let $\mathbf{K}$ be a number field satisfying $[\,\mathbf{K} : \mathbb{Q}\,] \geqslant 3$ and 2 be completely decomposed in the ring of integers $\mathbf{Z_K}$. Then, $\mathbf{Z_K}$ is not monogenic, i.e. there exists no $x \in \mathbf{Z_K}$ such that $\mathbf{Z_K} = \mathbb{Z}[x]$. Indeed, $\mathbf{Z_K}/2\mathbf{Z_K} \simeq \mathbb{F}_2^n$ and $\mathbb{F}_2^n$ does not admit any primitive element over $\mathbb{F}_2$ if $n \geqslant 3$.

4. By multiplying $1 \in \mathfrak{f} + \mathfrak{b}$ by $\mathbf{B}'$, we obtain $\mathbf{B}' \subseteq \mathfrak{f}\mathbf{B}' + \mathfrak{b}' \subseteq \mathbf{B} + \mathfrak{b}'$, which shows that $\mathbf{B} \to \mathbf{B}'/\mathfrak{b}'$ is surjective. Let us prove that $\mathbf{B} \to \mathbf{B}'/\mathfrak{b}'$ is injective, i.e. $\mathfrak{b}' \cap \mathbf{B} = \mathfrak{b}$. By multiplying $1 \in \mathfrak{f} + \mathfrak{b}$ by $\mathfrak{b}' \cap \mathbf{B}$ we obtain the inclusions

$$\mathfrak{b}' \cap \mathbf{B} \subseteq (\mathfrak{b}' \cap \mathbf{B})\mathfrak{f} + (\mathfrak{b}' \cap \mathbf{B})\mathfrak{b} \subseteq \mathfrak{b}\mathbf{B}'\mathfrak{f} + \mathfrak{b} \subseteq \mathfrak{b}\mathbf{B} + \mathfrak{b} \subseteq \mathfrak{b}.$$

5. In the previous context, let $x \in \mathbf{Z_K}$ be of degree $n = [\,\mathbf{K} : \mathbb{Q}\,]$.

Let $d = |\,\mathbf{Z_K} : \mathbb{Z}[x]\,|$. We have $d\mathbf{Z_K} \subseteq \mathbb{Z}[x]$ and d can serve as conductor of $\mathbf{Z_K}$ into $\mathbb{Z}[x]$. If $2 \not| \, d$, by the Dedekind avoidance, $\mathbf{Z_K}/2\mathbf{Z_K} \simeq \mathbb{Z}[x]/2\mathbb{Z}[x] = \mathbb{F}_2[\overline{x}]$. But $\mathbf{Z_K}/2\mathbf{Z_K} \simeq \mathbb{F}_2^n$ does not admit a primitive element over $\mathbb{F}_2$ for $n \geqslant 3$.

Problem 8. *1.* $z \in \mathbf{B}$ is a root of $\prod_{\sigma \in G}(T - z)$, a monic polynomial with coefficients in $\mathbf{A}$.

2. $\overline{\mathfrak{m}} = \mathfrak{m}$ is clear. Let us compute $\mathfrak{m}^2$ by letting $d = 4q + 1$, so $1 + d = 2(2q + 1)$:

$$\begin{aligned} \mathfrak{m}^2 &= \left\langle 1 + 2\sqrt{d} + d, 1 - d, 1 - 2\sqrt{d} + d \right\rangle \\ &= 2\left\langle 2q + 1 + \sqrt{d}, 2q, 2q + 1 - \sqrt{d} \right\rangle = 2\left\langle 1 + \sqrt{d}, 1 - \sqrt{d} \right\rangle = 2\mathfrak{m}. \end{aligned}$$

In addition, as a $\mathbb{Z}$-module, $\mathfrak{m} = \mathbb{Z}(1+\sqrt{d}) \oplus \mathbb{Z}(1-\sqrt{d}) = 2\mathbb{Z} \oplus \mathbb{Z}(1 \pm \sqrt{d})$. We cannot simplify $\mathfrak{m}^2 = 2\mathfrak{m}$ by $\mathfrak{m}$ (because $\mathfrak{m} \neq 2\mathbf{B}$ seeing that $1 \pm \sqrt{d} \notin 2\mathbf{B}$), therefore $\mathfrak{m}$ is not invertible. We have $\mathrm{N}_G(\mathfrak{m}) = 2\mathbb{Z}$ therefore $\mathrm{N}_G(\mathfrak{m})\mathbf{B} = 2\mathbf{B} \neq \mathrm{N}'_G(\mathfrak{m})$.

The canonical map $\mathbb{Z} \to \mathbf{B}/\mathfrak{m}$ is surjective (since $x + y\sqrt{d} \equiv x + y \bmod \mathfrak{m}$) with kernel $2\mathbb{Z}$, so $\mathbb{F}_2 \simeq \mathbf{B}/\mathfrak{m}$, and $x + y\sqrt{d} \mapsto (x + y) \bmod 2$ defines a surjective morphism *of rings* $\mathbf{B} \twoheadrightarrow \mathbb{F}_2$, with kernel $\mathfrak{m}$.

Let $\mathrm{N}(\mathfrak{b}) = \#(\mathbf{B}/\mathfrak{b})$ for nonzero $\mathfrak{b}$. If $z = x(1+\sqrt{d}) + y(1-\sqrt{d}) \in \mathfrak{m}$ with $x, y \in \mathbb{Z}$, then $\mathrm{N}_G(z) = (x + y)^2 - d(x - y)^2 \equiv 4xy \bmod 4$.

So $\mathrm{N}_G(z) \in 4\mathbb{Z}$ for $z \in \mathfrak{m}$, but $\mathrm{N}(\mathfrak{m}) = 2$. We have $\mathrm{N}(\mathfrak{m}^2) = \mathrm{N}(2\mathfrak{m}) = 4\mathrm{N}(\mathfrak{m}) = 8$, but $\mathrm{N}(\mathfrak{m})^2 = 4$.

3. Let $\mathfrak{b} = \langle b_1, \dots, b_n \rangle$ and let $\underline{X} = (X_1, \dots, X_n)$ be n indeterminates. Let us introduce the normic polynomial $h(\underline{X})$

$$h(\underline{X}) = \prod\nolimits_{\sigma \in G} h_\sigma(\underline{X}) \quad \text{with} \quad h_\sigma(\underline{X}) = \sigma(b_1)X_1 + \cdots + \sigma(b_n)X_n.$$

We have $h(\underline{X}) \in \mathbf{A}[\underline{X}]$. Let d be a generator of $\mathrm{c}(h)_\mathbf{A}$. As $\mathbf{B}$ is integrally closed and $\mathrm{c}(h)_\mathbf{B} = d\mathbf{B}$ is principal, we can apply Proposition 8.13: we then have $\prod_\sigma \mathrm{c}(h_\sigma)_\mathbf{B} = \mathrm{c}(h)_\mathbf{B} = d\mathbf{B}$, i.e. $\mathrm{N}'_G(\mathfrak{b}) = d\mathbf{B}$.

Since $\mathbf{A}$ is Bézout, it is integrally closed. Let $a \in \mathbf{A} \cap d\mathbf{B}$. Then the element $a/d \in \mathrm{Frac}(\mathbf{A})$ is integral over $\mathbf{A}$ (because $a/d \in \mathbf{B}$) so $a/d \in \mathbf{A}$, i.e. $a \in d\mathbf{A}$.

Recap: $\mathbf{A} \cap d\mathbf{B} = d\mathbf{A}$ i.e. $\mathrm{N}_G(\mathfrak{b}) = d\mathbf{A}$.

By definition, the evaluations of the normic polynomial h over $\mathbf{B}^n$ are the norms of elements of the ideal $\mathfrak{b}$; they belong to the ideal of $\mathbf{A}$ generated by the coefficients of the normic polynomial, this ideal of $\mathbf{A}$ being $\mathrm{N}_G(\mathfrak{b})$.

If $\#G = 2$, the coefficient of X_1X_2 in h is

$$h(1,1,\dots,0) - h(1,0,\dots,0) - h(0,1,\dots,0) = \mathrm{N}_G(b_1 + b_2) - \mathrm{N}_G(b_1) - \mathrm{N}_G(b_2).$$

This in fact reduces to writing $b_1\overline{b_2} + b_2\overline{b_1} = \mathrm{N}_G(b_1 + b_2) - \mathrm{N}_G(b_1) - \mathrm{N}_G(b_2)$. Similarly, the coefficient of X_iX_j in h is, for $i \neq j$, $\mathrm{N}_G(b_i + b_j) - \mathrm{N}_G(b_i) - \mathrm{N}_G(b_j)$. Consequently, the ideal of $\mathbf{A}$ generated by the norms $\mathrm{N}_G(b_i)$ and $\mathrm{N}_G(b_i + b_j)$ contains all the coefficients of $h(\underline{X})$. It is therefore the ideal $\mathrm{N}_G(\mathfrak{b})$.

Problem 9. *(Forking lemma)*

1. For $x \in \mathbf{L}$, we have $x = \sum_j \mathrm{Tr}_{\mathbf{L}/\mathbf{K}}(xe_j)e'_j$.

If $x \in \mathbf{B}$, then $\mathrm{Tr}_{\mathbf{L}/\mathbf{K}}(xe_j)$ is an element of $\mathbf{K}$ integral over $\mathbf{A}$ so in $\mathbf{A}$. This proves the middle inclusion.

By writing $e_i = \sum_j \mathrm{Tr}_{\mathbf{L}/\mathbf{K}}(e_ie_j)e'_j$, we obtain

$${}^{\mathrm{t}}\underline{e} = A\,{}^{\mathrm{t}}\underline{e}' \text{ where } A = \big(\mathrm{Tr}_{\mathbf{L}/\mathbf{K}}(e_ie_j)\big) \in \mathbb{M}_n(\mathbf{A}), \text{ with } \det(A) = \Delta,$$

the right-hand side inclusion.

2. The $\mathbb{Z}$-module F_k is the intersection of $\mathbf{B}$ and Z_k, which are two subfinitely generated modules of Z_{n-1}, free, of rank n. It is therefore a free $\mathbb{Z}$-module of finite rank, and the two inclusions $\delta Z_k \subseteq F_k \subseteq Z_k$ show that F_k is of rank $k+1$. The $\mathbb{Z}$-module $\pi_k(F_k)$ is a finitely generated sub$\mathbb{Z}$-module of $\frac{1}{\delta}\mathbb{Z}$. Therefore it is generated by a_k/δ (where a_k is the gcd of the numerators of the generators). Finally, as $1 = \pi_k(x^k)$, a_k must divide δ and we write $\frac{a_k}{\delta} = \frac{1}{d_k}$.

3. Let $k \geqslant 1$ and $z \in F_k$. If $\pi_k(z) = a/d_k$ (with $a \in \mathbb{Z}$) we have $\pi_k(z - ay_k) = 0$. So $z - ay_k \in F_{k-1}$. Thus $F_k = \mathbb{Z}y_k \oplus F_{k-1}$ and we conclude by induction on k that $z \in \bigoplus_{i=0}^k \mathbb{Z}y_k$.

4. We have $y_iy_j \in F_{i+j}$ so $\frac{1}{d_id_j} = \pi_{i+j}(y_iy_j) \in \frac{1}{d_{i+j}}\mathbb{Z}$. In other words d_{i+j} is a multiple of d_id_j.

5 and *6.* Let us first prove that $d_kF_k \subseteq \mathbb{Z}[x]$ by induction on k. The base case $k = 0$ is clear. We then use the fact that $xy_{k-1} \in F_k$ and $\pi_k(xy_{k-1}) = \frac{1}{d_{k-1}}$, therefore

$$xy_{k-1} = \tfrac{d_k}{d_{k-1}} y_k + w_{k-1} \quad \text{with } w_{k-1} \in F_{k-1}.$$

We get $d_k y_k = x d_{k-1} y_{k-1} - d_{k-1} w_{k-1}$ and the right-hand side is in $\mathbb{Z}[x]$, by the induction hypothesis. Therefore $d_k y_k \in \mathbb{Z}[x]$ and

$$d_k F_k = d_k(\mathbb{Z} y_k \oplus F_{k-1}) = \mathbb{Z} d_k y_k \oplus d_k F_{k-1} \subseteq \mathbb{Z}[x] + d_{k-1} F_{k-1} \subseteq \mathbb{Z}[x].$$

We have defined $f_k(X)$ monic, of degree k in $\mathbb{Q}[X]$, by the equality $f_k(x) = d_k y_k$. Since $(1, \ldots, x^{n-1})$ is as much a $\mathbb{Z}$-basis of $\mathbb{Z}[x]$ as a $\mathbb{Q}$-basis of $\mathbb{Q}[x]$, and since $d_k y_k \in \mathbb{Z}[X]$, we obtain $f_k \in \mathbb{Z}[X]$.

The rest follows easily.

Problem 10. *1.* If $F(G) = X$, we have $\mathrm{JAC}(F)(0) \circ \mathrm{JAC}(G)(0) = \mathrm{I}_{\mathbf{A}^n}$.
As $\mathrm{JAC}(G)(0)$ is invertible, we apply the result to G. We have $H \in \mathbf{S}^n$ with $G(H) = X$. Then $F = F \circ G \circ H = H$. Therefore F, G are inverses of each other (as transformations of $\mathbf{S}^n$).

2. Immediate. We can a posteriori verify $\Phi(\mathbf{S}^n) \subseteq \mathbf{S}^n$ as well as the equivalence

$$\Phi(G) = G \iff F(G) = X.$$

3. We write $F(X) = J_0 \cdot X + F_2(X)$, where the vector $F_2(X)$ is of degree $\geqslant 2$ in X. Then, $J_0^{-1} \cdot \big(F(G) - F(H)\big) = G - H + J_0^{-1} \cdot \big(F_2(G) - F_2(H)\big)$.
Then $\Phi(G) - \Phi(H) = -J_0^{-1} \cdot \big(F_2(G) - F_2(H)\big)$. Assume $G_i - H_i \in \mathfrak{m}^d$ $(d \geqslant 1)$, and let us prove that each component of $\Phi(G) - \Phi(H)$ belongs to $\mathfrak{m}^{d+1}$. The result will be the desired inequality. Such a component is an $\mathbf{A}$-linear combination of $G^\alpha - H^\alpha$ with $\alpha \in \mathbb{N}^n$ and $|\alpha| \geqslant 2$. To simplify the notation, let $n = 3$ and write

$$G^\alpha - H^\alpha = (G_1^{\alpha_1} - H_1^{\alpha_1}) G_2^{\alpha_2} G_3^{\alpha_3} + (G_2^{\alpha_2} - H_2^{\alpha_2}) H_1^{\alpha_1} G_3^{\alpha_3} + (G_3^{\alpha_3} - H_3^{\alpha_3}) H_1^{\alpha_1} H_2^{\alpha_2}.$$

Since the H_i's, G_i's are constant-free, we have $G^\alpha - H^\alpha \in \mathfrak{m}^{d+1}$, except perhaps for $(\alpha_2, \alpha_3) = (0,0)$ or $(\alpha_1, \alpha_3) = (0,0)$ or $(\alpha_1, \alpha_3) = (0,0)$. It remains to look at the special cases, for example $\alpha_2 = \alpha_3 = 0$. In this case, since $\alpha_1 - 1 \geqslant 1$,

$$G^\alpha - H^\alpha = G_1^{\alpha_1} - H_1^{\alpha_1} = (G_1 - H_1) \textstyle\sum_{i+j=\alpha_1-1} G_1^i H_1^j \in \mathfrak{m}^{d+1}.$$

We have therefore established $d\big(\Phi(G), \Phi(H)\big) \leqslant d(G,H)/2$. This guarantees in particular that there exists at most one fixed point of Φ. Let $G^{(0)} \in \mathbf{S}^n$, for example $G^{(0)} = 0$, and the sequence $G^{(d)}$ defined by induction by means of $G^{(d+1)} = \Phi(G^{(d)})$.

For $d \geqslant 1$, each component of $G^{(d)} - G^{(d-1)}$ is in $\mathfrak{m}^d$, which allows us to define $G \in \mathbf{S}^n$ by $G = \sum_{d \geqslant 1} \big(G^{(d)} - G^{(d-1)}\big)$.

Then, G is the limit of the $G^{(d)}$ for $d \mapsto \infty$, it is a fixed point of Φ, i.e. $F(G) = X$.

4. Assume $G(F) = X$, so $G\big(F(0)\big) = 0$.
Let $\widetilde{F} = F - F(0)$, $\widetilde{G} = G\big(X + F(0)\big)$. Then, $\widetilde{F}(0) = \widetilde{G}(0) = 0$ and $\widetilde{G}(\widetilde{F}) = X$.
Hence $\widetilde{F}(\widetilde{G}) = X$, then $F(G) = X$.

5. Check in both cases that $\mathrm{Jac}(F) = 1$. For the first, we obtain G (of same maximum degree as F) by iterating Φ four times:

$$G = (-X^2Z^3 - 2XY^2Z^2 + 2XYZ + X - Y^4Z + 2Y^3,\ -XZ^2 - Y^2Z + Y,\ Z).$$

For the second, we obtain $G = (G_1, \ldots, G_5)$ by iterating Φ four times:

$$\begin{aligned}
G_1 &= X_1 - 3X_2X_4^2 + 6X_2X_4X_5^3 - 3X_2X_5^6 + 2X_3X_4X_5 - 2X_3X_5^4 + \\
&\quad X_4^4X_5 - 4X_4^3X_5^4 + 6X_4^2X_5^7 - 4X_4X_5^{10} + X_5^{13}, \\
G_2 &= X_2 - X_4^2X_5 + 2X_4X_5^4 - X_5^7, \\
G_3 &= X_3 - X_4^3 + 3X_4^2X_5^3 - 3X_4X_5^6 + X_5^9, \\
G_4 &= X_4 - X_5^3, \qquad G_5 \;=\; X_4.
\end{aligned}$$

Note that the maximum degree of G is 13 whereas that of F is 3.

Bibliographic comments

The proof of the Dedekind-Mertens lemma 2.1 on page 90 is taken from Northcott [148] (he attributes it to Artin).

Kronecker's Theorem 3.3 on page 92 is found in [122, Kronecker]. It is also proven by Dedekind [56] and Mertens [141].

Concerning the resultants and subresultants in one variable, a reference work is [Apéry & Jouanolou]. However, we regret the lack of a bibliography. Even if the results are either very old or completely new, we do not see the use of hiding the exact sources. Another important book for algorithmic questions on the subject is [Basu, Pollack & Roy].

The construction of an abtract splitting field for a separable polynomial given in Theorem 6.15 is (almost exactly) that described by Jules Drach in [65], which also seems to be where the universal splitting algebra as a fundamental tool for studying algebraic extensions of fields was introduced.

The telegraphical proof of Theorem 8.12 was suggested to us by Thierry Coquand.

The Kronecker approach regarding the theory of ideals of number fields is the subject of a historical survey in [87, Fontana&Loper].

The proof of the Nullstellensatz given in Section 9 is inspired by the one in [Basu, Pollack & Roy], itself inspired by a van der Waerden proof.

Chapter IV

Finitely presented modules

Contents

Introduction

Over a ring the finitely presented modules play a similar role as that of the finite dimensional vector spaces over a field: the theory of finitely presented modules is a slightly more abstract, and at times more profitable, way to approach the subject of systems of linear equations.

In the first sections of the chapter, we provide the basics of the theory of finitely presented modules.

In Section 7, we treat the example of finitely presented modules over PIDs, and in Section 8 that of finitely presented modules over zero-dimensional rings.

Finally, Section 9 is dedicated to important invariants that are Fitting ideals, and Section 10 introduces the resultant ideal as a direct application of the Fitting ideals.

1. Definition, changing generator set

A *finitely presented module* is an $\mathbf{A}$-module M given by a finite number of generators and relations. Therefore it is a module with a finite generator set having a finitely generated syzygy module. Equivalently, it is a module M isomorphic to the cokernel of a linear map

$$\gamma : \mathbf{A}^m \longrightarrow \mathbf{A}^q.$$

The matrix $G \in \mathbf{A}^{q\times m}$ of γ has as its columns a generator set of the syzygy module between the generators g_i which are the images of the canonical base of $\mathbf{A}^q$ by the surjection $\pi : \mathbf{A}^q \to M$. Such a matrix is called a *presentation matrix of the module M for the generator set* $(g_1, \ldots, g_q)$. This translates into

- $[\,g_1 \ \cdots \ g_q\,]\,G = 0$, and
- every syzygy between the g_i's is a linear combination of the columns of G, i.e.: if $[\,g_1 \ \cdots \ g_q\,]\,C = 0$ with $C \in \mathbf{A}^{q\times 1}$, there exists a $C' \in \mathbf{A}^{m\times 1}$ such that $C = G\,C'$.

Examples. 1) A free module of rank k is a finitely presented module presented by a matrix column formed of k zeros.[1] More generally every simple matrix is the presentation matrix of a free module of finite rank.

2) Recall that a finitely generated projective module is a module P isomorphic to the image of a projection matrix $F \in \mathbb{M}_n(\mathbf{A})$ for a specific integer n. Since $\mathbf{A}^n = \mathrm{Im}(F) \oplus \mathrm{Im}(\mathrm{I}_n - F)$, we obtain $P \simeq \mathrm{Coker}(\mathrm{I}_n - F)$. This shows that every finitely generated projective module is finitely presented.

3) Let $\varphi : V \to V$ be an endomorphism of a finite-dimensional vector space over a discrete field $\mathbf{K}$. Consider V as a $\mathbf{K}[X]$-module with the following external law

$$\begin{cases} \mathbf{K}[X] \times V \to V \\ (P, u) \qquad \mapsto P \cdot u := P(\varphi)(u). \end{cases}$$

Let $(u_1, \ldots, u_n)$ be a basis of V as a $\mathbf{K}$-vector space and A be the matrix of φ with respect to this basis. Then we can show that a presentation matrix of V as a $\mathbf{K}[X]$-module for the generator set $(u_1, \ldots, u_n)$ is the matrix $X\,\mathrm{I}_n - A$ (see Exercise 3). ■

[1] If we consider that a matrix is given by two integers $q, m \geqslant 0$ and a family of elements of the ring indexed by the pairs (i, j) with $i \in [\![1..q]\!]$, $j \in [\![1..m]\!]$, we can accept an empty matrix of type $k \times 0$, which would be the canonical matrix to present a free module of rank k.

1.0. Lemma. *When we change a finite generator set for a given finitely presented module, the syzygies between the new generators form a finitely generated module again.*

D Suppose that indeed, with $M \simeq \operatorname{Coker} G$, another generator set of the $\mathbf{A}$-module M is $(h_1, \ldots, h_r)$. We therefore have matrices $H_1 \in \mathbf{A}^{q\times r}$ and $H_2 \in \mathbf{A}^{r\times q}$ such that

$$[\,g_1\ \cdots\ g_q\,]\,H_1 = [\,h_1\ \cdots\ h_r\,] \text{ and } [\,h_1\ \cdots\ h_r\,]\,H_2 = [\,g_1\ \cdots\ g_q\,].$$

Then, the syzygy module between the h_j's is generated by the columns of H_2G and that of $\mathrm{I}_r - H_2H_1$. Indeed on the one hand we clearly have

$$[\,h_1\ \cdots\ h_r\,]\,H_2\,G = 0 \quad\text{and}\quad [\,h_1\ \cdots\ h_r\,]\,(\mathrm{I}_r - H_2H_1) = 0.$$

On the other hand, if we have a syzygy $[\,h_1\ \cdots\ h_r\,]\,C = 0$, we deduce $[\,g_1\ \cdots\ g_q\,]\,H_1C = 0$, so $H_1C = GC'$ for some column vector C' and

$$C = \big((\mathrm{I}_r - H_2H_1) + H_2H_1\big)C = (\mathrm{I}_r - H_2H_1)C + H_2GC' = HC'',$$

where $H = [\,\mathrm{I}_r - H_2H_1 \mid H_2G\,]$ and $C'' = \begin{bmatrix} C \\ C' \end{bmatrix}$. □

This possibility of replacing a generator set by another while preserving a finite number of relations is an extremely general phenomenon. It applies to every form of algebraic structure which can be defined by generators and relations. For example, it applies to those structures for which every axiom is a universal equality. Here is how this works (it suffices to verify that the reasoning applies in each case).

Assume that we have generators $g_1,\ldots, g_n$ and relations

$$R_1(g_1, \ldots, g_n),\ \ldots,\ R_s(g_1, \ldots, g_n),$$

which "present" a structure M.

If we have other generators $h_1, \ldots, h_m$, we express them in terms of the g_j's in the form $h_i = H_i(g_1, \ldots, g_n)$. Let $S_i(h_i, g_1, \ldots, g_n)$ be this relation. We similarly express the g_j's in terms of the h_i's $g_j = G_j(h_1, \ldots, h_m)$. Let $T_j(g_j, h_1, \ldots, h_m)$ this relation.

The structure does not change if we replace the presentation

$$(g_1, \ldots, g_n\ ;\ R_1, \ldots, R_s)$$

with

$$(g_1, \ldots, g_n, h_1, \ldots, h_m\ ;\ R_1, \ldots, R_s, S_1, \ldots, S_m).$$

As the relations T_j are satisfied, they are consequences of the relations R_1, $\ldots$, R_s, S_1, $\ldots$, S_m, therefore the structure is always the same with the following presentation

$$(g_1, \ldots, g_n, h_1, \ldots, h_m\ ;\ R_1, \ldots, R_s, S_1, \ldots, S_m, T_1, \ldots, T_n).$$

Now in each of the relations R_k and S_ℓ, we can replace each g_j with its expression in terms of the h_i's (which is given in T_j) and this still does not change the presented structure. We obtain

$$(g_1, \ldots, g_n, h_1, \ldots, h_m \ ; \ R'_1, \ldots, R'_s, S'_1, \ldots, S'_m, T_1, \ldots, T_n).$$

Finally, if we subtract the pairs $(g_j; T_j)$ one-by-one, it is clear that the structure will still remain unchanged, so we obtain the finite presentation

$$(h_1, \ldots, h_m \ ; \ R'_1, \ldots, R'_s, S'_1, \ldots, S'_m).$$

In the case of finitely presented modules this reasoning can be expressed in matrix form.

First of all we note that we do not change the structure of M when we subject the presentation matrix G to one of the following transformations.

1. Adding a null column (this does not change the syzygy module between fixed generators).

2. Deleting a null column, except to obtain an empty matrix.

3. Replacing G, of type $q \times m$, with G' of type $(q+1) \times (m+1)$ obtained from G by adding a null row on the bottom then a column to the right with 1 in the position $(q+1, m+1)$, (this reduces to adding a vector among the generators, by indicating its dependence with respect to the previous generators)
$$G \ \mapsto \ G' \ = \ \begin{bmatrix} G & C \\ 0_{1,m} & 1 \end{bmatrix}.$$

4. The inverse of the previous operation, except in the case of an empty matrix.

5. Adding to a column a linear combination of the other columns (this does not change the syzygy module between fixed generators).

6. Adding to a row a linear combination of the other rows, (for example if we let L_i be the i^{th} row, replacing L_1 with $L_1 + \gamma L_2$ reduces to replacing the generator g_2 with $g_2 - \gamma g_1$).

7. Permuting columns or rows.

We then see that if G and H are two presentation matrices of the same module M, we can pass from one to the other by means of the transformations described above. Slightly better: we see that for every finite generator set of M, we can construct from G, by using these transformations, a presentation matrix of M for the new generator set. Note that consequently, a change of basis of $\mathbf{A}^q$ or $\mathbf{A}^m$, which corresponds to the multiplication of G (either on the left or right) by an invertible matrix, can be realized by the operations previously described.

More precisely, we obtain the following result.

1.1. Lemma. *Let $G \in \mathbf{A}^{q \times m}$ and $H \in \mathbf{A}^{r \times n}$ be two matrices. Then the following properties are equivalent.*

1. *The matrices G and H present "the same" module, i.e. their cokernels are isomorphic.*
2. *The two matrices of the figure below are elementarily equivalent.*
3. *The two matrices of the figure below are equivalent.*

$$\begin{array}{c|c|c|c|c|}
 & m & r & q & n \\ \hline
q & \mathrm{G} & 0 & 0 & 0 \\ \hline
r & 0 & \mathrm{I}_r & 0 & 0 \\ \hline
\end{array}$$

$$\begin{array}{c|c|c|c|c|}
\hline
q & 0 & 0 & \mathrm{I}_q & 0 \\ \hline
r & 0 & 0 & 0 & \mathrm{H} \\ \hline
\end{array}$$

The two matrices

As a first consequence of Lemma 1.0 we obtain a more abstract reformulation of coherence as follows.

1.2. Fact. *A ring is coherent if and only if every finitely generated ideal is finitely presented (as* **A***-module). An* **A***-module is coherent if and only if every finitely generated submodule is finitely presented.*

A digression on the algebraic computation

Besides their direct relationship to solving systems of linear equations another reason for the importance of finitely presented modules is the following.

Each time an algebraic computation reaches an "interesting result" in an **A**-module M this computation has only involved a finite number of elements $x_1, \ldots, x_n$ of M and a finite number of syzygies between the x_j's, so that there exist a finitely presented module $P = \mathbf{A}^n/R$ and a surjective linear map $\theta : P \to x_1\mathbf{A} + \cdots + x_n\mathbf{A} \subseteq M$ which sends the e_j's onto the x_j's. Note that e_j designates the class modulo R of the j^{th} vector of the canonical basis of $\mathbf{A}^n$. It must also be true of the above that the "interesting result" had already been held in P for the e_j's.

In a more scholarly language we express this idea as follows.
Every **A***-module is a filtering colimit (or filtering inductive limit) of finitely*

presented **A***-modules.*
However, this statement requires a more subtle treatment in constructive mathematics, and we therefore only indicate its existence.

2. Finitely presented ideals

Consider a ring **A** and a generator set $(a_1, \dots, a_n) = (\underline{a})$ for a finitely generated ideal $\mathfrak{a}$ of **A**. We are interested in the **A**-module structure of $\mathfrak{a}$.

Trivial syzygies

Among the syzygies between the a_i's there are what we call the *trivial syzygies* (or *trivial relators* if we see them as algebraic dependence relations over **k** when **A** is a **k**-algebra):

$$a_i a_j - a_j a_i = 0 \ \text{ for } \ i \neq j.$$

If $\mathfrak{a}$ is finitely presented, we can always take a presentation matrix of $\mathfrak{a}$ for the generator set $(\underline{a})$ in the form

$$W = [\, R_{\underline{a}} \mid U \,],$$

where $R_{\underline{a}}$ is "the" $n \times n(n-1)/2$ *matrix of trivial syzygies* (the order of the columns is without importance). For example, for $n = 4$

$$R_{\underline{a}} = \begin{bmatrix} a_2 & a_3 & 0 & a_4 & 0 & 0 \\ -a_1 & 0 & a_3 & 0 & a_4 & 0 \\ 0 & -a_1 & -a_2 & 0 & 0 & a_4 \\ 0 & 0 & 0 & -a_1 & -a_2 & -a_3 \end{bmatrix}.$$

2.1. Lemma. (Determinantal ideals of the matrix of trivial syzygies)
Using the above notations, we have the following results.

1. $\mathcal{D}_n(R_{\underline{a}}) = \{0\}$.
2. *If* $1 \leqslant r < n$, *then* $\mathcal{D}_r(R_{\underline{a}}) = \mathfrak{a}^r$ *and*

$$\mathfrak{a}^r + \mathcal{D}_r(U) \ \subseteq\ \mathcal{D}_r(W) \ \subseteq\ \mathfrak{a} + \mathcal{D}_r(U).$$

In particular, we have the equivalence

$$1 \in \mathcal{D}_{\mathbf{A},r}(W) \iff 1 \in \mathcal{D}_{\mathbf{A}/\mathfrak{a},r}(\overline{U}) \quad \textit{where } \overline{U} = U \bmod \mathfrak{a}.$$

3. $\mathcal{D}_n(W) = \mathcal{D}_n(U)$.

D *1.* These are algebraic identities and we can take for $a_1, \dots, a_n$ indeterminates over $\mathbb{Z}$. Since $[\, a_1 \ \cdots \ a_n \,] \cdot R_{\underline{a}} = 0$, we obtain the equality $\mathcal{D}_n(R_{\underline{a}})\,[\, a_1 \ \cdots \ a_n \,] = 0$. The result follows since a_1 is regular.

2. The inclusion $\mathcal{D}_r(R_{\underline{a}}) \subseteq \mathfrak{a}^r$ is obvious for all $r \geqslant 0$. For the reverse inclusion, let us take for example $r = 4$ and $n \geqslant 5$ and show that

$$\left\{a_1^4,\, a_1^3 a_2,\, a_1^2 a_2^2,\, a_1^2 a_2 a_3,\, a_1 a_2 a_3 a_4\right\} \subseteq \mathcal{D}_4(R_{\underline{a}}).$$

It suffices to consider the matrices below (we have deleted the 0's and replaced $\pm a_i$ with i to clarify the structure) extracted from $R_{\underline{a}}$, and the minors extracted on the last 4 rows.

$$\begin{bmatrix} 2 & 3 & 4 & 5 \\ 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{bmatrix}, \quad \begin{bmatrix} 2 & 3 & 4 & \\ 1 & & & 5 \\ & 1 & & \\ & & 1 & \\ & & & 2 \end{bmatrix}, \quad \begin{bmatrix} 2 & 3 & & \\ 1 & & 4 & 5 \\ & 1 & & \\ & & 2 & \\ & & & 2 \end{bmatrix},$$
$$\begin{bmatrix} 2 & 3 & & \\ 1 & & 4 & \\ & 1 & & 5 \\ & & 2 & \\ & & & 3 \end{bmatrix}, \quad \begin{bmatrix} 2 & & & \\ 1 & 3 & & \\ & 2 & 4 & \\ & & 3 & 5 \\ & & & 4 \end{bmatrix}.$$

The inclusion $\mathfrak{a}^r + \mathcal{D}_r(U) \subseteq \mathcal{D}_r(W)$ results from $\mathcal{D}_r(R_{\underline{a}}) + \mathcal{D}_r(U) \subseteq \mathcal{D}_r(W)$ and from the equality $\mathcal{D}_r(R_{\underline{a}}) = \mathfrak{a}^r$. The inclusion $\mathcal{D}_r(W) \subseteq \mathfrak{a} + \mathcal{D}_r(U)$ is immediate. Finally, the final equivalence results from the previous inclusions and from the equality

$$\mathcal{D}_{\mathbf{A}/\mathfrak{a},r}(\overline{U}) = \pi^{-1}_{\mathbf{A},\mathfrak{a}}\big(\mathfrak{a} + \mathcal{D}_r(U)\big).$$

3. We must show that if a matrix $A \in \mathbb{M}_n(\mathbf{A})$ extracted from W contains a column in $R_{\underline{a}}$, then $\det A = 0$. Take for example the first column of A equal to the first column of $R_{\underline{a}}$, ${}^{\mathrm{t}}[\, a_2 \;\; -a_1 \;\; 0 \;\cdots\; 0 \,]$. When $z_i = a_i$, Lemma 2.2 below implies $\det A = 0$, because the s_j's are null. □

Recall that $A_{\alpha,\beta}$ is the submatrix of A extracted on the rows α and the columns β. Let us also introduce the notation for a "scalar product"

$$\langle x \,|\, y \rangle \overset{\text{def}}{=} \textstyle\sum_{i=1}^n x_i y_i$$

for two column vectors x and y.

2.2. Lemma. *Let $A \in \mathbb{M}_n(\mathbf{A})$, $A_j = A_{1..n,j}$, and $z = {}^{\mathrm{t}}[\, z_1 \cdots z_n \,] \in \mathbf{A}^{n\times 1}$ with $A_1 = {}^{\mathrm{t}}[\, z_2 \;\; -z_1 \;\; 0 \;\cdots\; 0 \,]$. By letting $s_j = \langle z \,|\, A_j \rangle$ for $j \in [\![2..n]\!]$, we have*

$$\det A = \sum\nolimits_{j=2}^{n} (-1)^j \, s_j \, \det(A_{3..n,\,2..n\setminus\{j\}}).$$

In particular, $\det A \in \langle s_2, \ldots, s_n \rangle$.

D Let $B = A_{3..n,2..n}$, $B_j = A_{3..n,j}$ and $B_{\hat{\jmath}} = A_{3..n,\,2..n\setminus\{j\}}$. The Laplace expansion of the determinant of A according to the two first rows gives the equality:

$$\det A = \sum_{j=2}^{n} (-1)^j \begin{vmatrix} z_2 & a_{1j} \\ -z_1 & a_{2j} \end{vmatrix} \det(B_{\hat{\jmath}}) = \sum_{j=2}^{n} (-1)^j \, (z_1 a_{1j} + z_2 a_{2j}) \det(B_{\hat{\jmath}}).$$

The gap between this equality and the desired equality is

$$\textstyle\sum_{j=2}^{n} (-1)^j \, (z_3 a_{3j} + \cdots + z_n a_{nj}) \, \det(B_{\hat{\jmath}}). \qquad (*)$$

Cramer's syzygies between the columns of a matrix with $m = n_2$ gives for B the equalities

$$\textstyle\sum_{j=2}^{n}(-1)^j \det(B_{\hat{\jmath}})\, B_j = 0, \text{ a fortiori } \sum_{j=2}^{n}(-1)^j \,\langle y \,|\, B_j\rangle \det(B_{\hat{\jmath}}) = 0,$$

for any vector $y \in \mathbf{A}^{(n-2)\times 1}$. By taking $y = {}^{\mathrm{t}}[\, z_3 \;\cdots\; z_n \,]$, we see that the gap $(*)$ is null. □

Regular sequences

2.3. Definition. A sequence $(a_1, \ldots, a_k)$ in a ring $\mathbf{A}$ is *regular* if each a_i is regular in the ring $\mathbf{A}/\langle a_j \,;\, j < i\rangle$.

Remark. Here we have kept Bourbaki's definition. Most authors also require that the ideal $\langle a_1, \ldots, a_k\rangle$ does not contain 1. ■

As a first example, for every ring $\mathbf{k}$, the sequence $(X_1, \ldots, X_k)$ is regular in $\mathbf{k}[X_1, \ldots, X_k]$.

Our goal is to show that an ideal generated by a regular sequence is a finitely presented module.

We first establish a small lemma and a proposition.

Recall that a matrix $M = (m_{ij}) \in \mathbb{M}_n(\mathbf{A})$ is said to be *alternating* if it is the matrix of an alternating bilinear form, i.e. $m_{ii} = 0$ and $m_{ij} + m_{ji} = 0$ for i, $j \in [\![1..n]\!]$.

The $\mathbf{A}$-module of alternating matrices is free and of rank $\frac{n(n-1)}{2}$ and admits a natural basis. For example, for $n = 3$,

$$\begin{bmatrix} 0 & a & b \\ -a & 0 & c \\ -b & -c & 0 \end{bmatrix} = a\begin{bmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} + b\begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ -1 & 0 & 0 \end{bmatrix} + c\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{bmatrix}.$$

2.4. Lemma. *Let $a = {}^{\mathrm{t}}[\,\underline{a}\,] = {}^{\mathrm{t}}[\, a_1 \;\cdots\; a_n \,] \in \mathbf{A}^{n\times 1}$.*

1. *Let $M \in \mathbb{M}_n(\mathbf{A})$ be an alternating matrix; we have $\langle Ma \,|\, a\rangle = 0$.*
2. *A $u \in \mathbf{A}^{n\times 1}$ is in $\operatorname{Im} R_{\underline{a}}$ if and only if there exists an alternating matrix $M \in \mathbb{M}_n(\mathbf{A})$ such that $u = Ma$.*

D *1.* Indeed, $\langle Ma \,|\, a\rangle = \varphi(a, a)$, where φ is an alternating bilinear form.

2. For example, for the first column of $R_{\underline{a}}$ with $n = 4$, we have

$$\begin{bmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}\begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \end{bmatrix} = \begin{bmatrix} a_2 \\ -a_1 \\ 0 \\ 0 \end{bmatrix},$$

and the $\frac{n(n-1)}{2}$ columns of $R_{\underline{a}}$ thus correspond to $\frac{n(n-1)}{2}$ alternating matrices forming the natural basis of the $\mathbf{A}$-module of alternating matrices of $\mathbb{M}_n(\mathbf{A})$. □

2.5. Proposition. *Let* $(z_1, \dots, z_n) = (\underline{z})$ *be a regular sequence of elements of* $\mathbf{A}$ *and* $z = {}^{\mathrm{t}}[\, z_1 \ \cdots \ z_n \,] \in \mathbf{A}^{n\times 1}$. *If* $\langle u \,|\, z\rangle = 0$, *there exists an alternating matrix* $M \in \mathbb{M}_n(\mathbf{A})$ *such that* $u = Mz$, *and therefore* $u \in \operatorname{Im} R_{\underline{z}}$.

D We reason by induction on n. For $n = 2$, we start from $u_1z_1 + u_2z_2 = 0$. Therefore $u_2z_2 = 0$ in $\mathbf{A}/\langle z_1\rangle$, and since z_2 is regular modulo z_1, we have $u_2 = 0$ in $\mathbf{A}/\langle z_1\rangle$, say $u_2 = -az_1$ in $\mathbf{A}$. We get $u_1z_1 - az_2z_1 = 0$, and as z_1 is regular, $u_1 = az_2$, which is written as $\begin{bmatrix} u_1 \\ u_2 \end{bmatrix} = \begin{bmatrix} 0 & a \\ -a & 0 \end{bmatrix}\begin{bmatrix} z_1 \\ z_2 \end{bmatrix}$.
For $n + 1$ ($n \geqslant 2$), we start from $u_1z_1 + \cdots + u_{n+1}z_{n+1} = 0$. By using the fact that z_{n+1} is regular modulo $\langle z_1, \dots, z_n\rangle$, we obtain $u_{n+1} \in \langle z_1, \dots, z_n\rangle$, which we write as $a_1z_1 + \cdots + a_nz_n + u_{n+1} = 0$. Whence

$$(u_1 - a_1z_{n+1})z_1 + \cdots + (u_n - a_nz_{n+1})z_n = 0.$$

By induction hypothesis, we know how to construct an alternating matrix $M \in \mathbb{M}_n(\mathbf{A})$ with

$$\begin{bmatrix} u_1 - a_1z_{n+1} \\ \vdots \\ u_n - a_nz_{n+1} \end{bmatrix} = M \begin{bmatrix} z_1 \\ \vdots \\ z_n \end{bmatrix}, \text{ i.e. } \begin{bmatrix} u_1 \\ \vdots \\ u_n \end{bmatrix} = M \begin{bmatrix} z_1 \\ \vdots \\ z_n \end{bmatrix} + z_{n+1} \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix},$$

and we obtain the desired result

$$\begin{bmatrix} u_1 \\ \vdots \\ u_n \\ u_{n+1} \end{bmatrix} = \begin{bmatrix} & & & a_1 \\ & M & & \vdots \\ & & & a_n \\ -a_1 & \dots & -a_n & 0 \end{bmatrix} \begin{bmatrix} z_1 \\ \vdots \\ z_n \\ z_{n+1} \end{bmatrix}.$$

□

2.6. Theorem. *If* $(z_1, \dots, z_n)$ *is a regular sequence of elements of* $\mathbf{A}$, *the ideal* $\langle z_1, \dots, z_n\rangle$ *is a finitely presented* $\mathbf{A}$*-module. More precisely, we have the exact sequence*

$$\mathbf{A}^{n(n-1)/2} \xrightarrow{R_{\underline{z}}} \mathbf{A}^n \xrightarrow{(z_1,\dots,z_n)} \langle z_1, \dots, z_n\rangle \longrightarrow 0.$$

Remark. The objects defined above constitute an introduction to the first degree of the *Koszul complex* of $(z_1, \dots, z_n)$. ■

D This results from Proposition 2.5 and from Lemma 2.4. □

A geometry example

Let us begin with a most useful and obvious fact.

2.7. Proposition and definition. (Characters of an algebra)
Let $\imath : \mathbf{k} \to \mathbf{A}$ *be an algebra.*

- *A homomorphism of* $\mathbf{k}$*-algebras* $\varphi : \mathbf{A} \to \mathbf{k}$ *is called a* character.

- *If* $\mathbf{A}$ *has a character* φ*, then* $\varphi \circ \imath = \mathrm{Id}_{\mathbf{k}}$*,* $\imath \circ \varphi$ *is a projector and* $\mathbf{A} = \mathbf{k}.1_{\mathbf{A}} \oplus \operatorname{Ker}\varphi$*. In particular,* $\mathbf{k}$ *may be identified with* $\mathbf{k}.1_{\mathbf{A}}$*.*

D The proof is left to the reader. □

Now let $(\underline{f}) = (f_1, \ldots, f_s)$ be a polynomial system over a ring $\mathbf{k}$, with each $f_i \in \mathbf{k}[\underline{X}] = \mathbf{k}[X_1, \ldots, X_n]$. We let

$$\mathbf{A} = \mathbf{k}[x_1, \ldots, x_n] = \mathbf{k}[\underline{X}]/\langle\underline{f}\rangle.$$

In this subsection, we will formally say that $\mathbf{A}$ is the *ring of the affine variety* $\underline{f} = \underline{0}$.

For the algebra $\mathbf{A}$, the characters $\varphi : \mathbf{A} \to \mathbf{k}$ are given by the zeros in $\mathbf{k}^n$ of the polynomial system $(f_1, \ldots, f_s)$

$$(\underline{\xi}) = (\xi_1, \ldots, \xi_n) = \big(\varphi(x_1), \ldots, \varphi(x_n)\big), \quad \underline{f}(\underline{\xi}) = \underline{0}.$$

In this case, we say that $(\underline{\xi}) \in \mathbf{k}^n$ is a point of the variety $\underline{f} = \underline{0}$.

The ideal

$$\mathfrak{m}_{\underline{\xi}} \overset{\text{def}}{=} \langle x_1 - \xi_1, \ldots, x_n - \xi_n\rangle_{\mathbf{A}}$$

is called the *ideal of the point* $(\underline{\xi})$ *in the variety.* We then have as a special case of Proposition 2.7: $\mathbf{A} = \mathbf{k} \oplus \mathfrak{m}_{\underline{\xi}}$, with $\mathfrak{m}_{\underline{\xi}} = \operatorname{Ker}\varphi$.

In this subsection we show that the ideal $\mathfrak{m}_{\underline{\xi}}$ is a finitely presented $\mathbf{A}$-module by making a presentation matrix for the generator set $(x_1 - \xi_1, \ldots, x_n - \xi_n)$ explicit.

By translation, it suffices to treat the case where $\underline{\xi} = \underline{0}$, which we assume henceforth.

The simplest case, that for which there is no equation, has already been treated in Theorem 2.6.

Let us observe that every $f \in \mathbf{k}[\underline{X}]$ such that $f(\underline{0}) = 0$ is written, in many ways, in the form

$$f = X_1 u_1 + \cdots + X_n u_n, \qquad u_i \in \mathbf{k}[\underline{X}].$$

If $X_1 v_1 + \cdots + X_n v_n$ is another expression of f, we obtain by subtraction a syzygy between the X_i's in $\mathbf{k}[\underline{X}]$, and so

$${}^{\mathrm{t}}[\, v_1 \ \cdots \ v_n \,] - {}^{\mathrm{t}}[\, u_1 \ \cdots \ u_n \,] \in \operatorname{Im} R_{\underline{X}}.$$

For the polynomial system $(f_1, \ldots, f_s)$, we thus define (in a non-unique manner) a family of polynomials $(u_{ij})_{i\in[\![1..n]\!],j\in[\![1..s]\!]}$, with $f_j = \sum_{i=1}^{n} X_i u_{ij}$. This gives a matrix $U(\underline{X}) = (u_{ij})$ and its image $U(\underline{x}) = \big(u_{ij}(\underline{x})\big) \in \mathbf{A}^{n\times s}$.

2.8. Theorem. *For a polynomial system over a ring* $\mathbf{k}$ *and a zero* $(\underline{\xi}) \in \mathbf{k}^n$*, the ideal* $\mathfrak{m}_{\underline{\xi}}$ *of the point* $(\underline{\xi})$ *is a finitely presented* $\mathbf{A}$*-module.*

More precisely, with the previous notations, for the $\underline{\xi} = \underline{0}$ *case the matrix* $W = [\, R_{\underline{x}} \,|\, U(\underline{x}) \,]$ *is a presentation matrix of the ideal* $\mathfrak{m}_{\underline{0}}$ *for the generator* *set* $(x_1, \dots, x_n)$*. In other words we have an exact sequence*

$$\mathbf{A}^m \xrightarrow{[\,R_{\underline{x}}\,|\,U\,]} \mathbf{A}^n \xrightarrow{(x_1,\dots,x_n)} \mathfrak{m}_{\underline{0}} \longrightarrow 0 \qquad (m = \tfrac{n(n-1)}{2} + s).$$

D Take for example $n = 3$, $s = 4$, $X = {}^{\mathrm{t}}[\,X_1\ X_2\ X_3\,]$ and to save on indices let us write $f_1 = X_1a_1 + X_2a_2 + X_3a_3$, and f_2, f_3, f_4 by using the letters b, c, d. We claim to have the following presentation matrix for the generator set (x_1, x_2, x_3) of $\mathfrak{m}_{\underline{0}}$

$$\begin{bmatrix} x_2 & x_3 & 0 & a_1(\underline{x}) & b_1(\underline{x}) & c_1(\underline{x}) & d_1(\underline{x}) \\ -x_1 & 0 & x_3 & a_2(\underline{x}) & b_2(\underline{x}) & c_2(\underline{x}) & d_2(\underline{x}) \\ 0 & -x_1 & -x_2 & a_3(\underline{x}) & b_3(\underline{x}) & c_3(\underline{x}) & d_3(\underline{x}) \end{bmatrix}.$$

We define $A = {}^{\mathrm{t}}[\,a_1\ a_2\ a_3\,]$ in $\mathbf{k}[\underline{X}]^3$ (as well as B, C, D) so that

$$f_1 = \langle A \,|\, X \rangle,\ f_2 = \langle B \,|\, X \rangle\ \dots .$$

Let $v_1(\underline{x})x_1 + v_2(\underline{x})x_2 + v_3(\underline{x})x_3 = 0$ be a syzygy in $\mathbf{A}$. We lift it in $\mathbf{k}[\underline{X}]$

$$v_1X_1 + v_2X_2 + v_3X_3 \equiv 0 \bmod \left\langle \underline{f} \right\rangle,$$

which we write

$$v_1X_1 + v_2X_2 + v_3X_3 = \alpha f_1 + \beta f_2 + \gamma f_3 + \delta f_4, \qquad \alpha,\ \beta,\ \gamma,\ \delta \in \mathbf{k}[\underline{X}].$$

Therefore, with $V = {}^{\mathrm{t}}[\,v_1\ v_2\ v_3\,]$, $V - (\alpha A + \beta B + \gamma C + \delta D)$ is a syzygy for (X_1, X_2, X_3), which implies by Proposition 2.5

$$V - (\alpha A + \beta B + \gamma C + \delta D) \in \operatorname{Im} R_{\underline{X}}.$$

Thus, $V \in \operatorname{Im}[\,R_{\underline{X}} \,|\, U(\underline{X})\,]$, and ${}^{\mathrm{t}}[\,v_1(\underline{x})\ v_2(\underline{x})\ v_3(\underline{x})\,] \in \operatorname{Im}[\,R_{\underline{x}} \,|\, U(\underline{x})\,]$. □

3. The category of finitely presented modules

The category of finitely presented modules over $\mathbf{A}$ can be constructed from the category of free modules of finite rank over $\mathbf{A}$ by a purely categorical procedure.

1. A finitely presented module M is described by a triplet

   $$(\mathrm{K}_M, \mathrm{G}_M, \mathrm{A}_M),$$

   where A_M is a linear map between the free modules of finite ranks K_M and G_M. We have $M \simeq \operatorname{Coker} \mathrm{A}_M$ and $\pi_M : \mathrm{G}_M \to M$ is the surjective linear map with kernel $\operatorname{Im} \mathrm{A}_M$. The matrix of the linear map A_M is a presentation matrix of M.

2. A linear map φ of the module M (described by $(\mathrm{K}_M, \mathrm{G}_M, \mathrm{A}_M)$) to the module N (described by $(\mathrm{K}_N, \mathrm{G}_N, \mathrm{A}_N)$) is described by two linear maps $\mathrm{K}_\varphi : \mathrm{K}_M \to \mathrm{K}_N$ and $\mathrm{G}_\varphi : \mathrm{G}_M \to \mathrm{G}_N$ subject to the commutation

relation $\mathrm{G}_\varphi \circ \mathrm{A}_M = \mathrm{A}_N \circ \mathrm{K}_\varphi$.

$$\begin{tikzcd}
\mathrm{K}_M \arrow[r, "\mathrm{A}_M"] \arrow[d, "\mathrm{K}_\varphi"'] & \mathrm{G}_M \arrow[r, two heads, "\pi_M"] \arrow[d, "\mathrm{G}_\varphi"] & M \arrow[d, "\varphi"] \\
\mathrm{K}_N \arrow[r, "\mathrm{A}_N"'] & \mathrm{G}_N \arrow[r, two heads, "\pi_N"'] & N
\end{tikzcd}$$

3. The sum of two linear maps φ and ψ of M to N represented by $(\mathrm{K}_\varphi, \mathrm{G}_\varphi)$ and $(\mathrm{K}_\psi, \mathrm{G}_\psi)$ is represented by $(\mathrm{K}_\varphi + \mathrm{K}_\psi, \mathrm{G}_\varphi + \mathrm{G}_\psi)$.
   The linear map $a\varphi$ is represented by $(a\mathrm{K}_\varphi, a\mathrm{G}_\varphi)$.
4. To represent the composite of two linear maps, we compose their representations.
5. Finally, the linear map φ of M to N represented by $(\mathrm{K}_\varphi, \mathrm{G}_\varphi)$ is null if and only if there exists a $Z_\varphi : \mathrm{G}_M \to \mathrm{K}_N$ satisfying $\mathrm{A}_N \circ Z_\varphi = \mathrm{G}_\varphi$.

This shows that the problems concerning finitely presented modules can always be interpreted as problems regarding matrices, and are often reduced to problems concerning the solution of systems of linear equations over **A**. For example, given M, N and φ, if we look for a linear map $\sigma : N \to M$ satisfying $\varphi \circ \sigma = \mathrm{Id}_N$, we must find linear maps $\mathrm{K}_\sigma : \mathrm{K}_N \to \mathrm{K}_M$, $\mathrm{G}_\sigma : \mathrm{G}_N \to \mathrm{G}_M$ and $Z : \mathrm{G}_N \to \mathrm{K}_N$ satisfying

$$\mathrm{G}_\sigma \circ \mathrm{A}_N = \mathrm{A}_M \circ \mathrm{K}_\sigma \quad \text{and} \quad \mathrm{A}_N \circ Z = \mathrm{G}_\varphi \circ \mathrm{G}_\sigma - \mathrm{Id}_{\mathrm{G}_N}.$$

This is none other than a system of linear equations having as unknowns the coefficients of the matrices of the linear maps G_σ, K_σ and Z.

Analogously, if we have $\sigma : N \to M$ and if we want to know whether there exists a $\varphi : M \to N$ satisfying $\varphi \circ \sigma = \mathrm{Id}_N$, We will have to solve a system of linear equations whose unknowns are the coefficients of the matrices of the linear maps G_φ, K_φ and Z.

Similarly, if we have $\varphi : M \to N$ and if we want to know whether φ is locally simple, we must determine whether there exists a $\sigma : N \to M$ satisfying $\varphi \circ \sigma \circ \varphi = \varphi$, and we obtain a system of linear equations having as its unknowns the coefficients of the matrices of G_σ, K_σ and Z.

We deduce the corresponding local-global principles.

3.1. Concrete local-global principle. (For certain properties of the linear maps between finitely presented modules)

Let S_1, …, S_n be comaximal monoids of **A** *and $\varphi : M \to N$ be a linear map between finitely presented modules. Then the following properties are equivalent.*

1. *The* **A**-*linear map φ admits a left-inverse (resp. admits a right-inverse, resp. is locally simple).*
2. *For $i \in [\![1..n]\!]$, the $\mathbf{A}_{S_i}$-linear map $\varphi_{S_i} : M_{S_i} \to N_{S_i}$ admits a left-inverse (resp. admits a right-inverse, resp. is locally simple).*

4. Stability properties

4.1. Proposition. *Let N_1 and N_2 be two finitely generated $\mathbf{A}$-submodules of an $\mathbf{A}$-module M. If $N_1 + N_2$ is finitely presented, then $N_1 \cap N_2$ is finitely generated.*

D We can follow almost word for word the proof of item *1* of Theorem II-3.4 (necessary condition). □

4.2. Proposition. *Let N be an $\mathbf{A}$-submodule of M and $P = M/N$.*

1. *If M is finitely presented and N finitely generated, then P is finitely presented.*
2. *If M is finitely generated and P finitely presented, then N is finitely generated.*
3. *If P and N are finitely presented, then M is finitely presented. More precisely, if A and B are presentation matrices for N and P, we have a presentation matrix $D = \begin{array}{|c|c|}\hline A & C \\ \hline 0 & B \\ \hline \end{array}$ for M.*

D *1.* We can suppose that $M = \mathbf{A}^p/F$ with F finitely generated. If N is finitely generated, it is of the form $N = (F' + F)/F$ where F' is finitely generated, so $P \simeq \mathbf{A}^p/(F + F')$.
2. We write $M = \mathbf{A}^p/F$ and $N = (F' + F)/F$. We have $P \simeq \mathbf{A}^p/(F' + F)$, so $F' + F$ (and also N) is finitely generated (Section 1).
3. Let $x_1, \ldots, x_m$ be generators of N and $x_{m+1}, \ldots, x_n$ be elements of M whose classes modulo N generate P. Every syzygy on $(\overline{x_{m+1}}, \ldots, \overline{x_n})$ in P gives a syzygy on $(x_1, \ldots, x_n)$ in M. Similarly, every syzygy on $(x_1, \ldots, x_n)$ in M gives a syzygy on $(\overline{x_{m+1}}, \ldots, \overline{x_n})$ in P.

If A is a presentation matrix of N for $(x_1, \ldots, x_m)$ and if B is a presentation matrix of P for $(\overline{x_{m+1}}, \ldots, \overline{x_n})$, we obtain a presentation matrix D of M for $(x_1, \ldots, x_n)$ in the desired format. □

Note that in the proof of item *2* the submodules F and F' are not necessarily finitely generated.

Coherence and finite presentation

Propositions II-3.1 and II-3.7 (where we take $\mathbf{A}$ as the $\mathbf{A}$-module M) can be reread in the form of the following theorem.

4.3. Theorem. *On a coherent ring every finitely presented module is coherent. On a strongly discrete coherent ring every finitely presented module is strongly discrete and coherent.*

4.4. Proposition. *Let* $\mathbf{A}$ *be a coherent ring and* $\varphi : M \to N$ *be a linear map between finitely presented* $\mathbf{A}$*-modules, then* $\operatorname{Ker}\varphi$, $\operatorname{Im}\varphi$ *and* $\operatorname{Coker}\varphi$ *are finitely presented modules.*

4.5. Proposition. *Let* N *be a finitely generated* $\mathbf{A}$*-submodule of* M*.*

1. *If* M *is coherent,* M/N *is coherent.*
2. *If* M/N *and* N *are coherent,* M *is coherent.*

D *1.* Consider a finitely generated submodule $P = \langle \overline{x_1}, \dots, \overline{x_\ell} \rangle$ of M/N. Then $P \simeq (\langle x_1, \dots, x_\ell \rangle + N)/N$. We conclude by Proposition 4.2 that it is finitely presented.

2. Let Q be a finitely generated submodule of M. The module $(Q + N)/N$ is finitely generated in M/N therefore finitely presented. Since $(Q + N)/N$ and N are finitely presented, so is $Q + N$ (Proposition 4.2). Therefore $Q \cap N$ is finitely generated (Proposition 4.1). Since N is coherent, $Q \cap N$ is finitely presented. Since $Q/(Q \cap N) \simeq (Q + N)/N$ and $Q \cap N$ are finitely presented, Q is finitely presented (Proposition 4.2). □

Tensor product, exterior powers, symmetrical powers

Let M and N be two $\mathbf{A}$-modules. A bilinear map $\varphi : M \times N \to P$ is called a *tensor product* of the $\mathbf{A}$-modules M and N if every bilinear map $\psi : M \times N \to R$ is uniquely expressible in the form $\psi = \theta \circ \varphi$, where θ is an $\mathbf{A}$-linear map from P to R.

$$\begin{tikzcd}
M \times N \arrow[d, "\varphi"'] \arrow[dr, "\psi"] & & \text{bilinear maps} \\
P \arrow[r, dashed, "\theta\,!"'] & R & \text{linear maps.}
\end{tikzcd}$$

It is then clear that $\varphi : M \times N \to P$ is unique in the categorical sense, i.e. that for every other tensor product $\varphi' : M \times N \to P'$ there is a unique linear map $\theta : P \to P'$ which renders the suitable diagram commutative, and that θ is an isomorphism.

If $(\underline{g})$ is a generator set of M and $(\underline{h})$ a generator set of N, a bilinear map $\lambda : M \times N \to P$ is known from its values over the elements of $\underline{g} \times \underline{h}$. Furthermore, the values $\lambda(x, y)$ are linked by certain constraints, which are derived from syzygies between elements of $\underline{g}$ in M and from syzygies between elements of $\underline{h}$ in N.

For example, if we have a syzygy $a_1x_1 + a_2x_2 + a_3x_3 =_M 0$ between elements x_i of $\underline{g}$, with the a_i's in $\mathbf{A}$, this provides for each $y \in \underline{h}$ the following syzygy in P: $a_1\lambda(x_1, y) + a_2\lambda(x_2, y) + a_3\lambda(x_3, y) = 0$.

Actually, “those are the only essential constraints, and that shows that a tensor product can be constructed.”

More precisely, let $x \otimes y$ instead of (x, y) be an arbitrary element of $\underline{g} \times \underline{h}$. Consider then the **A**-module P generated by $x \otimes y$ elements linked by the syzygies described above ($a_1(x_1 \otimes y) + a_2(x_2 \otimes y) + a_3(x_3 \otimes y) =_P 0$ for the given example).

4.6. Proposition. *(With the above notations)*

1. *There exists a unique bilinear map $\varphi : M \times N \to P$ such that for all $(x, y) \in \underline{g} \times \underline{h}$, we have $\varphi(x, y) = x \otimes y$.*
2. *With this bilinear map P is a tensor product of the modules M and N. In particular, if M and N are free with bases $(\underline{g})$ and $(\underline{h})$, the module P is free with basis $(\underline{g} \otimes \underline{h}) := (x \otimes y)_{x\in\underline{g},\, y\in\underline{h}}$.*

D The proof is left to the reader. □

Thus, the tensor product of two **A**-modules exists and can always be defined from presentations of these modules. It is denoted by $M \otimes_{\mathbf{A}} N$.

The fact that follows is more or less a paraphrase of the previous proposition, but it can only be stated once we know that tensor products exist.

4.7. Fact.

1. *If two modules are finitely generated (resp. finitely presented) then so is their tensor product.*
2. *If M is free with basis $(g_i)_{i\in I}$ and N is free with basis $(h_j)_{j\in J}$, then $M \otimes N$ is free with basis $(g_i \otimes h_j)_{(i,j)\in I\times J}$.*
3. *If $M \simeq \operatorname{Coker} \alpha$ and $N \simeq \operatorname{Coker} \beta$, with $\alpha : L_1 \to L_2$ and $\beta : L_3 \to L_4$, the modules L_i being free, then the **A**-linear map*
$$(\alpha \otimes \mathrm{Id}_{L_4}) \oplus (\mathrm{Id}_{L_2} \otimes \beta) : (L_1 \otimes L_4) \oplus (L_2 \otimes L_3) \to L_2 \otimes L_4$$
has as its cokernel a tensor product of M and N.

Comments.

1) The theory of *universal algebra* provides profound reasons why the construction of the tensor product *cannot fail to work.* But this general theory is a little too heavy to be presented in this work, and it is best to soak up these kinds of things by impregnating examples.

2) The reader accustomed to classical mathematics would not have read without apprehension our "presentation" of the tensor product of M and N, which is a module constructed from presentations of M and N. If they have read Bourbaki, they will have noticed that our construction is the same as that of the illustrious multi-headed mathematician, except that Bourbaki limits himself to one "natural and universal" presentation: every module is generated by all its elements linked by all their syzygies. If Bourbaki's "presentation" has the merit of universality, it has the inconvenience of the weight of the hippopotamus.

In fact, in constructive mathematics, we do not have the same underlying "set theory" as in classical mathematics. Once we have *given* a module M by means of a presentation $\alpha : L_1 \to L_2$, we do not rush to forget α as we pretend to do in classical mathematics.[2] On the contrary, from a constructive point of view, the module M is nothing other than "an encoding of the linear map α" (for example in the form of a matrix if the presentation is finite), with the additional information that this is the presentation of a module. Furthermore, a "quotient set" is not seen as a set of equivalence classes, but as "the same preset equipped with a coarser equality relation;" the quotient set of $(E, =_E)$ by the equivalence relation $\sim$ is simply the set $(E, \sim)$. Consequently, our construction of the tensor product, consistent with its implementation on a machine, is entirely "natural and universal" in the framework of constructive set theory (the reader can consult the simple and brilliant Chapter 3 of [Bishop], or one of the other classic works of reference on constructive mathematics [Beeson, Bishop & Bridges, Bridges & Richman, MRR]).

3) To construct the tensor product of nondiscrete modules, we a priori need the notion of a free module over a nondiscrete set. For the constructive definition of this kind of free module, see Exercise VIII-16. We can avoid this kind of free module in the following way. We do not use generator sets of M and N in the construction. The elements of the tensor product $M \otimes_{\mathbf{A}} N$ are given as formal sums $\sum_{i=1}^{n} x_i \otimes y_i$ for finitely enumerated families in M and N. Now the problem is to give a correct definition of the equivalence relation which gives as quotient set the set underlying the module $M \otimes_{\mathbf{A}} N$. The details are left to the reader. ■

By its definition, the tensor product is "functorial," i.e. if we have two $\mathbf{A}$-linear maps $f : M \to M'$ and $g : N \to N'$, then there exists a unique linear map $h : M \otimes_{\mathbf{A}} N \to M' \otimes_{\mathbf{A}} N'$ satisfying the equalities $h(x \otimes y) = f(x) \otimes g(y)$ for $x \in M$ and $y \in N$. This linear map is naturally denoted by $h = f \otimes g$.

We also have the canonical isomorphisms

$$M \otimes_{\mathbf{A}} N \xrightarrow{\sim} N \otimes_{\mathbf{A}} M \quad \text{and} \quad M \otimes_{\mathbf{A}} (N \otimes_{\mathbf{A}} P) \xrightarrow{\sim} (M \otimes_{\mathbf{A}} N) \otimes_{\mathbf{A}} P,$$

which we express by saying that the tensor product is commutative and associative.

The following fact immediately results from the description of the tensor product by generators and relations.

[2] A detailed inspection of the object M constructed according to the set theory of classical mathematics reveals that the latter does not forget it either.

4.8. Fact. *For every exact sequence of* $\mathbf{A}$*-modules* $M \xrightarrow{f} N \xrightarrow{g} P \to 0$ *and for every* $\mathbf{A}$*-module* Q *the sequence*

$$M \otimes_{\mathbf{A}} Q \xrightarrow{f \otimes \mathrm{Id}_Q} N \otimes_{\mathbf{A}} Q \xrightarrow{g \otimes \mathrm{Id}_Q} P \otimes_{\mathbf{A}} Q \to 0$$

is exact.

We express this fact by saying that "the functor $\bullet \otimes Q$ is right exact."

We will not recall in detail the statement of the universal problems that solve the exterior powers (already given page 41), *symmetric powers* and the *exterior algebra* of an $\mathbf{A}$-module.

Here are however the corresponding "small diagrams" for the last two.

$$\begin{tikzcd}
M^k \arrow[d, "\mathbf{s}^k_{\mathbf{A}}"'] \arrow[dr, "\psi"] & \\
\mathbf{S}^k_{\mathbf{A}} M \arrow[r, dashed, "\theta\,!"'] & N
\end{tikzcd}$$

symmetric multilinear maps

linear maps.

$$\begin{tikzcd}
M \arrow[d, "\lambda_{\mathbf{A}}"'] \arrow[dr, "\psi"] & \\
\bigwedge_{\mathbf{A}} M \arrow[r, dashed, "\theta\,!"'] & \mathbf{B}
\end{tikzcd}$$

$\mathbf{A}$-modules

$\psi(x) \times \psi(x) = 0$ for all $x \in M$

associative $\mathbf{A}$-algebras.

As a corollary of Proposition 4.6 we obtain the following proposition.

4.9. Proposition. *If* M *is a finitely presented* $\mathbf{A}$*-module, then the same goes for* $\bigwedge^k_{\mathbf{A}} M$ *and for the symmetric powers* $\mathbf{S}^k_{\mathbf{A}} M$ $(k \in \mathbb{N})$*.*
More precisely, if M *is generated by the system* $(x_1, \ldots, x_n)$ *subjected to syzygies* $r_j \in \mathbf{A}^n$*, we obtain the following results.*

1. *The module* $\bigwedge^k_{\mathbf{A}} M$ *is generated by the* k*-vectors*
$$x_{i_1} \wedge \cdots \wedge x_{i_k} \text{ for } 1 \leqslant i_1 < \cdots < i_k \leqslant n,$$
subjected to the syzygies obtained by making the exterior product of the r_j *syzygies by the* $(k-1)$*-vectors* $x_{i_1} \wedge \cdots \wedge x_{i_{k-1}}$*.*
2. *The module* $\mathbf{S}^k_{\mathbf{A}} M$ *is generated by the* k*-symmetric tensors*
$$\mathbf{s}(x_{i_1}, \ldots, x_{i_k}) \text{ for } 1 \leqslant i_1 \leqslant \cdots \leqslant i_k \leqslant n,$$
subjected to the syzygies obtained by making the product of the r_j *syzygies by the* $(k-1)$*-symmetric tensors* $\mathbf{s}(x_{i_1}, \ldots, x_{i_{k-1}})$*.*

For example, with $n = 4$ and $k = 2$ a syzygy $a_1 x_1 + \cdots + a_4 x_4 = 0$ in M leads to 4 syzygies in $\bigwedge^2_{\mathbf{A}} M$

$$\begin{array}{rcrcrcl}
a_2\,(x_1 \wedge x_2) & + & a_3\,(x_1 \wedge x_3) & + & a_4\,(x_1 \wedge x_4) & = & 0 \\
a_1\,(x_1 \wedge x_2) & - & a_3\,(x_2 \wedge x_3) & - & a_4\,(x_2 \wedge x_4) & = & 0 \\
a_1\,(x_1 \wedge x_3) & + & a_2\,(x_2 \wedge x_3) & - & a_4\,(x_3 \wedge x_4) & = & 0 \\
a_1\,(x_1 \wedge x_4) & + & a_2\,(x_2 \wedge x_4) & + & a_3\,(x_3 \wedge x_4) & = & 0
\end{array}$$

and to 4 syzygies in $\mathbf{S}^2_{\mathbf{A}} M$

$$\begin{array}{l} a_1\,\mathrm{s}(x_1,x_1) \,+\, a_2\,\mathrm{s}(x_1,x_2) \,+\, a_3\,\mathrm{s}(x_1,x_3) \,+\, a_4\,\mathrm{s}(x_1,x_4) \,=\, 0 \\ a_1\,\mathrm{s}(x_1,x_2) \,+\, a_2\,\mathrm{s}(x_2,x_2) \,+\, a_3\,\mathrm{s}(x_2,x_3) \,+\, a_4\,\mathrm{s}(x_2,x_4) \,=\, 0 \\ a_1\,\mathrm{s}(x_1,x_3) \,+\, a_2\,\mathrm{s}(x_2,x_3) \,+\, a_3\,\mathrm{s}(x_3,x_3) \,+\, a_4\,\mathrm{s}(x_3,x_4) \,=\, 0 \\ a_1\,\mathrm{s}(x_1,x_4) \,+\, a_2\,\mathrm{s}(x_2,x_4) \,+\, a_3\,\mathrm{s}(x_3,x_4) \,+\, a_4\,\mathrm{s}(x_4,x_4) \,=\, 0 \end{array}$$

Remark. More generally, for every exact sequence

$$K \xrightarrow{u} G \xrightarrow{p} M \to 0$$

we have an exact sequence

$$K \otimes \bigwedge\nolimits^{k-1} G \xrightarrow{u'} \bigwedge\nolimits^{k} G \xrightarrow{\bigwedge^k p} \bigwedge\nolimits^{k} M \to 0$$

with $u'(z \otimes y) = u(z) \wedge y$ for $z \in K$, $y \in \bigwedge^{k-1} G$.
On the right-hand side, the surjectivity is immediate and it is clear that $(\bigwedge^k p) \circ u' = 0$, which allows us to define $p' : \operatorname{Coker} u' \to \bigwedge^k M$ by passage to the quotient. It remains to prove that p' is an isomorphism. For that, it suffices to construct a linear map $q' : \bigwedge^k M \to \operatorname{Coker} u'$ that is the inverse of p'. We do not have a choice: for $x_1, \ldots, x_k \in M$ with preimages $y_1, \ldots, y_k \in G$ by p

$$q'(x_1 \wedge \cdots \wedge x_k) = y_1 \wedge \cdots \wedge y_k \bmod \operatorname{Im} u'.$$

We leave it up to the reader to verify that q' is indeed defined and suitable. The analogous result is valid for the symmetric powers. ■

Example. Let $\mathbf{B}$ be the ring of polynomials $\mathbf{A}[x,y]$ in the indeterminates x and y over a nontrivial ring $\mathbf{A}$. Consider the ideal $\mathfrak{b} = \langle x, y\rangle$ of $\mathbf{B}$, and look at it as a $\mathbf{B}$-module that we denote by M. Then, M admits the generator set (x, y) for which a presentation matrix is equal to $\begin{bmatrix} y \\ -x \end{bmatrix}$. Deduce that $M \otimes_{\mathbf{B}} M$ admits $(x \otimes x, x \otimes y, y \otimes x, y \otimes y)$ as a generator set, with a presentation matrix equal to

$$\begin{array}{l} x \otimes x \\ x \otimes y \\ y \otimes x \\ y \otimes y \end{array} \qquad \begin{bmatrix} y & 0 & 0 & y \\ -x & 0 & y & 0 \\ 0 & y & 0 & -x \\ 0 & -x & -x & 0 \end{bmatrix}$$

We deduce the following annihilators

$$\operatorname{Ann}_{\mathbf{B}}(x \otimes y - y \otimes x) = \mathfrak{b}, \quad \operatorname{Ann}_{\mathbf{B}}(x \otimes y + y \otimes x) = \operatorname{Ann}_{\mathbf{A}}(2)\,\mathfrak{b},$$
$$\operatorname{Ann}_{\mathbf{B}}(x \otimes x) = \operatorname{Ann}_{\mathbf{B}}(x \otimes y) = \operatorname{Ann}_{\mathbf{B}}(y \otimes x) = \operatorname{Ann}_{\mathbf{B}}(y \otimes y) = 0.$$

The dual $M^\star = \mathrm{L}_{\mathbf{B}}(M, \mathbf{B})$ of M is free of rank 1, generated by the form

$$\alpha : M \longrightarrow \mathbf{B}, \quad z \longmapsto z,$$

which only gives partial information on the structure of M. For example, for every linear form $\beta : M \to \mathbf{B}$ we have $\beta(M) \subseteq \mathfrak{b}$ and therefore M does

not have any free direct summands of rank 1 (cf. Proposition II-5.1).
Similarly, the dual $(M \otimes_{\mathbf{B}} M)^\star$ of $M \otimes_{\mathbf{B}} M$ is free of rank 1, generated by the form

$$\varphi : M \otimes_{\mathbf{B}} M \longrightarrow \mathbf{B}, \quad z \otimes z' \longmapsto zz',$$

and $M \otimes_{\mathbf{B}} M$ does not possess a free direct summand of rank 1.
Concerning $\mathbf{S}^2_{\mathbf{B}} M$, we find that it admits a generator set equal to $\big(\mathbf{s}(x,x), \mathbf{s}(x,y), \mathbf{s}(y,y)\big)$, with the presentation matrix

$$\begin{array}{l c} \mathbf{s}(x,x) & \multirow{3}{*}{} \\ \mathbf{s}(x,y) & \\ \mathbf{s}(y,y) & \end{array} \qquad \begin{bmatrix} y & 0 \\ -x & y \\ 0 & -x \end{bmatrix}.$$

Concerning $\bigwedge^2_{\mathbf{B}} M$, we find that it is generated by $x \wedge y$ with the presentation matrix $[\, x \; y \,]$ which gives

$$\bigwedge\nolimits^2_{\mathbf{B}} M \simeq \mathbf{B}/\mathfrak{b} \simeq \mathbf{A}.$$

But be careful of the fact that $\mathbf{A}$ as a $\mathbf{B}$-module is a quotient and not a submodule of $\mathbf{B}$. ∎

Changing the base ring

Let $\rho : \mathbf{A} \to \mathbf{B}$ be an algebra. Every $\mathbf{B}$-module P can be equipped with an $\mathbf{A}$-module structure via ρ by letting $a.x \overset{\text{def}}{=} \rho(a)x$.

4.10. Definition. Let $\mathbf{A} \xrightarrow{\rho} \mathbf{B}$ be an $\mathbf{A}$-algebra.

1. Let M be an $\mathbf{A}$-module. An $\mathbf{A}$-linear map map $\varphi : M \to P$, where P is a $\mathbf{B}$-module, is called a *morphism of scalar extension* (from $\mathbf{A}$ to $\mathbf{B}$ for M), or a *change of the base ring* (from $\mathbf{A}$ to $\mathbf{B}$ for M), if the following universal property is satisfied.

$$\begin{tikzcd} M \arrow[dd, "\varphi"'] \arrow[ddr, "\psi"] & & \mathbf{A}\text{-modules} \\ & & \mathbf{A}\text{-linear maps} \\ P \arrow[r, dashed, "\theta\,!"'] & R & \mathbf{B}\text{-modules, } \mathbf{B}\text{-linear maps} \end{tikzcd}$$

For every $\mathbf{B}$-module R, every $\mathbf{A}$-linear map $\psi : M \to R$ is uniquely expressible in the form $\psi = \theta \circ \varphi$, where $\theta \in \mathrm{L}_{\mathbf{B}}(P, R)$.

2. A $\mathbf{B}$-module P such that there exist an $\mathbf{A}$-module M and a morphism of scalar extension $\varphi : M \to P$ is said to be *extended from* $\mathbf{A}$. We will also say that P *stems from the* $\mathbf{A}$*-module* M *by scalar extension.*

It is clear that a morphism of scalar extension $\varphi : M \to P$ is unique in the categorical sense, i.e. that for every other morphism of scalar extension $\varphi' : M \to P'$, there is a unique $\theta \in \mathrm{L}_{\mathbf{B}}(P, P')$ which renders the suitable diagram commutative, and that θ is an isomorphism.

If $(\underline{g})$ is a generator set of M and P an arbitrary $\mathbf{B}$-module, an $\mathbf{A}$-linear map $\lambda : M \to P$ is known from its values over the elements x of $\underline{g}$. In addition, the values $\lambda(x)$ are linked by certain constraints, which are derived from syzygies between elements of $\underline{g}$ in M. For example, if we have a syzygy $a_1x_1 + a_2x_2 + a_3x_3 =_M 0$ between elements x_i of $\underline{g}$, with the a_i's in $\mathbf{A}$, this provides the following syzygy between the $\lambda(x_i)$'s in P: $\rho(a_1)\lambda(x_1) + \rho(a_2)\lambda(x_2) + \rho(a_3)\lambda(x_3) = 0$.

Actually "those are the only essential constraints, and that shows that a scalar extension can be constructed."

More precisely, let $\rho_\star(x)$ replace x (an arbitrary element of $\underline{g}$). Consider then the $\mathbf{B}$-module M_1 generated by the $\rho_\star(x)$'s, linked by the syzygies described above ($\rho(a_1)\rho_\star(x_1)+\rho(a_2)\rho_\star(x_2)+\rho(a_3)\rho_\star(x_3) =_P 0$ for the given example).

4.11. Proposition. *(With the above notations)*

1. a. *There exists a unique $\mathbf{A}$-linear map $\varphi : M \to M_1$ such that for all $x \in \underline{g}$, we have $\varphi(x) = \rho_\star(x)$.*

   b. *This $\mathbf{A}$-linear map makes M_1 a scalar extension from $\mathbf{A}$ to $\mathbf{B}$ for M. We will denote it by $M_1 = \rho_\star(M)$.*

   c. *In the case of a finitely presented module, if M is (isomorphic to the) cokernel of a matrix $F = (f_{i,j}) \in \mathbf{A}^{q\times m}$, then M_1 is (isomorphic to the) cokernel of* the same matrix seen in $\mathbf{B}$, *i.e. the matrix $F^\rho = \big(\rho(f_{i,j})\big)$. In particular, if M is free with basis $(\underline{g})$, then M_1 is free with basis $\rho_\star(\underline{g})$.*

2. *Consequently the scalar extension from $\mathbf{A}$ to $\mathbf{B}$ for an arbitrary $\mathbf{A}$-module exists and can always be defined from a presentation of this module. If the module is finitely generated (resp. finitely presented) the scalar extension is as well.*

3. *Knowing that the scalar extensions exist, we can describe the previous construction (in a noncyclic manner) as follows:*
   if $M \simeq \operatorname{Coker}\alpha$ with $\alpha : L_1 \to L_2$, the modules L_i being free, then the module $M_1 = \operatorname{Coker}\big(\rho_\star(\alpha)\big)$ is a scalar extension from $\mathbf{A}$ to $\mathbf{B}$ for the module M.

4. *The scalar extension is transitive. If $\mathbf{A} \xrightarrow{\rho} \mathbf{B} \xrightarrow{\rho'} \mathbf{C}$ are two "successive" algebras and if $\rho'' = \rho' \circ \rho$ define the "composite" algebra , the canonical $\mathbf{C}$-linear map $\rho''_\star(M) \to \rho'_\star\big(\rho_\star(M)\big)$ is an isomorphism.*

5. *The scalar extension and the tensor product commute. If M, N are $\mathbf{A}$-modules and $\rho : \mathbf{A} \to \mathbf{B}$ is a homomorphism of rings, then the natural $\mathbf{B}$-linear map $\rho_\star(M \otimes_\mathbf{A} N) \to \rho_\star(M) \otimes_\mathbf{B} \rho_\star(N)$ is an isomorphism.*

6. *Similarly the scalar extension commutes with the construction of the exterior powers, of the symmetric powers and of the exterior algebra.*

7. *Seen as an* $\mathbf{A}$*-module,* $\rho_\star(M)$ *is (uniquely) isomorphic to the tensor product* $\mathbf{B}\otimes_{\mathbf{A}} M$ *(here* $\mathbf{B}$ *is equipped with its* $\mathbf{A}$*-module structure via* ρ*). In addition, the "external law"* $\mathbf{B}\times\rho_\star(M)\to\rho_\star(M)$*, which defines the* $\mathbf{B}$*-module structure of* $\rho_\star(M)$*, is interpreted via the previous isomorphism like the* $\mathbf{A}$*-linear map*
$$\pi\otimes_{\mathbf{A}}\mathrm{Id}_M : \mathbf{B}\otimes_{\mathbf{A}}\mathbf{B}\otimes_{\mathbf{A}} M \longrightarrow \mathbf{B}\otimes_{\mathbf{A}} M,$$
obtained from the $\mathbf{A}$*-linear map* $\pi : \mathbf{B}\otimes_{\mathbf{A}}\mathbf{B}\to\mathbf{B}$ *"product in* $\mathbf{B}$*"* $(\pi(b\otimes c) = bc)$*.*
8. *For every exact sequence of* $\mathbf{A}$*-modules* $M\xrightarrow{f}N\xrightarrow{g}P\to 0$ *the sequence*
$$\rho_\star(M)\xrightarrow{\rho_\star(f)}\rho_\star(N)\xrightarrow{\rho_\star(g)}\rho_\star(P)\to 0$$
is exact.

D The proof is left to the reader. □

Thus, a $\mathbf{B}$-module P is extended from $\mathbf{A}$ if and only if it is isomorphic to a module $\rho_\star(M)$. Care must be taken, however, to the fact that an extended $\mathbf{B}$-module can be derived from several non-isomorphic $\mathbf{A}$-modules. For example when we extend a $\mathbb{Z}$-module to $\mathbb{Q}$, "we kill the torsion," and $\mathbb{Z}$ and $\mathbb{Z}\oplus\mathbb{Z}/\langle 3\rangle$ both give by scalar extension a $\mathbb{Q}$-vector space of dimension 1.

Remark. With the tensorial notation of item *7* the canonical isomorphism given at item *5* is written as
$$\mathbf{C}\otimes_{\mathbf{A}} M\xrightarrow{\varphi}\mathbf{C}\otimes_{\mathbf{B}}(\mathbf{B}\otimes_{\mathbf{A}} M)\simeq(\mathbf{C}\otimes_{\mathbf{B}}\mathbf{B})\otimes_{\mathbf{A}} M,$$
with $\varphi(c\otimes x) = c\otimes(1_{\mathbf{B}}\otimes x)$. We will come back to this type of "associativity" in the remark that follows Corollary VIII-1.15. ■

Modules of linear maps

4.12. Proposition. *If* M *and* N *are finitely presented modules over a coherent ring* $\mathbf{A}$*, then* $\mathrm{L}_{\mathbf{A}}(M,N)$ *is finitely presented.*

D We use the notations of Section 3.
Giving an element φ of $\mathrm{L}_{\mathbf{A}}(M,N)$ reduces to giving the matrices of G_φ and K_φ that satisfy the condition $\mathrm{G}_\varphi\,\mathrm{A}_M = \mathrm{A}_N\,\mathrm{K}_\varphi$.
Since the ring is coherent, the solutions of the system of linear equations form a finitely generated $\mathbf{A}$-module, generated for example by the solutions corresponding to linear maps φ_1, …, φ_ℓ given by pairs of matrices $(\mathrm{G}_{\varphi_1},\mathrm{K}_{\varphi_1})$, …, $(\mathrm{G}_{\varphi_\ell},\mathrm{K}_{\varphi_\ell})$. Therefore $\mathrm{L}_{\mathbf{A}}(M,N) = \langle\varphi_1,\dots,\varphi_\ell\rangle$.
Furthermore, a syzygy $\sum_i a_i\varphi_i = 0$ is satisfied if and only if we have a linear map $Z_\varphi : \mathrm{G}_M\to\mathrm{K}_N$ satisfying $\mathrm{A}_N\,Z_\varphi = \sum_i a_i\mathrm{G}_{\varphi_i}$. By taking the corresponding system of linear equations, whose unknowns are the a_i's on the one hand and the coefficients of the matrix of Z_φ on the other, we note that the syzygy module for the generator set $(\varphi_1,\dots,\varphi_\ell)$ is indeed finitely generated. □

The local character of the finitely presented modules

The fact that an **A**-module is finitely presented is a local notion, in the following sense.

4.13. Concrete local-global principle. (Finitely presented modules) *Let S_1, …, S_n be comaximal monoids of a ring* **A**, *and M an* **A**-*module. Then, M is finitely presented if and only if each of the M_{S_i}'s is a finitely presented $\mathbf{A}_{S_i}$-module.*

D Assume that M_{S_i} is a finitely presented $\mathbf{A}_{S_i}$-module for each i. Let us show that M is finitely presented.
By the local-global principle II-3.6, M is finitely generated. Let $(g_1, \ldots, g_q)$ be a generator set of M.
Let $(a_{i,h,1}, \ldots, a_{i,h,q}) \in \mathbf{A}^q_{S_i}$ be syzygies between the $g_j/1 \in M_{S_i}$ (in other words, $\sum_j a_{i,h,j} g_j = 0$ in M_{S_i}) for $h = 1, \ldots, k_i$, which generate the $\mathbf{A}_{S_i}$-syzygy module between the $g_j/1$.
Suppose without loss of generality that the $a_{i,h,j}$'s are of the form $a'_{i,h,j}/1$, with $a'_{i,h,j} \in \mathbf{A}$. Then there exists some suitable $s_i \in S_i$ such that the vectors

$$s_i\,(a'_{i,h,1}, \ldots, a'_{i,h,q}) = (b_{i,h,1}, \ldots, b_{i,h,q})$$

are **A**-syzygies between the $g_j \in M$.
Let us show that the syzygies thus constructed between the g_j's generate all the syzygies. With this in mind, consider an arbitrary syzygy $(c_1, \ldots, c_q)$ between the g_j's. Let us view it as a syzygy between the $g_j/1 \in M_{S_i}$, and let us write it as an $\mathbf{A}_{S_i}$-linear combination of the vectors $(b_{i,h,1}, \ldots, b_{i,h,q})$ in $\mathbf{A}^q_{S_i}$. After multiplication by some suitable $s'_i \in S_i$ we obtain an equality in $\mathbf{A}^q$

$$s'_i(c_1, \ldots, c_q) = e_{i,1}(b_{i,1,1}, \ldots, b_{i,1,q}) + \cdots + e_{i,k_i}(b_{i,k_i,1}, \ldots, b_{i,k_i,q}).$$

We write $\sum_{i=1}^n u_i s'_i = 1$. We see that $(c_1, \ldots, c_q)$ is an **A**-linear combination of the $(b_{i,h,1}, \ldots, b_{i,h,q})$. □

Null tensors

Let M and N be two arbitrary **A**-modules, and $t = \sum_{i \in [\![1..n]\!]} x_i \otimes y_i \in M \otimes N$. The equality $\sum_i x_i \otimes y_i = 0$ does not a priori solely depend on knowing the submodules $\sum_i \mathbf{A}x_i \subseteq M$ and $\sum_i \mathbf{A}y_i \subseteq N$.
Consequently the notation $\sum_i x_i \otimes y_i$ is generally burdened with ambiguity, and is dangerous. We should use the following more precise notation: $\sum_i x_i \otimes_{\mathbf{A},M,N} y_i$, or at least write the equalities in the form

$$\textstyle\sum_i x_i \otimes y_i =_{M \otimes_{\mathbf{A}} N} \cdots$$

This precaution is not needed in the case where the two modules M and N are flat (see Chapter VIII), for instance when the ring **A** is a discrete field.

4.14. Null tensor lemma. *Let $M = \mathbf{A}x_1 + \cdots + \mathbf{A}x_n$ be a finitely generated module, N be another module and $t = \sum_{i\in[\![1..n]\!]} x_i \otimes y_i \in M \otimes_{\mathbf{A}} N$. With $X = [\,x_1 \cdots x_n\,] \in M^{1\times n}$ and $Y = {}^{\mathrm{t}}[\,y_1 \cdots y_n\,] \in N^{n\times 1}$, we use the notation $t = X \odot Y$. The following properties are equivalent.*

1. *$t =_{M\otimes_{\mathbf{A}} N} 0$.*
2. *We have a $Z \in N^{m\times 1}$ and a matrix $G \in \mathbf{A}^{n\times m}$ which satisfy*

$$XG =_{M^m} 0 \quad \text{and} \quad GZ =_{N^n} Y\,. \tag{1}$$

D *2 ⇒ 1.* Generally the equality $X \odot GZ = XG \odot Z$ is guaranteed for every matrix G with coefficients in $\mathbf{A}$ because $x \otimes \alpha z = \alpha x \otimes z$ when $x \in M$, $z \in N$ and $\alpha \in \mathbf{A}$.

1 ⇒ 2. The equality $t =_{M\otimes N} 0$ comes from a finite number of syzygies within the modules M and N. Therefore there exists a submodule N' such that

$$\mathbf{A}y_1 + \cdots + \mathbf{A}y_n \subseteq N' = \mathbf{A}z_1 + \cdots + \mathbf{A}z_m \subseteq N,$$

and $X \odot Y =_{M\otimes N'} 0$. We write $Z = {}^{\mathrm{t}}[\,z_1 \cdots z_m\,]$. We then have an exact sequence

$$K \xrightarrow{a} L \xrightarrow{\pi} N' \to 0$$

where L is free, with basis $(\ell_1, \ldots, \ell_m)$ and $\pi(\ell_j) = z_j$, which gives an exact sequence

$$M \otimes K \xrightarrow{\mathrm{I}\otimes a} M \otimes L \xrightarrow{\mathrm{I}\otimes\pi} M \otimes N' \to 0.$$

If $U \in M^{1\times m}$ satisfies $U \odot Z =_{M\otimes N'} 0$, this means that U seen as an element of $M \otimes L \simeq M^n$ (i.e. seen as $\sum_j u_j \otimes_{M\otimes L} \ell_j$) is in the submodule $\mathrm{Ker}(\mathrm{I}\otimes\pi) = \mathrm{Im}(\mathrm{I}\otimes a)$, in other words

$$\textstyle\sum_j u_j \otimes_{M\otimes L} \ell_j = \sum_i x_i \otimes \sum_{ij} a_{ij}\ell_j = \sum_j \big(\sum_i a_{ij}x_i\big) \otimes \ell_j$$

for $a_{ij} \in \mathbf{A}$ that satisfy $\sum_j a_{ij}z_j = 0$. In other words $U = XA$ for a matrix A satisfying $AZ = 0$.

If we write $Y = HZ$ with $H \in \mathbf{A}^{n\times m}$, we have $XH \odot Z = 0$, which gives an equality $XH = XA$ with a matrix A satisfying $AZ = 0$.

We then let $G = H - A$ and we have $XG = 0$ and $GZ = HZ = Y$. □

5. Classification problems for finitely presented modules

The first classification theorem concerns free $\mathbf{A}$-modules of finite rank: two $\mathbf{A}$-modules $M \simeq \mathbf{A}^m$ and $P \simeq \mathbf{A}^p$ with $m \neq p$ can only be isomorphic if $1 =_{\mathbf{A}} 0$ (Proposition II-5.2).

Remark. Note that we use the expression "M is a free module of rank k" to mean that M is isomorphic to $\mathbf{A}^k$, even in the case where we ignore whether the ring $\mathbf{A}$ is trivial or not. This therefore does not always imply that a priori this integer k is well-determined. ■

Rare are the rings for which we can give a "satisfactory" complete classification of the finitely presented modules. The case of discrete fields is well-known: every finitely presented module is free (this results from the Chinese pivot or from the freeness lemma). In this work we treat a few generalizations of this elementary case: the valuation rings, the PIDs and the reduced zero-dimensional rings (Sections 7 and 8), and certain Prüfer rings (Proposition XII-6.5 and Theorem XII-6.7).

Concerning the classification of the finitely generated modules, we note the following two important uniqueness results.

Two results concerning finitely generated modules

5.1. Theorem. *Let $\mathfrak{a}_1 \subseteq \cdots \subseteq \mathfrak{a}_n$ and $\mathfrak{b}_1 \subseteq \cdots \subseteq \mathfrak{b}_m$ be ideals of $\mathbf{A}$ with $n \leqslant m$. If an $\mathbf{A}$-module M is isomorphic to $\mathbf{A}/\mathfrak{a}_1 \oplus \cdots \oplus \mathbf{A}/\mathfrak{a}_n$ and to $\mathbf{A}/\mathfrak{b}_1 \oplus \cdots \oplus \mathbf{A}/\mathfrak{b}_m$, then*

1. *we have $\mathfrak{b}_k = \mathbf{A}$ for $n < k \leqslant m$,*
2. *and $\mathfrak{b}_k = \mathfrak{a}_k$ for $1 \leqslant k \leqslant n$.*

We say that $(\mathfrak{a}_1, \ldots, \mathfrak{a}_n)$ is the list of invariant factors[3] *of the module M.*

D *1.* It suffices to show that if $n < m$, then $\mathfrak{b}_m = \mathbf{A}$, in other words that the ring $\mathbf{B} := \mathbf{A}/\mathfrak{b}_m$ is null. By letting $M = \mathbf{A}/\mathfrak{a}_1 \oplus \cdots \oplus \mathbf{A}/\mathfrak{a}_n$, we have

$$\mathbf{B}^m = \bigoplus\nolimits_{j=1}^m \mathbf{A}/(\mathfrak{b}_j + \mathfrak{b}_m) \simeq M/\mathfrak{b}_m M \simeq \bigoplus\nolimits_{i=1}^n \mathbf{A}/(\mathfrak{a}_i + \mathfrak{b}_m).$$

But each $\mathbf{A}/(\mathfrak{a}_i + \mathfrak{b}_m)$ is a quotient ring of $\mathbf{B}$, so there exists a surjective linear map from $\mathbf{B}^n$ onto $\mathbf{B}^m$ and therefore $\mathbf{B}$ is null (Proposition II-5.2). We assume henceforth without loss of generality that $m = n$.

2. It suffices to show that $\mathfrak{b}_k \subseteq \mathfrak{a}_k$ for $k \in [\![1..n]\!]$. Notice that for an ideal $\mathfrak{a}$ and an element x of $\mathbf{A}$, the kernel of the linear map $y \mapsto yx \bmod \mathfrak{a}$, from $\mathbf{A}$ to $x(\mathbf{A}/\mathfrak{a})$ is the ideal $(\mathfrak{a} : x)$, and thus that $x(\mathbf{A}/\mathfrak{a}) \simeq \mathbf{A}/(\mathfrak{a} : x)$. Now let $x \in \mathfrak{b}_k$. For $j \in [\![k..n]\!]$, we have $(\mathfrak{b}_j : x) = \mathbf{A}$, and therefore

$$xM \simeq \bigoplus\nolimits_{j=1}^n \mathbf{A}/(\mathfrak{b}_j : x) = \bigoplus\nolimits_{j=1}^{k-1} \mathbf{A}/(\mathfrak{b}_j : x), \text{ and } xM \simeq \bigoplus\nolimits_{i=1}^n \mathbf{A}/(\mathfrak{a}_i : x).$$

By applying item *1* to the module xM with the integers $k-1$ and n, we obtain $(\mathfrak{a}_k : x) = \mathbf{A}$, i.e. $x \in \mathfrak{a}_k$. □

Note that in the previous theorem, we have not assumed anything regarding the ideals (it is not necessary that they be finitely generated nor detachable for the result to be constructively valid).

[3] Note that the list given here can be shortened or extended with terms $\mathfrak{a}_j = \langle 1 \rangle$ when we do not have a test for the equality in question. This is comparable to the list of coefficients of a polynomial that can be shortened or extended with 0's when the ring is not discrete.

5.2. Theorem. *Let M be a finitely generated $\mathbf{A}$-module and $\varphi : M \to M$ be a surjective linear map. Then, φ is an isomorphism and its inverse is a polynomial in φ. If a quotient module M/N of M is isomorphic to M, then $N = 0$.*

5.3. Corollary. *If M is a finitely generated module, every element φ right-invertible in $\mathrm{End}_{\mathbf{A}}(M)$ is invertible, and its inverse is a polynomial in φ.*

Proof of Theorem 5.2.
Let $(x_1, \ldots, x_n)$ be a generator set of M, $\mathbf{B} = \mathbf{A}[\varphi] \subseteq \mathrm{End}_{\mathbf{A}}(M)$, and $\mathfrak{a} = \langle \varphi \rangle$ be the ideal of $\mathbf{B}$ generated by φ. The ring $\mathbf{B}$ is commutative and we consider M as a $\mathbf{B}$-module. Since the linear map φ is surjective, there exists a $P \in \mathbb{M}_n(\mathfrak{a})$ with $P\ {}^{\mathrm{t}}[\,x_1 \ \cdots\ x_n\,] = {}^{\mathrm{t}}[\,x_1 \ \cdots\ x_n\,]$, i.e.

$$(\mathrm{I}_n - P)\ {}^{\mathrm{t}}[\,x_1 \ \cdots\ x_n\,] = {}^{\mathrm{t}}[\,0 \ \cdots\ 0\,]$$

(where $\mathrm{I}_n = (\mathrm{I}_n)_{\mathbf{B}}$ is the identity matrix of $\mathbb{M}_n(\mathbf{B})$), and so

$$\det(\mathrm{I}_n - P)\ {}^{\mathrm{t}}[\,x_1 \ \cdots\ x_n\,] = (\widetilde{\mathrm{I}_n - P})\,(\mathrm{I}_n - P)\ {}^{\mathrm{t}}[\,x_1 \ \cdots\ x_n\,] = {}^{\mathrm{t}}[\,0 \ \cdots\ 0\,].$$

Therefore $\det(\mathrm{I}_n - P) = 0_{\mathbf{B}}$, but $\det(\mathrm{I}_n - P) = 1_{\mathbf{B}} - \varphi\psi$ with $\psi \in \mathbf{B}$ (since P has coefficients in $\mathfrak{a} = \varphi\mathbf{B}$). Thus, $\varphi\psi = \psi\varphi = 1_{\mathbf{B}} = \mathrm{Id}_M$: φ is invertible in $\mathbf{B}$. □

6. Quasi-integral rings

In the following definition, we infinitesimally modify the notion of an integral ring usually given in constructive mathematics, not for pleasure, but because our definition better corresponds to algorithms implementing integral rings.

6.1. Definition. A ring is said to be *integral* if every element is null or regular.[4] A ring $\mathbf{A}$ is said to be *quasi-integral* when every element admits as its annihilator an (ideal generated by an) idempotent. In the literature, a quasi-integral ring is sometimes called a *pp-ring* (principal ideals are projective, cf. Section V-7).

As usual, the "or" in the previous definition must be read as an explicit or. An integral ring is therefore a discrete set if and only if furthermore it is trivial or nontrivial. So, our nontrivial integral rings are precisely the "discrete domains" of [MRR].

In this work, sometimes we speak of a "nonzero element" in an integral ring, but we should actually say "regular element" in order not to exclude the trivial ring case.

[4] An integral ring is also called a *domain* in the classical literature. But we prefer to keep "integral ring" in order to distinguish them from rings "witout zerodivisors". See the definition on page 458.

6.2. Fact. *A pp-ring is reduced.*

▷ If e is the idempotent annihilator of x and if $x^2 = 0$, then $x \in \langle e \rangle$, therefore $x = ex = 0$. □

A discrete field is an integral ring. A ring $\mathbf{A}$ is integral if and only if its total ring of fractions $\operatorname{Frac} \mathbf{A}$ is a discrete field. A finite product of pp-rings is a pp-ring. A ring is integral if and only if it is a connected pp-ring.

Equational definition of pp-rings

In a pp-ring, for $a \in \mathbf{A}$, let e_a be the unique idempotent such that $\operatorname{Ann}(a) = \langle 1 - e_a \rangle$. We have $\mathbf{A} \simeq \mathbf{A}[1/e_a] \times \mathbf{A}/\langle e_a \rangle$.

In the ring $\mathbf{A}[1/e_a]$, the element a is regular, and in $\mathbf{A}/\langle e_a \rangle$, a is null.

We then have $e_{ab} = e_a e_b$, $e_a a = a$ and $e_0 = 0$.

Conversely, suppose that a commutative ring is equipped with a unary law $a \mapsto a^\circ$ which satisfies the following three axioms

$$a^\circ\, a = a, \quad (ab)^\circ = a^\circ\, b^\circ, \quad 0^\circ = 0. \tag{2}$$

Then, for all $a \in \mathbf{A}$, we have $\operatorname{Ann}(a) = \langle 1 - a^\circ \rangle$, and a° is idempotent, such that the ring is a pp-ring.

Indeed, first of all $(1 - a^\circ)a = 0$, and if $ax = 0$, then

$$a^\circ\, x = a^\circ\, x^\circ\, x = (ax)^\circ\, x = 0^\circ\, x = 0,$$

so $x = (1 - a^\circ)x$. Hence $\operatorname{Ann}(a) = \langle 1 - a^\circ \rangle$. Next let us show that a° is idempotent. Apply the previous result to $x = 1 - a^\circ$ which satisfies $ax = 0$ (by the first axiom); the equality $x = (1 - a^\circ)x$ gives $x = x^2$, i.e. the element $1 - a^\circ$ is idempotent.

The following splitting lemma is almost immediate.

6.3. Quasi integral splitting lemma. *Let $x_1, \ldots, x_n$ be n elements in a pp-ring $\mathbf{A}$. There exists a fundamental system of orthogonal idempotents (e_j) of cardinality 2^n such that in each of the components $\mathbf{A}[1/e_j]$, each x_i is null or regular.*

▷ Let r_i be the idempotent such that $\langle r_i \rangle = \operatorname{Ann}(x_i)$, and $s_i = 1 - r_i$. By expanding the product $1 = \prod_{i=1}^n (r_i + s_i)$ we obtain the fundamental system of orthogonal idempotents indexed by $\mathcal{P}_n$: $e_J = \prod_{j \in J} r_j \prod_{k \notin J} s_k$. We can delete certain elements of this system when we say that they are null. □

From integral rings to pp-rings

Knowing how to systematically split a pp-ring into two components leads to the following general method. The essential difference with the previous splitting lemma is that we a priori do not know the finite family of elements which will provoke the splitting.

Elementary local-global machinery no. 1. *Most algorithms that work with nontrivial integral rings can be modified in order to work with pp-rings, by splitting the ring into two components each time that the algorithm written for the integral rings uses the "is this element null or regular?" test. In the first component the element in question is null, in the second it is regular.*

A first example of an application of this local-global machinery will be given on page 207. However, Corollary 6.5 below could already be obtained from the integral case, where it is obvious, by applying this local-global machinery.

Let us explain why we speak of elementary local-global machinery here. Generally a local-global principle says that a property P is true if and only if it is true "after localization at comaximal monoids." In the current case, the comaximal monoids are generated by elements $1 - r_i$ where the r_i's form a fundamental system of orthogonal idempotents. Consequently the ring is simply isomorphic to the product of the localized rings, and the situation is therefore perfectly simple, elementary.

Remark. The reader will have noticed the very informal formulation that we have given for this local-global machinery: "Most algorithms … " This is because it seemed quite difficult to give very precise requirements in advance for the indicated method to work. We could imagine an algorithm which works for every integral ring, but in a completely non-uniform manner, which would make the corresponding tree that we construct in the pp-ring case not finite. For example, in the integral case, a given starting configuration would require three tests (to end the computation) if the answers are $0, 0, 0$, but four tests if the answers are $0, 0, 1, 0$, then five tests if the answers are $0, 0, 1, 1, 0$, then six tests if they are $0, 0, 1, 1, 1, 1$, then seven tests if they are $0, 0, 1, 1, 1, 0, 1$, etc. Naturally, we can doubt that such an algorithm could exist without the existence of an integral ring that would fault it at the same time. In other words, an algorithm that is not sufficiently uniform is likely not an algorithm. But we do not assume anything.

Even if we have not so far encountered any example of the above type where the elementary local-global machinery would not apply, we cannot a priori exclude such a possibility. ■

Annihilators of the finitely generated ideals in pp-rings

The following lemma can be considered as an economical variant of the splitting lemma 6.3.

6.4. Lemma. *Let $x_1, \ldots, x_n$ be elements of an $\mathbf{A}$-module.*
If we have $\mathrm{Ann}(x_i) = \langle r_i \rangle$ where r_i is an idempotent ($i \in [\![1..n]\!]$), let

$$s_i = 1 - r_i,\ t_1 = s_1,\ t_2 = r_1 s_2,\ t_3 = r_1 r_2 s_3,\ \ldots,\ t_{n+1} = r_1 r_2 \cdots r_n.$$

Then $(t_1, \ldots, t_{n+1})$ is a fundamental system of orthogonal idempotents and the element $x = x_1 + t_2 x_2 + \cdots + t_n x_n$ satisfies

$$\mathrm{Ann}(x_1, \ldots, x_n) = \mathrm{Ann}(x) = \langle t_{n+1} \rangle\,.$$

NB: in the component $t_k = 1$ ($k \in [\![1..n]\!]$), we have x_k regular and $x_j = 0$ for $j < k$, and in the component $t_{n+1} = 1$, we have $x_1 = \cdots = x_n = 0$.

6.5. Corollary. *Over a pp-ring $\mathbf{A}$ every finitely generated submodule M of a free module has as its annihilator an ideal $\langle r \rangle$ with r idempotent, and M contains an element x having the same annihilator. This applies in particular to a finitely generated ideal of $\mathbf{A}$.*

*Proof of Lemma 6.4.*We have $t_1 x_1 = x_1$ and

$$\begin{aligned} 1 &= s_1 + r_1 = s_1 + r_1(s_2 + r_2) \ = \ s_1 + r_1 s_2 + r_1 r_2 (s_3 + r_3) \ = \ \cdots \\ &= s_1 + r_1 s_2 + r_1 r_2 s_3 + \cdots + r_1 r_2 \cdots r_{n-1} s_n + r_1 r_2 \cdots r_n \end{aligned}$$

so $t_1, \ldots, t_{n+1}$ is a fundamental system of orthogonal idempotents and $x = t_1 x_1 + t_2 x_2 + \cdots + t_n x_n$. It is clear that

$$\langle t_{n+1} \rangle \subseteq \mathrm{Ann}(x_1, \ldots, x_n) \subseteq \mathrm{Ann}(x).$$

Conversely, let $z \in \mathrm{Ann}(x)$. Then $zx = 0$, so $z t_i x_i = z t_i x = 0$ for $i \in [\![1..n]\!]$. Thus, $z t_i \in \mathrm{Ann}(x_i) = \langle r_i \rangle$ and $z t_i = z t_i r_i = 0$. Finally, since $z = \sum_{i=1}^{n+1} z t_i$, we have $z = z t_{n+1} \in \langle t_{n+1} \rangle$. □

Concrete local-global principle for the pp-rings

The property of being a pp-ring is local in the following sense.

6.6. Concrete local-global principle. (pp-rings)
Let $S_1, \ldots, S_n$ be comaximal monoids of $\mathbf{A}$. The following properties are equivalent.

1. *The ring $\mathbf{A}$ is a pp-ring.*
2. *For $i = 1, \ldots, n$, each ring $\mathbf{A}_{S_i}$ is a pp-ring.*

D Let $a \in \mathbf{A}$. For every monoid S of $\mathbf{A}$ we have $\mathrm{Ann}_{\mathbf{A}_S}(a) = \big(\mathrm{Ann}_{\mathbf{A}}(a)\big)_S$. Therefore the annihilator $\mathfrak{a}$ of a is finitely generated if and only if it is finitely generated after localization at the S_i's (local-global principle II-3.6). Next the inclusion $\mathfrak{a} \subseteq \mathfrak{a}^2$ is a matter of the basic concrete local-global principle II-2.3. □

7. Bézout rings

A ring $\mathbf{A}$ is called a *Bézout ring* when every finitely generated ideal is principal. This is the same as saying that every ideal with two generators is principal.

$$\forall a,\, b\ \ \exists u,\, v,\, g,\, a_1,\, b_1\ \ (au + bv = g,\, a = ga_1,\, b = gb_1)\,. \tag{3}$$

A Bézout ring is strongly discrete if and only if the divisibility relation is explicit. An integral Bézout ring is called a *Bézout domain.*

A *local ring* is a ring $\mathbf{A}$ where is satisfied the following axiom

$$\forall x,\, y \in \mathbf{A} \qquad x + y \in \mathbf{A}^\times \implies (x \in \mathbf{A}^\times \text{ or } y \in \mathbf{A}^\times)\,. \tag{4}$$

This is the same as asking

$$\forall x \in \mathbf{A} \qquad x \in \mathbf{A}^\times \ \text{ or } \ 1 - x \in \mathbf{A}^\times\,.$$

Note that according to this definition the trivial ring is local. Moreover, the "or" must be understood in the constructive sense: the alternative must be explicit. Most of the local rings with which we usually work in classical mathematics actually satisfy the previous definition if we look at it from a constructive point of view.

Every quotient ring of a local ring is local. A discrete field is a local ring.

7.1. Lemma. (Bézout always trivial for a local ring)
A ring is a local Bézout ring if and only if it satisfies the following property: $\forall a, b \in \mathbf{A}$, a divides b or b divides a.

D *The condition is sufficient.* First it is clear that the ring is Bézout. Now assume $x+y$ to be invertible. If x divides y, it divides $x+y$ which divides 1, so x is invertible. Symmetrically, if y divides x, it is invertible. So the ring is local.

The condition is necessary. Assume $\mathbf{A}$ is Bézout and local. We have $g(1 - ua_1 - vb_1) = 0$. Since $1 = ua_1 + vb_1 + (1 - ua_1 - vb_1)$, one of the three terms in the sum is invertible. If $1 - ua_1 - vb_1$ is invertible, then $g = a = b = 0$. If ua_1 is invertible, then so is a_1, and a divides g which divides b. If vb_1 is invertible, then so is b_1, and b divides g which divides a.□

Local Bézout rings are therefore "valuation rings" in the Kaplansky sense. We prefer the now usual definition: a *valuation ring* is a reduced local Bézout ring.

Finitely presented modules over valuation rings

A matrix $B = (b_{i,j}) \in \mathbf{A}^{m \times n}$ is said to be *in Smith form* if every coefficient out of the principal diagonal is null, and if for $1 \leqslant i < \inf(m,n)$, the diagonal coefficient $b_{i,i}$ divides the following $b_{i+1,i+1}$.

7.2. Proposition. *Let $\mathbf{A}$ be a local Bézout ring.*

1. *Every matrix of $\mathbf{A}^{m\times n}$ is elementarily equivalent to a matrix in Smith form.*
2. *Every finitely presented $\mathbf{A}$-module M is isomorphic to a direct sum of modules $\mathbf{A}/\langle a_i\rangle$: $M \simeq \bigoplus_{i=1}^{p} \mathbf{A}/\langle a_i\rangle$, with in addition, for each $i < p$, a_{i+1} divides a_i.*

D *1.* We use the Gauss pivot method by choosing for first pivot a coefficient of the matrix which divides all the others. We finish by induction.
2. Direct consequence of item *1.* □

Remark. This result is completed by the uniqueness theorem (Theorem 5.1) as follows.

1. In the reduced matrix in Smith form the ideals $\langle b_{i,i}\rangle$ are uniquely determined.
2. In the decomposition $\bigoplus_{i=1}^{p} \mathbf{A}/\langle a_i\rangle$, the ideals $\langle a_i\rangle$ are uniquely determined, except that ideals in excessive numbers can be equal to $\langle 1\rangle$: we can delete the corresponding terms, but this only happens without fail when we have an invertibility test in the ring. ■

A ring $\mathbf{A}$ is called a *strict Bézout ring* when every vector $[\,u\;v\,] \in \mathbf{A}^2$ can be transformed into a vector $[\,h\;0\,]$ by multiplication by a 2×2 invertible matrix.

Now we give an example of how the elementary local-global machinery no. 1 (described on page 204) is used.

Example. We will show that *every Bézout pp-ring is a strict Bézout ring.* Let us start with the integral case. Let u, $v \in \mathbf{A}$,

$$\exists\, h, a, b, u_1, v_1 \quad (h = au + bv,\ u = hu_1,\ v = hv_1).$$

If $\mathrm{Ann}(v) = 1$, then $v = 0$ and $[\,u\;0\,] = [\,u\;v\,]\,\mathrm{I}_2$.
If $\mathrm{Ann}(v) = 0$, then $\mathrm{Ann}(h) = 0$, $h(au_1 + bv_1) = h$, then $au_1 + bv_1 = 1$. Finally, $[\,h\;0\,] = [\,u\;v\,]\begin{bmatrix} a & -v_1 \\ b & u_1 \end{bmatrix}$ and the matrix has determinant 1.

Let us now apply the elementary local-global machinery no. 1 explained on page 204. Consider the idempotent e such that

$$\mathrm{Ann}(v) = \langle e\rangle \text{ and } f = 1 - e.$$

In $\mathbf{A}[1/e]$, we have $[\,u\;0\,] = [\,u\;v\,]\,\mathrm{I}_2$.
In $\mathbf{A}[1/f]$, we have $[\,h\;0\,] = [\,u\;v\,]\begin{bmatrix} a & -v_1 \\ b & u_1 \end{bmatrix}$.

Therefore in $\mathbf{A}$, we have $[\,ue + hf\;\;0\,] = [\,u\;v\,]\begin{bmatrix} fa + e & -fv_1 \\ fb & fu_1 + e \end{bmatrix}$, and the matrix has determinant 1. ■

Finitely presented modules over PIDs

Assume that $\mathbf{A}$ is a strict Bézout ring. If a and b are two elements on the same row (resp. column) in a matrix M with coefficients in $\mathbf{A}$, we can postmultiply (resp. premultiply) M by an invertible matrix, which will modify the columns (resp. the rows) where the coefficients a and b are, which are replaced by c and 0. When describing this transformation of matrices, we will speak of *Bézout manipulations*. The elementary manipulations can be seen as special cases of Bézout manipulations.

An integral ring is said to be a *principal ideal domain (PID)* when it is Bézout and when every ascending sequence of principal ideals admits two equal consecutive terms (cf. [MRR]). In other words a PID is a Noetherian Bézout domain (see definition II-3.2). Examples include $\mathbb{Z}$ and the polynomial ring $\mathbf{K}[X]$ when $\mathbf{K}$ is a discrete field.

7.3. Proposition. *Let $\mathbf{A}$ be a PID.*

1. *Every matrix $A \in \mathbf{A}^{m\times n}$ is equivalent to a matrix in Smith form. By letting b_i be the diagonal coefficients of the reduced matrix, the principal ideals $\langle b_1\rangle \supseteq \cdots \supseteq \langle b_q\rangle$ ($q = \inf(m, n)$) are invariants of the matrix A up to equivalence. A basis $(e_1, \ldots, e_m)$ of $\mathbf{A}^m$ such that $\mathrm{Im}(A) = \sum_{i=1}^{m} \langle b_i\rangle\, e_i$ is called a* basis adapted to the submodule $\mathrm{Im}(A)$.
2. *For every finitely presented $\mathbf{A}$-module M, there exist r, $p \in \mathbb{N}$ and regular elements a_1, …, a_p, with a_i dividing a_{i+1} for $i < p$, such that M is isomorphic to the direct sum $\left(\bigoplus_{i=1}^{p} \mathbf{A}/\langle a_i\rangle\right) \oplus \mathbf{A}^r$.*

If furthermore $\mathbf{A}$ is nontrivial and strongly discrete, we can ask in item 2 that no $\langle a_i\rangle$ be equal to $\langle 1\rangle$. In this case, we call invariant factors of the module M *the elements of the list* $\big(a_1, \ldots, a_p, \underbrace{0, \ldots, 0}_{r\ times}\big)$*, and the list of invariant factors of M is well-defined*[5] *"up to association."*

Proof idea. By the Bézout manipulations on the columns, we replace the first row with a vector $(g_1, 0, \ldots, 0)$. By the Bézout manipulations on the rows, we replace the first column with a vector $(g_2, 0, \ldots, 0)$. We continue the process until we have $g_k\mathbf{A} = g_{k+1}\mathbf{A}$ for an index k. For example, with odd k this means that the last row operations by means of Bézout manipulations have been mistakenly applied, since g_k divided the first column. We backtrack by a step, and use g_k as a Gauss pivot. We thus

[5] We find the given definition in Theorem 5.1. We will however note that the order is reversed and that here we have replaced the principal ideals by their generators, all of this to conform to the most common terminology.

obtain a matrix of the form

$$\begin{array}{|c|ccc|}
\hline
g & 0 & \cdots & 0 \\
\hline
0 & & & \\
\vdots & & B & \\
0 & & & \\
\hline
\end{array}$$

By induction we obtain a "diagonal" reduced matrix. We finally verify that we can pass, by Bézout manipulations and elementary manipulations, from a matrix $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$ to a matrix $\begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix}$ where c divides d.

Item *2* is a direct consequence of item *1*. □

Remarks.

1) A simpler algorithm can be devised if $\mathbf{A}$ is strongly discrete.

2) We still do not know (in 2014) if the conclusion of the previous proposition is true under the sole assumption that $\mathbf{A}$ is a Bézout domain. We have neither a proof, nor a counterexample.

However, we do know that the result is true for Bézout domains of dimension $\leqslant 1$; see the remark that follows Theorem XII-6.7. ■

8. Zero-dimensional rings

We will say that a ring is *zero-dimensional* when the following axiom is satisfied.

$$\forall x \in \mathbf{A}\ \exists a \in \mathbf{A}\ \exists k \in \mathbb{N} \qquad x^k = ax^{k+1} \tag{5}$$

A ring is said to be *Artinian* if it is zero-dimensional, coherent and Noetherian.

Basic properties

8.1. Fact.

- *Every finite ring and every discrete field is zero-dimensional.*
- *Every quotient ring and every localized ring of a zero-dimensional ring is zero-dimensional.*
- *Every finite product of zero-dimensional rings is a zero-dimensional ring.*
- *A Boolean algebra (cf. Section VII-3) is a zero-dimensional ring.*

8.2. Lemma. *The following properties are equivalent.*

1. $\mathbf{A}$ *is zero-dimensional.*
2. $\forall x \in \mathbf{A}\ \exists s \in \mathbf{A}\ \exists d \in \mathbb{N}^*$ *such that* $\langle x^d \rangle = \langle s \rangle$ *and* s *idempotent.*
3. *For every finitely generated ideal* $\mathfrak{a}$ *of* $\mathbf{A}$*, there exists a* $d \in \mathbb{N}^*$ *such that* $\mathfrak{a}^d = \langle s \rangle$ *where* s *is an idempotent, and in particular,* $\mathrm{Ann}(\mathfrak{a}^d) = \langle 1 - s \rangle$ *and* $\mathfrak{a}^e = \mathfrak{a}^d$ *for* $e \geqslant d$.

D *1* ⇒ *2.* For all $x \in \mathbf{A}$, there exist $a \in \mathbf{A}$ and $k \in \mathbb{N}$ such that $x^k = ax^{k+1}$. If $k = 0$ we have $\langle x \rangle = \langle 1 \rangle$, we take $s = 1$ and $d = 1$.
If $k \geqslant 1$, we take $d = k$; by multiplying k times by ax, we obtain the equalities $x^k = ax^{k+1} = a^2x^{k+2} = \cdots = a^kx^{2k}$. Therefore the element $s = a^kx^k$ is an idempotent, $x^k = sx^k$, and $\langle x^k \rangle = \langle s \rangle$.

2 ⇒ *1.* We have $s = bx^d$ and $x^ds = x^d$. Therefore, by letting $a = bx^{d-1}$, we obtain the equalities $x^d = bx^{2d} = ax^{d+1}$.

2 ⇒ *3.* If $\mathfrak{a} = x_1\mathbf{A} + \cdots + x_n\mathbf{A}$, there exist idempotents $s_1, \ldots, s_n \in \mathbf{A}$ and integers $d_1, \ldots, d_n \geqslant 1$ such that $x_i^{d_i}\mathbf{A} = s_i\mathbf{A}$. Let

$$s = 1 - (1 - s_1) \cdots (1 - s_n),$$

such that $s\mathbf{A} = s_1\mathbf{A} + \cdots + s_n\mathbf{A}$. It is clear that the idempotent s belongs to $\mathfrak{a}$, and so to all the powers of $\mathfrak{a}$. Moreover, if $d \geqslant d_1 + \cdots + d_n - (n-1)$ we have

$$\mathfrak{a}^d \subseteq x_1^{d_1}\mathbf{A} + \cdots + x_n^{d_n}\mathbf{A} = s_1\mathbf{A} + \cdots + s_n\mathbf{A} = s\mathbf{A}.$$

The result follows since $\mathfrak{a}^d = s\mathbf{A}$.

Finally, *3* clearly implies *2*. □

8.3. Corollary. *If* $\mathfrak{a}$ *is a faithful finitely generated ideal of a zero-dimensional ring, then* $\mathfrak{a} = \langle 1 \rangle$*. In particular, in a zero-dimensional ring, every regular element is invertible.*

D For d large enough the ideal $\mathfrak{a}^d$ is generated by an idempotent s. This ideal is regular, therefore the idempotent s is equal to 1. □

8.4. Lemma. (Local zero-dimensional rings)
The following properties are equivalent.

1. $\mathbf{A}$ *is local and zero-dimensional.*
2. *Every element of* $\mathbf{A}$ *is invertible or nilpotent.*
3. $\mathbf{A}$ *is zero-dimensional and connected.*

Consequently a discrete field can also be defined as a reduced local zero-dimensional ring.

Reduced zero-dimensional rings

Characteristic properties

The equivalences of the following lemma are easy (see the proof of the analogous lemma, Lemma 8.2).

8.5. Lemma. (Reduced zero-dimensional rings)
The following properties are equivalent.

1. *The ring* $\mathbf{A}$ *is reduced and zero-dimensional.*
2. *Every principal ideal is idempotent (i.e.,* $\forall a \in \mathbf{A},\ a \in \langle a^2 \rangle$*).*
3. *Every principal ideal is generated by an idempotent.*
4. *Every finitely generated ideal is generated by an idempotent.*
5. *For every finite list* $(a_1, \ldots, a_k)$ *of elements of* $\mathbf{A}$*, there exist orthogonal idempotents* $(e_1, \ldots, e_k)$ *such that for* $j \in [\![1..k]\!]$
$$\langle a_1, \ldots, a_j \rangle = \langle a_1e_1 + \cdots + a_je_j \rangle = \langle e_1 + \cdots + e_j \rangle .$$
6. *Every ideal is idempotent.*
7. *The product of two ideals is always equal to their intersection.*
8. *The ring* $\mathbf{A}$ *is a pp-ring and every regular element is invertible.*

8.6. Fact.

1. *Let* $\mathbf{A}$ *be an arbitrary ring. If* $\mathrm{Ann}(a) = \langle \varepsilon \rangle$ *with* ε *idempotent, then the element* $b = a + \varepsilon$ *is regular and* $ab = a^2$*.*
2. *If* $\mathbf{A}$ *is a pp-ring,* $\mathrm{Frac}\,\mathbf{A}$ *is reduced zero-dimensional and every idempotent of* $\mathrm{Frac}\,\mathbf{A}$ *is in* $\mathbf{A}$*.*

D *1.* Work modulo ε and modulo $1 - \varepsilon$.

2. For some $a \in \mathbf{A}$, we must find $x \in \mathrm{Frac}\,\mathbf{A}$ such that $a^2x = a$.
Let $b = a + (1 - e_a) \in \mathrm{Reg}\,\mathbf{A}$, then $ab = a^2$, and we take $x = b^{-1}$.
Now let a/b be an idempotent of $\mathrm{Frac}\,\mathbf{A}$. We have $a^2 = ab$.
— Modulo $1 - e_a$, we have $b = a$ and $a/b = 1 = e_a$ (because a is regular).
— Modulo e_a, we have $a/b = 0 = e_a$ (because $a = 0$). In short, $a/b = e_a$.□

8.7. Fact. *A reduced zero-dimensional ring is coherent. It is strongly discrete if and only if there is an equality to zero test for the idempotents.*

We also easily obtain the following equivalences.

8.8. Fact. *For a zero-dimensional ring* $\mathbf{A}$ *the following properties are equivalent.*

1. $\mathbf{A}$ *is connected (resp.* $\mathbf{A}$ *is connected and reduced).*
2. $\mathbf{A}$ *is local (resp.* $\mathbf{A}$ *is local and reduced).*
3. $\mathbf{A}_{\mathrm{red}}$ *is integral (resp.* $\mathbf{A}$ *is integral).*
4. $\mathbf{A}_{\mathrm{red}}$ *is a discrete field (resp.* $\mathbf{A}$ *is a discrete field).*

Equational definition of reduced zero-dimensional rings

A not necessarily commutative ring satisfying

$$\forall x\,\exists a \quad xax = x$$

is often qualified as *Von Neumann regular.* In the commutative case they are the reduced zero-dimensional rings. We also call them *absolutely flat rings*, because they are also characterized by the following property: every **A**-module is flat (see Proposition VIII-2.3).

In a commutative ring, two elements a and b are said to be *quasi-inverse* if we have

$$a^2b = a, \qquad b^2a = b \tag{6}$$

We also say that b is <u>the</u> *quasi-inverse* of a. Indeed, we check that it is unique. That is, if $a^2b = a = a^2c$, $b^2a = b$ and $c^2a = c$, then

$$c - b = a(c^2 - b^2) = a(c - b)(c + b) = a^2(c - b)(c^2 + b^2) = 0,$$

since $ab = a^2b^2$, $ac = a^2c^2$ and $a^2(c - b) = a - a = 0$.

Moreover, if $x^2y = x$, we check that xy^2 is the quasi-inverse of x.

Thus *a ring is reduced zero-dimensional if and only if every element admits a quasi-inverse.*

As the quasi-inverse is unique, a reduced zero-dimensional ring can be regarded as a ring fitted with an additional unary law $a \mapsto a^\bullet$ subject to axiom (6) with $a^\bullet$ instead of b.
Note that $(a^\bullet)^\bullet = a$ and $(a_1a_2)^\bullet = a_1^\bullet a_2^\bullet$.

8.9. Fact. *A reduced zero-dimensional ring* $\mathbf{A}$ *is a pp-ring, with the idempotent* $e_a = aa^\bullet$*:* $\mathrm{Ann}(a) = \langle 1 - e_a\rangle$*. We have* $\mathbf{A} \simeq \mathbf{A}[1/e_a] \times \mathbf{A}/\langle e_a\rangle$*. In* $\mathbf{A}[1/e_a]$*, a is invertible, and in* $\mathbf{A}/\langle e_a\rangle$*, a is null.*

Zero-dimensional splitting lemma

The following splitting lemma is almost immediate. The proof resembles that of the quasi-integral splitting lemma 6.3.

8.10. Lemma. *Let* $(x_i)_{i\in I}$ *be a finite family of elements in a zero-dimensional ring* $\mathbf{A}$*. There exists a fundamental system of orthogonal idempotents* $(e_1, \ldots, e_n)$ *such that in each component* $\mathbf{A}[1/e_j]$*, each* x_i *is nilpotent or invertible.*

From discrete fields to reduced zero-dimensional rings

Reduced zero-dimensional rings look a lot like finite products of discrete fields, and this manifests itself precisely as follows.

Elementary local-global machinery no. 2.
Most algorithms that work with nontrivial discrete fields can be modified in order to work with reduced zero-dimensional rings, by splitting the ring into two components each time that the algorithm written for discrete fields uses the "is this element null or invertible?" test. In the first component the element in question is null, in the second it is invertible.

Remarks. 1) We used the term "most" rather than "all" since the statement of the result of the algorithm for the discrete fields must be written in a form that does not specify that a discrete field is connected.
2) Moreover, the same remark as the one we made on page 204 concerning the elementary local-global machinery no. 1 applies here. The algorithm given in the discrete field case must be sufficiently uniform in order to avoid leading to an infinite tree when we want to transform it into an algorithm for the reduced zero-dimensional rings. ■

We immediately give an application example of this machinery.

8.11. Proposition. *For a ring* $\mathbf{A}$ *the following properties are equivalent.*

1. $\mathbf{A}$ *is a reduced zero-dimensional ring.*
2. $\mathbf{A}[X]$ *is a strict Bézout pp-ring.*
3. $\mathbf{A}[X]$ *is a Bézout pp-ring.*

D *1* ⇒ *2.* For discrete fields this is a classical fact: we use Euclid's extended algorithm to compute in the form $g(X) = a(X)u(X) + b(X)v(X)$ a gcd of $a(X)$ and $b(X)$. In addition, we obtain a matrix $\begin{bmatrix} u & -b_1 \\ v & a_1 \end{bmatrix}$ with determinant 1 which transforms $[\,a\;\;b\,]$ into $[\,g\;\;0\,]$. This matrix is the product of matrices $\begin{bmatrix} 0 & -1 \\ 1 & -q_i \end{bmatrix}$ where the q_i's are the successive quotients.

Let us move on to the reduced zero-dimensional ring case (so a pp-ring). First of all $\mathbf{A}[X]$ is a pp-ring as the annihilator of a polynomial is the intersection of the annihilators of its coefficients (see Corollary III-2.3 *2*), hence generated by the product of the corresponding idempotents. The "strict Bézout" character of the algorithm which has just been explained for discrete fields a priori stumbles upon the obstacle of the non-invertibility of the leading coefficients in the successive divisions. Nonetheless this obstacle is avoided each time by considering a suitable idempotent e_i, the annihilator of the coefficient to be inverted. In $\mathbf{A}_i[1/e_i]$, (where $\mathbf{A}_i = \mathbf{A}[1/u_i]$ is the "current" ring with a certain idempotent u_i) the divisor polynomial has a smaller degree than expected and we start again with the following coefficient. In $\mathbf{A}_i[1/f_i]$, ($f_i = 1 - e_i$ in $\mathbf{A}_i$), the leading coefficient of the divisor is invertible and the division can be executed. In this way we obtain a computation tree whose leaves have the desired result. At each leaf the result is obtained in a localized ring $\mathbf{A}[1/h]$ for a certain idempotent h, and the h's at the leaves of the tree form a fundamental system of orthogonal idempotents. This allows us to glue together all the equalities.[6]

3 ⇒ *1.* This results from the following lemma.

Lemma. *For an arbitrary ring* $\mathbf{A}$*, if the ideal* $\langle a, X\rangle$ *is a principal ideal of* $\mathbf{A}[X]$*, then* $\langle a\rangle = \langle e\rangle$ *for a certain idempotent* e*.*

Suppose that $\langle a, X\rangle = \langle p(X)\rangle$ with $p(X)q(X) = X$. We therefore have

$$\langle a\rangle = \langle p(0)\rangle,\;\; p(0)q(0) = 0 \;\;\text{and}\;\; 1 = p(0)q'(0) + p'(0)q(0),$$

hence $p(0) = p(0)^2q'(0)$. Thus, $e = p(0)q'(0)$ is idempotent and $\langle a\rangle = \langle e\rangle$.□

Remark. The notion of a reduced zero-dimensional ring can be seen as the non-Noetherian analogue of the notion of a discrete field, since if the Boolean algebra of the idempotents is infinite, the Noetherianity is lost. Let us illustrate this with the example of the Nullstellensatz, for which it is not a priori clear if the Noetherianity is an essential ingredient or a simple

[6] For a more direct proof, see Exercise 12.

accident. A precise constructive statement of Hilbert's Nullstellensatz (weak form) is formulated as follows.

Let $\mathbf{k}$ *be a nontrivial discrete field,* $(f_1, \dots, f_s)$ *be a list of elements of* $\mathbf{k}[\underline{X}]$*, and* $\mathbf{A} = \mathbf{k}[\underline{X}]/\langle \underline{f} \rangle$ *be the quotient algebra. Then, either* $1 \in \langle f_1, \dots, f_s \rangle$*, or there exists a quotient of* $\mathbf{A}$ *that is a nonzero finite dimensional* $\mathbf{k}$*-vector space.*

As the proof is given by a uniform algorithm (for further details see Theorem VII-1.5 and Exercise VII-3), we obtain by applying the elementary local-global machinery no. 2 the following result, without disjunction, which implies the previous Nullstellensatz for a nontrivial discrete field (this example also illustrates the first remark on page 213). An $\mathbf{A}$-module M is said to be *quasi-free* if it is isomorphic to a finite direct sum of ideals $\langle e_i \rangle$ with the e_i's idempotent. We can then in addition require that $e_i e_j = e_j$ if $j > i$, since for two idempotents e and f, we have

$$\langle e \rangle \oplus \langle f \rangle \simeq \langle e \vee f \rangle \oplus \langle e \wedge f \rangle, \text{ where } e \wedge f = ef \text{ and } e \vee f = e + f - ef.$$

Let $\mathbf{k}$ *be a reduced zero-dimensional ring,* $(f_1, \dots, f_s)$ *be a list of elements of* $\mathbf{k}[X_1, \dots, X_n]$ *and* $\mathbf{A}$ *be the quotient algebra. Then the ideal* $\langle f_1, \dots, f_s \rangle \cap \mathbf{k}$ *is generated by an idempotent* e*, and by letting* $\mathbf{k}_1 = \mathbf{k}/\langle e \rangle$*, there exists a quotient* $\mathbf{B}$ *of* $\mathbf{A}$ *which is a quasi-free* $\mathbf{k}_1$*-module, the natural homomorphism* $\mathbf{k}_1 \to \mathbf{B}$ being injective. ■

Finitely presented modules over reduced zero-dimensional rings

8.12. Theorem. (The reduced zero-dimensional ring paradise)
Let $\mathbf{A}$ *be a reduced zero-dimensional ring.*

1. *Every matrix is equivalent to a matrix in Smith form with idempotents on the principal diagonal.*
2. *Every finitely presented module is quasi-free.*
3. *Every finitely generated submodule of a finitely presented module is a direct summand.*

D The results are classical ones for the discrete field case (a constructive proof can be based on the pivot method). The elementary local-global machinery no. 2 then provides (for each of the three items) the result separately in each $\mathbf{A}[1/e_j]$, after splitting the ring into a product of localized rings $\mathbf{A}[1/e_j]$ for a fundamental system of orthogonal idempotents $(e_1, \dots, e_k)$. But the result is in fact formulated in such a way that it is globally true as soon as it is true in each of the components. □

Zero-dimensional polynomial systems

In this subsection we study a particularly important example of a zero-dimensional ring, provided by the quotient algebras associated with zero-dimensional polynomial systems over discrete fields.

Recall the context studied in Section III-9 dedicated to Hilbert's Nullstellensatz. If $\mathbf{K} \subseteq \mathbf{L}$ are discrete fields, and if $(f_1, \ldots, f_s)$ is a polynomial system in $\mathbf{K}[X_1, \ldots, X_n] = \mathbf{K}[\underline{X}]$, we say that $(\xi_1, \ldots, \xi_n) = (\underline{\xi})$ is a zero of $\underline{f}$ in $\mathbf{L}^n$ if the equations $f_i(\underline{\xi}) = 0$ are satisfied.
The study of the variety of the zeros of the system is closely related to that of the *quotient algebra associated with the polynomial system*, namely

$$\mathbf{A} = \mathbf{K}[\underline{X}]/\langle \underline{f} \rangle = \mathbf{K}[\underline{x}] \quad (x_i \text{ is the class of } X_i \text{ in } \mathbf{A}).$$

Indeed, it amounts to the same to take a zero $(\underline{\xi})$ of the polynomial system in $\mathbf{L}^n$ or to take a homomorphism of $\mathbf{K}$-algebras $\psi : \mathbf{A} \to \mathbf{L}$ (ψ is defined by $\psi(x_i) = \xi_i$ for $i \in \llbracket 1..n \rrbracket$). For $h \in \mathbf{A}$, we write $h(\underline{\xi}) = \psi(h)$ for the evaluation of h at $\underline{\xi}$.

When $\mathbf{K}$ is infinite, Theorem III-9.5 gives us a Noether position by a linear change of variables, and an integer $r \in \llbracket -1..n \rrbracket$ satisfying the following properties (we do not change the name of the variables, which is a slight abuse).

1. If $r = -1$, then $\mathbf{A} = 0$, i.e. $1 \in \langle \underline{f} \rangle$.
2. If $r = 0$, each x_i is integral over $\mathbf{K}$, and $\mathbf{A} \neq 0$.
3. If $0 < r < n$, then $\mathbf{K}[X_1, \ldots, X_r] \cap \langle \underline{f} \rangle = 0$ and the x_i for $i \in \llbracket r+1..n \rrbracket$ are integral over $\mathbf{K}[x_1, \ldots, x_r]$ (which is isomorphic to $\mathbf{K}[X_1, \ldots, X_r]$).
4. If $r = n$, $\langle \underline{f} \rangle = 0$ and $\mathbf{A} = \mathbf{K}[\underline{X}]$

8.13. Lemma. (Precisions on Theorem III-9.5)

1. In the case where $r = 0$, the quotient algebra $\mathbf{A}$ is finite over $\mathbf{K}$.

2. If the quotient algebra $\mathbf{A}$ is finite over $\mathbf{K}$, it is strictly finite over $\mathbf{K}$, and it is a zero-dimensional ring. We then say that the polynomial system is zero-dimensional.

3. If the ring $\mathbf{A}$ is zero-dimensional, then $r \leqslant 0$.

4. Every strictly finite algebra over the discrete field $\mathbf{K}$ can be seen as (is isomorphic to) the quotient algebra of a zero-dimensional polynomial system over $\mathbf{K}$.

D *1.* Indeed, if $p_i(x_i) = 0$ for $i \in \llbracket 1..n \rrbracket$, the algebra $\mathbf{A}$ is a quotient of

$$\mathbf{B} = \mathbf{K}[\underline{X}]/\big\langle \big(p_i(X_i)\big)_{i \in \llbracket 1..n \rrbracket} \big\rangle,$$

which is a finite dimensional $\mathbf{K}$-vector space.

2. We start as we did in item *1.* To obtain the algebra $\mathbf{A}$, it suffices to take the quotient of $\mathbf{B}$ by the ideal $\langle f_1(\underline{z}), \ldots, f_s(\underline{z}) \rangle$ (where the z_i's are the

classes of X_i's in $\mathbf{B}$). We easily see that this ideal is a finitely generated linear subspace of $\mathbf{B}$, so the quotient is again a finite dimensional $\mathbf{K}$-vector space. Thus, $\mathbf{A}$ is strictly finite over $\mathbf{K}$.
Let us show that $\mathbf{A}$ is zero-dimensional. Every $x \in \mathbf{A}$ annihilates its minimal polynomial, say $f(T)$, so that we have an equality $x^k\big(1 + xg(x)\big) = 0$ (multiply f by the inverse of the nonzero coefficient of lower degree).

4. The algebra $\mathbf{A}$ is generated by a finite number of elements x_i (for example a basis as a $\mathbf{K}$-vector space), each of which annihilate their minimal polynomial, say $p_i(T)$. Thus $\mathbf{A}$ is a quotient of an algebra

$$\mathbf{B} = \mathbf{K}[\underline{X}]\Big/\big\langle\big(p_i(X_i)\big)_{i\in[\![1..n]\!]}\big\rangle = \mathbf{A}[z_1, \ldots, z_n].$$

The corresponding surjective morphism, from $\mathbf{B}$ over $\mathbf{A}$, is a linear map whose kernel can be computed (since $\mathbf{A}$ and $\mathbf{B}$ are finite dimensional vector spaces), for example by specifying a generator set $\big(g_1(\underline{z}), \ldots, g_\ell(\underline{z})\big)$.
In conclusion, the algebra $\mathbf{A}$ is isomorphic to the quotient algebra associated with the polynomial system $\big(p_1(X_1), \ldots, p_n(X_n), g_1(\underline{X}), \ldots, g_\ell(\underline{X})\big)$.

3. This point results from the following two lemmas. □

Remark. Traditionally, we reserve the term zero-dimensional polynomial system to the $r = 0$ case, but the quotient algebra is also zero-dimensional when $r = -1$. ■

8.14. Lemma. *If the ring $\mathbf{C}[X_1, \ldots, X_r]$ is zero-dimensional with $r > 0$, then the ring $\mathbf{C}$ is trivial.*

D We write $X_1^m\big(1 - X_1P(X_1, \ldots, X_r)\big) = 0$. The coefficient of X_1^m is both equal to 0 and to 1. □

8.15. Lemma. *Let $\mathbf{k} \subseteq \mathbf{A}$ and $\mathbf{A}$ be integral over $\mathbf{k}$. If $\mathbf{A}$ is a zero-dimensional ring, $\mathbf{k}$ is a zero-dimensional ring.*

D Let $x \in \mathbf{k}$, then we have a $y \in \mathbf{A}$ such that $x^k = yx^{k+1}$. Suppose for example that $y^3 + b_2y^2 + b_1y + b_0 = 0$ with $b_i \in \mathbf{k}$.
Then, $x^k = yx^{k+1} = y^2x^{k+2} = y^3x^{k+3}$, and so

$$\begin{aligned} 0 &= (y^3 + b_2y^2 + b_1y + b_0)x^{k+3} \\ &= x^k + b_2x^{k+1} + b_1x^{k+2} + b_0x^{k+3} = x^k\big(1 + x(b_2 + b_1x + b_0x^2)\big). \end{aligned}$$

□

8.16. Theorem. (Zero-dimensional system over a discrete field)
*Let $\mathbf{K}$ be a discrete field and $(f_1, \ldots, f_s)$ in $\mathbf{K}[X_1, \ldots, X_n] = \mathbf{K}[\underline{X}]$.
Let $\mathbf{A} = \mathbf{K}[\underline{X}]/\langle\underline{f}\rangle$ be the quotient algebra associated with this polynomial system.
The following properties are equivalent.*

1. *$\mathbf{A}$ is finite over $\mathbf{K}$.*
2. *$\mathbf{A}$ is strictly finite over $\mathbf{K}$.*

3. *$\mathbf{A}$ is a zero-dimensional ring.*

If $\mathbf{K}$ is contained in a algebraically closed discrete field $\mathbf{L}$, these properties are also equivalent to the following.

4. *The polynomial system has a finite number of zeros in $\mathbf{L}^n$.*
5. *The polynomial system has a bounded number of zeros in $\mathbf{L}^n$.*

D When $\mathbf{K}$ is infinite, we obtain the equivalences by applying Lemma 8.13 and Theorem III-9.5.
In the general case, we can also obtain a Noether position by using a (not necessarily linear) general change of variables as described in Lemma VII-1.4 (see Theorem VII-1.5). □

A variation on the previous theorem is given in Theorem VI-3.15.

Remark. Rather than using a non-linear change of variables as proposed in the previous proof, we can resort to using the technique of "changing the base field." This works as follows. Consider an infinite field $\mathbf{K}_1 \supseteq \mathbf{K}$, for example $\mathbf{K}_1 = \mathbf{K}(t)$, or an algebraically closed field $\mathbf{K}_1$ containing $\mathbf{K}$ if we know how to construct one. Then the equivalence of items *1*, *2* and *3* is assured for the algebra $\mathbf{A}_1$ for the same polynomial system seen on $\mathbf{K}_1$. The algebra $\mathbf{A}_1$ is obtained from $\mathbf{A}$ by scalar extension from $\mathbf{K}$ to $\mathbf{K}_1$. It remains to see that each of the three items is satisfied for $\mathbf{A}$ if and only if it is satisfied for $\mathbf{A}_1$. A task we leave to the reader.[7] ■

8.17. Theorem. (Stickelberger's theorem)
Same context as in Theorem 8.16, now with $\mathbf{K}$ being an algebraically closed field.

1. *The polynomial system admits a finite number zeros over $\mathbf{K}$.*
   We write them as $\underline{\xi}_1, \dots, \underline{\xi}_\ell$.
2. *For each $\underline{\xi}_k$ there exists an idempotent $e_k \in \mathbf{A}$ satisfying $e_k(\underline{\xi}_j) = \delta_{j,k}$ (Kronecker symbol) for all $j \in [\![1..\ell]\!]$.*
3. *The idempotents $(e_1, \dots, e_\ell)$ form a fundamental system of orthogonal idempotents.*
4. *Each algebra $\mathbf{A}[1/e_k]$ is a zero-dimensional local ring (every element is invertible or nilpotent).*
5. *Let m_k be the dimension of the $\mathbf{K}$-vector space $\mathbf{A}[1/e_k]$.*
   We have $[\mathbf{A} : \mathbf{k}] = \sum_{k=1}^{\ell} m_k$ and for all $h \in \mathbf{A}$ we have
   $$\mathrm{C}_{\mathbf{A}/\mathbf{k}}(h)(T) = \prod_{k=1}^{\ell} \big(T - h(\underline{\xi}_k)\big)^{m_k}.$$
   In particular, $\mathrm{Tr}_{\mathbf{A}/\mathbf{k}}(h) = \sum_{k=1}^{\ell} m_k h(\underline{\xi}_k)$ and $\mathrm{N}_{\mathbf{A}/\mathbf{k}}(h) = \prod_{k=1}^{\ell} h(\underline{\xi}_k)^{m_k}$.
6. *Let $\pi_k : \mathbf{A} \to \mathbf{K}$, $h \mapsto h(\underline{\xi}_k)$ be the evaluation at $\underline{\xi}_k$, and $\mathfrak{m}_k = \operatorname{Ker} \pi_k$.*
   Then $\langle e_k - 1 \rangle = \mathfrak{m}_k^{m_k}$ and $\mathfrak{m}_k = \sqrt{\langle e_k - 1 \rangle}$.

[7] See on this subject Theorems VIII-6.2, VIII-6.7 and VIII-6.8.

D Let $V = \{\underline{\xi}_1, \dots, \underline{\xi}_\ell\}$ be the variety of zeros of the system in $\mathbf{K}^n$.

2 and *3*. We have multivariate Lagrange interpolating polynomials $L_k \in \mathbf{K}[\underline{X}]$ which satisfy $L_k(\underline{\xi}_j) = \delta_{j,k}$. Consider the L_k's as elements of $\mathbf{A}$.

Since $\mathbf{A}$ is zero-dimensional, there exist an integer d and an idempotent e_k with $\langle e_k \rangle = \langle L_k \rangle^d$, therefore $e_k L_k^d = L_k^d$ and $L_k^d b_k = e_k$ for a certain b_k. This implies that $e_k(\underline{\xi}_j) = \delta_{j,k}$.

For $j \neq k$, $e_j e_k$ is null over V, so by the Nullstellensatz, $e_j e_k$ is nilpotent in $\mathbf{A}$. As it is an idempotent, $e_j e_k = 0$.

The sum of the e_j's is therefore an idempotent e. This element vanishes nowhere, i.e. it has the same zeros as 1. By the Nullstellensatz, we obtain $1 \in \sqrt{\langle e \rangle}$. Thus $e = 1$ because it is an invertible idempotent of $\mathbf{A}$.

4. The $\mathbf{K}$-algebra $\mathbf{A}_k = \mathbf{A}[1/e_k] = \mathbf{A}/\langle 1 - e_k \rangle$ is the quotient algebra associated with the polynomial system $(f_1, \dots, f_s, 1 - e_k)$ which admits $\underline{\xi}_k$ as its only zero. Consider an arbitrary element $h \in \mathbf{A}_k$. By reasoning as in the previous item, we obtain by the Nullstellensatz that if $h(\underline{\xi}_k) = 0$, then h is nilpotent, and if $h(\underline{\xi}_k) \neq 0$, then h is invertible.

5. Since $\mathbf{A} \simeq \prod_{k=1}^{\ell} \mathbf{A}_k$, it suffices to prove that for $h \in \mathbf{A}_k$, we have the equality $\mathrm{C}_{\mathbf{A}_k/\mathbf{k}}(h)(T) = \big(T - h(\underline{\xi}_k)\big)^{m_k}$. We identify $\mathbf{K}$ with its image in $\mathbf{A}_k$. The element $h_k = h - h(\underline{\xi}_k)$ vanishes in $\underline{\xi}_k$, so it is nilpotent. If μ designates multiplication by h_k in $\mathbf{A}_k$, μ is a nilpotent endomorphism. With respect to a suitable basis, its matrix is strictly lower triangular and that of the multiplication by h is triangular with $h(\underline{\xi}_k)$'s on the diagonal, therefore its characteristic polynomial is $\big(T - h(\underline{\xi}_k)\big)^{m_k}$.

6. We clearly have $e_k - 1 \in \mathfrak{m}_k$. If $h \in \mathfrak{m}_k$, the element $e_k h$ is null everywhere over V, so nilpotent. Therefore $h^N e_k = 0$ for a certain N and $h \in \sqrt{\langle e_k - 1 \rangle}$. To show that $\mathfrak{m}_k^{m_k} = \langle e_k - 1 \rangle$, we can locate ourselves in $\mathbf{A}_k$, where $\langle e_k - 1 \rangle = 0$. In this ring, the ideal $\mathfrak{m}_k$ is a $\mathbf{K}$-vector space of dimension $m_k - 1$. The successive powers of $\mathfrak{m}_k$ then form a decreasing sequence of finite dimensional $\mathbf{K}$-linear subspaces, which stabilizes as soon as two consecutive terms are equal. Thus $\mathfrak{m}_k^{m_k}$ is a finitely generated strict idempotent ideal, therefore null. □

Remarks.

1) The fact that the polynomial system is zero-dimensional results from a rational computation in the field of coefficients (in a Noether positioning or computation of a Gröbner basis).

2) Item *5* of Stickelberger's theorem allows us to compute all the useful information on the zeros of the system by basing ourselves on the only trace form. In addition, the trace form can be computed in the field of coefficients of the polynomials of the system. This has important applications in computer algebra (see for example [Basu, Pollack & Roy]). ■

For examples, consult Exercise 15 and Problem 1. For a purely local study of the isolated zeros, see Section IX-4.

9. Fitting ideals

The theory of the Fitting ideals of finitely presented modules is an extremely efficient computing machinery from a theoretical constructive point of view. It has an “elimination theory” side in so far as it is entirely based on computations of determinants, and it more or less disappeared for a while from the literature under the influence of the idea that we had to “eliminate the elimination” to escape the quagmire of computations whose meaning seemed unclear.

The Fitting ideals are becoming fashionable once again and it is for the best. For more details, please consult [Northcott].

Fitting ideals of a finitely presented module

9.1. Definition.
If $G \in \mathbf{A}^{q\times m}$ is a presentation matrix of an $\mathbf{A}$-module M given by q generators, the *Fitting ideals of* M are the ideals

$$\mathcal{F}_{\mathbf{A},n}(M) = \mathcal{F}_n(M) := \mathcal{D}_{\mathbf{A},q-n}(G)$$

where n is an arbitrary integer.

This definition is legitimized by the following easy but fundamental lemma.

9.2. Lemma. *The Fitting ideals of the finitely presented module M are well-defined, in other words these ideals do not depend on the chosen presentation G for M.*

D To prove this lemma we must essentially show that the ideals $\mathcal{D}_{q-n}(G)$ do not change,

1. on the one hand, when we add a new syzygy, a linear combination of the already present syzygies,
2. on the other hand, when we add a new element to a generator set, with a syzygy that expresses this new element in relation to the previous generators.

The details are left to the reader. □

We immediately have the following facts.

9.3. Fact. *For every finitely presented module M with q generators, we have the inclusions*

$$\langle 0\rangle = \mathcal{F}_{-1}(M) \subseteq \mathcal{F}_0(M) \subseteq \cdots \subseteq \mathcal{F}_q(M) = \langle 1\rangle\,.$$

If N is a finitely presented quotient module of M, we have the inclusions $\mathcal{F}_k(M) \subseteq \mathcal{F}_k(N)$ for all $k \geqslant 0$.

Remark. In particular, if $\mathcal{F}_r(M) \neq \langle 1\rangle$ the module M cannot be generated by r elements. We will see (lemma of the number of local generators page 496) that the meaning of the equality $\mathcal{F}_r(M) = \langle 1\rangle$ is that the module is *locally* generated by r elements. ■

9.4. Fact. *Let M be a rank k free $\mathbf{A}$-module. Then,*

$$\mathcal{F}_0(M) = \cdots = \mathcal{F}_{k-1}(M) = \langle 0\rangle \subseteq \mathcal{F}_k(M) = \langle 1\rangle\,.$$

More generally, if M is quasi-free isomorphic to $\bigoplus_{1\leqslant i\leqslant k}\langle f_i\rangle$, where the f_i's are idempotents such that $f_i f_j = f_j$ if $j > i$, then $\mathcal{F}_k(M) = \langle 1\rangle$ and $\mathcal{F}_i(M) = \langle 1 - f_{i+1}\rangle$ for $0 \leqslant i < k$.

Note that this provides a clever proof that if a module is free with two distinct ranks, the ring is trivial.

Examples.

1. For a finite Abelian group H considered as a $\mathbb{Z}$-module, the ideal $\mathcal{F}_0(H)$ is generated by the order of the group whilst the annihilator is generated by its exponent. In addition, the structure of the group is entirely characterized by its Fitting ideals. A generalization is given in Exercise 16.

2. Let us reuse the $\mathbf{B}$-module M of Example on page 195. The computation gives the following results.

- For M: $\mathcal{F}_0(M) = 0$, $\mathcal{F}_1(M) = \mathfrak{b}$ and $\mathcal{F}_2(M) = \langle 1\rangle$,
- for $M' = M \otimes M$: $\mathcal{F}_0(M') = 0$, $\mathcal{F}_1 = \mathfrak{b}^3$, $\mathcal{F}_2 = \mathfrak{b}^2$, $\mathcal{F}_3 = \mathfrak{b}$ and $\mathcal{F}_4 = \langle 1\rangle$,
- for $M'' = \mathbf{S}^2(M)$: $\mathcal{F}_0(M'') = 0$, $\mathcal{F}_1 = \mathfrak{b}^2$, $\mathcal{F}_2 = \mathfrak{b}$ and $\mathcal{F}_3 = \langle 1\rangle$,
- for $\bigwedge^2 M$: $\mathcal{F}_0(\bigwedge^2 M) = \mathfrak{b}$ and $\mathcal{F}_1(\bigwedge^2 M) = \langle 1\rangle$. ■

9.5. Fact. (Changing the base ring)
Let M be a finitely presented $\mathbf{A}$-module, $\rho : \mathbf{A} \to \mathbf{B}$ be a homomorphism of rings, and $\rho_\star(M)$ be the $\mathbf{B}$-module obtained by scalar extension to $\mathbf{B}$. We have for every integer $n \geqslant 0$ the equality $\big\langle \rho\big(\mathcal{F}_n(M)\big)\big\rangle = \mathcal{F}_n\big(\rho_\star(M)\big)$.
In particular, if S is a monoid, we have $\mathcal{F}_n(M_S) = \big(\mathcal{F}_n(M)\big)_S$.

The two following facts are less obvious.

9.6. Lemma. (Annihilator and first Fitting ideal)
Let M be a finitely presented $\mathbf{A}$-module generated by q elements, we have

$$\mathrm{Ann}(M)^q \subseteq \mathcal{F}_0(M) \subseteq \mathrm{Ann}(M).$$

D Let $(x_1, \ldots, x_q)$ be a generator set of M, $X = [\,x_1 \ \cdots \ x_q\,]$ and G a presentation matrix for X. Let $a_1, \ldots, a_q \in \mathrm{Ann}(M)$. Then, the diagonal matrix $\mathrm{Diag}(a_1, \ldots, a_q)$ has as its columns linear combinations of the columns of G, so its determinant $a_1 \cdots a_q$ belongs to $\mathcal{F}_0(M)$. This proves the first inclusion.
Let δ be a minor of order q extracted from G. We will show that $\delta \in \mathrm{Ann}(M)$, hence the second inclusion. If δ corresponds to a submatrix H of G we have $X H = 0$, therefore $\delta X = 0$, and this indeed means that $\delta \in \mathrm{Ann}(M)$. □

9.7. Fact. (Fitting ideals and exact sequences)
Let $0 \to N \to M \to P \to 0$ be an exact sequence of finitely presented modules. For all $p \geqslant 0$ we have

$$\mathcal{F}_p(M) \supseteq \textstyle\sum_{r \geqslant 0, s \geqslant 0, r+s=p} \mathcal{F}_r(N)\mathcal{F}_s(P),$$

and if $M \simeq N \oplus P$, the inclusion is an equality.

D We can consider that $N \subseteq M$ and $P = M/N$. We use the notations of item *3* of Proposition 4.2. We have a presentation matrix D of M which is written "in a triangular form" $D = \begin{bmatrix} A & C \\ 0 & B \end{bmatrix}$. Then every product of a minor of order k of A and of a minor of order ℓ of B is equal to a minor of order $k + \ell$ of D. This implies the stated result for Fitting ideals.
The second case is clear, with $C = 0$. □

Example. On the polynomial ring $\mathbf{A} = \mathbb{Z}[a, b, c, d]$, let us consider the module $M = \mathbf{A}g_1 + \mathbf{A}g_2 = \mathrm{Coker}\, F$ where $F = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. Here g_1 and g_2 are images of the natural basis (e_1, e_2) of $\mathbf{A}^2$. Let $\delta = \det(F)$.
It is easily seen that $\delta\, e_1$ is a basis of the submodule $\mathrm{Im}\, F \cap e_1\mathbf{A}$ of $\mathbf{A}^2$.
Let $N = \mathbf{A}g_1$ and $P = M/N$. Then the module N admits the presentation matrix $[\,\delta\,]$ for the generator set (g_1) and P admits the presentation matrix $[\,c\ d\,]$ for the generator set $(\overline{g_2})$. Consequently, we get $\mathcal{F}_0(M) = \mathcal{F}_0(N) = \langle \delta \rangle$ and $\mathcal{F}_0(P) = \langle c, d \rangle$. So the inclusion $\mathcal{F}_0(N)\mathcal{F}_0(P) \subseteq \mathcal{F}_0(M)$ is strict. ■

Fitting ideals of a finitely generated module

We can generalize the definition of the Fitting ideals to an arbitrary finitely generated module M as follows. If $(x_1, \ldots, x_q)$ is a generator set of M and if $X = {}^{\mathrm{t}}[\,x_1 \ \cdots \ x_q\,]$, we define $\mathcal{F}_{q-k}(M)$ as the ideal generated by all the minors of order k of every matrix $G \in \mathbf{A}^{k \times q}$ satisfying $GX = 0$. An alternative definition is that each $\mathcal{F}_j(M)$ is the sum of all the $\mathcal{F}_j(N)$'s where N ranges over the finitely presented modules that are surjectively sent onto M.

This shows that the ideals defined thus do not depend on the considered generator set.

The following remark is often useful.

9.8. Fact. *Let M be a finitely generated $\mathbf{A}$-module.*

1. *If $\mathcal{F}_k(M)$ is a finitely generated ideal, then M is the quotient of a finitely presented module M' for which $\mathcal{F}_k(M') = \mathcal{F}_k(M)$.*
2. *If all the Fitting ideals are finitely generated, then M is the quotient of a finitely presented module M' having the same Fitting ideals as M.*

10. Resultant ideal

In what follows, we consider a ring $\mathbf{k}$ that we do not assume to be discrete. The resultant of two polynomials is at the heart of elimination theory. If f, $g \in \mathbf{k}[X]$ with f monic, the basic elimination lemma page 121 can be read in the algebra $\mathbf{B} = \mathbf{k}[X]/\langle f\rangle$ by writing

$$\mathrm{D}_{\mathbf{B}}(\overline{g}) \cap \mathbf{k} = \mathrm{D}_{\mathbf{k}}\big(\mathrm{Res}_X(f,g)\big).$$

It can then be generalized with the following result, which can be regarded as a very precise formulation of the Lying Over (see Lemma VI-3.12).

10.1. General elimination lemma.

1. *Let $\mathbf{k} \xrightarrow{\rho} \mathbf{C}$ be an algebra which is a $\mathbf{k}$-module generated by m elements, $\mathfrak{a} = \mathcal{F}_{\mathbf{k},0}(\mathbf{C})$ its first Fitting ideal and $\mathfrak{c} = \mathrm{Ker}\,\rho$. Then*
   a. *$\mathfrak{c} = \mathrm{Ann}_{\mathbf{k}}(\mathbf{C})$,*
   b. *$\boxed{\mathfrak{c}^m \subseteq \mathfrak{a} \subseteq \mathfrak{c}}$ and so $\boxed{\mathrm{D}_{\mathbf{k}}(\mathfrak{c}) = \mathrm{D}_{\mathbf{k}}(\mathfrak{a})}$,*
   c. *if by some scalar extension $\varphi : \mathbf{k} \to \mathbf{k}'$ we obtain the algebra $\rho' : \mathbf{k}' \to \mathbf{C}'$, then the ideal $\mathfrak{a}' := \mathcal{F}_0(\mathbf{C}')$ is equal to $\varphi(\mathfrak{a})\mathbf{k}'$ and as a $\mathbf{k}'$-module, it is isomorphic to $\mathbf{k}' \otimes_{\mathbf{k}} \mathfrak{a} \simeq \varphi_\star(\mathfrak{a})$.*
2. *Let $\mathbf{B} \supseteq \mathbf{k}$ be a $\mathbf{k}$-algebra which is a free $\mathbf{k}$-module of rank m, and $\mathfrak{b}$ be a finitely generated ideal of $\mathbf{B}$.*
   a. *The elimination ideal $\mathfrak{b} \cap \mathbf{k}$ is the kernel of the canonical homomorphism $\rho : \mathbf{k} \to \mathbf{B}/\mathfrak{b}$, i.e. the annihilator of the $\mathbf{k}$-module $\mathbf{B}/\mathfrak{b}$.*
   b. *The $\mathbf{k}$-module $\mathbf{B}/\mathfrak{b}$ is finitely presented and we have*
   $\boxed{(\mathfrak{b} \cap \mathbf{k})^m \subseteq \mathcal{F}_0(\mathbf{B}/\mathfrak{b}) \subseteq \mathfrak{b} \cap \mathbf{k}}$ *and* $\boxed{\mathrm{D}_{\mathbf{B}}(\mathfrak{b}) \cap \mathbf{k} = \mathrm{D}_{\mathbf{k}}\big(\mathcal{F}_0(\mathbf{B}/\mathfrak{b})\big)}$.
   We denote by $\mathfrak{Res}(\mathfrak{b}) := \mathcal{F}_{\mathbf{k},0}(\mathbf{B}/\mathfrak{b})$ what we call the resultant ideal of $\mathfrak{b}$.

D *1a* and *1b.* Indeed, $a \in \mathbf{k}$ annihilates $\mathbf{C}$ if and only if it annihilates $1_{\mathbf{C}}$, if and only if $\rho(a) = 0$. The desired double inclusion is therefore given by Lemma 9.6 (also valid for finitely generated modules).

1c. The Fitting ideals are well-behaved under scalar extension.

2. Apply item *1* with $\mathbf{C} = \mathbf{B}/\mathfrak{b}$. □

Remarks. 1) The resultant ideal in item *2* can be precisely described as follows. If $\mathfrak{b} = \langle b_1, \ldots, b_s \rangle$ we consider the *generalized Sylvester mapping*

$$\psi : \mathbf{B}^s \to \mathbf{B}, \quad (y_1, \ldots, y_s) \mapsto \psi(\underline{y}) = \textstyle\sum_i y_i b_i.$$

It is a $\mathbf{k}$-linear map between free $\mathbf{k}$-modules of ranks ms and m. Then, we have $\mathfrak{Res}(\mathfrak{b}) = \mathcal{D}_m(\psi)$.

2) There are many generators for the ideal $\mathfrak{Res}(\mathfrak{b})$. Actually, there exist diverse techniques to decrease the number of generators by replacing $\mathfrak{Res}(\mathfrak{b})$ by a finitely generated ideal having considerably fewer generators but having the same nilradical. On this subject see the work given in Section III-9, especially Lemma III-9.2, the results of Chapter XIII on the number of radical generators of a radically finitely generated ideal (Theorem XIV-1.3), and the paper [61]. ■

Now here is a special case of the general elimination lemma. This theorem completes Lemma III-9.2.

10.2. Theorem. (Algebraic elimination theorem: the resultant ideal) *Let $(f, g_1, \ldots, g_r)$ be polynomials of $\mathbf{k}[X]$ with f monic of degree m. We let*

$$\mathfrak{f} = \langle f, g_1, \ldots, g_r \rangle \subseteq \mathbf{k}[X] \textit{ and } \mathbf{B} = \mathbf{k}[X]/\langle f \rangle.$$

Let $\psi : \mathbf{B}^r \to \mathbf{B}$ be the generalized Sylvester mapping *defined by*

$$(y_1, \ldots, y_r) \mapsto \psi(\underline{y}) = \textstyle\sum_i y_i \overline{g_i}.$$

It is a $\mathbf{k}$-linear map between free $\mathbf{k}$-modules of respective ranks mr and m. Let $\mathfrak{a}$ be the determinantal ideal $\mathcal{D}_m(\psi)$.

1. *We have $\mathfrak{a} = \mathcal{F}_{\mathbf{k},0}(\mathbf{k}[X]/\mathfrak{f})$, and*
$$(\mathfrak{f} \cap \mathbf{k})^m \subseteq \mathfrak{a} \subseteq \mathfrak{f} \cap \mathbf{k}, \quad \textit{and so} \quad \mathrm{D}_{\mathbf{k}[X]}(\mathfrak{f}) \cap \mathbf{k} = \mathrm{D}_{\mathbf{k}}(\mathfrak{a}).$$
2. *Assume that $\mathbf{k} = \mathbf{A}[Y_1, \ldots, Y_q]$ and that f and the g_i's are of total degree $\leqslant d$ in $\mathbf{A}[\underline{Y}, X]$. Then the generators of $\mathcal{D}_m(\psi)$ are of total degree $\leqslant d^2$ in $\mathbf{A}[\underline{Y}]$.*
3. *The ideal $\mathfrak{a}$ does not depend on $\mathfrak{f}$ (under the sole assumption that $\mathfrak{f}$ contains a monic polynomial). We call it* the resultant ideal of $\mathfrak{f}$ w.r.t. the indeterminate X *and we denote it by $\mathfrak{Res}_X(f, g_1, \ldots, g_r)$ or $\mathfrak{Res}_X(\mathfrak{f})$, or $\mathfrak{Res}(\mathfrak{f})$.*
4. *If by some scalar extension $\theta : \mathbf{k} \to \mathbf{k}'$ we obtain the ideal $\mathfrak{f}'$ of $\mathbf{k}'[X]$, then the ideal $\mathfrak{Res}_X(\mathfrak{f}') \subseteq \mathbf{k}'$ is equal to $\theta\big(\mathfrak{Res}_X(\mathfrak{f})\big)\mathbf{k}'$, and as a module it is isomorphic to $\mathbf{k}' \otimes_{\mathbf{k}} \mathfrak{Res}_X(\mathfrak{f}) \simeq \theta_\star\big(\mathfrak{Res}_X(\mathfrak{f})\big)$.*

NB. Consider the basis $\mathcal{E} = (1, \ldots, X^{m-1})$ of $\mathbf{B}$ over $\mathbf{k}$. Let $F \in \mathbf{k}^{m \times mr}$ be the matrix of ψ for the deduced bases of $\mathcal{E}$. Its columns are the $X^j g_k \bmod f$ for $j \in [\![0..m-1]\!]$, $k \in [\![1..r]\!]$ written over the basis $\mathcal{E}$. We say that F is a *generalized Sylvester matrix*. By definition we have $\mathfrak{Res}_X(\mathfrak{f}) = \mathcal{D}_m(F)$. ■

D Let $\mathfrak{b} = \mathfrak{f} \bmod f = \langle \overline{g_1}, \ldots, \overline{g_r} \rangle \subseteq \mathbf{B}$. We apply items *2* and *1c* of the general elimination lemma by noticing that $\mathbf{k}[X]/\mathfrak{f} \simeq \mathbf{B}/\mathfrak{b}$, with $\mathfrak{f} \cap \mathbf{k} = \mathfrak{b} \cap \mathbf{k}$. □

Remark. Thus Theorem 10.2 establishes a very narrow link between the elimination ideal and the resultant ideal. The advantages introduced by the resultant ideal over the elimination ideal are the following

- the resultant ideal is finitely generated,
- its computation is *uniform*,
- it is well-behaved under scalar extension.

Note that in the case where $\mathbf{k} = \mathbf{K}[Y_1, \ldots, Y_q]$, for $\mathbf{K}$ a discrete field, the elimination ideal is also finitely generated but its computation, for instance via Gröbner bases, is not uniform.
However, the resultant ideal is only defined when $\mathfrak{f}$ contains a monic polynomial and this limits the scope of the theorem. ■

Exercises and problems

Exercise 1. We recommend that the proofs which are not given, or are sketched, or left to the reader, etc, be done. But in particular, we will cover the following cases.

- Give a detailed proof of Lemma 1.1.
- Explain why Propositions II-3.1 and II-3.7 (when we take $\mathbf{A}$ as an $\mathbf{A}$-module M) can be read in the form of Theorem 4.3.
- Prove Propositions 4.1 and 4.4. Give a detailed proof of Propositions 4.6 and 4.11. Show that $\mathbf{A}/\mathfrak{a} \otimes_{\mathbf{A}} \mathbf{A}/\mathfrak{b} \simeq \mathbf{A}/(\mathfrak{a} + \mathfrak{b})$.
- Justify the statements contained in the Example on page 195.
- Prove Lemmas or Facts 8.4, 8.5, 8.7 and 8.8.
- Give algorithms for the three items of Theorem 8.12.
- Prove Fact 9.8.

Exercise 2. Let $M \subseteq N$ be $\mathbf{A}$-modules with M as direct factor in N. Prove that if N is finitely generated (resp. finitely presented), then so is M.

Exercise 3. *(Structure of an $\mathbf{A}[X]$-module over $\mathbf{A}^n$ associated with $A \in \mathbb{M}_n(\mathbf{A})$)*
Let $\mathbf{A}$ be a commutative ring and $A \in \mathbb{M}_n(\mathbf{A})$. We give $\mathbf{A}^n$ the structure of an $\mathbf{A}[X]$-module by letting

$$Q \cdot x = Q(A) \cdot x \text{ for } Q \in \mathbf{A}[X] \text{ and } x \in \mathbf{A}^n.$$

We aim to give a presentation matrix for this $\mathbf{A}[X]$-module. This generalizes Example 3) on page 179 given at the beginning of Section 1, where $\mathbf{A}$ is a discrete field.

Let $\theta_A : \mathbf{A}[X]^n \twoheadrightarrow \mathbf{A}^n$ be the unique $\mathbf{A}[X]$-morphism which transforms the canonical basis of $\mathbf{A}[X]^n$ into that of $\mathbf{A}^n$. By labeling these two canonical bases by the same name $(e_1, \dots, e_n)$, θ_A therefore transforms $Q_1 e_1 + \cdots + Q_n e_n$ into $Q_1(A) \cdot e_1 + \cdots + Q_n(A) \cdot e_n$. We will show that the sequence below is exact

$$\mathbf{A}[X]^n \xrightarrow{X\mathrm{I}_n - A} \mathbf{A}[X]^n \xrightarrow{\theta_A} \mathbf{A}^n \to 0$$

In other words $\mathbf{A}^n$ is a finitely presented $\mathbf{A}[X]$-module and $X\mathrm{I}_n - A$ is a presentation matrix for the generator set $(e_1, \dots, e_n)$.

1. Show that we have a direct sum of $\mathbf{A}$-modules $\mathbf{A}[X]^n = \mathrm{Im}(X\mathrm{I}_n - A) \oplus \mathbf{A}^n$.

2. Conclude the result.

Exercise 4. *(Description of the null tensors)*
Let M and N be two $\mathbf{A}$-modules and $z = \sum_{i \in [\![1..n]\!]} x_i \otimes y_i \in M \otimes N$.

1. Show that $z = 0$ if and only if there exists a finitely generated submodule M_1 of M such that we have $\sum_{i \in [\![1..n]\!]} x_i \otimes y_i =_{M_1 \otimes N} 0$.

2. We write $M_1 = \mathbf{A}x_1 + \cdots + \mathbf{A}x_p$ where $p \geqslant n$. Let $y_k =_N 0$ for $n < k \leqslant p$. Use the null tensor lemma with the equality $\sum_{i \in [\![1..p]\!]} x_i \otimes y_i =_{M_1 \otimes N} 0$ to give a characterization of the null tensors in the general setting.

Exercise 5. Let M be an $\mathbf{A}$-module, $\mathfrak{a}$ be an ideal and S be a monoid of $\mathbf{A}$.

1. Show that the canonical linear map $M \to M/\mathfrak{a}M$ solves the universal problem of the scalar extension for the homomorphism $\mathbf{A} \to \mathbf{A}/\mathfrak{a}$ (i.e. according to Definition 4.10, this linear map is a morphism of scalar extension from $\mathbf{A}$ to $\mathbf{A}/\mathfrak{a}$ for M). Deduce that the natural linear map $\mathbf{A}/\mathfrak{a} \otimes_{\mathbf{A}} M \to M/\mathfrak{a}M$ is an isomorphism.

2. Show that the canonical linear map $M \to M_S$ solves the universal problem of the scalar extension for the homomorphism $\mathbf{A} \to \mathbf{A}_S$. Deduce that the natural linear map $\mathbf{A}_S \otimes_{\mathbf{A}} M \to M_S$ is an isomorphism.

Exercise 6. Prove that every matrix over a Bézout domain is equivalent to a matrix of the form $\begin{bmatrix} T & 0 \\ 0 & 0 \end{bmatrix}$, where T is triangular and the elements on the diagonal of T are nonzero (naturally, the rows or columns indicated as zero can be absent). This equivalence can be obtained by Bézout manipulations.

Generalize to pp-rings by using the general method explained on page 204.

Exercise 7. *(Strict Bézout rings)*
1. For a ring $\mathbf{A}$, show that the following properties are equivalent.

- *a.* If $A \in \mathbf{A}^{n\times m}$, there exists a $Q \in \mathbb{GL}_m(\mathbf{A})$ such that AQ is a lower triangular matrix.
- *b.* Same as item a with $(n, m) = (1, 2)$, i.e. $\mathbf{A}$ is a strict Bézout ring.
- *c.* For a, $b \in \mathbf{A}$, there exist comaximal x, $y \in \mathbf{A}$ such that $ax + by = 0$.
- *d.* For $(\underline{a}) = (a_1, \ldots, a_n)$ in $\mathbf{A}$, there exist a $d \in \mathbf{A}$ and a unimodular vector $(\underline{a'}) = (a'_1, \ldots, a'_n)$ satisfying $(\underline{a}) = d(\underline{a'})$; we then have $\langle \underline{a} \rangle = \langle d \rangle$.
- *e.* Same as item d with $n = 2$.

2. Show that the class of strict Bézout rings is stable under finite products, quotients and localization.

In the following, we assume that $\mathbf{A}$ is a strict Bézout ring.

3. Let a, b, $d_2 \in \mathbf{A}$ such that $\langle a, b\rangle = \langle d_2\rangle$. Show that there exist comaximal a_2, $b_2 \in \mathbf{A}$ such that $(a, b) = d_2(a_2, b_2)$. We can consider d_1, a_1, b_1, u_1, v_1 where $(a, b) = d_1(a_1, b_1)$, $1 = u_1a_1 + v_1b_1$ and introduce

$$(\star) \quad \begin{bmatrix} a_2 \\ b_2 \end{bmatrix} = \begin{bmatrix} v_1 & a_1 \\ -u_1 & b_1 \end{bmatrix} \begin{bmatrix} \varepsilon \\ k_{12} \end{bmatrix} \text{ where } d_1 = k_{12}d_2,\ d_2 = k_{21}d_1,\ \varepsilon = k_{12}k_{21} - 1.$$

4. Same as in the previous item but with an arbitrary number of elements; i.e. for given $(\underline{a}) = (a_1, \ldots, a_n)$ in $\mathbf{A}$ and d satisfying $\langle \underline{a} \rangle = \langle d \rangle$, there exists $(\underline{a'}) = (a'_1, \ldots, a'_n)$, comaximal, such that $\underline{a} = d\underline{a'}$.

5. Show that every diagonal matrix $\mathrm{Diag}(a_1, \ldots, a_n)$ is $\mathbb{SL}_n$-equivalent to a diagonal matrix $\mathrm{Diag}(b_1, \ldots, b_n)$ where $b_1 \mid b_2 \mid \cdots \mid b_n$.
Moreover, if we let $\mathfrak{a}_i = \langle a_i \rangle$, $\mathfrak{b}_i = \langle b_i \rangle$, we have $\mathfrak{b}_i = S_i(\mathfrak{a}_1, \ldots, \mathfrak{a}_n)$ where S_i is the "i^{th} elementary symmetric function of $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$" obtained by replacing each product with an intersection. For example,

$$S_2(\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3) = (\mathfrak{a}_1 \cap \mathfrak{a}_2) + (\mathfrak{a}_1 \cap \mathfrak{a}_3) + (\mathfrak{a}_2 \cap \mathfrak{a}_3).$$

In particular, $\mathfrak{b}_1 = \sum_i \mathfrak{a}_i$, $\mathfrak{b}_n = \bigcap_i \mathfrak{a}_i$. Moreover $\prod_i \mathbf{A}/\mathfrak{a}_i \simeq \prod_i \mathbf{A}/\mathfrak{b}_i$.
This last result will be generalized to arithmetic rings (Corollary XII-1.7).
Other "true" elementary symmetric functions of ideals intervene in Exercise 16.

Exercise 8. *(Smith rings, or elementary divisor rings)*
Define a *Smith ring* as a ring over which every matrix admits a reduced Smith form (cf. Section 7, page 206). Such a ring is a strict Bézout ring (cf. Exercise 7). Since over a strict Bézout ring, every square diagonal matrix is equivalent to a Smith matrix (Exercise 7, question *5*), a ring is a Smith ring if and only if every matrix is equivalent to a "diagonal" matrix, without the condition of divisibility over the coefficients. These rings have been studied in particular by Kaplansky in [118], including the noncommutative case, then by Gillman & Henriksen in [92]. Here we will limit ourselves to the commutative case.
Show that the following properties are equivalent.

1. $\mathbf{A}$ is a Smith ring.
2. $\mathbf{A}$ is a strict Bézout ring and every triangular matrix in $\mathbb{M}_2(\mathbf{A})$ is equivalent to a diagonal matrix.

3. **A** is a strict Bézout ring, and if $1 \in \langle a, b, c\rangle$, then there exist (p, q), (p', q') such that $1 = pp'a + qp'b + qq'c$.

4. **A** is a strict Bézout ring, and if $\langle a, b, c\rangle = \langle g\rangle$, then there exist (p, q), (p', q') such that $g = pp'a + qp'b + qq'c$.

This gives a nice structure theorem for finitely presented modules, by taking into account the uniqueness of Theorem 5.1. Also note that this theorem implies the uniqueness of the Smith reduced matrix of a matrix A (by considering the cokernel module) in the following sense. By denoting by b_i the diagonal coefficients of the reduced matrix, the principal ideals $\langle b_1\rangle \supseteq \cdots \supseteq \langle b_q\rangle$ ($q = \inf(m, n)$) are invariants of the matrix A up to equivalence.

In terms of modules, these principal ideals characterize, up to automorphism of $\mathbf{A}^m$, the inclusion morphism $P = \mathrm{Im}(A) \to \mathbf{A}^m$.

A basis $(e_1, \ldots, e_m)$ of $\mathbf{A}^m$ such that $P = b_1\mathbf{A}\, e_1 + \cdots + b_m\mathbf{A}\, e_m$ is called a *basis of* $\mathbf{A}^m$ *adapted to the submodule* P.

Let $b_r = 0$ if $m \geqslant r > n$, then we have $\langle b_1\rangle \supseteq \cdots \supseteq \langle b_r\rangle$. The principal ideals $\neq \langle 1\rangle$ of this list are the invariant factors of the module $M = \mathrm{Coker}(A)$. Theorem 5.1 tells us that this list characterizes the structure of the module M.

Finally, note that the Smith rings are stable under finite products, localization and passage to the quotient.

Exercise 9. *(Elementary example of determination of the group of units)*

1. Let $\mathbf{k}$ be a reduced ring and $\mathbf{A} = \mathbf{k}[Y, Z]/\langle YZ\rangle = \mathbf{k}[y, z]$ with $yz = 0$. Show, by using a Noether positioning of $\mathbf{A}$ over $\mathbf{k}$, that $\mathbf{A}^\times = \mathbf{k}^\times$.

2. Let $\mathbf{A} = \mathbb{Z}[a, b, X, Y]/\langle X - aY, Y - bX\rangle = \mathbb{Z}[\alpha, \beta, x, y]$ with $x = \alpha y$ and $y = \beta x$. Show that $\mathbf{A}^\times = \{\pm 1\}$; we therefore have $\mathbf{A}x = \mathbf{A}y$ but $y \notin \mathbf{A}^\times x$.

Exercise 10. *(Sufficient conditions for the surjectivity of* $\mathbf{A}^\times \to (\mathbf{A}/\mathfrak{a})^\times$*)*

Also see Exercise IX-16.

For an ideal $\mathfrak{a}$ of a ring $\mathbf{A}$, we consider the property $(\star)$

$$(\star) \qquad\qquad \mathbf{A}^\times \to (\mathbf{A}/\mathfrak{a})^\times \text{ is surjective,}$$

i.e. for $x \in \mathbf{A}$ invertible modulo $\mathfrak{a}$, there exists a $y \in \mathbf{A}^\times$ such that $y \equiv x \bmod \mathfrak{a}$, or if $\mathbf{A}x + \mathfrak{a}$ meets $\mathbf{A}^\times$, then $x + \mathfrak{a}$ meets $\mathbf{A}^\times$.

1. Show that $(\star)$ is satisfied when $\mathbf{A}$ is zero-dimensional.

2. If $(\star)$ is satisfied for all principal ideals $\mathfrak{a}$, then it also is for all ideals $\mathfrak{a}$.

3. Assume $(\star)$ is satisfied. Let x, y be two elements of an $\mathbf{A}$-module such that $\mathbf{A}x = \mathbf{A}y$; show that $y = ux$ for some $u \in \mathbf{A}^\times$.

NB: Exercise 9 provides an example of a ring $\mathbf{A}$ with x, $y \in \mathbf{A}$ and $\mathbf{A}x = \mathbf{A}y$, but $y \notin \mathbf{A}^\times x$.

4. Let $\mathbf{A}' = \mathbf{A}/\mathrm{Rad}\,\mathbf{A}$, $\pi : \mathbf{A} \twoheadrightarrow \mathbf{A}'$ be the canonical surjection and $\mathfrak{a}' = \pi(\mathfrak{a})$. Show that if $(\star)$ is satisfied for $(\mathbf{A}', \mathfrak{a}')$, then it is satisfied for $(\mathbf{A}, \mathfrak{a})$.

Exercise 11. *(Computation of a torsion submodule)*
Let $\mathbf{A}$ be an integral coherent ring and M be a finitely presented $\mathbf{A}$-module. Then the torsion submodule of M is a finitely presented module.
More precisely, if we have a presentation matrix E for M with an exact sequence

$$\mathbf{A}^n \xrightarrow{E} \mathbf{A}^\ell \xrightarrow{\pi} M \to 0$$

and if F is a matrix such that we have an exact sequence

$$\mathbf{A}^m \xrightarrow{F} \mathbf{A}^\ell \xrightarrow{{}^{\mathrm{t}}E} \mathbf{A}^n$$

(the existence of the matrix F results from the fact that $\mathbf{A}$ is coherent) then the torsion submodule $\mathrm{T}(M)$ of M is equal to $\pi(\mathrm{Ker}\,{}^{\mathrm{t}}F)$ and isomorphic to $\mathrm{Ker}\,{}^{\mathrm{t}}F/\,\mathrm{Im}\,E$.

Also show that the result can be generalized to the case where $\mathbf{A}$ is a coherent pp-ring.

Exercise 12. *(Euclid's algorithm in the reduced zero-dimensional case)*
Here we give a more uniform version of the proof of Proposition 8.11 and we generalize it. Consider a reduced zero-dimensional ring $\mathbf{A}$.

1. Let $\mathbf{B}$ be an arbitrary ring and $b \in \mathbf{B}$ such that $\langle b \rangle$ is generated by an idempotent. For $a \in \mathbf{B}$, find a matrix $M \in \mathbb{E}_2(\mathbf{B})$ and $d \in \mathbf{B}$ satisfying the equality $M \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} d \\ 0 \end{bmatrix}$. In particular $\langle a, b \rangle = \langle d \rangle$.

2. Give a "uniform" Euclidean algorithm for two polynomials of $\mathbf{A}[X]$.

3. The ring $\mathbf{A}[X]$ is a Smith ring: give an algorithm which reduces every matrix over $\mathbf{A}[X]$ to a Smith form by means of elementary manipulations of rows and of columns.

Exercise 13. *(Syzygies in dimension* 0*)*
Here we give the generalization of the theorem according to which $n+1$ vectors of $\mathbf{K}^n$ are linearly dependent, from the discrete fields case to that of the reduced zero-dimensional rings. Note that the syzygy, to be worthy of the name, must have comaximal coefficients.

Let $\mathbf{K}$ be a reduced zero-dimensional ring, and $y_1, \ldots, y_{n+1} \in \mathbf{K}^n$.

1. Construct a fundamental system of orthogonal idempotents $(e_j)_{j \in [\![1..n+1]\!]}$ such that, in each component $\mathbf{K}[1/e_j]$, the vector y_j is a linear combination of the y_i's that precede it.

2. Deduce that there exists a system of comaximal elements $(a_1, \ldots, a_{n+1})$ in $\mathbf{K}$ such that $\sum_i a_i y_i = 0$.

Remarks. 1) Recall the convention according to which we accept that certain elements of a fundamental system of orthogonal idempotents are null. We see in this example that the statement of the desired property is greatly facilitated by it.

2) We can either give an adequate working of the matrix of the y_i's by elementary manipulations by basing ourselves on Lemma 6.4, or treat the discrete fields case then use the elementary local-global machinery no. 2 (page 213). ■

Exercise 14. Let S_1, …, S_n be comaximal monoids of $\mathbf{A}$. Show that $\mathbf{A}$ is zero-dimensional if and only if each of the $\mathbf{A}_{S_i}$'s is zero-dimensional.

Exercise 15. *(Presentation of an algebra which is free and finite as a module)* Let $\mathbf{B}$ be a free $\mathbf{A}$-algebra of rank n with basis $\underline{e} = (e_1, \dots, e_n)$. We let

$$\varphi : \mathbf{A}[\underline{X}] = \mathbf{A}[X_1, \dots, X_n] \twoheadrightarrow \mathbf{B}$$

be the (surjective) homomorphism of $\mathbf{A}$-algebras which performs $X_i \mapsto e_i$. Let c_{ij}^k be the structure constants defined by $e_ie_j = \sum_k c_{ij}^k e_k$. Consider a_1, …, $a_n \in \mathbf{A}$ defined by $1 = \sum_k a_k e_k$ and let

$$R_0 = 1 - \sum_k a_k X_k, \qquad R_{ij} = X_iX_j - \sum c_{ij}^k X_k.$$

Let $\mathfrak{a} = \langle R_0, R_{ij}, i \leqslant j \rangle$. Show that every $f \in \mathbf{A}[\underline{X}]$ is congruent modulo $\mathfrak{a}$ to a homogeneous polynomial of degree 1. Deduce that $\operatorname{Ker} \varphi = \mathfrak{a}$.

Exercise 16. *(Some computations of Fitting ideals)*

1. Determine the Fitting ideals of an $\mathbf{A}$-module presented by a matrix in Smith form.

2. Determine the Fitting ideals of $\mathbf{A}/\mathfrak{a}$.

3. Let E be a finitely generated $\mathbf{A}$-module and $\mathfrak{a}$ be an ideal. Show that

$$\mathcal{F}_k(E \oplus \mathbf{A}/\mathfrak{a}) = \mathcal{F}_{k-1}(E) + \mathcal{F}_k(E)\,\mathfrak{a}.$$

4. Determine the Fitting ideals of the $\mathbf{A}$-module $M = \mathbf{A}/\mathfrak{a}_1 \oplus \cdots \oplus \mathbf{A}/\mathfrak{a}_n$ in the case where $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots \subseteq \mathfrak{a}_n$.

5. Determine the Fitting ideals of the $\mathbf{A}$-module $M = \mathbf{A}/\mathfrak{a}_1 \oplus \cdots \oplus \mathbf{A}/\mathfrak{a}_n$ without making any inclusion assumptions for the ideals $\mathfrak{a}_k$.
Compare $\mathcal{F}_0(M)$ and $\operatorname{Ann}(M)$.

Exercise 17. *(The Fitting ideals of a finitely generated* **A***-module)*
Show that Facts 9.3, 9.5, 9.7 and Lemma 9.6 remain valid for finitely generated modules.

Exercise 18. One of the characteristic properties of *Prüfer rings* (which will be studied in Chapter XII) is the following: if $A \in \mathbf{A}^{n \times m}$, $B \in \mathbf{A}^{n \times 1}$, and if the determinantal ideals of A and $[\,A\,|\,B\,]$ are the same, then the system of linear equations $AX = B$ admits a solution.

1. Let M be a finitely generated module over a Prüfer ring and N be a quotient of M. Show that if M and N have the same Fitting ideals, then $M = N$.

2. Show that if a finitely generated module M over a Prüfer ring has finitely generated Fitting ideals, then it is a finitely presented module.

Exercise 19. *(Kaplansky ideals)*
For an $\mathbf{A}$-module M and an integer r we denote by $\mathcal{K}_r(M)$ the ideal which is a sum of all the conductors $\big(\langle m_1, \dots m_r \rangle : M\big)$ for all the systems $(m_1, \dots m_r)$ in M. We call it *the Kaplansky ideal of order r of the module M*. Thus, $\mathcal{K}_0(M) = \operatorname{Ann}(M)$, and if M is generated by q elements, we have $\mathcal{K}_q(M) = \langle 1 \rangle$.

- Show that if $\mathcal{K}_q(M) = \langle 1 \rangle$, M is finitely generated.

- Show that if M is finitely generated, then for every integer r we have the inclusions
$$\mathcal{F}_r(M) \subseteq \mathcal{K}_r(M) \subseteq \sqrt{\mathcal{F}_r(M)} = \sqrt{\mathcal{K}_r(M)}.$$

NB: see also Exercise IX-12.

Exercise 20. *(An elementary example of resultant ideals)*
Let f, g_1, $\ldots$, $g_r \in \mathbf{A}[X]$, f be monic of degree $d \geqslant 1$ and $\mathfrak{f} = \langle f, g_1, \ldots, g_r\rangle \subseteq \mathbf{A}[X]$. We will compare the ideal
$$\mathfrak{a} = \mathfrak{R}(f, g_1, \ldots, g_r) = \mathrm{c}_T\big(\mathrm{Res}(f, g_1 + g_2T + \cdots + g_rT^{r-1})\big)$$
(Section III-9), and the resultant ideal $\mathfrak{b} = \mathfrak{Res}(\mathfrak{f}) = \mathcal{F}_{\mathbf{A},0}(\mathbf{A}[X]/\mathfrak{f})$ (see the general elimination lemma of Section 10).

1. Let $\mathfrak{a}' = \mathrm{c}_{\underline{T}}\big(\mathrm{Res}(f, g_1T_1 + g_2T_2 + \cdots + g_rT_r)\big)$. Show the inclusions
$$\mathfrak{a} \subseteq \mathfrak{a}' \subseteq \mathfrak{b} \subseteq \mathfrak{f} \cap \mathbf{A}.$$

2. Let $\mathbf{A} = \mathbb{Z}[a, b, c]$ where a, b, c are three indeterminates, $f = X^d$, $g_1 = a$, $g_2 = b$ and $g_3 = c$. Determine the ideals $\mathfrak{f} \cap \mathbf{A}$, $\mathfrak{a}$, $\mathfrak{a}'$, $\mathfrak{b}$ and check that they are distinct. Also check that $\mathfrak{R}(f, g_1, g_2, g_3)$ depends on the order of the g_i's.
Do we have $(\mathfrak{f} \cap \mathbf{A})^d \subseteq \mathfrak{a}$?

Exercise 21. *(Relators and elimination ideal)*
Let $f_1(\underline{X}), \ldots, f_s(\underline{X}) \in \mathbf{k}[\underline{X}] = \mathbf{k}[X_1, \ldots, X_n]$ ($\mathbf{k}$ is a commutative ring).
Let $\mathfrak{a} \subseteq \mathbf{k}[\underline{Y}] = \mathbf{k}[Y_1, \ldots, Y_s]$ be the ideal of the relators over $\mathbf{k}$ of $(f_1, \ldots, f_s)$, i.e. $\mathfrak{a} = \operatorname{Ker}\varphi$, where $\varphi : \mathbf{k}[\underline{Y}] \to \mathbf{k}[\underline{X}]$ is the evaluation morphism $Y_i \mapsto f_i$.
Let $g_i = f_i(\underline{X}) - Y_i \in \mathbf{k}[\underline{Y}, \underline{X}]$ and $\mathfrak{f} = \langle g_1, \ldots, g_s\rangle$.
Prove that $\mathfrak{a} = \mathfrak{f} \cap \mathbf{k}[\underline{Y}]$. Thus, $\mathfrak{a}$ is the elimination ideal of the variables X_j in the polynomial system of the g_i's.

Problem 1. *(An example of a zero-dimensional system)*
Let $\mathbf{k}$ be a ring and a, b, $c \in \mathbb{N}^*$ with $a \leqslant b \leqslant c$ and at least one strict inequality. We define three polynomials $f_i \in \mathbf{k}[X, Y, Z]$
$$f_1 = X^c + Y^b + Z^a, \quad f_2 = X^a + Y^c + Z^b, \quad f_3 = X^b + Y^a + Z^c.$$
This is a matter of studying the system defined by these three polynomials. We denote by $\mathbf{A} = \mathbf{k}[x, y, z]$ the $\mathbf{k}$-algebra $\mathbf{k}[X, Y, Z]/\langle f_1, f_2, f_3\rangle$.

1. For an arbitrary ring $\mathbf{k}$, is $\mathbf{A}$ free and finite over $\mathbf{k}$? If so, compute a basis and give the dimension.

2. Give a detailed study of the system for $\mathbf{k} = \mathbb{Q}$ and $(a, b, c) = (2, 2, 3)$. That is, determine all the zeros of the system in a certain finite extension of $\mathbb{Q}$ (to be specified), their number and their multiplicities.

3. Is the localized algebra $\mathbf{A}_{1+\langle x,y,z\rangle}$ free over $\mathbf{k}$? If so, give a basis.

Problem 2. *(The generic resultant ideal)*
Let d, r be two fixed integers with $d \geqslant 1$. In this exercise we study the generic resultant ideal $\mathfrak{b} = \mathfrak{Res}(f, g_1, \dots, g_r)$ where f is monic of degree d, and g_1, …, g_r are of degree $d-1$, the coefficients of these polynomials being indeterminates over $\mathbb{Z}$. The base ring is therefore $\mathbf{k} = \mathbb{Z}[(a_i)_{i\in[\![1..d]\!]}, (b_{ji})_{j\in[\![1..r]\!], i\in[\![1..d]\!]}]$ with

$$f = X^d + \sum\nolimits_{i=1}^{d} a_i X^{d-i} \quad \text{and} \quad g_j = \sum\nolimits_{i=1}^{d} b_{ji} X^{d-i}.$$

1. Put weights on the a_i's and b_{ij}'s such that $\mathfrak{b}$ is a homogeneous ideal.

2. If S is the generalized Sylvester matrix of $(f, g_1, \dots, g_r)$, specify the weight of the coefficients of S and those of its minors of order d.

3. Using a Computer Algebra system, study the minimal number of generators of $\mathfrak{b}$. We could replace $\mathbb{Z}$ with $\mathbb{Q}$, introduce the ideal $\mathfrak{m}$ of $\mathbf{k}$ generated by all the indeterminates and consider $E = \mathfrak{b}/\mathfrak{m}\mathfrak{b}$ which is a finite dimensional vector space over $\mathbf{k}/\mathfrak{m} = \mathbb{Q}$.

Problem 3. *(Homogeneous Nakayama lemma and regular sequences)*
1. (Regular sequence and algebraic independence) Let $(a_1, \dots, a_n)$ be a regular sequence of a ring $\mathbf{A}$ and $\mathbf{k} \subseteq \mathbf{A}$ be a subring such that $\mathbf{k} \cap \langle a_1, \dots, a_n \rangle = \{0\}$. Show that a_1, …, a_n are algebraically independent over $\mathbf{k}$.

2. (Homogeneous Nakayama lemma) Let $\mathbf{A} = \mathbf{A}_0 \oplus \mathbf{A}_1 \oplus \mathbf{A}_2 \oplus \dots$ be a graded ring and $E = E_0 \oplus E_1 \oplus E_2 \oplus \dots$ be a graded $\mathbf{A}$-module.
We denote by $\mathbf{A}_+$ the ideal $\mathbf{A}_1 \oplus \mathbf{A}_2 \oplus \dots$, so that $\mathbf{A}/\mathbf{A}_+ \simeq \mathbf{A}_0$.

- *a.* Show that if $\mathbf{A}_+ E = E$, then $E = 0$.
- *b.* Let $(e_i)_{i\in I}$ be a family of homogeneous elements of E. Show that if the e_i's generate the $\mathbf{A}_0$-module $E/\mathbf{A}_+E$, then they generate the $\mathbf{A}$-module E.

Note that we do not assume that E is finitely generated.

3. Let $\mathbf{B} = \mathbf{B}_0 \oplus \mathbf{B}_1 \oplus \mathbf{B}_2 \oplus \dots$ be a graded ring and h_1, …, h_d be homogeneous elements of the ideal $\mathbf{B}_+$. Let $\mathfrak{b} = \langle h_1, \dots, h_d \rangle$ and $\mathbf{A} = \mathbf{B}_0[h_1, \dots, h_d]$. We therefore have $\mathbf{B}_0 \cap \mathfrak{b} = \{0\}$, and $\mathbf{A}$ is a graded subring of $\mathbf{B}$. Finally, let $(e_i)_{i\in I}$ be a family of homogeneous elements of $\mathbf{B}$ that generate the $\mathbf{B}_0$-module $\mathbf{B}/\mathfrak{b}$.

- *a.* Verify that $\mathbf{A}_0 = \mathbf{B}_0$ and that $\mathfrak{b} = \mathbf{A}_+\mathbf{B}$ then show that the e_i's form a generator set of the $\mathbf{A}$-module $\mathbf{B}$.
- *b.* Suppose that $(h_1, \dots, h_d)$ is a regular sequence and that the e_i's form a basis of the $\mathbf{B}_0$-module $\mathbf{B}/\mathfrak{b}$. Show that h_1, …, h_d are algebraically independent over $\mathbf{B}_0$ and that the e_i's form a basis of the $\mathbf{A}$-module $\mathbf{B}$.

Recap: Let $\mathbf{B} = \mathbf{B}_0 \oplus \mathbf{B}_1 \oplus \mathbf{B}_2 \oplus \dots$ be a graded ring and $(h_1, \dots, h_d)$ be a homogeneous regular sequence of the ideal $\mathbf{B}_+$. If $\mathbf{B}/\langle h_1, \dots, h_d \rangle$ is a free $\mathbf{B}_0$-module, then $\mathbf{B}$ is a free $\mathbf{B}_0[h_1, \dots, h_d]$-module and $\mathbf{B}_0[h_1, \dots, h_d]$ is a ring of polynomials in $(h_1, \dots, h_d)$.

4. As a converse. Let $\mathbf{B} = \mathbf{B}_0 \oplus \mathbf{B}_1 \oplus \mathbf{B}_2 \oplus \dots$ be a graded ring and h_1, …, h_d be homogeneous elements of the ideal $\mathbf{B}_+$, algebraically independent over $\mathbf{B}_0$. If $\mathbf{B}$ is a free $\mathbf{B}_0[h_1, \dots, h_d]$-module, then the sequence $(h_1, \dots, h_d)$ is regular.

Some solutions, or sketches of solutions

Exercise 2. It suffices to apply Proposition 4.2. Directly: we consider a projector $\pi : N \to N$ having M as its image. If X is a generator set of N, then $\pi(X)$ is a generator set of M. If N is finitely presented, the syzygy module for $\pi(X)$ is obtained by taking the syzygies for X in N and the syzygies $\pi(x) = x$ for each element x of X.

Exercise 3. We start by noting that $\theta_A \circ (X\mathrm{I}_n - A) = 0$ and that θ_A is the identity over $\mathbf{A}^n$.

1. Let us show that $\mathrm{Im}(X\mathrm{I}_n - A) \cap \mathbf{A}^n = 0$. Let $x \in \mathrm{Im}(X\mathrm{I}_n - A) \cap \mathbf{A}^n$, the preliminary computations give $\theta_A(x) = x$ and $\theta_A(x) = 0$. Let us show that $\mathbf{A}[X]^n = \mathrm{Im}(X\mathrm{I}_n - A) + \mathbf{A}^n$. It suffices to show that $X^k e_i \in \mathrm{Im}(X\mathrm{I}_n - A) + \mathbf{A}^n$ for $k \geqslant 0$ and $i \in [\![1..n]\!]$. If $k = 0$ it is clear. For $k > 0$ we write

$$X^k\mathrm{I}_n - A^k = (X\mathrm{I}_n - A) \textstyle\sum_{j+\ell=k-1} X^j A^\ell.$$

By applying this equality to e_i, we obtain $X^k e_i - A^k e_i \in \mathrm{Im}(X\mathrm{I}_n - A)$, so $X^k e_i$ belongs to $\mathrm{Im}(X\mathrm{I}_n - A) + A^k e_i \subseteq \mathrm{Im}(X\mathrm{I}_n - A) + \mathbf{A}^n$.

2. Let $y \in \mathrm{Ker}\,\theta_A$. Let $y = z + w$ with $z \in \mathrm{Im}(X\mathrm{I}_n - A)$ and $w \in \mathbf{A}^n$.
Therefore $0 = \theta_A(y) = \theta_A(z) + \theta_A(w) = 0 + w$ and $y = z \in \mathrm{Im}(X\mathrm{I}_n - A)$.

Exercise 4. (Description of the null tensors, general situation)
1. This results from the definition of the tensor product and from the fact that in algebra, computations are finite.
2. Let $X = [\,x_1 \,\cdots\, x_p\,] \in M_1^{1\times p}$, $Y = {}^{\mathrm{t}}[\,y_1 \,\cdots\, y_p\,] \in N^{p\times 1}$.
We have $M_1 = \mathbf{A}x_1 + \cdots + \mathbf{A}x_p$ and $\sum_{i\in[\![1..p]\!]} x_i \otimes y_i =_{M_1\otimes N} 0$, and by the null tensor lemma, this equality holds if and only if there exist $q \in \mathbb{N}$, $G \in \mathbf{A}^{p\times q}$ and $Z = {}^{\mathrm{t}}[\,z_1 \,\cdots\, z_q\,] \in N^{q\times 1}$ that satisfy

$$XG =_{M^q} 0 \quad \text{and} \quad GZ =_{N^p} Y\,.$$

Exercise 7. *1* and *2* are left to the reader.

3. By construction, ε annihilates d_2 (i.e. annihilates a, b). We therefore have the equalities

$$d_2 \begin{bmatrix} a_2 \\ b_2 \end{bmatrix} = \begin{bmatrix} v_1 & a_1 \\ -u_1 & b_1 \end{bmatrix} \begin{bmatrix} d_2\varepsilon \\ d_2k_{12} \end{bmatrix} = \begin{bmatrix} v_1 & a_1 \\ -u_1 & b_1 \end{bmatrix} \begin{bmatrix} 0 \\ d_1 \end{bmatrix} = d_1 \begin{bmatrix} a_1 \\ b_1 \end{bmatrix} = \begin{bmatrix} a \\ b \end{bmatrix}$$

It remains to see that $1 \in \langle a_2, b_2\rangle$. By inverting the 2×2 matrix in $(\star)$ (of determinant 1), we see that the ideal $\langle a_2, b_2\rangle$ contains ε and k_{12}, so it contains $1 = k_{12}k_{21} - \varepsilon$.

4. By induction on n, $n = 2$ being the previous question. Suppose $n \geqslant 3$. By induction, there exist d and comaximal $b_1, \ldots, b_{n-1}$ such that

$$(a_1, \ldots, a_{n-1}) = d(b_1, \ldots, b_{n-1}), \text{ so } \langle \underline{a}\rangle = \langle d, a_n\rangle\,.$$

Item *3* gives comaximal u, v and δ such that $(d, a_n) = \delta(u, v)$.
Then $(a_1, \ldots, a_n) = (db_1, \ldots, db_{n-1}, \delta v) = \delta(ub_1, \ldots, ub_{n-1}, v)$, and $\langle 1\rangle = \langle u, v\rangle = \langle ub_1, \ldots, ub_{n-1}, v\rangle$.

5. First for $n = 2$ with (a, b). There is a d with $(a, b) = d(a', b')$ and $1 = ua' + vb'$. Let $m = da'b' = ab' = ba' \in \langle a\rangle \cap \langle b\rangle$; we have $\langle a\rangle \cap \langle b\rangle = \langle m\rangle$ because if

$x \in \langle a \rangle \cap \langle b \rangle$, then $x = x(ua' + vb') \in \langle ba' \rangle + \langle ab' \rangle = \langle m \rangle$. The $\mathbb{SL}_2(\mathbf{A})$-equivalence is provided by the equality below

$$\begin{bmatrix} 1 & -1 \\ vb' & ua' \end{bmatrix} \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} = \begin{bmatrix} d & 0 \\ 0 & m \end{bmatrix} \begin{bmatrix} a' & -b' \\ v & u \end{bmatrix}.$$

For $n \geqslant 3$. By using the $n = 2$ case for the positions $(1,2)$, $(1,3)$, …, $(1,n)$, we obtain $\mathrm{Diag}(a_1, a_2, \ldots, a_n) \sim \mathrm{Diag}(a_1', a_2', \ldots, a_n')$ with $a_1' \mid a_i'$ for $i \geqslant 2$.
By induction, $\mathrm{Diag}(a_2', \ldots, a_n') \sim \mathrm{Diag}(b_2, \ldots, b_n)$ where $b_2 \mid b_3 \cdots \mid b_n$. We then check that $a_1' \mid b_2$ and we let $b_1 = a_1'$. The scrupulous reader will check the property regarding elementary symmetric functions.

Exercise 8. *(Smith rings, or elementary divisor rings)*
Preliminary computation with $A = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$ and B of the form

$$B = \begin{bmatrix} p' & q' \\ * & * \end{bmatrix} A \begin{bmatrix} p & * \\ q & * \end{bmatrix}.$$

The coefficient b_{11} of B is equal to $b_{11} = p'(pa + qb) + q'qc$.

2 ⇒ *3.* The matrix A is equivalent to a diagonal matrix $\mathrm{Diag}(g, h)$, which gives (p, q) and (p', q') comaximal with $g = p'(pa+qb)+q'qc$ (preliminary computation), and we have $\langle a, b, c \rangle = \langle g, h \rangle$. As $\mathbf{A}$ is a strict Bézout ring, we can suppose that $g \mid h$ and since $1 \in \langle a, b, c \rangle$, g is invertible and so 1 is expressed as required.

3 ⇒ *4.* Beware, here g is imposed. But by question *4* of Exercise 7, we can write $(a, b, c) = g\,(a', b', c')$ with (a', b', c') comaximal. We apply item *3* to (a', b', c') and multiply the obtained result by g.

4 ⇒ *2.* Let $A \in \mathbb{M}_2(\mathbf{A})$ be triangular, $A = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$. With the parameters of item *4*, we construct (preliminary computation) a matrix B equivalent to A with coefficient $b_{11} = g$. As g divides all the coefficients of B, we have $B \overset{\mathbb{E}_2(\mathbf{A})}{\sim} \mathrm{Diag}(g, h)$.

1 ⇔ *2.* Left to the reader (who can consult Kaplansky's paper).

Exercise 9. *1.* Let $s = y + z$. Then $\mathbf{k}[s]$ is a polynomial ring in s, and y, z are integral over $\mathbf{k}[s]$, because they are zeros of $(T - y)(T - z) = T(T - s) \in \mathbf{k}[s][T]$. We easily check that $\mathbf{A}$ is free over $\mathbf{k}[s]$ with $(1, y)$ as its basis. For u, $v \in \mathbf{k}[s]$, the norm over $\mathbf{k}[s]$ of $u + vy$ is

$$\mathrm{N}_{\mathbf{A}/\mathbf{k}[s]}(u + vy) = (u + vy)(u + vz) = u^2 + suv = u(u + sv).$$

The element $u + vy$ is invertible in $\mathbf{A}$ if and only if $u(u + sv)$ is invertible in $\mathbf{k}[s]$. As $\mathbf{k}$ is reduced, $(\mathbf{k}[s])^\times = \mathbf{k}^\times$. Therefore $u \in \mathbf{k}^\times$ and $v = 0$.

2. We have $\mathbf{A} = \mathbb{Z}[\alpha, \beta, y] = \mathbb{Z}[a, b, Y]/\langle (ab - 1)Y \rangle$ with $y(\alpha\beta - 1) = 0$. Let t be an indeterminate over $\mathbb{Z}$ and $\mathbf{k} = \mathbb{Z}[t, t^{-1}]$. Consider the $\mathbf{k}$-algebra $\mathbf{k}[y, z]$ with the sole syzygy $yz = 0$. We have a morphism $\mathbf{A} \to \mathbf{k}[y, z]$ which performs

$$\alpha \mapsto t(z + 1),\ \beta \mapsto t^{-1},\ y \mapsto y,$$

and we check that it is an injection.
Then an element $w \in \mathbf{A}^\times$ is also in $\mathbf{k}[y, z]^\times$, and as $\mathbf{k}$ is reduced, $w \in \mathbf{k}^\times$. Finally, the units of $\mathbf{k} = \mathbb{Z}[t, t^{-1}]$ are the $\pm t^k$ with $k \in \mathbb{Z}$, so $w = \pm 1$.

Exercise 10. *1.* We know that $\langle x^n\rangle = \langle e\rangle$. We look for $y \in \mathbf{A}^\times$ such that $y \equiv x \bmod \mathfrak{a}$ over the components $\mathbf{A}_e$ and $\mathbf{A}_{1-e}$. First, we have $x^n(1 - ax) = 0$ and x invertible modulo $\mathfrak{a}$, so $ax \equiv 1 \bmod \mathfrak{a}$ then $e \equiv 1 \bmod \mathfrak{a}$, i.e. $1 - e \in \mathfrak{a}$.
In the component $\mathbf{A}_e$, x is invertible, so we can take $y = x$. In the component $\mathbf{A}_{1-e}$, $1 \in \mathfrak{a}$, so we can take $y = 1$. Globally, we therefore propose that $y = ex + 1 - e$ which is indeed invertible (with inverse $ea^n x^{n-1} + 1 - e$) and which satisfies $y \equiv x \bmod \mathfrak{a}$. Remark: $y = ex + (1 - e)u$ with $u \in \mathbf{A}^\times$ is also suitable.

2. Let x be invertible modulo $\mathfrak{a}$ so $1 - ax \in \mathfrak{a}$ for some $a \in \mathbf{A}$.
Then, x is invertible modulo the principal ideal $\langle 1 - ax\rangle$, therefore there exists a $y \in \mathbf{A}^\times$ such that $y \equiv x \bmod \langle 1 - ax\rangle$, a fortiori $y \equiv x \bmod \mathfrak{a}$.

3. We write $y = bx$, $x = ay$ so $(1 - ab)x = 0$; b is invertible modulo $\langle 1 - ab\rangle$ so there exists a $u \in \mathbf{A}^\times$ such that $u \equiv b \bmod \langle 1 - ab\rangle$ whence $ux = bx = y$.

4. Let x be invertible modulo $\mathfrak{a}$. Then $\pi(x)$ is invertible modulo $\mathfrak{a}'$, whence $y \in \mathbf{A}$ such that $\pi(y)$ is invertible in $\mathbf{A}'$ and $\pi(y) \equiv \pi(x) \bmod \mathfrak{a}'$. Then, y is invertible in $\mathbf{A}$ and $y - x \in \mathfrak{a} + \operatorname{Rad}\mathbf{A}$, i.e. $y = x + a + z$ with $a \in \mathfrak{a}$ and $z \in \operatorname{Rad}\mathbf{A}$. Thus, the element $y - z$ is invertible in $\mathbf{A}$, and $y - z \equiv x \bmod \mathfrak{a}$.

Exercise 11. Let us call $\mathbf{A}_1$ the quotient field of $\mathbf{A}$ and let us put an index 1 to indicate that we are performing a scalar extension from $\mathbf{A}$ to $\mathbf{A}_1$. Thus M_1 is the $\mathbf{A}_1$-vector space corresponding to the exact sequence

$$\mathbf{A}_1^n \xrightarrow{E_1} \mathbf{A}_1^\ell \xrightarrow{\pi_1} M_1 \to 0$$

and the submodule $\mathrm{T}(M)$ of M is the kernel of the natural $\mathbf{A}$-linear map from M to M_1, i.e. the module $\pi(\mathbf{A}^\ell \cap \operatorname{Ker}\pi_1)$, or the module $\pi(\mathbf{A}^\ell \cap \operatorname{Im} E_1)$ (by regarding $\mathbf{A}^\ell$ as a submodule of $\mathbf{A}_1^\ell$).

The exact sequence $\mathbf{A}^m \xrightarrow{F} \mathbf{A}^\ell \xrightarrow{{}^{\mathrm{t}}E} \mathbf{A}^n$ gives by localization the exact sequence

$$\mathbf{A}_1^m \xrightarrow{F_1} \mathbf{A}_1^\ell \xrightarrow{{}^{\mathrm{t}}E_1} \mathbf{A}_1^n$$

and since $\mathbf{A}_1$ is a discrete field this gives by duality the exact sequence

$$\mathbf{A}_1^n \xrightarrow{E_1} \mathbf{A}_1^\ell \xrightarrow{{}^{\mathrm{t}}F_1} \mathbf{A}_1^m.$$

Thus $\operatorname{Im} E_1 = \operatorname{Ker}{}^{\mathrm{t}}F_1$, so $\mathbf{A}^\ell \cap \operatorname{Im} E_1 = \mathbf{A}^\ell \cap \operatorname{Ker}{}^{\mathrm{t}}F_1$. Finally, we have the equality $\mathbf{A}^\ell \cap \operatorname{Ker}{}^{\mathrm{t}}F_1 = \operatorname{Ker}{}^{\mathrm{t}}F$ because the natural morphism $\mathbf{A} \to \mathbf{A}_1$ is injective.
Conclusion: $\mathrm{T}(M)$ is equal to $\pi(\operatorname{Ker}{}^{\mathrm{t}}F)$, isomorphic to $\operatorname{Ker}{}^{\mathrm{t}}F/\operatorname{Im} E$, and therefore is finitely presented (because $\mathbf{A}$ is coherent).

If $\mathbf{A}$ is a coherent pp-ring, the total ring of fractions $\mathbf{A}_1 = \operatorname{Frac}\mathbf{A}$ is reduced zero-dimensional, and all the arguments given in the integral case work similarly.

Exercise 12. All the results can be obtained from the discrete field case, for which the algorithms are classical, by using the elementary local-global machinery of zero-dimensional rings. Here we will clarify this very general affirmation.
Let us put two preliminary remarks for an arbitrary ring $\mathbf{A}$.
First, let e be idempotent and E be an elementary matrix modulo $1 - e$. If we lift E to a matrix $F \in \mathbb{M}_n(\mathbf{A})$, then the matrix $(1 - e)\mathrm{I}_n + eF \in \mathbb{E}_n(\mathbf{A})$ is elementary, it acts like E in the component $\mathbf{A}/\langle 1 - e\rangle$, and it does nothing in the component $\mathbf{A}/\langle e\rangle$. This allows us to understand how we can retrieve the desired results over $\mathbf{A}$ by using analogous results modulo the idempotents $1 - e_i$ when we

have a fundamental system of orthogonal idempotents $(e_1,\dots,e_k)$ (provided by the algorithm that we build).
Second, if $g \in \mathbf{A}[X]$ is monic of degree $m \geqslant 0$, for all $f \in \mathbf{A}[X]$, we can divide f by g: $f = gq + r$ with r of formal degree $m-1$.

1. Let e be the idempotent such that $\langle e\rangle = \langle b\rangle$. It suffices to solve the question modulo e and $1-e$. In the branch $e=1$, b is invertible, $\langle a,b\rangle = \langle 1\rangle$ and the problem is solved (Gauss pivot). In the branch $e=0$, b is null and the problem is solved. If $e = bx$, we find $d = e + (1-e)a$ and

$$M = \mathrm{E}_{21}(-be)\mathrm{E}_{12}\big(ex(1-a)\big) = \begin{bmatrix} 1 & ex(1-a) \\ -eb & ae+(1-e) \end{bmatrix}.$$

2. We start from two polynomials f and g. We will build a polynomial h and a matrix $M \in \mathbb{E}_2(\mathbf{A}[X])$ such that $M\begin{bmatrix} f \\ g \end{bmatrix} = \begin{bmatrix} h \\ 0 \end{bmatrix}$. A fortiori $\langle f,g\rangle = \langle h\rangle$.
We proceed by induction on m, the formal degree of g, with formally leading coefficient b. If we initiate the induction at $m=-1$, $g=0$ and $\mathrm{I}_2\begin{bmatrix} f \\ g \end{bmatrix} = \begin{bmatrix} f \\ 0 \end{bmatrix}$, we can treat $m=0$, with $g \in \mathbf{A}$ and use item *1* ($\mathbf{B} = \mathbf{A}[X]$, $a=f$, $b=g$). But it is pointless to treat this case separately (and so we no longer use item *1*). Indeed, if e is the idempotent such that $\langle e\rangle = \langle b\rangle$, it suffices to solve the question modulo e and $1-e$ and what follows holds for all $m \geqslant 0$.
In the branch $e=1$, b is invertible, and since $m \geqslant 0$, we can perform a classical Euclidean division of f by g: $f = qg - r$ with the formal degree of r equal to $m-1$. We get a matrix $N \in \mathbb{E}_2(\mathbf{A}[X])$ such that $N\begin{bmatrix} f \\ g \end{bmatrix} = \begin{bmatrix} g \\ r \end{bmatrix}$, namely $N = \begin{bmatrix} 0 & 1 \\ -1 & q \end{bmatrix}$. We can then apply the induction hypothesis.
In the branch $e=0$, g is of formal degree $m-1$ and the induction hypothesis applies.

In the following, we use item *2* by saying that we pass from ${}^{\mathrm{t}}[\,f\ g\,]$ to ${}^{\mathrm{t}}[\,h\ 0\,]$ by means of "Bézout manipulations."

3. By relying on the result of item *2* we are inspired by the proof of Proposition 7.3 (a PID is a Smith ring). If we were in a nontrivial discrete field, the algorithm would terminate in a finite number of steps which can be directly bounded in terms of (D,m,n), where D is the maximum degree of the coefficients of the matrix $M \in \mathbf{A}[X]^{m\times n}$ that we want to reduce to the Smith form. It follows that when $\mathbf{A}$ is reduced zero-dimensional the number of splittings produced by the gcd computations (as in item *2*) is also bounded in terms of (D,m,n), where D is now the maximum formal degree of the entries of the matrix. This shows that the complete algorithm, given the preliminary remark, also terminates in a number of steps bounded in terms of (D,m,n).

Remark. The algorithms do not require that $\mathbf{A}$ be discrete. ■

Exercise 15. It is clear that $\mathfrak{a} \subseteq \operatorname{Ker}\varphi$. Let $\mathcal{E} \subseteq \mathbf{A}[\underline{X}]$ be the set of polynomials f congruent modulo $\mathfrak{a}$ to a homogeneous polynomial of degree 1.
We have $1 \in \mathcal{E}$ and $f \in \mathcal{E} \Rightarrow X_i f \in \mathcal{E}$ because if $f \equiv \sum_j \alpha_j X_j \bmod \mathfrak{a}$, then

$$X_i f \equiv \textstyle\sum_j \alpha_j X_i X_j \equiv \sum_{j,k} \alpha_j c_{ij}^k X_k \bmod \mathfrak{a}.$$

Therefore $\mathcal{E} = \mathbf{A}[\underline{X}]$. Let $f \in \operatorname{Ker}\varphi$. We write $f \equiv \sum_k \alpha_k X_k \bmod \mathfrak{a}$.
Then $\varphi(f) = 0 = \sum_k \alpha_k e_k$, so $\alpha_k = 0$, then $f \in \mathfrak{a}$.

Exercise 16.
2. If $\mathfrak{a}$ is finitely generated a presentation matrix of the module $M = \mathbf{A}/\mathfrak{a}$ is a matrix row L having for coefficients generators of the ideal. We deduce that $\mathcal{D}_1(L) = \mathfrak{a}$. Therefore $\mathcal{F}_{-1}(M) = 0 \subseteq \mathcal{F}_0(M) = \mathfrak{a} \subseteq \mathcal{F}_1(M) = \langle 1 \rangle$. The result can be generalized to an arbitrary ideal $\mathfrak{a}$.

3. Results from *2* and Fact 9.7.

4 and *5.* In the general case by applying *2* and *3* we find

$$\mathcal{F}_0(M) = \textstyle\prod_{i=1}^n \mathfrak{a}_i,\ \mathcal{F}_{n-1}(M) = \sum_{i=1}^n \mathfrak{a}_i,$$

and for the intermediate ideals the “symmetric functions”

$$\mathcal{F}_{n-k}(M) = \textstyle\sum_{1 \leqslant i_1 < \ldots < i_k \leqslant n} \prod_{\ell=1}^k \mathfrak{a}_{i_\ell}.$$

In addition, $\operatorname{Ann}(M) = \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n$.
When $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots \subseteq \mathfrak{a}_n$ the result is a little simpler

$$\mathcal{F}_{n-1}(M) = \mathfrak{a}_n,\ \mathcal{F}_{n-2}(M) = \mathfrak{a}_n\,\mathfrak{a}_{n-1},\ \ldots\quad \mathcal{F}_{n-k}(M) = \mathfrak{a}_n \cdots \mathfrak{a}_{n-k+1}.$$

We then find for item *1* the result of the direct computation given by the determinantal ideals of a matrix in Smith form.

Exercise 18. Let us prove item *1* (afterwards we can apply Fact 9.8).
Take $M = \langle g_1, \ldots, g_q \rangle$. Consider a syzygy $\sum_i \alpha_i g_i =_N 0$. The aim is to show that the column vector $V = (\alpha_1, \ldots, \alpha_q)$ is a syzygy in M.

First case, M is finitely presented.
Adding the V column to a presentation matrix F of M for $(g_1, \ldots, g_q)$ does not change the determinantal ideals of this matrix, so V is a linear combination of the columns of F.

Second case, M is finitely generated.
Since $\mathcal{D}_1(V) \subseteq \mathcal{F}_{q-1}(M)$, there exists a matrix F_1 of syzygies for $(g_1, \ldots, g_q)$ in M with $\mathcal{D}_1(V) \subseteq \mathcal{D}_1(F_1)$. Since $\mathcal{D}_2(V|F_1) \subseteq \mathcal{F}_{q-2}(M)$, there exists a matrix F_2 of syzygies for $(g_1, \ldots, g_q)$ in M with $\mathcal{D}_2(V|F_1) \subseteq \mathcal{D}_2(F_1|F_2)$, but also of course $\mathcal{D}_1(V|F_1) \subseteq \mathcal{D}_1(F_1|F_2)$, and so on until there exists a matrix $F = [\,F_1 \mid \cdots \mid F_q\,]$ of syzygies for $(g_1, \ldots, g_q)$ in M such that the determinantal ideals of $[V|F]$ are contained in those of F. Therefore V is a linear combination of the columns of F.

Exercise 19. If a Kaplansky ideal is equal to 1, then the module is finitely generated, because the module is finitely generated in the localized rings $\mathbf{A}[1/a_i]$'s with the a_i's being comaximal.
Key idea: the Kaplansky ideals are a little more general, but apparently useless in the case where the module is not finitely generated. The Kaplansky ideals present the advantage over the Fitting ideals of allowing a characterization of the finitely generated modules.

For the second item, here is what happens.
If a is a typical generator of $\mathcal{K}_r(M)$ and if M is generated by $(g_1, ..., g_q)$, we know that there exists $(h_1, ..., h_r)$ in M such that aM is contained in $\langle h_1, ..., h_r \rangle$.
A matrix of syzygies for the generator set $(g_1, ..., g_q, h_1, ..., h_r)$ is then of the following form $\begin{bmatrix} a\mathrm{I}_q \\ B \end{bmatrix}$ with B of size $r \times q$. This simply means that we can express ag_j in terms of the h_i's. Therefore in the Fitting ideal of order r of the module there is a typical generator which is the determinant of $a\mathrm{I}_q$ i.e. a^q. Thus, every typical generator of the Kaplansky ideal is in the nilradical of the corresponding Fitting ideal. Note that the exponent that intervenes here is simply the number of generators of the module.
Now if a is a typical generator of $\mathcal{F}_r(M)$ we obtain a as a minor of order $q - r$ for a matrix of syzygies between q generators $(g_1, ..., g_q)$. Even if it involves renumbering the generators, this matrix can be expressed as $\begin{bmatrix} N \\ D \end{bmatrix}$ where D is a square matrix of order $q - r$, N is an $r \times (q - r)$ matrix, and $\det D = a$.
By linear combinations of the columns (precisely by right-multiplying by the cotransposed matrix of D) we obtain other syzygies for the same generators in the form $\begin{bmatrix} N' \\ a\mathrm{I}_{q-r} \end{bmatrix}$ and this implies that the last $q-r$ generators multiplied by a fall in the module generated by the first r generators. In short every typical generator of the Fitting ideal is also a typical generator of the corresponding Kaplansky ideal.

Exercise 20.
2. We have $\mathfrak{f} \cap \mathbf{A} = \langle a, b, c \rangle$ (if $x \in \mathbf{A}$ satisfies $x \in \left\langle X^d, a, b, c \right\rangle_{\mathbf{A}[X]}$, make $X := 0$), and also $\mathfrak{b} = \langle a, b, c \rangle^d$. The ideal $\mathfrak{a}$ is the content in T of the polynomial $(a + bT + cT^2)^d$ whereas $\mathfrak{a}'$ is the content in $\underline{T}$ of the polynomial $(aT_1 + bT_2 + cT_3)^d$. For example for $d = 2$:

$$\mathfrak{a} = \left\langle a^2, ab^2, 2ab, 2ac + b^2, b^3, b^2c, 2bc, c^2 \right\rangle, \quad \mathfrak{a}' = \left\langle a^2, 2ab, 2ac, b^2, 2bc, c^2 \right\rangle.$$

We have $\mathfrak{a} \subsetneq \mathfrak{a}' \subsetneq \mathfrak{b} \subsetneq \mathfrak{f} \cap \mathbf{A}$ and $\mathfrak{b} = (\mathfrak{f} \cap \mathbf{A})^d$. We also see that $\mathfrak{a}$ is not symmetrical in a, b, c. Still for $d = 2$, we have $(\mathfrak{f} \cap \mathbf{A})^4 \subsetneq \mathfrak{a}$ and $(\mathfrak{f} \cap \mathbf{A})^3 \not\subseteq \mathfrak{a}'$. For arbitrary d, it seems that $(\mathfrak{f} \cap \mathbf{A})^{3d-2} \subseteq \mathfrak{a}$.

Exercise 21. Let $\widetilde{\varphi} : \mathbf{k}[\underline{X}, \underline{Y}] \to \mathbf{k}[\underline{X}]$ be the evaluation morphism $Y_i \mapsto f_i$, the base ring being $\mathbf{k}[\underline{X}]$. We have

$$\operatorname{Ker} \widetilde{\varphi} = \langle Y_1 - f_1, \ldots, Y_s - f_s \rangle = \langle g_1, \ldots, g_s \rangle,$$

and since $\widetilde{\varphi}$ extends φ, $\operatorname{Ker} \varphi = \mathbf{k}[\underline{Y}] \cap \operatorname{Ker} \widetilde{\varphi}$, as required.

Problem 1. First, the cycle $\sigma = (1, 2, 3)$ performs $\sigma(f_1) = f_2$, $\sigma(f_2) = f_3$ and $\sigma(f_3) = f_1$. Therefore $C_3 = \langle \sigma \rangle$ operates on $\mathbf{A} = \mathbf{k}[x, y, z]$. If in addition $a = b$ or $b = c$, then $\{f_1, f_2, f_3\}$ is invariant under S_3. Finally, note that the origin is a zero of the system, but also that solutions with $x = y = z \neq 0$ (in an extension of $\mathbf{k}$) exist.

1. There are two cases: the $a \leqslant b < c$ case, the easier one to study (case I), and the $a < b = c$ case (case II).

• case I ($b < c$).
Consider on the monomials of $\mathbf{k}[X, Y, Z]$ the order `deglex` (see Exercise III-3). Let us show that $\mathbf{A} = \sum_{p,q,r:\max(p,q,r)<c} \mathbf{k}\, x^p y^q z^r$.
Let $m = x^i y^j z^k$ with $\max(i, j, k) \geqslant c$. If $i \geqslant c$, we replace in m, x^c with $x^{i-c}x^c = -x^{i-c}(y^b + z^a$
Similarly if $j \geqslant c$ or if $k \geqslant c$. We then get

$$m = -(m_1 + m_2) \text{ with } m_1, m_2 = \begin{cases} x^{i-c}y^{b+j}z^k,\ x^{i-c}y^j z^{a+k} & \text{if } i \geqslant c,\\ x^{a+i}y^{j-c}z^k,\ x^i y^{j-c}z^{b+k} & \text{if } j \geqslant c,\\ x^{b+i}y^j z^{k-c},\ x^i y^{a+j}z^{k-c} & \text{if } k \geqslant c. \end{cases}$$

We then see that $m_1 < m$ and $m_2 < m$; we finish by induction. The reader will check that the $x^p y^q z^r$ with p, q, $r < c$ form a $\mathbf{k}$-basis of $\mathbf{A}$. For those familiar with the material: when $\mathbf{k}$ is a discrete field, (f_1, f_2, f_3) is a Gröbner basis for the monomial order `deglex`. Recap: $\dim_{\mathbf{k}} \mathbf{A} = c^3$.

• case II ($a < b = c$). This case is more difficult.
First suppose that 2 is invertible in $\mathbf{k}$. We introduce

$$\begin{aligned} g_1 &= -f_1 + f_2 + f_3 = 2Z^c + X^a + Y^a - Z^a,\\ g_2 &= f_1 - f_2 + f_3 = 2X^c - X^a + Y^a + Z^a,\\ g_3 &= f_1 + f_2 - f_3 = 2Y^c + X^a - Y^a + Z^a. \end{aligned}$$

We then have

$$2f_1 = g_2 + g_3, \quad 2f_2 = g_1 + g_3, \quad 2f_3 = g_1 + g_2,$$

such that $\langle f_1, f_2, f_3\rangle = \langle g_1, g_2, g_3\rangle$. Then we can operate with the g_j's as we did with the f_i's in case I. If $\mathbf{k}$ is a discrete field, (g_1, g_2, g_3) is a Gröbner basis for the graded lexicographic order `deglex`.
Recap: $\dim_{\mathbf{k}} \mathbf{A} = c^3$ and the $x^p y^q z^r$'s with p, q, $r < c$ form a $\mathbf{k}$-basis of $\mathbf{A}$.

• Case II with a discrete field $\mathbf{k}$ of characteristic 2 is left to the sagacity of the reader. The ring $\mathbf{A}$ is not always zero-dimensional! This happens for example when $\mathbf{k} = \mathbb{F}_2$ and $(a, b) = (1, 3)$, $(1, 7)$, $(2, 6)$, $(3, 9)$. When it is zero-dimensional, it seems that $\dim_{\mathbf{k}} \mathbf{A} < c^3$.

2. For $(a, b, c) = (2, 2, 3)$, we know that $\dim_{\mathbf{k}} \mathbf{k}[x, y, z] = 3^3 = 27$. We use Stickelberger's theorem 8.17, except that we do not know the zeros of the system. We check, with the help of a Computer Algebra system, that the characteristic polynomial of x over $\mathbf{k}$ can be factorized into irreducible polynomials ($\mathbf{k} = \mathbb{Q}$)

$$\mathrm{C}_x = t^8(t + 2)(t^3 - t^2 + 1)^2(t^4 - 2t^3 + 4t^2 - 6t + 4)(t^4 + t^3 + t^2 - t + 2)^2,$$

but the factorization of C_{x+2y} is of the type $1^8 \cdot 1^1 \cdot 4^1 \cdot 4^1 \cdot 4^1 \cdot 6^1$. Consequently, the projection $(x, y, z) \mapsto x$ does not separate the zeros of the system, whereas the projection $(x, y, z) \mapsto x + 2y$ does. Moreover, we see that the origin is the only zero with multiplicity (equal to 8). Thanks to the factorization of C_x and by performing a few additional small computations, we obtain

- Another zero defined over $\mathbf{k}$, $(x, y, z) = (-2, -2, -2)$, which is simple.
- If α, β, γ are the three distinct roots of $t^3 - t^2 + 1$, we obtain 6 simple zeros by making the group S_3 act on the zero (α, β, γ). If s_1, s_2, s_3 are the elementary symmetric functions of (X, Y, Z), then, over $\mathbb{Q}$, we have the equality of ideals $\langle f_1, f_2, f_3, s_1 - 1\rangle = \langle s_1 - 1, s_2, s_3 + 1\rangle$, i.e. the algebra of these 6 zeros is the universal splitting algebra of the polynomial $t^3 - t^2 + 1$.

- Let δ_i be a root of $t^4+t^3+t^2-t+2$ ($i \in [\![1..4]\!]$).
  By letting $y = x = \delta_i$ and $z = 2/(x+1) = -(x^3+x-2)/2$, we obtain a zero of the system. The minimal polynomial of z over $\mathbb{Q}$ is the one we see in the factorization of C_x: $t^4-2t^3+4t^2-6t+4$. We thus obtain four simple zeros of the system.
- We can make A_3 act on the four previous zeros.

We have therefore obtained $1+6+3\times 4 = 19$ simple zeros and a zero of multiplicity 8. This adds up as required.
Remark: whereas $\dim_{\mathbf{k}} \mathbf{k}[x,y,z] = 27$, we have

$$\dim_{\mathbf{k}} \mathbf{k}[x] = \dim_{\mathbf{k}} \mathbf{k}[y] = \dim_{\mathbf{k}} \mathbf{k}[z] = 14,$$
$$\dim_{\mathbf{k}} \mathbf{k}[x,y] = \dim_{\mathbf{k}} \mathbf{k}[x,z] = \dim_{\mathbf{k}} \mathbf{k}[y,z] = 23.$$

Thus, neither $\mathbf{k}[x,y]$ nor $\mathbf{k}[x,y,z]$ are free over $\mathbf{k}[x]$, and $\mathbf{k}[x,y,z]$ is not free over $\mathbf{k}[x,y]$.

3. If $\mathbf{k}$ is a discrete field, in case I in characteristic $\neq 2$, we find, experimentally, that the local algebra of the origin is $\mathbf{k}[X,Y,Z]/\langle X^a, Y^a, Z^a\rangle$ and so the multiplicity of the origin would be a^3. As for case II, this seems quite mysterious.

Problem 2. *1.* We put the following weights on $\mathbf{k}[X]$: X is of weight 1, and the weight of a_i and b_{ji} is i. Thus f and g_j are homogeneous of weight d. We easily check for all $k \geqslant 0$ that $(X^k g_j) \bmod f$ is homogeneous of weight $d+k$.

2. We index the d rows of S by $1,\dots,d$, the i^{th} row corresponding to the weight i via $i \leftrightarrow X^{d-i} \leftrightarrow a_i$. The matrix S is the horizontal concatenation of r square matrices of order d, the j^{th} square matrix being that of the multiplication by g_j modulo f in the basis $(X^{d-1},\dots,X,1)$. If we number the columns of the first square submatrix of order d of S (corresponding to g_1) by $(0,1,\dots,d-1)$, then the coefficient of index (i,j) is homogeneous of weight $i+j$. Similarly for the other coefficients with analogous conventions.
For example, for $d=3$, if $f = X^3+a_1X^2+a_2X+a_3$, $g = b_1X^2+b_2X+b_3$, the matrix of the multiplication by $g \bmod f$ is

$$\begin{array}{cccc}
 & g & Xg \bmod f & X^2g \bmod f\\
X^{d-1} \leftrightarrow 1 & b_1 & -a_1b_1+b_2 & a_1^2b_1-a_1b_2-a_2b_1+b_3\\
X^{d-2} \leftrightarrow 2 & b_2 & -a_2b_1+b_3 & a_1a_2b_1-a_2b_2-a_3b_1\\
X^{d-3} \leftrightarrow 3 & b_3 & -a_3b_1 & a_1a_3b_1-a_3b_2
\end{array} \quad \text{of weights} \quad \begin{bmatrix} 1 & 2 & 3\\ 2 & 3 & 4\\ 3 & 4 & 5 \end{bmatrix}.$$

Let M be a submatrix of order d of S, $(k_1,\dots,k_d)$ the exponents of X corresponding to its columns ($k_i \in [\![0..d-1]\!]$, and the columns are $X^{k_i}g_j \bmod f$).
Then, $\det(M)$ is homogeneous, and its weight is the sum of the weights of the diagonal coefficients, i.e.

$$(1+k_1)+(2+k_2)+\cdots+(d+k_d) = d(d+1)/2 + \textstyle\sum_{i=1}^{d} k_i.$$

For example, the weight of the first minor of order d of S (corresponding to multiplication by g_1) is $d(d+1)/2 + \sum_{k=0}^{d-1} k = d^2$.
The weight of each of the $\binom{rd}{d}$ minors is bounded below by $d(d+1)/2$ (bound obtained for $k_i = 0$) and bounded above by $d(3d-1)/2$ (bound obtained for $k_i = d-1$). These bounds are reached if $r \geqslant d$.

3. The number $\dim_{\mathbb{Q}} E$ is the lower bound of the cardinality of any arbitrary generator set of $\mathfrak{b}$. We experimentally find, for small values of r and d, that $\dim_{\mathbb{Q}} E = r^d$. But we can do better. Indeed, the consideration of graded objects allows us to assert the following result (homogeneous Nakayama lemma, problem 3): every graded family of $\mathfrak{b}$ whose image in E is a homogeneous generator set of the graded $\mathbb{Q}$-vector space E is a (homogeneous) generator set of $\mathfrak{b}$. In particular, there exists a homogeneous generator set of $\mathfrak{b}$ of cardinality $\dim_{\mathbb{Q}} E$, conjecturally, r^d. We can go further by examining the weights of the minimal homogeneous generator sets of $\mathfrak{b}$. Those are unique and provided by the (finite) series of the graded $\mathbb{Q}$-vector space E. For example, for $d = 5$, $r = 2$, this series is

$$6t^{25} + 4t^{24} + 6t^{23} + 6t^{22} + 6t^{21} + 2t^{20} + 2t^{19},$$

which means that in any minimal homogeneous generator set of $\mathfrak{b}$, there are 6 polynomials of weight 25, 4 polynomials of weight 24, …, 2 polynomials of weight 19 (with $6 + 4 + \cdots + 2 = 32 = 2^5 = r^d$). In this example, the number $\binom{rd}{d}$ of minors of order d of S is 252.

Conjecturally, it would seem that $\mathfrak{b}$ is generated by homogeneous polynomials of weight $\leqslant d^2$, with $\binom{d+r-1}{r-1}$ polynomials of weight d^2 exactly.

Problem 3.

1. We perform a proof by induction on n.

Case $n = 0$: trivial result.

For $n \geqslant 1$, we consider $\mathbf{A}' = \mathbf{A}/\langle a_1 \rangle$. We have $\mathbf{k} \hookrightarrow \mathbf{A}'$ because $\mathbf{k} \cap \langle a_1 \rangle = \{0\}$. The sequence $(\overline{a_2}, \cdots, \overline{a_n})$ in $\mathbf{A}'$ satisfies the right assumptions for the induction on n. Suppose $f(a_1, \ldots, a_n) = 0$ with $f \in \mathbf{k}[X_1, \ldots, X_n]$ and $\deg_{X_1}(f) \leqslant d$.

We write $f = X_1 q(X_1, \ldots, X_n) + r(X_2, \ldots, X_n)$ with q, r with coefficients in $\mathbf{k}$ and q of degree $\leqslant d - 1$ in X_1. In $\mathbf{A}'$, we have $r(\overline{a_2}, \ldots, \overline{a_n}) = 0$. By induction on n, we have $r = 0$. Since a_1 is regular, $q(a_1, \ldots, a_n) = 0$. By induction on d, we obtain $q = 0$, so $f = 0$.

2a. By definition, $\mathbf{A}_+ E \subseteq E_1 \oplus E_2 \oplus \ldots$; and since $\mathbf{A}_+ E = E$, we get $E_0 = 0$. Then $\mathbf{A}_+ E \subseteq E_2 \oplus E_3 \oplus \ldots$, and by using $\mathbf{A}_+ E = E$ again, we get $E_1 = 0$, and so on. So $E_n = 0$ for all n, therefore $E = 0$.

2b. Let F be the $\mathbf{A}$-submodule of E generated by the e_i's. It is a graded submodule because the e_i's are homogeneous. The hypothesis is equivalent to $F + \mathbf{A}_+ E = E$ or $\mathbf{A}_+(E/F) = E/F$. By question *2a*, we have $E/F = 0$ i.e. $E = F$; the e_i's generate the $\mathbf{A}$-module E.

3a. It is clear that $\mathbf{A}_0 = \mathbf{B}_0$ and $\mathfrak{b} = \mathbf{A}_+ \mathbf{B}$. By applying the previous question to the graded $\mathbf{A}$-module $\mathbf{B}$ and to e_i, we obtain that the e_i's form a generator set of the $\mathbf{A}$-module $\mathbf{B}$.

3b. Let $S = \sum_i \mathbf{B}_0 e_i$ (actually, it is a direct sum).

Let us show that $\langle h_1, \ldots, h_d \rangle \cap S = \{0\}$. If $s = \sum_i \lambda_i e_i \in \langle h_1, \ldots, h_d \rangle$ with $\lambda_i \in \mathbf{B}_0$, then by reducing modulo $\langle h_1, \ldots, h_d \rangle$, we get $\sum_i \lambda_i \overline{e_i} = 0$, therefore $\lambda_i = 0$ for all i and $s = 0$.

For $\alpha = (\alpha_1, \dots, \alpha_d) \in \mathbb{N}^d$, let $h^\alpha = h_1^{\alpha_1} \cdots h_d^{\alpha_d}$. Let us show that

$$(\star) \qquad \sum\nolimits_\alpha s_\alpha h^\alpha = 0 \text{ with } s_\alpha \in S \implies s_\alpha = 0 \quad \text{for all } \alpha.$$

For this, we will prove by (decreasing) induction on i, that

$$\big(f \in S[X_i, \dots, X_d] \text{ and } f(h_i, \dots, h_d) \equiv 0 \bmod \langle h_1, \dots, h_{i-1}\rangle\big) \implies f = 0.$$

First for $i = d$. The hypothesis is $s_m h_d^m + \cdots + s_1 h_d + s_0 \equiv 0 \bmod \langle h_1, \dots, h_{d-1}\rangle$ and we want $s_k = 0$ for all k. We have $s_0 \in S \cap \langle h_1, \dots, h_d\rangle = \{0\}$. We can simplify the congruence by h_d (which is regular modulo $\langle h_1, \dots, h_{d-1}\rangle$) to obtain $s_m h_d^{m-1} + \cdots + s_1 \equiv 0 \bmod \langle h_1, \dots, h_{d-1}\rangle$. By iterating the process, we obtain that all the s_k's are null.
Passing from $i + 1$ to i.
Let $f \in S[X_i, \dots, X_d]$ of degree $\leqslant m$ with $f(h_i, \dots, h_d) \equiv 0 \bmod \langle h_1, \dots, h_{i-1}\rangle$. We write $f = X_i q(X_i, \dots X_d) + r(X_{i+1}, \dots, X_d)$ with q, r with coefficients in S and q of degree $\leqslant m - 1$. We therefore have $r(h_{i+1}, \dots, h_d) \equiv 0 \bmod \langle h_1, \dots, h_i\rangle$, hence by induction on i, $r = 0$. We can simplify the congruence by h_i (which is regular modulo $\langle h_1, \dots, h_{i-1}\rangle$) to obtain $q(h_i, \dots, h_d) \equiv 0 \bmod \langle h_1, \dots, h_{i-1}\rangle$. Therefore $q = 0$ by induction on m, then $f = 0$.
Recap: we therefore have the result for $i = 1$ and this result is none other than $(\star)$.
Once $(\star)$ is proved, we can show that the e_i's are linearly independent over $\mathbf{A}$. Let $\sum_i a_i e_i = 0$ with $a_i \in \mathbf{A}$; we write $a_i = \sum_\alpha \lambda_{\alpha,i} h^\alpha$ and

$$\sum\nolimits_i a_i e_i = \sum\nolimits_{i,\alpha} \lambda_{i,\alpha} h^\alpha e_i = \sum\nolimits_\alpha s_\alpha h^\alpha \quad \text{with} \quad s_\alpha = \sum\nolimits_i \lambda_{i,\alpha} e_i \in S.$$

Therefore $s_\alpha = 0$ for all α, then $\lambda_{i,\alpha} = 0$ for all i, and $a_i = 0$.

4. Generally , if $(a_1, \dots, a_d)$ is a regular sequence of a ring $\mathbf{A}$, it is L-regular for all free $\mathbf{A}$-modules L (left to the reader). We apply this to the ring $\mathbf{A} = \mathbf{B}_0[h_1, \dots, h_d]$, to the sequence $(h_1, \dots, h_d)$ (which is indeed a regular sequence of $\mathbf{A}$) and to $L = \mathbf{B}$ (which is a free $\mathbf{A}$-module by the hypothesis).

Bibliographic comments

Bourbaki (Algebra, Chapter X, or Commutative algebra, Chapter I) calls what we have called a coherent module (in accordance with the common usage, especially in the English literature) a *pseudo coherent module*, and what we call a finitely presented coherent module Bourbaki calls a coherent module. This is naturally to be related to the “Faisceaux Algébriques Cohérents” by J.-P. Serre (precursors of sheaves of modules on a Grothendieck scheme) which are locally given by finitely presented coherent modules. It should also be noted that [Stacks-Project] adopts the Bourbaki's definition for coherent modules.

Theorem 5.1 is taken from [MRR] Chap. V, Th. 2.4. Theorem 5.2 is taken from [MRR] Chap. III, Exercise 9 p. 80.

The standard reference for Fitting ideals is [Northcott].

As for purely equational algebraic structures and universal algebra one can consult [Burris & Sankappanavar].

A first introduction to categories is found in [Cohn].
Dedicated books on the subject that we can recommend are [Mac Lane] and [Lawvere & Rosebrugh].

The Kaplansky ideals of a module M studied in Exercise 19 are used in [Kunz, Chap. IV] and [Ischebeck & Rao, Chap. 9].

The strict Bézout rings (Exercise 7) and the Smith rings (Exercise 8) have been studied by Kaplansky in [118] in a more general framework of not necessarily commutative rings. He respectively calls them "Hermite rings" and "elementary divisor rings." But this terminology is not fixed. In [Lam06], where Exercise 7 finds its source, Lam uses *K-Hermite ring* for strict Bézout ring. That is to be distinguished from *Hermite ring*: today a ring **A** is called a *Hermite ring* if every stably free **A**-module is free, i.e. if every unimodular vector is completable (see Chapter V, Section V-4). As for the "elementary divisors," they are now often used in a more particular sense. For example, in the literature it is often said that the $\mathbb{Z}$-module

$$\mathbb{Z}/\langle 900\rangle \oplus \mathbb{Z}/\langle 10\rangle \simeq \mathbb{Z}/\langle 25\rangle \oplus \mathbb{Z}/\langle 5\rangle \oplus \mathbb{Z}/\langle 4\rangle \oplus \mathbb{Z}/\langle 2\rangle \oplus \mathbb{Z}/\langle 9\rangle$$

admits for invariant factors the list $(10, 900)$ and for elementary divisors the unordered list $(25, 5, 4, 2, 9)$.

Exercise 11 was provided to us by Thierry Coquand.

Chapter V

Finitely generated projective modules, 1

Contents

1. Introduction

Recall that a finitely generated projective module is a module isomorphic to a direct summand in a free **A**-module of finite rank. This notion happens to be the natural generalization, for modules over a commutative ring, of the notion of a finite dimensional vector space over a discrete field. This chapter develops the basic theory of these modules.

One of the initial motivations of this book was to understand *in concrete terms* the following theorems concerning finitely generated projective modules.

1.1. Theorem. (Local structure theorem for finitely generated projective modules) *An* $\mathbf{A}$*-module* P *is finitely generated projective if and only if it is* locally free *in the following sense. There exist comaximal elements* $s_1, \ldots, s_\ell$ *in* $\mathbf{A}$ *such that the modules* P_{s_i} *obtained from* P *by scalar extension to the rings* $\mathbf{A}_{s_i} = \mathbf{A}[1/s_i]$ *are free.*

1.2. Theorem. (Characterization of finitely generated projective modules by their Fitting ideals) *A finitely presented* $\mathbf{A}$*-module is projective if and only if its Fitting ideals are (principal ideals generated by) idempotents.*

1.3. Theorem. (Decomposition of a finitely generated projective module into a direct sum of modules of constant rank) *If* P *is a finitely generated projective* $\mathbf{A}$*-module generated by* n *elements, there exists a fundamental system of orthogonal idempotents* $(r_0, r_1, \ldots, r_n)$ *(some eventually null) such that each* r_kP *is a projective module of rank* k *over the ring* $\mathbf{A}/\langle 1 - r_k\rangle$*. Then* $P = \bigoplus_{k>0} r_kP$ *and* $\mathrm{Ann}(P) = \langle r_0\rangle$*.*

In this direct sum we can naturally limit ourselves to the indices $k > 0$ such that $r_k \neq 0$.

1.4. Theorem. (Characterization of finitely generated projective modules by their flatness) *A finitely presented* $\mathbf{A}$*-module is projective if and only if it is flat.*

In this chapter we will prove the first three of these theorems. They will be taken up again with new proofs in Chapter X. The fourth one will be proven in Chapter VIII, which is dedicated to flat modules.

Other important theorems regarding finitely generated projective modules will be proven in Chapters X, XIV and XVI. The theory of algebras which are finitely generated projective modules (we will call them strictly finite algebras) is developed in Chapter VI.

2. Generalities

Recall that a finitely generated projective module is finitely presented (Example 2, page 179).

Characteristic properties

When M and N are two $\mathbf{A}$-modules, we have a natural $\mathbf{A}$-linear map $\theta_{M,N} : M^\star \otimes N \to \mathrm{L}_\mathbf{A}(M,N)$ given by

$$\theta_{M,N}(\alpha \otimes y) = \big(x \mapsto \alpha(x)y\big). \tag{1}$$

We also write θ_M for $\theta_{M,M}$.

Remark. We sometimes write $\alpha \otimes y$ for $\theta_{M,N}(\alpha \otimes y)$ but it is certainly not recommended when $\theta_{M,N}$ is not injective. ■

The following theorem gives some immediately equivalent properties.

2.1. Theorem. (Finitely generated projective modules)
For an $\mathbf{A}$*-module* P*, the following properties are equivalent.*

(a) *P is a* finitely generated projective module*, i.e. there exist an integer n, an* $\mathbf{A}$*-module N and an isomorphism of $P \oplus N$ over* $\mathbf{A}^n$*.*

($b1$) *There exist an integer n, elements $(g_i)_{i\in[\![1..n]\!]}$ of P and linear forms $(\alpha_i)_{i\in[\![1..n]\!]}$ over P such that for all $x \in P$, $x = \sum_i \alpha_i(x)\, g_i$.*

($b2$) *The module P is finitely generated, and for every finite system of generators $(h_i)_{i\in[\![1..m]\!]}$ of P there exist linear forms $(\beta_i)_{i\in[\![1..m]\!]}$ over P such that for all $x \in P$, $x = \sum_i \beta_i(x)\, h_i$.*

($b3$) *The image of $P^\star \otimes_\mathbf{A} P$ in $\mathrm{L}_\mathbf{A}(P,P)$ under the canonical homomorphism θ_P contains Id_P.*

($c1$) *There exist an integer n and two linear maps $\varphi : P \to \mathbf{A}^n$ and $\psi : \mathbf{A}^n \to P$, such that $\psi \circ \varphi = \mathrm{Id}_P$. We then have $\mathbf{A}^n = \mathrm{Im}(\varphi) \oplus \mathrm{Ker}(\psi)$ and $P \simeq \mathrm{Im}(\varphi \circ \psi)$.*

($c2$) *The module P is finitely generated, and for every surjective linear map $\psi : \mathbf{A}^m \to P$, there exists a linear map $\varphi : P \to \mathbf{A}^m$ such that $\psi \circ \varphi = \mathrm{Id}_P$. We then have $\mathbf{A}^m = \mathrm{Im}(\varphi) \oplus \mathrm{Ker}(\psi)$ and $P \simeq \mathrm{Im}(\varphi \circ \psi)$.*

($c3$) *Like ($c2$) but by replacing $\mathbf{A}^m$ by an arbitrary $\mathbf{A}$-module M: the module P is finitely generated, and for every surjective linear map $\psi : M \to P$, $\mathrm{Ker}(\psi)$ is a direct summand.*

($c4$) *The module P is finitely generated and the functor $\mathrm{L}_{\mathbf{A}}(P, \bullet)$ transforms the surjective linear maps into surjective maps.*
In other words, for all $\mathbf{A}$-modules M, N, for every surjective linear map $\psi : M \to N$ and every linear map $\Phi : P \to N$, there exists a linear map $\varphi : P \to M$ such that $\psi \circ \varphi = \Phi$.

$$\begin{tikzcd} & M \arrow[d, "\psi"] \\ P \arrow[ru, dashed, "\varphi"] \arrow[r, "\Phi"'] & N \end{tikzcd}$$

D Item ($b1$) (resp. ($b2$)) is simply a reformulation of ($c1$) (resp. ($c2$)).
Item ($b3$) is simply a reformulation of ($b1$).
We trivially have ($c3$) ⇒ ($c2$) ⇒ ($c1$).
(a) ⇒ ($c1$) Consider the canonical maps

$$P \to P \oplus N \text{ and } P \oplus N \to P.$$

($c1$) ⇒ (a) Consider $\pi = \varphi \circ \psi$. We have $\pi^2 = \pi$. This defines a projection of $\mathbf{A}^n$ over $\mathrm{Im}\,\pi = \mathrm{Im}\,\varphi \simeq P$ parallel to $N = \mathrm{Ker}\,\pi = \mathrm{Ker}\,\psi$.
($b1$) ⇒ ($c4$) If $\Phi(g_i) = \psi(y_i)$ ($i \in \llbracket 1..n \rrbracket$), we let $\varphi(x) = \sum \alpha_i(x)\, y_i$. We then have for all $x \in P$,

$$\Phi(x) = \Phi\big(\textstyle\sum \alpha_i(x)\, g_i\big) = \sum \alpha_i(x)\, \psi(y_i) = \psi\big(\sum \alpha_i(x)\, y_i\big) = \psi\big(\varphi(x)\big).$$

($c4$) ⇒ ($c3$) We take $N = P$ and $\Phi = \mathrm{Id}_P$. □

We also directly have ($b1$) ⇒ ($b2$) as follows: by expressing the g_i's as linear combinations of the h_j's we obtain the β_j's from the α_i's.

In practice, according to the original definition, we consider a finitely generated projective module as (an isomorphic copy of) the image of a projection matrix F. Such a matrix, or the linear map that it represents, is again called a *projector*. More generally, every idempotent endomorphism of a module M is called a *projector*.

When we see a finitely generated projective module according to the definition ($c1$), the projection matrix is that of the linear map $\varphi \circ \psi$. Similarly, if we use the definition ($b1$), the projection matrix is the one which has for coefficients every $\alpha_i(g_j)$ in position (i, j).

A system $\big((g_1, \dots, g_n), (\alpha_1, \dots, \alpha_n)\big)$ that satisfies ($b1$) is called a *coordinate system* for the projective module P. Some authors speak of a *basis* of the finitely generated projective module, but we will not be following their lead on this matter.

2.2. Fact. (Dual of a finitely generated projective module, 1)
Let $\big((g_1,\dots,g_n),(\alpha_1,\dots,\alpha_n)\big)$ be a coordinate system for a finitely generated projective module P. Then

- *the g_i's generate P,*
- *the α_j's generate $\mathrm{L}(P,\mathbf{A}) = P^\star$,*
- *the module $P^\star$ is finitely generated projective,*
- *the module $(P^\star)^\star$ is canonically isomorphic to P,*
- *via this canonical identification, $\big((\alpha_1,\dots,\alpha_n),(g_1,\dots,g_n)\big)$ is a coordinate system for $P^\star$.*

In particular, if P is (isomorphic to) the image of a projection matrix F, the dual module $P^\star$ is (isomorphic to) the image of the projection matrix ${}^{\mathrm{t}}F$.

D The first item is clear. All the rest is clear from the moment where we show that $\lambda = \sum \lambda(g_i)\,\alpha_i$ for all $\lambda \in P^\star$, and this equality is proven by evaluating both sides at an arbitrary element x of P:

$$\lambda(x) = \lambda\big(\textstyle\sum\, \alpha_i(x)\, g_i\big) = \textstyle\sum\, \alpha_i(x)\,\lambda(g_i) = \big(\textstyle\sum\, \lambda(g_i)\,\alpha_i\big)(x). \qquad \square$$

2.3. Theorem. *Let $\mathbf{A}^m \xrightarrow{\psi} \mathbf{A}^q \xrightarrow{\pi} P \to 0$ be a presentation of a module P. Then, P is finitely generated projective if and only if ψ is locally simple.*

Recall that "ψ is locally simple" means that there exists a $\varphi : \mathbf{A}^q \to \mathbf{A}^m$ satisfying $\psi\,\varphi\,\psi = \psi$. Moreover, by Theorem II-5.14 every linear map which has a rank in the sense of Definition II-5.7 is locally simple.

D If ψ is locally simple, Fact II-5.18 tells us that $\operatorname{Im}\psi$ is a direct summand, and $\operatorname{Coker}\psi$ is isomorphic to a complementary submodule of $\operatorname{Im}\psi$. Conversely, if the module $P := \operatorname{Coker}\psi$ is projective, we apply the property ($c2$) of Theorem 2.1 to the projection $\pi : \mathbf{A}^q \to P$. We obtain $\tau : P \to \mathbf{A}^q$ with $\pi \circ \tau = \mathrm{Id}_P$, such that $\mathbf{A}^q = \operatorname{Im}\tau \oplus \operatorname{Im}\psi$. Therefore $\operatorname{Im}\psi$ is finitely generated projective and we can apply the property ($c2$) to $\psi : \mathbf{A}^m \to \operatorname{Im}\psi$, which gives us φ over the component $\operatorname{Im}\psi$ (and we take for example 0 over $\operatorname{Im}\tau$). □

Local-global principle

The fact that an $\mathbf{A}$-module is finitely generated projective is a local notion in the following sense.

2.4. Concrete local-global principle. (Finitely generated projective modules) *Let S_1, …, S_n be comaximal monoids of $\mathbf{A}$ and P be an $\mathbf{A}$-module. If the P_{S_i}'s are free, P is finitely generated and projective.*
More generally, the module P is finitely generated and projective if and only if the P_{S_i}'s are finitely generated projective $\mathbf{A}_{S_i}$-modules.

D This results from Theorem 2.3, from the local-global principle IV-4.13 for finitely presented modules and from the local-global principle II-5.19 for locally simple linear maps. □

The local-global principle 2.4 establishes the implication "if" in Theorem 1.1. The converse "only if" has been proven in Theorem II-5.26 which will give us Theorem 6.1. We will give for this converse a more precise statement and a more conceptual proof with Theorem X-1.5.

Projective modules and Schanuel's lemma

The notion of a projective module can be defined for modules which are not finitely generated. In the following we will rarely use such modules, but it is however useful to give some precisions on this subject.

2.5. Definition. An $\mathbf{A}$-module P (not necessarily finitely generated) is said to be *projective* if it satisfies the following property.
For all $\mathbf{A}$-modules M, N, for every surjective linear map $\psi : M \to N$ and every linear map $\Phi : P \to N$, there exists a linear map $\varphi : P \to M$ such that $\psi \circ \varphi = \Phi$.

$$\begin{tikzcd}
 & M \arrow[d, "\psi"] \\
P \arrow[ur, dashed, "\varphi"] \arrow[r, "\Phi"'] & N
\end{tikzcd}$$

Thus, given the characterization ($c4$) in Theorem 2.1, an $\mathbf{A}$-module is finitely generated projective if and only if it is projective and finitely generated.
In the following fact, the last property resembles the implication ($c4$) ⇒ ($c3$) in this theorem.
A linear map $\varphi : E \to F$ is called a *split surjection* if there exists a $\psi : F \to E$ with $\varphi \circ \psi = \mathrm{Id}_F$. In this case we say that ψ is a *section* of φ, and we have $E = \operatorname{Ker} \varphi \oplus \psi(F) \simeq \operatorname{Ker} \varphi \oplus F$.
A short exact sequence is said to be *split* if its surjection is split.

2.6. Fact.

1. *A free module whose basis is a set in bijection with $\mathbb{N}$ is projective. For example the ring of polynomials $\mathbf{A}[X]$ is a projective $\mathbf{A}$-module.*
2. *Every module that is a direct summand in a projective module is projective.*

3. *If P is projective, every short exact sequence $0 \to N \to M \to P \to 0$ splits.*

Comment. In constructive mathematics the free modules *are not always* projective. Furthermore, it seems impossible to represent every module as a quotient of a free and projective module. Similarly it seems impossible to place every projective module as a direct summand in a free and projective module. For more details on this matter consult Exercise VIII-16 and [MRR]. ■

2.7. Lemma. *Consider two surjective* $\mathbf{A}$*-linear maps with the same image* $P_1 \xrightarrow{\varphi_1} M \to 0$, $P_2 \xrightarrow{\varphi_2} M \to 0$ *with the modules* P_1 *and* P_2 *being projective.*

1. *There exist reciprocal isomorphisms* $\alpha, \beta : P_1 \oplus P_2 \to P_1 \oplus P_2$ *such that* $(\varphi_1 \oplus 0_{P_2}) \circ \alpha = 0_{P_1} \oplus \varphi_2$ *and* $\varphi_1 \oplus 0_{P_2} = (0_{P_1} \oplus \varphi_2) \circ \beta$.
2. *If we let* $K_1 = \operatorname{Ker} \varphi_1$ *and* $K_2 = \operatorname{Ker} \varphi_2$*, we obtain by restriction of* α *and* β *reciprocal isomorphisms between* $K_1 \oplus P_2$ *and* $P_1 \oplus K_2$.

D There exists a $u : P_1 \to P_2$ such that $\varphi_2 \circ u = \varphi_1$ and $v : P_2 \to P_1$ such that $\varphi_1 \circ v = \varphi_2$.

$$\begin{tikzcd}
P_1 \arrow[dr, "\varphi_1"] \arrow[dd, dashed, "u"'] & \\
& M \\
P_2 \arrow[ur, "\varphi_2"'] &
\end{tikzcd}
\qquad
\begin{tikzcd}
P_1 \arrow[dr, "\varphi_1"] & \\
& M \\
P_2 \arrow[ur, "\varphi_2"'] \arrow[uu, dashed, "v"'] &
\end{tikzcd}
\qquad
\begin{tikzcd}
P_1 \oplus P_2 \arrow[dr, "\varphi_1 \oplus 0_{P_2}"] \arrow[dd, dashed, bend left, "\beta"] & \\
& M \\
P_1 \oplus P_2 \arrow[ur, "0_{P_1} \oplus \varphi_2"'] \arrow[uu, dashed, bend left, "\alpha"] &
\end{tikzcd}$$

We verify that α and β defined by the matrices below are suitable.

$$\alpha = \begin{bmatrix} \mathrm{Id}_{P_1} - vu & v \\ -u & \mathrm{Id}_{P_2} \end{bmatrix} \qquad \beta = \begin{bmatrix} \mathrm{Id}_{P_1} & -v \\ u & \mathrm{Id}_{P_2} - uv \end{bmatrix}.$$

NB: the matrix β is a sophisticated variant of what would be the cotransposed matrix of α if Id_{P_1}, Id_{P_2}, u and v were scalars. □

2.8. Corollary. (Schanuel's lemma) *Consider two exact sequences*

$$\begin{array}{ccccccccc}
0 & \to & K_1 & \xrightarrow{j_1} & P_1 & \xrightarrow{\varphi_1} & M & \to & 0 \\
0 & \to & K_2 & \xrightarrow{j_2} & P_2 & \xrightarrow{\varphi_2} & M & \to & 0
\end{array}$$

with the modules P_1 *and* P_2 *being projective. Then,* $K_1 \oplus P_2 \simeq K_2 \oplus P_1$.

The category of finitely generated projective modules

A purely categorical construction

The category of finitely generated projective modules over $\mathbf{A}$ can be constructed from the category of free modules of finite rank over $\mathbf{A}$ by a purely categorical procedure.

1. A finitely generated projective module P is described by a pair $(\mathrm{L}_P, \mathrm{Pr}_P)$ where L_P is a free module of finite rank and $\mathrm{Pr}_P \in \mathrm{End}(\mathrm{L}_P)$ is a projector. We have $P \simeq \mathrm{Im}\,\mathrm{Pr}_P \simeq \mathrm{Coker}(\mathrm{Id}_{\mathrm{L}_P} - \mathrm{Pr}_P)$.
2. A linear map φ from the module P (described by $(\mathrm{L}_P, \mathrm{Pr}_P)$) to the module Q (described by $(\mathrm{L}_Q, \mathrm{Pr}_Q)$) is described by a linear map $\mathrm{L}_\varphi : \mathrm{L}_P \to \mathrm{L}_Q$ subjected to commutation relations
$$\mathrm{Pr}_Q \circ \mathrm{L}_\varphi = \mathrm{L}_\varphi = \mathrm{L}_\varphi \circ \mathrm{Pr}_P\,.$$
In other words L_φ is null over $\mathrm{Ker}(\mathrm{Pr}_P)$ and its image is contained in $\mathrm{Im}(\mathrm{Pr}_Q)$.
3. The identity of P is represented by $\mathrm{L}_{\mathrm{Id}_P} = \mathrm{Pr}_P$.
4. The sum of two linear maps φ and ψ from P to Q represented by L_φ and L_ψ is represented by $\mathrm{L}_\varphi + \mathrm{L}_\psi$. The linear map $a\varphi$ is represented by $a\mathrm{L}_\varphi$.
5. To represent the composition of two linear maps, we compose their representations.
6. Finally, a linear map φ from P to Q represented by L_φ is null if and only if $\mathrm{L}_\varphi = 0$.

This shows that the problems relating to the finitely generated projective modules can always be interpreted as problems regarding projection matrices, and often come down to problems about solving systems of linear equations over $\mathbf{A}$.

An equivalent category, better adapted to computations, is the category whose objects are the projection matrices with coefficients in $\mathbf{A}$, a morphism from F to G being a matrix H of a suitable format satisfying the equalities
$$GH = H = HF.$$

Using coordinate systems

The following fact uses the assertions of the previous paragraph while taking the coordinate system point of view.

2.9. Fact. *Let P and Q be two finitely generated projective modules with coordinate systems*
$$\big((x_1, \dots, x_n), (\alpha_1, \dots, \alpha_n)\big) \textit{ and } \big((y_1, \dots, y_m), (\beta_1, \dots, \beta_m)\big),$$
and let $\varphi : P \to Q$ be an $\mathbf{A}$-linear map.
Then, we can encode P and Q by the matrices
$$F \overset{\text{def}}{=} \big(\alpha_i(x_j)\big)_{i,j\in[\![1..n]\!]} \qquad \textit{and} \qquad G \overset{\text{def}}{=} \big(\beta_i(y_j)\big)_{i,j\in[\![1..m]\!]}.$$
More precisely, we have the isomorphisms
$$\pi_1 : P \to \mathrm{Im}\,F\,, \qquad x \mapsto {}^{\mathrm{t}}[\,\alpha_1(x)\ \cdots\ \alpha_n(x)\,],$$
$$\pi_2 : Q \to \mathrm{Im}\,G\,, \qquad y \mapsto {}^{\mathrm{t}}[\,\beta_1(y)\ \cdots\ \beta_m(y)\,].$$

As for the linear map φ, it is encoded by the matrix

$$H \overset{\text{def}}{=} \big(\beta_i(\varphi(x_j))\big)_{i\in[\![1..n]\!],j\in[\![1..m]\!]}$$

which satisfies $GH = H = HF$. The matrix H is that of the linear map

$$\mathbf{A}^n \to \mathbf{A}^m, \quad \pi_1(x) + z \;\mapsto\; \pi_2\big(\varphi(x)\big) \qquad \textit{if } x \in P \textit{ and } z \in \operatorname{Ker} F.$$

We say that the matrix H represents the linear map φ in the coordinate systems $\big((\underline{x}),(\underline{\alpha})\big)$ and $\big((\underline{y}),(\underline{\beta})\big)$.

Application: the isomorphisms between finitely generated projective modules

Lemma 2.10 says that, for $F \in \mathbb{AG}_m(\mathbf{A})$ and $G \in \mathbb{AG}_n(\mathbf{A})$, if $\operatorname{Im} F$ and $\operatorname{Im} G$ are isomorphic, even if it means "enlarging" the matrices F and G, they can be assumed to be similar.

In the sequel, we use the notation $\operatorname{Diag}(M_1,\dots,M_k)$ more freely than we have until now. Instead of a list of elements of the ring, we consider for $(M_1,\dots,M_k)$ a list of square matrices. The matrix represented as such is usually called a *block diagonal matrix.*

2.10. Lemma. (Enlargement lemma)
Consider the matrix encoding of the category of finitely generated projective modules. If an isomorphism φ of $\operatorname{Im} F$ over $\operatorname{Im} G$ is encoded by U and its inverse encoded by U', we obtain a matrix $A \in \mathbb{E}_{n+m}(\mathbf{A})$

$$A = \begin{bmatrix} \mathrm{I}_m - F & -U' \\ U & \mathrm{I}_n - G \end{bmatrix} = \begin{bmatrix} \mathrm{I}_m & 0 \\ U & \mathrm{I}_n \end{bmatrix} \begin{bmatrix} \mathrm{I}_m & -U' \\ 0 & \mathrm{I}_n \end{bmatrix} \begin{bmatrix} \mathrm{I}_m & 0 \\ U & \mathrm{I}_n \end{bmatrix},$$

with

$$\begin{bmatrix} 0_m & 0 \\ 0 & G \end{bmatrix} = A \begin{bmatrix} F & 0 \\ 0 & 0_n \end{bmatrix} A^{-1}. \tag{2}$$

Conversely, a conjugation between $\operatorname{Diag}(0_m, G)$ *and* $\operatorname{Diag}(F, 0_n)$ *provides an isomorphism between* $\operatorname{Im} F$ *and* $\operatorname{Im} G$*.*

D The following matrix

$$\begin{array}{c|cccc|} & \operatorname{Im} F & \operatorname{Ker} F & \operatorname{Im} G & \operatorname{Ker} G \\ \operatorname{Im} F & 0 & 0 & -\varphi^{-1} & 0 \\ \operatorname{Ker} F & 0 & \mathrm{Id} & 0 & 0 \\ \operatorname{Im} G & \varphi & 0 & 0 & 0 \\ \operatorname{Ker} G & 0 & 0 & 0 & \mathrm{Id} \end{array},$$

once $\operatorname{Im} F \oplus \operatorname{Ker} F$ is replaced by $\mathbf{A}^m$ and $\operatorname{Im} G \oplus \operatorname{Ker} G$ by $\mathbf{A}^n$, gives the matrix A. The presence of the $-$ sign is due to the classical decomposition into a product of elementary matrices

$$\begin{bmatrix} 0 & -a^{-1} \\ a & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ a & 1 \end{bmatrix} \begin{bmatrix} 1 & -a^{-1} \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ a & 1 \end{bmatrix}.$$

□

When the image of a projection matrix is free

If a projector $P \in \mathbb{AG}_n(\mathbf{A})$ has as its image a free module of rank r, its kernel is not systematically free, and the matrix is therefore not necessarily similar to the standard matrix $\mathrm{I}_{r,n}$.

It is interesting to find a simple characterization of the fact that the image is free.

2.11. Proposition. (Projection matrices whose image is free)
Let $P \in \mathbb{M}_n(\mathbf{A})$. The matrix P is idempotent and its image is free of rank r if and only if there exist two matrices $X \in \mathbf{A}^{n\times r}$ and $Y \in \mathbf{A}^{r\times n}$ such that $YX = \mathrm{I}_r$ and $P = XY$. In addition we have the following.

1. $\mathrm{Ker}\, P = \mathrm{Ker}\, Y$, $\mathrm{Im}\, P = \mathrm{Im}\, X \simeq \mathrm{Im}\, Y$, *and the columns of X form a basis of* $\mathrm{Im}\, P$.
2. *For every matrices X', Y' of the same respective formats as X and Y, and such that $P = X'Y'$, there exists a unique matrix $U \in \mathbb{GL}_r(\mathbf{A})$ such that*
$$X' = XU \ \text{ and } \ Y = UY'.$$
In fact, $U = YX'$, $U^{-1} = Y'X$ and $Y'X' = \mathrm{I}_r$.

D Suppose that P is idempotent with a free image of rank r. For columns of X we take a basis of $\mathrm{Im}\, P$. Then, there exists a unique matrix Y such that $P = XY$. Since $PX = X$ (because $\mathrm{Im}\, X \subseteq \mathrm{Im}\, P$ and $P^2 = P$), we obtain $XYX = X$. Since the columns of X are independent and $X(\mathrm{I}_r - YX) = 0$, we obtain $\mathrm{I}_r = YX$.

Conversely, suppose $YX = \mathrm{I}_r$ and $P = XY$. Then
$$P^2 = XYXY = X\mathrm{I}_rY = XY = P \ \text{ and } \ PX = XYX = X.$$
Therefore $\mathrm{Im}\, P = \mathrm{Im}\, X$. In addition, the columns of X are independent because $XZ = 0$ implies $Z = YXZ = 0$.

1. The sequence $\mathbf{A}^n \xrightarrow{\mathrm{I}_n - P} \mathbf{A}^n \xrightarrow{Y} \mathbf{A}^r$ is exact. Indeed, $Y(\mathrm{I}_n - P) = 0$, and if $YZ = 0$, then $PZ = 0$, so $Z = (\mathrm{I}_n - P)Z$. Thus
$$\mathrm{Ker}\, Y = \mathrm{Im}(\mathrm{I}_n - P) = \mathrm{Ker}\, P, \text{ and}$$
$$\mathrm{Im}\, Y \simeq \mathbf{A}^n/\mathrm{Ker}\, Y = \mathbf{A}^n/\mathrm{Ker}\, P \simeq \mathrm{Im}\, P\,.$$

2. Now if X', Y' are of the same respective formats as X, Y, and if $P = X'Y'$, we let $U = YX'$ and $V = Y'X$. Then

- $UV = YX'Y'X = YPX = YX = \mathrm{I}_r$,
- $X'V = X'Y'X = PX = X$, therefore $X' = XU$,
- $UY' = YX'Y' = YP = Y$, therefore $Y' = VY$.

Finally, $Y'X' = VYXU = VU = \mathrm{I}_r$. □

3. Finitely generated projective modules over zero-dimensional rings

The following theorem generalizes Theorem IV-8.12.

3.1. Theorem. *Let* $\mathbf{A}$ *be a zero-dimensional ring.*

1. *If* $\mathbf{A}$ *is reduced every finitely presented module* M *is quasi-free, and every finitely generated submodule of* M *is a direct summand*
2. (Zero-dimensional freeness lemma)
   Every finitely generated projective $\mathbf{A}$*-module is quasi-free.*
3. *Every matrix* $G \in \mathbf{A}^{q\times m}$ *of rank* $\geqslant k$ *is equivalent to a matrix*
   $$\begin{bmatrix} \mathrm{I}_k & 0_{k,m-k} \\ 0_{q-k,k} & G_1 \end{bmatrix}$$
   with $\mathcal{D}_r(G_1) = \mathcal{D}_{k+r}(G)$ *for all* $r \geqslant 0$*. In particular, every matrix of rank* k *is simple.*
4. *Every finitely presented module* M *such that* $\mathcal{F}_r(M) = \langle 1\rangle$ *(i.e. locally generated by* r *elements, cf. Definition IX-2.5) is generated by* r *elements.*
5. (Incomplete basis theorem)
   If a submodule P *of a finitely generated projective module* Q *is finitely generated projective, it has a complementary submodule. If* Q *is free of rank* q *and* P *free of rank* p*, every complementary subspace is free of rank* $q-p$*.*
6. *Let* Q *be a finitely generated projective* $\mathbf{A}$*-module and* $\varphi : Q \to Q$ *an endomorphism. The following properties are equivalent.*
   a. φ *is injective.*
   b. φ *is surjective.*
   c. φ *is an isomorphism.*

D Item *1* is a reminder of Theorem IV-8.12.

2. We consider a presentation matrix A of the module and we start by noting that since the module is projective, $\mathcal{D}_1(A) = \langle e\rangle$ with e idempotent. We may assume that the first step of the computation is performed at the level of the ring $\mathbf{A}_e = \mathbf{A}[1/e]$. We are reduced to the case where $\mathcal{D}_1(A) = e = 1$, which we assume henceforth. We apply item *3* with $k = 1$ and conclude by induction.

Item *3* resembles an invertible minor lemma (II-5.9) without an invertible minor in the hypothesis. We apply with the ring $\mathbf{A}_{\mathrm{red}}$ item *1* of Theorem IV-8.12. We then obtain the desired matrix, but only modulo $\mathrm{D}_{\mathbf{A}}(0)$. We notice that the matrix $\mathrm{I}_k + R$ with $R \in \mathbb{M}_k\big(\mathrm{D}_{\mathbf{A}}(0)\big)$ has an invertible determinant, which allows us to apply the invertible minor lemma.

4. Results from item *3* applied to a presentation matrix of the module.

5. Let us first look at the second case. Consider the matrix G whose column vectors form a basis for the submodule P. Since G is the matrix of an injective linear map, its determinantal ideal of order p is regular, therefore equal to $\langle 1\rangle$ (Corollary IV-8.3). It remains to apply item *3*. In the general case, if P is generated by p elements, let us consider a P' such that $P \oplus P' \simeq \mathbf{A}^p$. The module $Q \oplus P'$ is finitely generated projective, therefore is a direct summand in a module $L \simeq \mathbf{A}^n$. Then, by the second case, $P \oplus P'$ is a direct summand in L. We deduce that P is the image of a projection $\pi : L \to L$. Finally, the restriction of π to Q is a projection whose image is P.

6. We already know that *b* and *c* are equivalent because Q is finitely generated (Theorem IV-5.2). To prove that *a* implies *b*, we can assume that Q is free (even if that means considering Q' such that $Q \oplus Q'$ is free). Then, φ is represented by a matrix whose determinant is regular therefore invertible.□

The previous theorem admits an important corollary in number theory.

3.2. Corollary. (One and a half theorem)

1. *Let $\mathfrak{a}$ be an ideal of $\mathbf{A}$. Assume that it is a finitely presented $\mathbf{A}$-module with $\mathcal{F}_1(\mathfrak{a}) = \langle 1\rangle$ and that there exists an $a \in \mathfrak{a}$ such that the ring $\mathbf{B} = \mathbf{A}/\langle a\rangle$ is zero-dimensional. Then, there exists a $c \in \mathfrak{a}$ such that $\mathfrak{a} = \langle a, c\rangle = \langle a^m, c\rangle$ for all $m \geqslant 1$.*
2. *Let $\mathbf{Z}$ be the ring of integers of a number field $\mathbf{K}$ and $\mathfrak{a}$ be a nonzero finitely generated ideal of $\mathbf{Z}$. For all $a \neq 0$ in $\mathfrak{a}$ there exists a $c \in \mathfrak{a}$ such that $\mathfrak{a} = \langle a, c\rangle = \langle a^m, c\rangle$ for all $m \geqslant 1$.*

D *1.* The $\mathbf{B}$-module $\mathfrak{a}/a\mathfrak{a}$ is obtained from the $\mathbf{A}$-module $\mathfrak{a}$ by scalar extension from $\mathbf{A}$ to $\mathbf{B}$, so its first Fitting ideal remains equal to $\langle 1\rangle$. We apply item *4* of Theorem 3.1: there exists some $c \in \mathfrak{a}$ such that $\mathfrak{a}/a\mathfrak{a} = \langle c\rangle$ as a $\mathbf{B}$-module. This means that $\mathfrak{a} = c\mathbf{A} + a\mathfrak{a}$ and gives the desired result.

2. If $\mathfrak{a} = \langle x_1, \dots, x_n\rangle$ is a finitely generated ideal of $\mathbf{Z}$, there exists a finitely generated ideal $\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{b} = \langle a\rangle$ (Theorem III-8.21).
Let $\underline{x} = [\, x_1 \ \cdots \ x_n \,]$. Therefore there exist $y_1, \dots, y_n$ in $\mathfrak{b}$ such that $\underline{x}\,{}^{\mathrm{t}}\underline{y} = \sum_i x_i y_i = a$. If $y_i x_j = \alpha_{ij} a$, we have $\alpha_{ii} x_k = \alpha_{ki} x_i$. Therefore, the ideal $\mathfrak{a}$ becomes principal in $\mathbf{Z}[1/\alpha_{ii}]$, equal to $\langle x_i\rangle$, which is free of rank 1 (we can assume that the x_i's are nonzero).
Since $\sum_i \alpha_{ii} = 1$, the α_{ii}'s are comaximal, therefore $\mathfrak{a}$ is finitely generated projective and $\mathcal{F}_1(\mathfrak{a}) = \langle 1\rangle$ (this is true locally and therefore globally).
To apply item *1* it remains to verify that $\mathbf{Z}/\langle a\rangle$ is zero-dimensional. The element a annihilates a monic polynomial $P \in \mathbb{Z}[X]$ of nonzero constant coefficient, which we write as $aQ(a) = r \neq 0$. Therefore, $\mathbf{Z}/\langle a\rangle$ is a quotient ring of $\mathbf{C} = \mathbf{Z}/\langle r\rangle$. It suffices to show that $\mathbf{C}$ is zero-dimensional. Let $\mathbf{A} = \mathbb{Z}/\langle r\rangle$. Let $\overline{u} \in \mathbf{C}$. Since u annihilates a monic polynomial $R \in \mathbb{Z}[T]$ of degree n, the ring $\mathbf{A}[\overline{u}]$ is a quotient ring of the ring $\mathbf{A}[T]/\big\langle \overline{R}(T)\big\rangle$, which is a free

$\mathbf{A}$-module of rank n, and so is finite. Therefore we can explicitly find $k \geqslant 0$ and $\ell \geqslant 1$ such that $\overline{u}^k(1 - \overline{u}^\ell) = 0$. □

Remark. The matrix $A = (\alpha_{ij})$ satisfies the following equalities

$$^{\mathrm{t}}\underline{y}\,\underline{x} = aA,\ A^2 = A,\ \mathcal{D}_2(A) = 0,\ \mathrm{Tr}(A) = 1,\ \underline{x}A = \underline{x}.$$

We deduce that A is a projection matrix of rank 1.
Moreover, we have $\underline{x}(\mathrm{I}_n - A) = 0$, and if $\underline{x}\,^{\mathrm{t}}\underline{z} = 0$, then $^{\mathrm{t}}\underline{y}\,\underline{x}\,^{\mathrm{t}}\underline{z} = 0 = aA\,^{\mathrm{t}}\underline{z}$, so $A\,^{\mathrm{t}}\underline{z} = 0$ and $^{\mathrm{t}}\underline{z} = (\mathrm{I}_n - A)\,^{\mathrm{t}}\underline{z}$. This shows that $\mathrm{I}_n - A$ is a presentation matrix of $\mathfrak{a}$ (over the generator set $(x_1, \ldots, x_n)$). Therefore, $\mathfrak{a}$ is isomorphic as a $\mathbf{Z}$-module to $\mathrm{Im}\,A \simeq \mathrm{Coker}(\mathrm{I}_n - A)$. ■

4. Stably free modules

Recall that a module M is said to be *stably free* if it *is a direct complement of a free module in a free module*, in other words if there exists an isomorphism between $\mathbf{A}^n$ and $M \oplus \mathbf{A}^r$ for two integers r and n.
We will then say that M is *of rank* $s = n - r$.[1] The rank of a stably free module over a nontrivial ring is well-defined. Indeed, if $M \oplus \mathbf{A}^r \simeq \mathbf{A}^n$ and $M \oplus \mathbf{A}^{r'} \simeq \mathbf{A}^{n'}$, then we have $\mathbf{A}^r \oplus \mathbf{A}^{n'} \simeq \mathbf{A}^{r'} \oplus \mathbf{A}^n$ by Shanuel's lemma 2.8. From an isomorphism $M \oplus \mathbf{A}^r \to \mathbf{A}^n$, we obtain the projection $\pi : \mathbf{A}^n \to \mathbf{A}^n$ over $\mathbf{A}^r$ parallel to M. This also gives a surjective $\mathbf{A}$-linear map $\varphi : \mathbf{A}^n \to \mathbf{A}^r$ with $\mathrm{Ker}\,\pi = \mathrm{Ker}\,\varphi \simeq M$: it suffices to let $\varphi(x) = \pi(x)$ for all $x \in \mathbf{A}^n$.

Conversely, if we have a surjective linear map $\varphi : \mathbf{A}^n \to \mathbf{A}^r$, there exists a $\psi : \mathbf{A}^r \to \mathbf{A}^n$ such that $\varphi \circ \psi = \mathrm{Id}_{\mathbf{A}^r}$. Then $\pi = \psi \circ \varphi : \mathbf{A}^n \to \mathbf{A}^n$ is a projection, with $\mathrm{Ker}\,\pi = \mathrm{Ker}\,\varphi$, $\mathrm{Im}\,\pi = \mathrm{Im}\,\psi$ and $\mathrm{Ker}\,\pi \oplus \mathrm{Im}\,\pi = \mathbf{A}^n$, and since $\mathrm{Im}\,\pi \simeq \mathrm{Im}\,\varphi = \mathbf{A}^r$, the module

$$M = \mathrm{Ker}\,\varphi = \mathrm{Ker}\,\pi \simeq \mathrm{Coker}\,\pi = \mathrm{Coker}\,\psi$$

is stably free, and isomorphic to $\mathrm{Im}(\mathrm{Id}_{\mathbf{A}^n} - \pi)$. Recall that by Theorem II-5.22, saying that $\varphi : \mathbf{A}^n \to \mathbf{A}^r$ is surjective amounts to saying that φ is of rank r, i.e. that $\mathcal{D}_r(\varphi) = \langle 1 \rangle$ in this case.

Finally, if we start from an injective linear map $\psi : \mathbf{A}^r \to \mathbf{A}^n$, saying that there exists a $\varphi : \mathbf{A}^n \to \mathbf{A}^r$ such that $\varphi \circ \psi = \mathrm{Id}_{\mathbf{A}^r}$ amounts to saying that $\mathcal{D}_r(\psi) = \langle 1 \rangle$ (Theorem II-5.14). Let us summarize the previous discussion.

[1] This notion of rank will be generalized, Definitions 8.5 and X-2.2, and the reader will be able to note that those are indeed generalizations.

4.1. Fact. *For a module M the following properties are equivalent.*

1. *M is stably free.*
2. *M is isomorphic to the kernel of a surjective matrix.*
3. *M is isomorphic the cokernel of an injective matrix of maximum rank.*

This result can allow us to define a new encoding, specific to stably free modules. Such a module will be encoded by the matrices of the linear maps φ and ψ. As for the dual of M it will be encoded by the transposed matrices, as indicated in the following fact.

4.2. Fact. *Using the previous notations, $M^\star$ is stably free, canonically isomorphic to* $\mathrm{Coker}\,{}^{\mathrm{t}}\!\varphi$ *and to* $\mathrm{Ker}\,{}^{\mathrm{t}}\!\psi$.

This is a special case of the following more general result (see also Fact II-6.3).

4.3. Proposition. *Let $\varphi : E \to F$ be a split surjection and $\psi : F \to E$ be a section of φ. Let $\pi : E \to E$ be the projection $\psi \circ \varphi$, and $j :$ $\mathrm{Ker}\,\varphi \to E$ be the canonical injection.*

1. *$E = \mathrm{Im}\,\psi \oplus \mathrm{Ker}\,\varphi$, $\mathrm{Ker}\,\varphi = \mathrm{Ker}\,\pi \simeq \mathrm{Coker}\,\pi = \mathrm{Coker}\,\psi$.*
2. $\mathrm{Ker}\,{}^{\mathrm{t}}\!j = \mathrm{Im}\,{}^{\mathrm{t}}\!\varphi$ *and ${}^{\mathrm{t}}\!j$ is surjective, which by factorization gives a canonical isomorphism* $\mathrm{Coker}\ {}^{\mathrm{t}}\!\varphi \xrightarrow{\sim} (\mathrm{Ker}\,\varphi)^\star$.

D The linear map ψ is a generalized inverse of φ (Definition II-5.16). We therefore have $E = \mathrm{Im}\,\psi \oplus \mathrm{Ker}\,\varphi$, and ψ and φ define reciprocal isomorphisms between F and $\mathrm{Im}\,\psi$. The proposition easily follows (see Fact II-5.17). □

When is a stably free module free?

We then obtain the following results, formulated in terms of the kernel of a surjective matrix.

4.4. Proposition. (When a stably free module is free, 1)
Let $n = r + s$ and $R \in \mathbf{A}^{r\times n}$. The following properties are equivalent.

1. *R is surjective and the kernel of R is free.*
2. *There exists a matrix $S \in \mathbf{A}^{s\times n}$ such that the matrix $\begin{bmatrix} S \\ R \end{bmatrix}$ is invertible.*

In particular, every stably free module of rank 1 *is free.*

D *1 ⇒ 2.* If R is surjective, there exists an $R' \in \mathbf{A}^{n\times r}$ with $RR' = \mathrm{I}_r$. The matrices R and R' correspond to the linear maps φ and ψ in the preliminary discussion. In particular, we have $\mathbf{A}^n = \mathrm{Ker}\,R \oplus \mathrm{Im}\,R'$. Consider a matrix S' whose column vectors constitute a basis of the kernel of R. Since $\mathbf{A}^n = \mathrm{Ker}\,R \oplus \mathrm{Im}\,R'$, the matrix $A' = [\,S' \mid R'\,]$ has as its columns a basis of $\mathbf{A}^n$. It is invertible and its inverse is of the form $\begin{bmatrix} S \\ R \end{bmatrix}$ because R is the only matrix that satisfies $R\,A' = [\,0_{r,n-r} \mid \mathrm{I}_r\,]$.

2 ⇒ *1.* Let $A = \begin{bmatrix} S \\ R \end{bmatrix}$ and let $A' = A^{-1}$, which we write in the form $[\,S' \mid R'\,]$. We have $RS' = 0_{r,n-r}$, therefore

$$\operatorname{Im} S' \subseteq \operatorname{Ker} R \qquad (\alpha),$$

and $RR' = \mathrm{I}_r$. Therefore

$$\operatorname{Ker} R \oplus \operatorname{Im} R' = \mathbf{A}^n = \operatorname{Im} S' \oplus \operatorname{Im} R' \qquad (\beta).$$

Finally, (α) and (β) imply $\operatorname{Im} S' = \operatorname{Ker} R$.

If M is a stably free module of rank 1, it is the kernel of a surjective matrix $R \in \mathbf{A}^{(n-1)\times n}$. Since the matrix is surjective, we obtain $1 \in \mathcal{D}_{n-1}(R)$, and this gives the row S to complete R as an invertible matrix (develop the determinant according to the first row). □

4.5. Corollary. (When a stably free module is free, 2)
Consider $R \in \mathbf{A}^{r\times n}$ and $R' \in \mathbf{A}^{n\times r}$ with $RR' = \mathrm{I}_r$, $s := n - r$. Then, the modules Ker R *and* Coker R' *are isomorphic and the following properties are equivalent.*

1. *The kernel of R is free.*
2. *There exists a matrix $S' \in \mathbf{A}^{s\times n}$ such that $[\,S' \mid R'\,]$ is invertible.*
3. *There exist a matrix $S' \in \mathbf{A}^{s\times n}$ and a matrix $S \in \mathbf{A}^{s\times n}$ such that*

$$\begin{array}{|c|}\hline S \\ \hline R \\ \hline \end{array}\;\begin{array}{|c|c|}\hline S' & R' \\ \hline \end{array} = \mathrm{I}_n.$$

Recall that a vector $x \in \mathbf{A}^q$ is said to be *unimodular* when its coordinates are comaximal elements. It is said to be *completable* if it is the first vector (row or column) of an invertible matrix.

4.6. Proposition. *The following properties are equivalent.*

1. *Every stably free* **A***-module of rank $\geqslant m$ is free.*
2. *Every unimodular vector in $\mathbf{A}^{q\times 1}$ with $q > m$ is completable.*
3. *Every unimodular vector in $\mathbf{A}^q$ with $q > m$ generates the direct complement of a free module in $\mathbf{A}^q$.*

D Items *2* and *3* are clearly equivalent.

1 ⇒ *3.* Let $x \in \mathbf{A}^q$ be a unimodular vector with $q > m$. Then, we can write $\mathbf{A}^q = M \oplus \mathbf{A}x$, and M is stably free of rank $q - 1 \geqslant m$, therefore free.

3 ⇒ *1.* Let M be a stably free **A**-module of rank $n \geqslant m$. We can write $L = M \oplus \mathbf{A}x_1 \oplus \cdots \oplus \mathbf{A}x_r$, where $L \simeq \mathbf{A}^{n+r}$. If $r = 0$, there is nothing left to do. Otherwise, x_r is a unimodular vector in L, therefore by hypothesis $\mathbf{A}x_r$ admits a free complementary subspace in L. Thus, $L/\mathbf{A}x_r \simeq \mathbf{A}^{n+r-1}$, and similarly with $M \oplus \mathbf{A}x_1 \oplus \cdots \oplus \mathbf{A}x_{r-1}$, which is isomorphic to $L/\mathbf{A}x_r$. We can therefore conclude by induction on r that M is free. □

Bass' stable range

The notion of a stable range is linked to the elementary manipulations (of rows or columns) and allows us to some extent to control the stably free modules.

4.7. Definition. Let $n \geqslant 0$. A ring $\mathbf{A}$ is said to be of *Bass' stable range less than or equal to n* when we can "shorten" the unimodular vectors of length $n+1$ in the following sense

$$1 \in \langle a, a_1, \dots, a_n \rangle \implies \exists\, x_1, \dots, x_n,\ 1 \in \langle a_1 + x_1 a, \dots, a_n + x_n a \rangle.$$

In this case we write "$\mathsf{Bdim}\,\mathbf{A} < n$."

In the acronym Bdim, B alludes to "Bass."

The notation $\mathsf{Bdim}\,\mathbf{A} < n$ is legitimized on the one hand by item *1* in the following fact, and on the other hand by results to come which compare Bdim to natural dimensions in commutative algebra.[2]

Item *3.* uses the ideal $\mathrm{Rad}\,\mathbf{A}$ which will be defined in Chapter IX. The thing to note is that an element of $\mathbf{A}$ is invertible if and only if it is invertible modulo $\mathrm{Rad}\,\mathbf{A}$.

4.8. Fact. *Let $\mathbf{A}$ be a ring and $\mathfrak{a}$ be an ideal.*

1. *If $\mathsf{Bdim}\,\mathbf{A} < n$ and $n < m$ then $\mathsf{Bdim}\,\mathbf{A} < m$.*
2. *For all $n \geqslant 0$, we have $\mathsf{Bdim}\,\mathbf{A} < n \Rightarrow \mathsf{Bdim}\,\mathbf{A}/\mathfrak{a} < n$. Abbreviated, we write this implication in the form: $\mathsf{Bdim}\,\mathbf{A}/\mathfrak{a} \leqslant \mathsf{Bdim}\,\mathbf{A}$.*
3. *We have $\mathsf{Bdim}(\mathbf{A}/\mathrm{Rad}\,\mathbf{A}) = \mathsf{Bdim}\,\mathbf{A}$ (by using the same abbreviation).*

D *1.* We take $m = n+1$. Let $(a, a_0, \dots, a_n)$ with $1 \in \langle a, a_0, \dots, a_n \rangle$. We have $1 = ua + va_0 + \dots$, so $1 \in \langle a', a_1, \dots, a_n \rangle$ with $a' = ua + va_0$. Therefore we have $x_1, \dots, x_n$ in $\mathbf{A}$ with $1 \in \langle a_1 + x_1 a', \dots, a_n + x_n a' \rangle$, and consequently $1 \in \langle a_0 + y_0 a, \dots, a_n + y_n a \rangle$ with $y_0 = 0$ and $y_i = x_i u$ for $i \geqslant 1$.

2 and *3.* Left to the reader. □

4.9. Fact. (Unimodular vectors and elementary transformations)
Let $n \geqslant 0$. If $\mathsf{Bdim}\,\mathbf{A} < n$ and $V \in \mathbf{A}^{n+1}$ is unimodular, it can be transformed into the vector $(1, 0 \dots, 0)$ by elementary operations.

D Let $V = (v_0, v_1, \dots, v_n)$, with $1 \in \langle v_0, v_1, \dots, v_n \rangle$. Applying the definition with $a = v_0$, we obtain $x_1, \dots, x_n$ such that

$$1 \in \langle v_1 + x_1 v_0, \dots, v_n + x_n v_0 \rangle\,.$$

The vector V can be transformed by elementary operations into the vector $V' = (v_0, v_1 + x_1 v_0, \dots, v_n + x_n v_0) = (v_0, v'_1, \dots, v'_n)$, and we have y_i's such

[2] See for example the results in Chapter XIV which establish a comparison with the Krull and Heitmann dimensions.

that $\sum_{i=1}^{n} y_i v_i' = 1$. By elementary operations, we can transform V' into $(1, v_1', \dots, v_n')$, and then into $(1, 0, \dots, 0)$. □

Proposition 4.6 and Fact 4.9 give the following “Bass’ theorem.” Actually, the real Bass’ theorem is rather the conjunction of the following theorem with a theorem that provides a sufficient condition to have $\mathsf{Bdim}\,\mathbf{A} < n$. We will present several different variants in Theorems XIV-1.4 and XIV-2.6 and Fact XIV-3.3.

4.10. Theorem. (Bass’ theorem, stably free modules)
If $\mathsf{Bdim}\,\mathbf{A} < n$, every stably free $\mathbf{A}$-module of rank $\geqslant n$ is free.

5. Natural constructions

5.1. Proposition. (Changing the base ring)
If P is a finitely generated projective $\mathbf{A}$-module and if $\rho : \mathbf{A} \to \mathbf{B}$ is a ring homomorphism, then the $\mathbf{B}$-module $\rho_\star(P)$ obtained by scalar extension to $\mathbf{B}$ is finitely generated projective. If P is isomorphic to the image of a projection matrix $F = (f_{i,j})$, $\rho_\star(P)$ is isomorphic to the image of the same matrix seen in $\mathbf{B}$, *i.e. the projection matrix $F^\rho = \big(\rho(f_{i,j})\big)$.*

D Changing the base ring preserves the direct sums and the projections. □

In the following proposition, we can a priori take as the sets of indices $I = [\![1..m]\!]$ and $J = [\![1..n]\!]$, but the set $I \times J$, which serves as a set of indices for the square matrix that defines the *Kronecker product* of the two matrices F and G is not equal to $[\![1..mn]\!]$. This is an important argument in favor of the definition of matrices à la Bourbaki, i.e. with finite row and column index sets which are not necessarily of the type $[\![1..m]\!]$.

5.2. Proposition. (Tensor product)
If P and Q are projective modules represented by the projection matrices $F = (p_{i,j})_{i,j \in I} \in \mathbf{A}^{I \times I}$ and $G = (q_{k,\ell})_{k,\ell \in J} \in \mathbf{A}^{J \times J}$, then the tensor product $P \otimes Q$ is a finitely generated projective module represented by the Kronecker product

$$F \otimes G = \big(r_{(i,k),(j,\ell)}\big)_{(i,k),(j,\ell) \in I \times J},$$

where $r_{(i,k),(j,\ell)} = p_{i,j} q_{k,\ell}$.

D Suppose $P \oplus P' = \mathbf{A}^m$ and $Q \oplus Q' = \mathbf{A}^n$. The matrix F (resp. G) represents the projection over P (resp. Q) parallel to P' (resp. Q'). Then, the Kronecker product matrix $F \otimes G$ represents the projection of $\mathbf{A}^m \otimes \mathbf{A}^n$ over $P \otimes Q$, parallel to the subspace $(P' \otimes Q) \oplus (P \otimes Q') \oplus (P' \otimes Q')$. □

5.3. Proposition. (Dual of a finitely generated projective module, 2)
If P is represented by the projection matrix $F = (p_{i,j})_{i,j\in I} \in \mathbf{A}^{I\times I}$, then the dual of P is a finitely generated projective module represented by the transposed matrix of F. If x is a column vector in $\operatorname{Im} F$ and α a column vector in the image of ${}^{\mathrm{t}}F$, the scalar $\alpha(x)$ is the unique coefficient of the matrix ${}^{\mathrm{t}}\alpha\, x$.

D This results from Fact 2.2. □

5.4. Proposition. (Modules of linear maps)

1. *If P or Q is finitely generated projective, the natural homomorphism (page 247)*
$$\theta_{P,Q} : P^\star \otimes Q \to \mathrm{L}_{\mathbf{A}}(P,Q)$$
is an isomorphism.
2. *If P and Q are finitely generated projective, the module $\mathrm{L}_{\mathbf{A}}(P,Q)$ is a finitely generated projective module canonically isomorphic to $P^\star \otimes Q$, represented by the matrix ${}^{\mathrm{t}}F \otimes G$.*
3. *An $\mathbf{A}$-module P is finitely generated projective if and only if the natural homomorphism θ_P is an isomorphism.*

D *1.* Suppose $P \oplus P' = \mathbf{A}^m$. We have isomorphisms

$$\begin{aligned} \mathrm{L}_{\mathbf{A}}(\mathbf{A}^m, Q) &\simeq \mathrm{L}_{\mathbf{A}}(P,Q) \oplus \mathrm{L}_{\mathbf{A}}(P',Q), \\ (\mathbf{A}^m)^\star \otimes Q &\simeq (P \oplus P')^\star \otimes Q \\ &\simeq (P^\star \oplus (P')^\star) \otimes Q \\ &\simeq \big(P^\star \otimes Q\big) \oplus \big((P')^\star \otimes Q\big). \end{aligned}$$

These isomorphisms are compatible with the natural homomorphisms

$$\begin{aligned} Q^m \simeq (\mathbf{A}^m)^\star \otimes Q &\longrightarrow \mathrm{L}_{\mathbf{A}}(\mathbf{A}^m, Q) \simeq Q^m, \\ P^\star \otimes Q &\longrightarrow \mathrm{L}_{\mathbf{A}}(P,Q), \\ (P')^\star \otimes Q &\longrightarrow \mathrm{L}_{\mathbf{A}}(P',Q). \end{aligned}$$

As the first is an isomorphism, so are the others.
The case where Q is finitely generated projective is treated analogously.

2. Special case of item *1*.

3. Results from item *1* and from the fact that P is finitely generated projective if the image of θ_P contains Id_P (Theorem 2.1 ($b3$)). □

By using the commutation of the scalar extension with the tensor product we then obtain the following corollary.

5.5. Corollary. *If P or Q is finitely generated projective (over $\mathbf{A}$), and if $\mathbf{A} \xrightarrow{\rho} \mathbf{B}$ is an algebra, the natural homomorphism*
$$\rho_\star\big(\mathrm{L}_{\mathbf{A}}(P,Q)\big) \to \mathrm{L}_{\mathbf{B}}\big(\rho_\star(P), \rho_\star(Q)\big)$$
is an isomorphism.

6. Local structure theorem

In this work, we give several proofs of the local structure theorem for finitely generated projective modules. The shortest path to the solution of this question is that provided by Fitting ideals. This is the object of this section.

There is a lightning method based a kind of magic formula given in Exercise X-3. This miracle solution is actually directly inspired by another approach to the problem, based on a "dynamic reread" of the local freeness lemma (page 494). This dynamic reread is explained on page 872 in Section XV-5.

However, we consider a more enlightening approach is that based entirely on projection matrices and on the more structural explanations involving the systematic use of the determinant of the endomorphisms of finitely generated projective modules. This will be done in Chapter X.

6.1. Theorem. (Local structure and Fitting ideals of a finitely generated projective module, 1)

1. *A finitely presented* $\mathbf{A}$*-module* P *is finitely generated projective if and only if its Fitting ideals are (generated by) idempotents.*
2. *More precisely for the converse, suppose that a finitely presented* $\mathbf{A}$*-module* P *has idempotents Fitting ideals, and that* $G \in \mathbf{A}^{q\times n}$ *is a presentation matrix of* P*, corresponding to a system of* q *generators.*
   Let f_h *be the idempotent that generates* $\mathcal{F}_h(P)$*, and* $r_h := f_h - f_{h-1}$*.*
   a. $(r_0, \dots, r_q)$ *is a fundamental system of orthogonal idempotents.*
   b. *Let* $t_{h,j}$ *be a minor of order* $q-h$ *of* G*, and* $s_{h,j} := t_{h,j}r_h$*. Then, the* $\mathbf{A}[1/s_{h,j}]$*-module* $P[1/s_{h,j}]$ *is free of rank* h*.*
   c. *The elements* $s_{h,j}$ *are comaximal.*
   d. *We have* $r_k = 1$ *if and only if the matrix* G *is of rank* $q-k$*.*
   e. *The module* P *is finitely generated projective.*
3. *In particular, a finitely generated projective module becomes free after localization at a finite number of comaximal elements.*

D Theorem 2.3 tells us that the module P presented by the matrix G is projective if and only if the matrix G is locally simple. We then apply the characterization of locally simple matrices by their determinantal ideals given in Theorem II-5.26, as well as the precise description of the structure of the locally simple matrices given in this theorem (items *5* and *7* of the theorem).

Note: item *3* can be obtained more directly by applying Theorem II-5.26 to an idempotent matrix (therefore locally simple) whose image is isomorphic to the module P. □

Thus, the finitely generated projective modules are locally free, in the strong sense given in Theorem 1.1.

In Section X-1 we give an alternative proof of Theorem 1.1, more intuitive and more enlightening than the one we just gave. In addition, the comaximal elements that provide free localizations are fewer.

Remark. We can therefore test if a finitely presented module is projective or not when we know how to test whether its Fitting ideals are idempotents or not. This is possible if we know how to test the membership $x \in \langle a_1, \dots, a_h \rangle$ for every system $(x, a_1, \dots, a_h)$ of elements of $\mathbf{A}$, i.e. if the ring is strongly discrete. One can now compare with [MRR] Chap. III Exercise 4 p. 96. ■

Annihilator of a finitely generated projective module

6.2. Lemma. *The annihilator of a finitely generated projective module P is equal to its first Fitting ideal $\mathcal{F}_0(P)$, generated by an idempotent.*

D We know that the Fitting ideals are generated by idempotents. We also know that $\mathcal{F}_0(P) \subseteq \mathrm{Ann}(P)$ (Lemma IV-9.6).
Let us look at the opposite inclusion. Fact II-6.6 implies that the annihilator of a finitely generated module is well-behaved under localization, so for every monoid S, we have $\mathrm{Ann}_{\mathbf{A}_S}(P_S) = \big(\mathrm{Ann}_{\mathbf{A}}(P)\big)_S$. We know that the same holds for the Fitting ideals of a finitely presented module. Moreover, to prove an inclusion of ideals, we can localize at some comaximal elements. We therefore choose comaximal elements that render the module P free, in which case the result is obvious. □

The previous proof is an example of the strength of the local structure theorem (item *3* of Theorem 6.1). The following section describes another such example.

7. Locally cyclic projective modules and finitely generated projective ideals

Locally cyclic modules

An $\mathbf{A}$-module M is said to be *cyclic* if it is generated by a single element: $M = \mathbf{A}a$. In other words, if it is isomorphic to a quotient $\mathbf{A}/\mathfrak{a}$.

In classical mathematics a module is said to be *locally cyclic* if it becomes cyclic after localization at any arbitrary prime ideal. It seems difficult to provide an equivalent statement that makes sense in constructive mathematics. Recall also that the remark page 33 shows that the notion does not seem pertinent when the module is not assumed to be finitely generated. Nevertheless when we restrict ourselves to the finitely generated modules there is no issue. The following definition has already been given before Fact II-2.5.

7.1. Definition. A *finitely generated* $\mathbf{A}$-module M is said to be *locally cyclic* if there exist comaximal monoids $S_1, \dots, S_n$ of $\mathbf{A}$ such that each M_{S_j} is cyclic as an $\mathbf{A}_{S_j}$-module. In the case of an ideal we speak of a *locally principal ideal.*

Note that the property "concrete local" in the previous definition, without the hypothesis that M is finitely generated, implies that M is finitely generated (local-global principle II-3.6).

We will need the following remark.

7.2. Fact. (Successive localizations lemma, 1)
If $s_1, \dots, s_n$ are comaximal elements of $\mathbf{A}$ and if for each i, we have elements $s_{i,1}, \dots, s_{i,k_i}$, comaximal in $\mathbf{A}[1/s_i]$, then the elements $s_i s_{i,j}$ are comaximal in $\mathbf{A}$.

Item *3* of the following theorem presents an efficient computational machinery for locally cyclic modules.

7.3. Theorem. (Locally cyclic finitely generated modules)
Let $M = \mathbf{A}x_1 + \cdots + \mathbf{A}x_n$ be a finitely generated module. The following properties are equivalent.

1. *The module M is locally cyclic.*
2. *There exist n comaximal elements s_i of $\mathbf{A}$ such that for each i we have $M =_{\mathbf{A}_{s_i}} \langle x_i \rangle$.*
3. *There exists a matrix $A = (a_{ij}) \in \mathbb{M}_n(\mathbf{A})$ that satisfies*
$$\left\{\begin{array}{rcl} \sum a_{ii} & = & 1 \\ a_{\ell j} x_i & = & a_{\ell i} x_j \qquad \forall i, j, \ell \in [\![1..n]\!] \end{array}\right. \tag{3}$$
in other words, for each row ℓ, the following matrix is formally of rank $\leqslant 1$ (its minors of order 2 are null)
$$\begin{bmatrix} a_{\ell 1} & \cdots & a_{\ell n} \\ x_1 & \cdots & x_n \end{bmatrix}.$$
4. *$\bigwedge^2_{\mathbf{A}}(M) = 0$.*
5. *$\mathcal{F}_1(M) = \langle 1 \rangle$.*

6. After localization at any prime ideal, M is cyclic.*
7. After localization at any maximal ideal, M is cyclic.*

D *3* ⇒ *2* ⇒ *1*. Clear, with $s_i = a_{ii}$ in item *2*.
Let us show that a cyclic module satisfies condition *3*.
If $M = \langle g \rangle$, we have $g = \sum_{i=1}^n u_i x_i$ and $x_i = g y_i$. Let $b_{ij} = u_i y_j$.
Then, for all i, j, $\ell \in [\![1..n]\!]$, we have $b_{\ell j} x_i = u_\ell y_i y_j g = b_{\ell i} x_j$. In addition
$$g = \textstyle\sum_{i=1}^n u_i x_i = \sum_{i=1}^n u_i y_i g = \big(\sum_{i=1}^n b_{ii}\big) g.$$
Let $s = 1 - \sum_{i=1}^n b_{ii}$. We have $sg = 0$, and so $s x_k = 0$ for all k.
Take $a_{ij} = b_{ij}$ for $(i,j) \neq (n,n)$ and $a_{nn} = b_{nn} + s$. Then, the matrix (a_{ij}) indeed satisfies Equations (3).

1 ⇒ *3.* The property *3* can be seen as the existence of a solution of a system of linear equations whose coefficients are expressed in terms of the generators x_i. However, a cyclic module satisfies the property *3.* We can therefore apply the basic local-global principle.

Thus, *1* ⇔ *2* ⇔ *3.*

1 ⇒ *4* and *1* ⇒ *5.* Because the functors $\bigwedge^2_{\mathbf{A}} \bullet$ and $\mathcal{F}_1(\bullet)$ are well-behaved under localization.

5 ⇒ *1.* M is the quotient module of a finitely presented module M' such that $\mathcal{F}_1(M') = \langle 1 \rangle$. We can therefore suppose without loss of generality that M is finitely presented with a presentation matrix $B \in \mathbf{A}^{n \times m}$. By hypothesis, the minors of order $n-1$ of the matrix B are comaximal. When we invert one of these minors, by the invertible minor lemma (page 45), the matrix B is equivalent to a matrix

$$\begin{bmatrix} \mathrm{I}_{n-1} & 0_{n-1,m-n+1} \\ 0_{1,n-1} & B_1 \end{bmatrix},$$

and the matrix $B_1 \in \mathbf{A}^{1 \times (m-n+1)}$ is also a presentation matrix of M.

Assume *4* and $n \geqslant 2$, and let us show that M is, after localization at suitable comaximal elements, generated by $n-1$ elements. This will be sufficient to show (by using an induction on n) that *4* implies *1*, by using Fact 7.2. The module $\bigwedge^2_{\mathbf{A}}(M)$ is generated by the elements $v_{j,k} = x_j \wedge x_k$ $(1 \leqslant j < k \leqslant n)$ and the syzygies between the $v_{j,k}$'s are all obtained from the syzygies between the x_i's. Therefore if $\bigwedge^2_{\mathbf{A}}(M) = 0$, M is the quotient of a finitely presented module M' such that $\bigwedge^2_{\mathbf{A}}(M') = 0$. We then suppose without loss of generality that M is finitely presented with a presentation matrix $A = (a_{ij})$. A presentation matrix B for $\bigwedge^2_{\mathbf{A}}(M)$ with the generators $v_{j,k}$ is obtained as indicated in Proposition IV-4.9. It is a matrix of format $\frac{n(n-1)}{2} \times m$ (for some suitable m), and each coefficient of B is null or equal to some a_{ij}. This matrix is surjective, therefore $\mathcal{D}_{n(n-1)/2}(B) = \langle 1 \rangle$ and the a_{ij}'s are comaximal. However, when we pass from $\mathbf{A}$ to $\mathbf{A}[1/a_{ij}]$, x_i becomes linear combination of the x_k's $(k \neq i)$ and M is generated by $n-1$ elements.

1 ⇒ *6** ⇒ *7*.* Obvious.

The proof that *7** implies *3* is nonconstructive: in the proof that *1* implies *3*, we replace the existence of a solution of a system of linear equations under the basic local-global principle by the existence of a solution under the corresponding abstract local-global principle. □

A matrix (a_{ij}) which satisfies Equations (3) is called a *cyclic localization matrix for the n-tuple* $(x_1, \dots, x_n)$. If the x_i's are elements of $\mathbf{A}$, they generate a locally principal ideal and we speak of a *principal localization matrix.*

Remark. In the case of a module generated by 2 elements $M = \mathbf{A}x + \mathbf{A}y$, Equations (3) are very simple and a cyclic localization matrix for (x, y) is a matrix $\begin{bmatrix} 1-u & -b \\ -a & u \end{bmatrix}$ which satisfies

$$\begin{vmatrix} 1-u & -b \\ x & y \end{vmatrix} = \begin{vmatrix} -a & u \\ x & y \end{vmatrix} = 0, \text{ i.e. } (1-u)y = bx \text{ and } ux = ay. \tag{4}$$

∎

7.4. Proposition. *Let $M = \mathbf{A}x_1 + \cdots + \mathbf{A}x_n$ be a finitely generated $\mathbf{A}$-module.*

1. *If M is locally cyclic and if $A = (a_{ij})$ is a cyclic localization matrix for $(x_1, \ldots, x_n)$, we have the following results.*
   - *a.* $\begin{bmatrix} x_1 & \cdots & x_n \end{bmatrix} A = \begin{bmatrix} x_1 & \cdots & x_n \end{bmatrix}$.
   - *b. The ideals $\mathcal{D}_2(A)$ and $\mathcal{D}_1(A^2 - A)$ annihilate M.*
   - *c. One has $a_{ii}M \subseteq \mathbf{A}x_i$, and over the ring $\mathbf{A}_i = \mathbf{A}[\frac{1}{a_{ii}}]$, $M =_{\mathbf{A}_i} \mathbf{A}_i x_i$.*
   - *d.* $\langle a_{1j}, \ldots, a_{nj} \rangle M = \mathbf{A}x_j$.
   - *e. More generally, for any arbitrary element $y = \sum \alpha_i x_i$ of M, if we let $\alpha = {}^t[\alpha_1 \ \cdots \ \alpha_n]$ and $\beta = A\,\alpha$, then $y = \sum_i \beta_i x_i$ and we obtain an equality of square matrices with coefficients in M:*

   $$\beta x = \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix} \begin{bmatrix} x_1 & \cdots & x_n \end{bmatrix} = A\,y, \quad \textit{i.e.} \quad \forall i, j \ \beta_i x_j = a_{ij} y \tag{5}$$

   In particular, $\langle \beta_1, \ldots, \beta_n \rangle M = \mathbf{A}y$.
2. *The following properties are equivalent.*
   - *M is isomorphic to the image of a projection matrix of rank* 1.
   - *M is faithful (i.e.* $\operatorname{Ann}(M) = 0$*) and locally cyclic.*

   In this case, let A be a cyclic localization matrix for $(x_1, \ldots, x_n)$. We obtain
   - *A is a projection matrix of rank* 1,
   - *the following sequence is exact* $\mathbf{A}^n \xrightarrow{\mathrm{I}_n - A} \mathbf{A}^n \xrightarrow{[\,x_1\ \cdots\ x_n\,]} M \to 0$,
   - $M \simeq \operatorname{Im} A$.

D *1.* Item *1c* is clear, and *1d* is a special case of *1e*.

1a. The j^{th} coordinate of $\begin{bmatrix} x_1 & \cdots & x_n \end{bmatrix} A$ is written as

$$\sum\nolimits_{i=1}^{n} a_{ij} x_i = \sum\nolimits_{i=1}^{n} a_{ii} x_j = x_j.$$

1b. Let us show that every minor of order 2 of A annihilates x_i. Consider the following matrix

$$\begin{bmatrix} a_{ji} & a_{j\ell} & a_{jh} \\ a_{ki} & a_{k\ell} & a_{kh} \\ x_i & x_\ell & x_h \end{bmatrix}.$$

Its determinant is null (by expanding with respect to the first row) and the expansion with respect to the first column provides

$$(a_{j\ell}a_{kh} - a_{jh}a_{k\ell})x_i = 0.$$

Let us show that $A^2 = A$ modulo $\mathrm{Ann}(M)$. What follows is written modulo this annihilator. We come to show that the minors of order 2 of A are null. Thus A is a cyclic localization matrix for each of its rows L_i. By item *1a* applied to L_i, we have $L_i\,A = L_i$, and so $A^2 = A$.

1e. Let $\underline{x} = \begin{bmatrix} x_1 & \cdots & x_n \end{bmatrix}$. On the one hand

$$\sum\nolimits_i \beta_i x_i = \underline{x}\beta = \underline{x}A\alpha = \underline{x}\alpha = \sum\nolimits_i \alpha_i x_i.$$

On the other hand,

$$\beta_i x_j = \sum\nolimits_k \alpha_k\, a_{ik}\, x_j = \sum\nolimits_k \alpha_k\, a_{ij}\, x_k = a_{ij}\left(\sum\nolimits_k \alpha_k x_k\right) = a_{ij}\, y.$$

This shows Equality (5) and we deduce that $\langle \beta_1, \ldots, \beta_n \rangle\, M = \mathbf{A}y$.

2. First assume that M is isomorphic to the image of a projection matrix A of rank 1. Let x_i be the i^{th} column of A. As $\mathcal{D}_2(A) = 0$, we have the equalities $a_{\ell j}x_i = a_{\ell i}x_j$ for $i, j, \ell \in [\![1..n]\!]$. This implies that over the ring $\mathbf{A}[1/a_{\ell j}]$, M is generated by x_j, and since $\mathcal{D}_1(A) = \langle 1 \rangle$, the module is locally cyclic. Finally, let $b \in \mathrm{Ann}(M)$, then $bA = 0$, and $\mathcal{D}_1(A) = \langle 1 \rangle$ implies $b = 0$; the module is faithful.

Now assume that M is locally cyclic, and that A is a cyclic localization matrix for a generator set $(x_1, \ldots, x_n)$. If M is faithful, given *1b*, we have $\mathcal{D}_2(A) = 0$ and $A^2 = A$ so A is a projection matrix of rank $\leqslant 1$. Since $\mathrm{Tr}(A) = 1$, A is of rank 1. Given *1a*, the matrix $\mathrm{I}_n - A$ is a matrix of syzygies for $(x_1, \ldots, x_n)$. Now let $\sum_{i=1}^n \alpha_i x_i = 0$ be an arbitrary syzygy of the x_i's. As in *1e*, let

$$\beta = {}^{\mathrm{t}}[\, \beta_1 \ \cdots \ \beta_n \,] = A\ {}^{\mathrm{t}}[\, \alpha_1 \ \cdots \ \alpha_n \,],$$

we obtain $\langle \beta_1, \ldots, \beta_n \rangle\, M = 0$ and, since M is faithful, $\beta = 0$.

Thus, $A\ {}^{\mathrm{t}}[\, \alpha_1 \ \cdots \ \alpha_n \,] = 0$ and $(\mathrm{I}_n - A)\ {}^{\mathrm{t}}[\, \alpha_1 \ \cdots \ \alpha_n \,] = {}^{\mathrm{t}}[\, \alpha_1 \ \cdots \ \alpha_n \,]$: every syzygy for $(x_1, \ldots, x_n)$ is a linear combination of the columns of $\mathrm{I}_n - A$. This shows that $\mathrm{I}_n - A$ is a presentation matrix of M for the generator set $(x_1, \ldots, x_n)$. Since $A^2 = A$, we have $M \simeq \mathrm{Coker}(\mathrm{I}_n - A) \simeq \mathrm{Im}\, A$. □

Cyclic projective modules

The following description applies in particular to projective principal ideals.

7.5. Lemma. *For a cyclic module M, the following properties are equivalent.*

1. *M is a finitely generated projective $\mathbf{A}$-module.*
2. *$\mathrm{Ann}(M) = \langle s \rangle$ with s idempotent.*
3. *$M \simeq \langle r \rangle$ with r idempotent.*

D The implications *2* ⇒ *3* ⇒ *1* are obvious, and the implication *1* ⇒ *2* is given in Lemma 6.2. □

We deduce that a ring $\mathbf{A}$ is *quasi-integral* if and only if every principal ideal is projective, which justifies the English terminology *pp-ring* (principal ideals are projective).

Locally cyclic projective modules

The following lemma generalizes the equivalence given in Proposition 7.4 between faithful locally cyclic modules and images of projection matrices of rank 1.

7.6. Lemma. *The following properties are equivalent.*

1. *M is locally cyclic and $\mathrm{Ann}(M)$ is generated by an idempotent.*
2. *M is finitely generated projective and locally cyclic.*
3. *M is isomorphic to the image of a projection matrix of rank $\leqslant 1$.*

D *1* ⇒ *2.* We localize at comaximal elements that render the module cyclic and we apply Lemma 7.5.

In *2* and *3* we let F be a square projection matrix of order n, with M as its image. After localization at comaximal elements it becomes similar to a standard projection matrix $\mathrm{I}_{k,n}$, k depending on the localization.

2 ⇒ *3.* If $k > 1$, we obtain at the corresponding localization $\mathcal{F}_1(M) = \langle 0 \rangle$. As we have already $\mathcal{F}_1(M) = \langle 1 \rangle$, the localization is trivial. The rank of F is therefore $\leqslant 1$ at all the localizations.

3 ⇒ *1.* After localization, as the matrix is of rank $\leqslant 1$, we have $k \leqslant 1$. The module therefore becomes cyclic. Moreover, by Lemma 6.2, $\mathrm{Ann}(M)$ is generated by an idempotent. □

Finitely generated projective ideals

Recall that an ideal $\mathfrak{a}$ is said to be *faithful* if it is faithful as an $\mathbf{A}$-module.

Remark. In the most common terminology, an ideal is called regular if it contains a regular element. A fortiori this is a faithful ideal. We will not use this terminology as we find it ambiguous. ■

7.7. Lemma.

1. *If* $\mathfrak{a} \subseteq \mathfrak{b}$ *with* $\mathfrak{a}$ *finitely generated and* $\mathfrak{b}$ *locally principal, there exists a finitely generated ideal* $\mathfrak{c}$ *such that* $\mathfrak{bc} = \mathfrak{a}$*.*
2. *An ideal* $\mathfrak{a}$ *is finitely generated projective if and only if it is locally principal and its annihilator is generated by an idempotent.*
3. *An ideal* $\mathfrak{a}$ *is quasi-free if and only if it is principal and its annihilator is generated by an idempotent.*
4. *Let* $\mathfrak{a}_1$ *and* $\mathfrak{a}_2$ *be ideals and* $\mathfrak{b}$ *be a faithful finitely generated projective ideal. If* $\mathfrak{b}\mathfrak{a}_1 = \mathfrak{b}\mathfrak{a}_2$*, then* $\mathfrak{a}_1 = \mathfrak{a}_2$*.*
5. *An ideal is invertible if and only if it is locally principal and it contains a regular element.*

D *1.* It is enough to show that for an arbitrary $a \in \mathfrak{b}$ there exists a finitely generated ideal $\mathfrak{c}$ such that $\mathfrak{b}\,\mathfrak{c} = \langle a \rangle$. This is given by item *1e* of Proposition 7.4 when $M = \mathfrak{b}$.

2. The direct implication uses Corollary II-5.23: if a linear map $\mathbf{A}^k \to \mathbf{A}$ is injective with $k > 1$, the ring is trivial. Therefore at each localization, the ideal $\mathfrak{a}$ is not only free but principal. The converse implication is in Lemma 7.6.

3. For the direct implication, we write $\mathfrak{a} \simeq \bigoplus_{i \in [\![1..n]\!]} \langle e_i \rangle$, where the e_i's are idempotents with e_{i+1} being a multiple of e_i. We want to show that if $n > 1$, $e_2 = 0$. We localize the injection $\mathfrak{a} \to \mathbf{A}$ at e_2 and we obtain an injection

$$\mathbf{A}_{e_2} \oplus \mathbf{A}_{e_2} \simeq e_1\mathbf{A}_{e_2} \oplus e_2\mathbf{A}_{e_2} \hookrightarrow \bigoplus e_i\mathbf{A}_{e_2} \simeq \mathfrak{a}\mathbf{A}_{e_2} \hookrightarrow \mathbf{A}_{e_2},$$

so $\mathbf{A}_{e_2}$ is null (Corollary II-5.23).

4. The ideal $\mathfrak{b}$ becomes free (after localization), and cyclic by item *2*. If in addition it is faithful, its annihilator is null, and the generator is a regular element.

5. Item *1* implies that a locally principal ideal that contains a regular element is invertible. Conversely, let $\mathfrak{a} = \langle a_1, \dots, a_n \rangle$ be an invertible ideal. There exists a c regular in $\mathfrak{a}$ and an ideal $\mathfrak{b}$ such that $\mathfrak{a}\,\mathfrak{b} = \langle c \rangle$. Let b_1, $\dots$, $b_n \in \mathfrak{b}$ with $\sum_i a_i b_i = c$. We have for each i, $j \in [\![1..n]\!]$ some $c_{ij} \in \mathbf{A}$ such that $b_i a_j = c\,c_{ij}$. By using the fact that c is regular we verify without difficulty that the matrix $(c_{ij})_{1 \leqslant i,j \leqslant n}$ is a principal localization matrix for $(a_1, \dots, a_n)$. □

8. Determinant, characteristic polynomial, fundamental polynomial and rank polynomial

If M is an $\mathbf{A}$-module, we denote by $M[X]$ the $\mathbf{A}[X]$-module obtained by scalar extension.

When $\mathbf{A}$ is an integral ring, if P is a finitely generated projective module, isomorphic to the image of a projector $F \in \mathbb{AG}_n(\mathbf{A})$, by scalar extension to the quotient field we obtain a vector space P' of finite dimension, say k. We deduce that the characteristic polynomial of the matrix F is equal to $(X-1)^k X^{n-k}$. Even simpler, the determinant of the multiplication by X in $P'[X]$ is equal to X^k, i.e.

$$\det\big((\mathrm{I}_n - F) + XF\big) = X^k.$$

When $\mathbf{A}$ is an arbitrary ring, we will see that we can define the analogue of the above polynomial X^k. First of all, we introduce the determinant of an endomorphism of a finitely generated projective module.

The determinant, the characteristic polynomial and the cotransposed endomorphism

8.1. Theorem and definition. *Let P be a finitely generated projective module.*

1. *Let $\varphi \in \mathrm{End}(P)$. Suppose that $P \oplus Q_1$ is isomorphic to a free module and let $\varphi_1 = \varphi \oplus \mathrm{Id}_{Q_1}$.*
   a. *The determinant of φ_1 only depends on φ. The scalar defined as such is called the* determinant of the endomorphism φ. *We denote it by* $\det(\varphi)$ *or* $\det\varphi$.
   b. *The determinant of the endomorphism $X\mathrm{Id}_{P[X]} - \varphi$ of $P[X]$ is called the* characteristic polynomial of the endomorphism φ.
   We denote it by $\mathrm{C}_\varphi(X)$; we have $\mathrm{C}_{-\varphi}(0) = \det\varphi$.
   c. *Consider the cotransposed endomorphism $\mathrm{Adj}(\varphi_1) = \widetilde{\varphi_1}$ of φ_1. It operates on P and the endomorphism of P defined as such only depends on φ. We call it* the cotransposed endomorphism of φ *and we denote it by $\widetilde{\varphi}$ or $\mathrm{Adj}(\varphi)$.*
   d. *Let $\rho : \mathbf{A} \to \mathbf{B}$ be a morphism. By scalar extension from $\mathbf{A}$ to $\mathbf{B}$, we get a finitely generated projective module $\rho_\star(P)$ with an endomorphism $\rho_\star(\varphi)$. Then we have the following good "functorial" properties*

$$\det\big(\rho_\star(\varphi)\big) = \rho\big(\det(\varphi)\big), \qquad \mathrm{C}_{\rho_\star(\varphi)}(X) = \rho\big(\mathrm{C}_\varphi(X)\big),$$
$$\mathrm{Adj}\big(\rho_\star(\varphi)\big) = \rho_\star\big(\mathrm{Adj}(\varphi)\big).$$

2. If $\psi : P \to P$ is another endomorphism of P, we have

$$\det(\varphi \circ \psi) = \det(\varphi)\det(\psi).$$

3. If P' is another finitely generated projective module and if $\psi = \begin{array}{|c|c|}\hline \varphi & \gamma \\ \hline 0 & \varphi' \\ \hline \end{array}$ is an endomorphism of $P \oplus P'$ "block-triangular," we have

$$\det(\psi) = dd' \quad \text{and} \quad \widetilde{\psi} = \begin{array}{|c|c|}\hline d'\widetilde{\varphi} & \eta \\ \hline 0 & d\widetilde{\varphi'} \\ \hline \end{array}, \quad \text{where } d = \det(\varphi),\ d' = \det(\varphi').$$

4. If $\varphi : P \to P$ and $\varphi' : P' \to P'$ are endomorphisms of finitely generated projective modules, and if $\alpha \circ \varphi = \varphi' \circ \alpha$ for an isomorphism $\alpha : P \to P'$, then $\det(\varphi) = \det(\varphi')$.

5. The linear map φ is an isomorphism (resp. is injective) if and only if $\det(\varphi)$ is invertible (resp. is regular).

6. We have the "classical" equality

$$\widetilde{\varphi} \circ \varphi \;=\; \varphi \circ \widetilde{\varphi} \;=\; \det(\varphi)\,\mathrm{Id}_P.$$

7. The Cayley-Hamilton theorem applies: $\mathrm{C}_\varphi(\varphi) = 0$.

8. Let

$$\Gamma_\varphi(X) \quad := \quad -\frac{\mathrm{C}_{-\varphi}(-X) - \mathrm{C}_{-\varphi}(0)}{X} \quad = \quad \frac{-\mathrm{C}_{-\varphi}(-X) + \det(\varphi)}{X},$$

such that $\mathrm{C}_{-\varphi}(-X) = -X\Gamma_\varphi(X) + \det(\varphi)$. Then $\widetilde{\varphi} = \Gamma_\varphi(\varphi)$.

D We remark that the definitions given in item *1* indeed reproduces the usual objects of the same name in the case where the module is free. Similarly the formula in *8* gives, when φ is an endomorphism of a free module, the same Γ_φ as the formula of Lemma III-1.4. So there is no conflict of notation.

1a. Assume that $\mathbf{A}^m \simeq P \oplus Q_1$ and $\mathbf{A}^n \simeq P \oplus Q_2$, and consider the direct sum

$$\mathbf{A}^{m+n} \simeq P \,\oplus\, Q_1 \oplus P \,\oplus\, Q_2. \qquad (*)$$

Let $\varphi_1 = \varphi \,\oplus\, \mathrm{Id}_{Q_1}$ and $\varphi_2 = \varphi \,\oplus\, \mathrm{Id}_{Q_2}$. One has to show the equality $\det\varphi_1 = \det\varphi_2$. Consider the endomorphism of $\mathbf{A}^{m+n}$

$$\phi = \varphi \,\oplus\, \mathrm{Id}_{Q_1} \oplus\, \mathrm{Id}_P \oplus\, \mathrm{Id}_{Q_2},$$

such that ϕ is conjugated of $\varphi_1 \oplus \mathrm{Id}_{\mathbf{A}^n}$ and of $\varphi_2 \oplus \mathrm{Id}_{\mathbf{A}^m}$. Hence $\det\phi = \det\varphi_1$ and $\det\phi = \det\varphi_2$.

1c. We proceed similarly. The cotransposition of the endomorphisms satisfies item *3* in the case of free modules, so $\widetilde{\phi}$ operates on $P \oplus Q_1$ and is restricted at $\widetilde{\varphi_1}$. Moreover, since $\widetilde{\phi} = \Gamma_\phi(\phi)$, $\widetilde{\phi}$ operates on each component in the direct sum $(*)$. Similarly $\widetilde{\phi}$ operates on $P \oplus Q_2$ and is restricted at $\widetilde{\varphi_2}$. Therefore $\widetilde{\varphi}_1$ and φ_2 both operate on P in the same way that $\widetilde{\psi}$ does. Note that $\widetilde{\varphi} = \Gamma_\phi(\varphi)$.

1d. This is a direct consequence of the definitions.

All the remaining items of the theorem are consequences of the free case (where the results are clear), of the local structure theorem and of item *1d.* Indeed the statements can be certified by verifying them after localization at comaximal elements, and the finitely generated projective modules we consider become simultaneously free after localization at a suitable system of comaximal elements. Nevertheless we give more direct proofs.

The assertions *2*, *3*, *4* and *5* easily result from the definitions, knowing that the results are true in the free case.

6. We have defined $\widetilde{\varphi}$ as the restriction of $\widetilde{\varphi_1}$ at P. Since φ_1 is an endomorphism of a free module, we get

$$\widetilde{\varphi_1} \circ \varphi_1 = \det(\varphi_1)\,\mathrm{Id}_{P\oplus Q_1},$$

which gives by restriction at P the desired equality $\widetilde{\varphi} \circ \varphi = \det(\varphi)\,\mathrm{Id}_P$, since $\det \varphi = \det \varphi_1$.

7. We can reproduce the following proof, classical in the case of free modules. Consider the endomorphism

$$\psi = X\mathrm{Id}_{P[X]} - \varphi \in \mathrm{End}_{\mathbf{A}[X]}(P[X]).$$

By item *6* we have

$$\widetilde{\psi}\psi = \psi\widetilde{\psi} = \mathrm{C}_\varphi(X)\,\mathrm{Id}_{P[X]}. \qquad (+)$$

Moreover, $\widetilde{\psi}$ is a polynomial in X with coefficients in $\mathbf{A}[\varphi]$. Therefore we can write $\widetilde{\psi} = \sum_{k\geqslant 0} \phi_k X^k$, where each $\phi_k : P \to P$ is a polynomial in φ. By letting $\mathrm{C}_\varphi(X) = \sum_{k\geqslant 0} a_k X^k$ and by identifying both sides of the equality (+) we obtain (by agreeing to $\phi_{-1} = 0$)

$$\phi_{k-1} - \phi_k\varphi = a_k\mathrm{Id}_P \text{ for all } k \geqslant 0.$$

Then, $\mathrm{C}_\varphi(\varphi) = \sum_{k\geqslant 0}(\phi_{k-1} - \phi_k\varphi)\varphi^k = 0$.

8. The polynomial Γ_φ has been defined in order to satisfy

$$\mathrm{C}_{-\varphi}(-X) = -X\Gamma_\varphi(X) + \det(\varphi).$$

By evaluating $X := \varphi$, we obtain $\varphi\Gamma_\varphi(\varphi) = \det(\varphi)\mathrm{Id}_P$ (Cayley-Hamilton theorem), so $\varphi\Gamma_\varphi(\varphi) = \varphi\widetilde{\varphi}$. By replacing φ by $\theta := T\mathrm{Id}_{P[T]} + \varphi$, we obtain $\theta\Gamma_\theta(\theta) = \theta\widetilde{\theta}$, then $\Gamma_\theta(\theta) = \widetilde{\theta}$, because θ is a regular element of $\mathbf{A}[T,\varphi] = \mathbf{A}[\varphi][T]$. We finish the proof by putting $T := 0$. □

Remark. The determinant of the identity map of every finitely generated projective module, including the module reduced to $\{0\}$, is equal to 1 (by following the above definition). ■

8.2. Corollary. *Let $\varphi : P \to P$ be an endomorphism of a finitely generated projective module, and $x \in P$ satisfying $\varphi(x) = 0$, then* $\det(\varphi)x = 0$.

D Results from $\widetilde{\varphi} \circ \varphi = \det(\varphi)\mathrm{Id}_P$. □

The fundamental polynomial and the rank polynomial

We are interested in the characteristic polynomial of the identity of a finitely generated projective module. It is however simpler to introduce another polynomial which is directly related to it and which is the analogue of the polynomial X^k, which we spoke of at the beginning of Section 8.

8.3. Definitions and notations. Let P be a finitely generated projective $\mathbf{A}$-module and φ an endomorphism of P. Consider the $\mathbf{A}[X]$-module $P[X]$ and define the polynomials $\mathrm{F}_{\mathbf{A},\varphi}(X)$ and $\mathrm{R}_{\mathbf{A},P}(X)$ (or $\mathrm{F}_\varphi(X)$ and $\mathrm{R}_P(X)$ if the context is clear) by the following equalities

$$\mathrm{F}_\varphi(X) = \det(\mathrm{Id}_{P[X]} + X\varphi) \quad \text{and} \quad \mathrm{R}_P(X) = \det(X\mathrm{Id}_{P[X]}).$$

Therefore $\mathrm{R}_P(1+X) = \mathrm{F}_{\mathrm{Id}_P}(X)$.

- The polynomial $\mathrm{F}_\varphi(X)$ is called the *fundamental polynomial* of the endomorphism φ.
- The coefficient of X in the fundamental polynomial is called the *trace* of φ and is denoted by $\mathrm{Tr}_P(\varphi)$.
- The polynomial $\mathrm{R}_P(X)$ is called the *rank polynomial*[3] of the module P.

Note that

$$\mathrm{F}_\varphi(0) = 1 = \mathrm{R}_P(1), \ \ \mathrm{C}_\varphi(0) = \det(-\varphi), \ \text{ and } \ \mathrm{F}_{a\varphi}(X) = \mathrm{F}_\varphi(aX),$$

but $\mathrm{C}_\varphi(X)$ is not always monic (see the Example on page 277).

Also note that for all $a \in \mathbf{A}$ we get

$$\det(a\varphi) = \det(a\,\mathrm{Id}_P)\det(\varphi) = \mathrm{R}_P(a)\det(\varphi). \tag{6}$$

We deduce the following equalities

$$\begin{aligned} \mathrm{R}_P(0) &= \det(0_{\mathrm{End}_{\mathbf{A}}(P)}),\\ \mathrm{C}_{-\varphi}(-X) = \det(\varphi - X\mathrm{Id}_{P[X]}) &= \det\big(-(X\mathrm{Id}_{P[X]} - \varphi)\big) = \mathrm{R}_P(-1)\mathrm{C}_\varphi(X),\\ \det(\varphi) &= \mathrm{R}_P(-1)\ \mathrm{C}_\varphi(0). \end{aligned}$$

The last equality replaces the equality $\det(\varphi) = (-1)^k\,\mathrm{C}_\varphi(0)$ valid for the free modules of rank k.

We will say that a polynomial $R(X)$ is *multiplicative* when $R(1) = 1$ and $R(XY) = R(X)R(Y)$.

8.4. Theorem. (The fundamental system of orthogonal idempotents associated with a finitely generated projective module)

1. *If P is a finitely generated projective module over a ring $\mathbf{A}$ the rank polynomial $\mathrm{R}_P(X)$ is multiplicative.*

[3] This terminology is justified by the fact that for a free module of rank k the rank polynomial is equal to X^k, as well as by Theorem 8.4.

2. *In other words, the coefficients of* $\mathrm{R}_P(X)$ *form a fundamental system of orthogonal idempotents. If* $\mathrm{R}_P(X) = r_0 + r_1X + \cdots + r_nX^n$*, we denote* r_h *by* $\mathrm{e}_h(P)$*: it is called* the idempotent associated with the integer h and with the module P *(if* $h > n$ *we let* $\mathrm{e}_h(P) := 0$*).*
3. *Every rank polynomial* $\mathrm{R}_P(X)$ *is a regular element of* $\mathbf{A}[X]$*.*
4. *A generalization of the equality* $\mathrm{rk}(P \oplus Q) = \mathrm{rk}(P) + \mathrm{rk}(Q)$ *regarding the ranks of the free modules is given for the finitely generated projective modules by*
$$\mathrm{R}_{P\oplus Q}(X) = \mathrm{R}_P(X)\ \mathrm{R}_Q(X)\,.$$
5. *If* $P \oplus Q \simeq \mathbf{A}^n$ *and* $\mathrm{R}_P(X) = \sum_{k=0}^n r_kX^k$*, then* $\mathrm{R}_Q(X) = \sum_{k=0}^n r_kX^{n-k}$*.*
6. *The equality* $\mathrm{R}_P(X) = 1$ *characterizes, among the finitely generated projective modules, the module* $P = \{0\}$*. It is also equivalent to* $\mathrm{e}_0(P) = \mathrm{R}_P(0) = 1$*.*

D *1* and *2.* If μ_a designates multiplication by a in $P[X,Y]$, we clearly have the equality $\mu_X\mu_Y = \mu_{XY}$, so $\mathrm{R}_P(X)\ \mathrm{R}_P(Y) = \mathrm{R}_P(XY)$ (Theorem 8.1.*2*). Since $\mathrm{R}_P(1) = \det(\mathrm{Id}_P) = 1$, we deduce that the coefficients of $\mathrm{R}_P(X)$ form a fundamental system of orthogonal idempotents.

3. Results from McCoy's lemma (Corollary III-2.3). We could also prove it using the basic local-global principle (by localizing at the r_i's).

4. Results from item *3* in Theorem 8.1.

5. Results from items *3* and *4* since $\big(\sum_{k=0}^n r_kX^k\big)\big(\sum_{k=0}^n r_{n-k}X^k\big) = X^n$.

6. We have $r_0 = \det(0_{\mathrm{End}(P)})$. Since the r_i's form a fundamental system of orthogonal idempotents, the equalities $\mathrm{R}_P = 1$ and $r_0 = 1$ are equivalent.
If $P = \{0\}$, then $0_{\mathrm{End}(P)} = \mathrm{Id}_P$, so $r_0 = \det(\mathrm{Id}_P) = 1$.
If $r_0 = 1$, then $0_{\mathrm{End}(P)}$ is invertible, therefore $P = \{0\}$. □

If P is a free $\mathbf{A}$-module of rank k, we have $\mathrm{R}_P(X) = X^k$, the following definition is therefore a legitimate extension from free modules to finitely generated projective modules.

8.5. Definition. A finitely generated projective module P is said to be *of rank equal to* k if $\mathrm{R}_P(X) = X^k$. If we do not specify the value of the rank, we simply say that the module is *of constant rank.* We will use the notation $\mathrm{rk}(M) = k$ to indicate that a module (assumed to be projective of constant rank) is of rank k.

Note that by Proposition 8.11, every projective module of rank $k > 0$ is faithful.

8.6. Fact. *The characteristic polynomial of an endomorphism of a projective module of constant rank k is monic of degree k.*

D We can give an elegant direct proof (see Exercise 20). We could also avoid all effort and use a localization argument, by relying on the local structure theorem and on Fact 8.8, which asserts that everything goes well for the characteristic polynomial by localization. □

The convention in the following remark allows for a more uniform formulation of the theorems and the proofs hereinafter.

Remark. When the ring $\mathbf{A}$ is reduced to $\{0\}$, all the $\mathbf{A}$-modules are trivial. Nevertheless, in accordance with the above definition, the null module over the null ring is a projective module of constant rank equal to k, for any value of the integer $k \geqslant 0$. Moreover, it is immediate that if a finitely generated projective module P has two distinct constant ranks, then the ring is trivial. We have $\mathrm{R}_P(X) = 1_{\mathbf{A}}X^h = 1_{\mathbf{A}}X^k$ with $h \neq k$ therefore the coefficient of X^h is equal to both $1_{\mathbf{A}}$ and $0_{\mathbf{A}}$. ■

Some explicit computations

The fundamental polynomial of an endomorphism φ is easier to use than the characteristic polynomial. This comes from the fact that the fundamental polynomial is invariant when we add "as a direct sum" a null endomorphism to φ. This allows us to systematically and easily reduce the computation of a fundamental polynomial to the case where the projective module is free. Precisely, we are able to compute the previously defined polynomials by following the lemma stated below.

8.7. Lemma. (Explicit computation of the determinant, of the fundamental polynomial, of the characteristic polynomial, of the rank polynomial and of the cotransposed endomorphism)
Let $P \simeq \operatorname{Im} F$ be an $\mathbf{A}$-module with $F \in \mathbb{AG}_n(\mathbf{A})$. Let $Q = \operatorname{Ker}(F)$, such that $P \oplus Q \simeq \mathbf{A}^n$, and $\mathrm{I}_n - F$ is the matrix of the projection π_Q over Q parallel to P. An endomorphism φ of P is characterized by the matrix H of the endomorphism $\varphi_0 = \varphi \oplus 0_Q$ of $\mathbf{A}^n$. Such a matrix H is subjected to the unique restriction $F \cdot H \cdot F = H$. Let $G = \mathrm{I}_n - F + H$.

1. *Computation of the determinant:*

$$\det(\varphi) = \det(\varphi \oplus \mathrm{Id}_Q) = \det(G).$$

2. *Therefore also*

$$\det(X\mathrm{Id}_{P[X,Y]} + Y\varphi) = \det\big((X\mathrm{Id}_{P[X,Y]} + Y\varphi) \oplus \mathrm{Id}_Q\big) =$$
$$\det(\mathrm{I}_n - F + XF + YH) = \det(\mathrm{I}_n + (X-1)F + YH).$$

3. *Computation of the rank polynomial of P:*

$$\mathrm{R}_P(1+X) = \det\big((1+X)\mathrm{Id}_{P[X]}\big) = \det(\mathrm{I}_n + XF),$$

in particular,

$$\mathrm{R}_P(0) = \det(\mathrm{I}_n - F),$$

and $\mathrm{R}_P(1+X) = 1 + u_1X + \cdots + u_nX^n$*, where* u_h *is the sum of the principal minors of order* h *of the matrix* F*.*

4. *Computation of the fundamental polynomial of* φ*:*

$$\mathrm{F}_\varphi(Y) = \det(\mathrm{Id}_{P[Y]} + Y\varphi) = \det(\mathrm{I}_n + YH) = 1 + \sum\nolimits_{k=1}^{n} v_kY^k,$$

where v_k *is the sum of the principal minors of order* k *of the matrix* H*. In particular,* $\mathrm{Tr}_P(\varphi) = \mathrm{Tr}(H)$*.*

5. *Computation of the characteristic polynomial of* φ*:*

$$\mathrm{C}_\varphi(X) = \det(X\mathrm{Id}_{P[X]} - \varphi) = \det(\mathrm{I}_n - H + (X-1)F).$$

6. *Computation of the cotransposed endomorphism* $\widetilde{\varphi}$ *of* φ*: it is defined by the matrix*

$$\widetilde{G}\cdot F = F\cdot\widetilde{G} = \widetilde{G} - \det(\varphi)(\mathrm{I}_n - F).$$

For the last item we apply item *3* of Theorem 8.1 with φ and Id_Q by remarking that G is the matrix of $\psi = \varphi \oplus \mathrm{Id}_Q = \varphi_0 + \pi_Q$.

Note that the characteristic polynomial of Id_P is equal to $\mathrm{R}_P(X-1)$.

The following fact is an immediate consequence of Proposition 5.1 and of the previous lemma.

8.8. Fact. *The determinant, the cotransposed endomorphism, the characteristic polynomial, the fundamental polynomial and the rank polynomial are well-behaved under scalar extension via a homomorphism* $\mathbf{A} \to \mathbf{B}$*.*
In particular, if $\varphi : P \to P$ *is an endomorphism of a finitely generated projective* $\mathbf{A}$*-module and* S *a monoid of* $\mathbf{A}$*, then* $\det(\varphi)_S = \det(\varphi_S)$ *(or, if we prefer,* $\det(\varphi)/1 =_{\mathbf{A}_S} \det(\varphi_S)$*). The same thing holds for the cotransposed endomorphism, the fundamental polynomial, the characteristic polynomial and the rank polynomial.*

Example. Let e be an idempotent of $\mathbf{A}$ and $f = 1 - e$. The module $\mathbf{A}$ is a direct sum of the submodules $e\mathbf{A}$ and $f\mathbf{A}$ which are therefore finitely generated projective. The 1×1 matrix having for unique coefficient e is a matrix F whose image is $P = e\mathbf{A}$. For $a \in \mathbf{A}$ consider $\mu_a = \mu_{P,a} \in \mathrm{End}_{\mathbf{A}}(P)$. The matrix H has for unique coefficient ea. We then have, by applying the previous formulas,

$$\det(0_{e\mathbf{A}}) = f,\ \mathrm{R}_{e\mathbf{A}}(X) = f + eX,\ \mathrm{C}_{\mathrm{Id}_{e\mathbf{A}}}(X) = f - e + eX,$$
$$\det(\mu_a) = f + ea,$$
$$\mathrm{F}_{\mu_a}(X) = 1 + eaX,\ \mathrm{C}_{\mu_a}(X) = 1 - ea + e(X-1) = f - ea + eX.$$

Note that the characteristic polynomial of μ_a is not monic if $e \neq 1, 0$, and we indeed have the Cayley-Hamilton theorem

$$\mathrm{C}_{\mu_a}(\mu_a) = (f - ea)\mathrm{Id}_{e\mathbf{A}} + e\mu_a = (f - ea + ea)\mathrm{Id}_{e\mathbf{A}} = f\mathrm{Id}_{e\mathbf{A}} = 0_{e\mathbf{A}}.$$ ■

With a coordinate system

When we use a coordinate system Lemma 8.7 leads to the following result.

8.9. Fact. *Let P be a finitely generated projective module with a coordinate system $\big((x_1,\dots,x_n),(\alpha_1,\dots,\alpha_n)\big)$ and φ be an endomorphism of P. Recall (Fact 2.9) that we can encode P by the matrix*

$$F \overset{\mathrm{def}}{=} \big(\alpha_i(x_j)\big)_{i,j\in[\![1..n]\!]}$$

(P is isomorphic to $\operatorname{Im} F \subseteq \mathbf{A}^n$ by means of $x \mapsto \pi(x) = {}^{\mathrm{t}}[\,\alpha_1(x)\ \cdots\ \alpha_n(x)\,]$). In addition the endomorphism φ is represented by the matrix

$$H \overset{\mathrm{def}}{=} \big(\alpha_i(\varphi(x_j))\big)_{i,j\in[\![1..n]\!]}$$

which satisfies $H = HF = FH$.

1. *We have $\mathrm{F}_\varphi(X) = \det(\mathrm{I}_n + XH)$ and $\mathrm{Tr}(\varphi) = \mathrm{Tr}(H) = \sum_i \alpha_i\big(\varphi(x_i)\big)$.*
2. *For $\nu \in P^\star$ and x, $y \in P$, recall that $\theta_P(\nu\otimes x)(y) = \nu(y)x$. The trace of this endomorphism is given by $\mathrm{Tr}_P\,\big(\theta_P(\nu\otimes x)\big) = \nu(x)$.*

D The matrix H is also that of the $\mathbf{A}$-linear map φ_0 introduced in Lemma 8.7

$$\pi(x) + y \mapsto \pi\big(\varphi(x)\big) \text{ with } \pi(x) \in \operatorname{Im} F \text{ and } y \in \operatorname{Ker} F.$$

Item *2* therefore results from Lemma 8.7.

3. By item *2*, we have

$$\mathrm{Tr}\big(\theta_P(\nu\otimes x)\big) = \textstyle\sum_i \alpha_i(\nu(x_i)x) = \sum_i \nu(x_i)\alpha_i(x) = \nu\big(\sum_i \alpha_i(x)x_i\big) = \nu(x).$$

□

8.10. Lemma. *Let M, N be two finitely generated projective $\mathbf{k}$-modules and let $\varphi \in \mathrm{End}_{\mathbf{k}}(M)$ and $\psi \in \mathrm{End}_{\mathbf{k}}(N)$ be endomorphisms. Then, $\mathrm{Tr}_{M\otimes N}(\varphi\otimes\psi) = \mathrm{Tr}_M(\varphi)\,\mathrm{Tr}_N(\psi)$.*

D Consider coordinate systems for M and N and apply the formula for the trace of the endomorphisms (Fact 8.9). □

The annihilator of a finitely generated projective module

We have already established certain results regarding this annihilator by relying on the local structure theorem for finitely generated projective modules, proven by using the Fitting ideals (see Lemma 6.2).

Here we give some additional results by using a proof that does not rely on the local structure theorem.

8.11. Proposition. *Let P be a finitely generated projective $\mathbf{A}$-module. Consider the ideal $J_P = \langle \alpha(x) \,|\, \alpha \in P^\star,\ x \in P \rangle$. Let $r_0 = \mathrm{R}_P(0) = \mathrm{e}_0(P)$.*

1. *$\langle r_0 \rangle = \mathrm{Ann}(P) = \mathrm{Ann}(J_P)$.*
2. *$J_P = \langle s_0 \rangle$, where s_0 is the idempotent $1 - r_0$.*

D We obviously have $\mathrm{Ann}(P) \subseteq \mathrm{Ann}(J_P)$. Let $\big((x_i)_{i\in[\![1..n]\!]}, (\alpha_i)_{i\in[\![1..n]\!]}\big)$ be a coordinate system over P. Then

$$J_P = \langle \alpha_i(x_j)\,;\, i,j \in [\![1..n]\!] \rangle\,,$$

and the projection matrix $F = \big(\alpha_i(x_j)\big)_{i,j\in[\![1..n]\!]}$ has an image isomorphic to P. By definition, r_0 is the idempotent $r_0 = \det(\mathrm{I}_n - F)$.
Since $(\mathrm{I}_n - F)F = 0$, we have $r_0 F = 0$, i.e. $r_0 P = 0$.
Therefore $\langle r_0 \rangle \subseteq \mathrm{Ann}(P) \subseteq \mathrm{Ann}(J_P)$ and $J_P \subseteq \mathrm{Ann}(r_0)$.
Moreover, we have $\mathrm{I}_n - F \equiv \mathrm{I}_n$ modulo J_P, so by taking the determinants, we have $r_0 \equiv 1$ modulo J_P, i.e. $s_0 \in J_P$, then $\mathrm{Ann}(J_P) \subseteq \mathrm{Ann}(s_0)$.
We can therefore conclude

$$\langle r_0 \rangle \subseteq \mathrm{Ann}(P) \subseteq \mathrm{Ann}(J_P) \subseteq \mathrm{Ann}(s_0) = \langle r_0 \rangle \ \text{ and } \ \langle s_0 \rangle \subseteq J_P \subseteq \mathrm{Ann}(r_0) = \langle s_0 \rangle\,.$$

□

Canonical decomposition of a projective module

8.12. Definition. Let P be a finitely generated projective $\mathbf{A}$-module and $h \in \mathbb{N}$. If $r_h = \mathrm{e}_h(P)$, we denote by $P^{(h)}$ the $\mathbf{A}$-submodule $r_h P$. It is called the *component of the module P in rank h.*

Recall that, for an idempotent e and an $\mathbf{A}$-module M, the module obtained by scalar extension to $\mathbf{A}[1/e] \simeq \mathbf{A}/\langle 1-e \rangle$ can be identified with the submodule eM, itself isomorphic to the quotient module $M/(1-e)M$.

8.13. Theorem. *Let P be a finitely generated projective $\mathbf{A}$-module.*

1. *The module $r_h P = P^{(h)}$ is a projective $\mathbf{A}[1/r_h]$-module of rank h.*
2. *The module P is the direct sum of the $P^{(h)}$'s.*
3. *The ideal $\langle r_0 \rangle$ is the annihilator of the $\mathbf{A}$-module P.*
4. *For $h > 0$, $P^{(h)} = \{0\}$ implies $r_h = 0$.*

D *1.* Localize at r_h: we obtain $\mathrm{R}_{P^{(h)}}(X) =_{\mathbf{A}[1/r_h]} \mathrm{R}_P(X) =_{\mathbf{A}[1/r_h]} X^h$.
2. Because the r_h's form a fundamental system of orthogonal idempotents.
3. Already proved (Proposition 8.11).
4. Results immediately from item *3.* □

Note that, except if $r_h = 1$ or $h = 0$, the module r_hP is not of constant rank when considered as an **A**-module..

The previous theorem gives a “structural” proof of Theorem 1.3.

Remark. If P is (isomorphic to) the image of a projection matrix F the idempotents $r_k = \mathrm{e}_k(P)$ attached to the module P can be linked to the characteristic polynomial of the matrix F as follows

$$\det(X\mathrm{I}_n - F) = \textstyle\sum_{k=0}^{n} r_k X^{n-k}(X-1)^k.$$

(Note that the $X^{n-k}(X-1)^k$ form a basis of the module of polynomials of degree $\leqslant n$, triangular with respect to the usual basis.) ■

Rank polynomial and Fitting ideals

The proof of Theorem 8.14 that follows relies on Theorem 6.1, which asserts that a finitely generated projective module becomes free after localization at comaximal elements.

We have placed the theorem here because it answers to the questions that we naturally ask ourselves after Theorem 8.4. First, check that a projection matrix is of rank k if and only if its image is a projective module of constant rank k. More generally, characterize the fundamental system of orthogonal idempotents that occurs in the rank polynomial in terms of the Fitting ideals of the module.

Actually, we can give an alternative proof of Theorem 8.14 without taking the route of a localization argument, by making use of exterior powers (see Proposition X-1.2).

Let us point out that for a finitely presented module M the equality $\mathcal{F}_h(M) = \langle 1 \rangle$ means that M is locally generated by h elements (we have seen this in the case $h = 1$ in Theorem 7.3, in the general case, see the local number of generators lemma on page 496 and Definition IX-2.5).

8.14. Theorem. (Local structure and Fitting ideals of a finitely generated projective module, 2)
Let $F \in \mathbb{A}\mathbb{G}_q(\mathbf{A})$, $P \simeq \operatorname{Im} F$ and $\mathrm{R}_P(X) = \sum_{i=0}^{q} r_i X^i$.

1. *Let $S(X) = \mathrm{R}_P(1+X) = 1 + u_1X + \cdots + u_qX^q$ (u_h is the sum of the principal minors of order h of the matrix F).*
   We have, for all $h \in \llbracket 0..q \rrbracket$,

$$\begin{cases} \mathcal{D}_h(F) = \langle r_h + \cdots + r_q \rangle = \langle r_h, \ldots, r_q \rangle = \langle u_h, \ldots, u_q \rangle \\ \mathcal{F}_h(P) = \langle r_0 + \cdots + r_h \rangle = \langle r_0, \ldots, r_h \rangle \end{cases}$$

2. *In particular*
   a. $\mathrm{rk}(F) = h \iff \mathrm{rk}(P) = h$,
   b. $\mathrm{rk}(F) \leqslant h \iff \deg \mathrm{R}_P \leqslant h$,
   c. $\mathrm{rk}(F) > h \iff r_0 = \cdots = r_h = 0 \iff \mathcal{F}_h(P) = 0$.

D The equality $\langle u_h, \ldots, u_q \rangle = \langle r_h, \ldots, r_q \rangle$ results from the equalities

$$S(X) = \mathrm{R}_P(1 + X) \ \text{ and } \ \mathrm{R}_P(X) = S(X - 1).$$

To check the equalities $\mathcal{D}_h(F) = \langle r_h + \cdots + r_q \rangle = \langle r_h, \ldots, r_q \rangle$ and

$$\mathcal{D}_{q-h}(\mathrm{I}_q - F) = \langle r_0 + \cdots + r_h \rangle = \langle r_0, \ldots, r_h \rangle\,,$$

it suffices to do it after localization at comaximal elements. However, the kernel and the image of F become free after localization at comaximal elements (Theorem II-5.26 or Theorem 6.1), and the matrix therefore becomes similar to a standard projection matrix. □

9. Properties of finite character

The purpose of this section is to illustrate the idea that the good concepts in algebra are those that are controllable by finite procedures.

We have in mind to highlight "good properties." There are naturally those that submit to the local-global principle: for the property to be true it is sufficient and necessary that it be true after localization at comaximal monoids. It is a phenomenon that we have frequently encountered, and will continue to encounter hereafter.

Recall that a property is said to be "of finite character" if it is preserved by localization (by passing from $\mathbf{A}$ to $S^{-1}\mathbf{A}$) and if, when it is satisfied after localization at S, then it is satisfied after localization at s for some $s \in S$.

In Fact* II-2.12 we proved in classical mathematics that for the finite character properties, the concrete local-global principle (localization at comaximal monoids) is equivalent to the abstract local-global principle (localization at all the maximal ideals). However, a constructive proof of the concrete local-global principle a priori contains more precise information than a classical proof of the abstract local-global principle.

9.1. Proposition. *Let S be a monoid of $\mathbf{A}$.*

1. *Let $AX = B$ be a system of linear equations over $\mathbf{A}$. Then, if it admits a solution in $\mathbf{A}_S$, there exists an $s \in S$ such that it admits a solution in $\mathbf{A}_s$.*
2. *Let M and N be two $\mathbf{A}$-submodules of a same module,* with M finitely generated. *Then, if $M_S \subseteq N_S$, there exists an $s \in S$ such that $M_s \subseteq N_s$.*

3. *Let* $\mathbf{A}$ *be a* coherent *ring,* M*,* N*,* P *be* finitely presented $\mathbf{A}$*-modules, and* $\varphi : M \to N$*,* $\psi : N \to P$ *be two linear maps.*

   If the sequence $M \xrightarrow{\varphi} N \xrightarrow{\psi} P$ *becomes exact after localization at* S *there exists an* $s \in S$ *such that the sequence becomes exact after localization at* s*.*
4. *Let* M *and* N *be two* finitely presented $\mathbf{A}$*-modules. Then, if* $M_S \simeq N_S$*, there exists an* $s \in S$ *such that* $M_s \simeq N_s$*.*
5. *Let* M *be a finitely presented* $\mathbf{A}$*-module. If* M_S *is free, there exists some* $s \in S$ *such that* M_s *is free. Similarly, if* M_S *is stably free, there exists some* $s \in S$ *such that* M_s *is stably free.*
6. *If a finitely presented module becomes projective after localization at* S*, it becomes projective after localization at an element* s *of* S*.*

D Let us prove item *3*. We first find some $u \in S$ such that $u\,\psi\big(\varphi(x_j)\big) = 0$ for generators x_j's of N. We deduce that $\psi\circ\varphi$ becomes null after localization at u. Moreover, the hypotheses assure us that $\operatorname{Ker}\psi$ is finitely generated. Let $y_1, \dots, y_n$ be generators of $\operatorname{Ker}\psi$. For each of them we find a z_j in N and an $s_j \in S$ such that $s_j(\varphi(z_j) - y_j) = 0$. We take for s the product of u and the s_j's.

Let us prove item *4*. Let G and H be presentation matrices for M and N. Let G_1 and H_1 be the two matrices given in Lemma IV-1.1. By hypothesis there exist two square matrices Q and R with coefficients in $\mathbf{A}$ such that $v = \det(Q)\det(R) \in S$ and $Q\,G_1 =_{\mathbf{A}_S} H_1\,R$. This means that we have over $\mathbf{A}$ an equality

$$w\,(Q\,G_1 - H_1\,R) = 0, \quad w \in S.$$

It therefore suffices to take $s = vw$. □

We have seen that the scalar extension is well-behaved with respect to tensor products, exterior powers and symmetrical powers. For the functor $\mathrm{L}_{\mathbf{A}}$ things do not always go so well. The following are important results for the remainder of this work.

9.2. Proposition. *Let* $f : M \to N$ *and* $g : M \to N$ *be two linear maps between* $\mathbf{A}$*-modules,* with M finitely generated*. Then,* $f_S = g_S$ *if and only if there exists an* $s \in S$ *such that* $sf = sg$*. In other words, the canonical map* $\big(\mathrm{L}_{\mathbf{A}}(M, N)\big)_S \to \mathrm{L}_{\mathbf{A}_S}(M_S, N_S)$ *is injective.*

9.3. Proposition. *Let* M *and* N *be two* $\mathbf{A}$*-modules and* $\varphi : M_S \to N_S$ *be an* $\mathbf{A}$*-linear map. We assume that* M *is finitely presented, or that* $\mathbf{A}$ *is integral,* M *finitely generated and* N *torsion-free (i.e.* $a \in \mathbf{A}$*,* $x \in N$*,* $ax = 0$ *implies* $a = 0$ *or* $x = 0$*).*

Then, there exists an $\mathbf{A}$*-linear map* $\phi : M \to N$ *and some* $s \in S$ *such that*

$$\forall x \in M \quad \varphi(x/1) = \phi(x)/s,$$

and the canonical map $\big(\mathrm{L}_{\mathbf{A}}(M, N)\big)_S \to \mathrm{L}_{\mathbf{A}_S}(M_S, N_S)$ *is bijective.*

D The second case, which is easy, is left to the reader. To follow the proof of the first case one must look at the following figure. Suppose that M is the cokernel of the linear map $g : \mathbf{A}^m \to \mathbf{A}^q$ with a matrix $G = (g_{i,j})$ with respect to the canonical bases, then by Fact II-6.4 the module M_S is the cokernel of the linear map $g_S : \mathbf{A}_S^m \to \mathbf{A}_S^q$, represented by the matrix $G_S = (g_{i,j}/1)$ over the canonical bases. Let

$$\mathbf{A}^m \xrightarrow{j_m} \mathbf{A}_S^m,\ \mathbf{A}^q \xrightarrow{j_q} \mathbf{A}_S^q,\ M \xrightarrow{j_M} M_S,\ N \xrightarrow{j_N} N_S,\ \mathbf{A}^q \xrightarrow{\pi} M,\ \mathbf{A}_S^q \xrightarrow{\pi_S} M_S,$$

be the canonical maps. Let $\psi := \varphi \circ \pi_S$, so that $\psi \circ g_S = 0$. Therefore $\psi \circ g_S \circ j_m = 0 = \psi \circ j_q \circ g$. There exists some $s \in S$, a common denominator for the images under ψ of the vectors of the canonical basis. Hence a linear map $\Psi : \mathbf{A}^q \to N$ with $(s\psi) \circ j_q = j_N \circ \Psi$.

$$\begin{tikzcd}
\mathbf{A}^m \arrow[rr, "j_m"] \arrow[d, "g"'] & & \mathbf{A}_S^m \arrow[d, "g_S"] & \\
\mathbf{A}^q \arrow[rr, "j_q"] \arrow[d, "\pi"'] \arrow[ddr, dashed, "\Psi"] & & \mathbf{A}_S^q \arrow[d, "\pi_S"'] \arrow[ddr, "\psi"] & \\
M \arrow[rr, "j_M"] \arrow[dr, dashed, "\phi"'] & & M_S \arrow[dr, "\varphi"'] & \\
& N \arrow[rr, "j_N"] & & N_S
\end{tikzcd}$$

Localization of the homomorphisms

Thus, $j_N \circ \Psi \circ g = s(j_m \circ g_S \circ \psi) = 0$. By Proposition 9.2 applied to $\Psi \circ g$, the equality $j_N \circ (\Psi \circ g) = 0$ in N_S implies that there exists an $s' \in S$ such that $s'(\Psi \circ g) = 0$. Therefore $s'\Psi$ can be factorized in the form $\phi \circ \pi$. We then obtain

$$(ss'\varphi) \circ j_M \circ \pi = ss'(\varphi \circ \pi_S \circ j_q) = ss'\psi \circ j_q = s'j_N \circ \Psi = j_N \circ \phi \circ \pi,$$

and since π is surjective, $ss'\varphi \circ j_M = j_N \circ \phi$. Thus, for all $x \in M$, we have $\varphi(x/1) = \phi(x)/ss'$. □

9.4. Corollary. *Suppose that* M *and* N *are finitely presented, or that they are finitely generated, torsion-free and that* $\mathbf{A}$ *is integral. If* $\varphi : M_S \to N_S$ *is an isomorphism, there exist an* $s \in S$ *and an isomorphism* $\psi : M_s \to N_s$ *such that* $\psi_S = \varphi$.

D Let $\varphi' : N_S \to M_S$ be the inverse of φ. By the previous proposition, there exist $\phi : M \to N$, $\phi' : N \to M$, $s \in S$, $s' \in S$ such that $\varphi = \phi_S/s$, $\varphi' = \phi'_S/s'$. Let $t = ss'$ and define $\psi = \phi_t/s : M_t \to N_t$, $\psi' = \phi'_t/s' : N_t \to M_t$. Then, $(\psi' \circ \psi)_S$ is the identity over M_S, and $(\psi \circ \psi')_S$ is the identity over N_S. We deduce the existence of a $u \in S$ such that $(\psi' \circ \psi)_{tu}$ is the identity over M_{tu}, and $(\psi \circ \psi')_{tu}$ is the identity over N_{tu}. Consequently, $\psi_{tu} : M_{tu} \to N_{tu}$ is an isomorphism such that $(\psi_{tu})_S = \varphi$. □

Exercises and problems

Exercise 1. We recommend that the proofs which are not given, or are sketched, or left to the reader, etc, be done. But in particular, we will cover the following cases.

- Show Facts 2.6 and 2.9.
- Check the details of Lemma 8.7.
- Show Fact 9.2 as well as the second case in Proposition 9.3.

Exercise 2. *(Projectors having the same image)*
Let a, c be in a not necessarily commutative ring $\mathbf{B}$. The following properties are equivalent.

- $ac = c$ and $ca = a$.
- $a^2 = a$, $c^2 = c$ and $a\mathbf{B} = c\mathbf{B}$.

In such a case let $h = c - a$ and $x = 1 + h$. Show the following results.

$ha = hc = 0$, $ah = ch = h$, $h^2 = 0$, $x \in \mathbf{B}^\times$, $ax = c$, $xa = x^{-1}a = a$ and $\boxed{x^{-1}ax = c}$.

It should be noted in passing that the equality $ax = c$ returns the equality $a\mathbf{B} = c\mathbf{B}$.
Special case. $\mathbf{A}$ is a commutative ring, M is an $\mathbf{A}$-module, and $\mathbf{B} = \mathrm{End}_{\mathbf{A}}(M)$: two projectors that have the same image are similar.

Exercise 3. *(Two equivalent projectors are similar)*
In a (not necessarily) commutative ring $\mathbf{B}$, consider two *equivalent* idempotents ($a^2 = a$, $b^2 = b$, $\exists p, q \in \mathbf{B}^\times$, $b = paq$). We will show that they are *conjugate* ($\exists d \in \mathbf{B}^\times$, $dad^{-1} = b$).

- In this question, a, $b \in \mathbf{B}$ are equivalent ($b = paq$), but are not assumed to be idempotents. Show that the element $c = p^{-1}bp$ satisfies $a\mathbf{B} = c\mathbf{B}$.
- In particular, if b is idempotent, c is a conjugate idempotent of b which satisfies $a\mathbf{B} = c\mathbf{B}$. Conclude by using the previous exercise.

Special case. $\mathbf{A}$ is a commutative ring, M is an $\mathbf{A}$-module, and $\mathbf{B} = \mathrm{End}_{\mathbf{A}}(M)$: two equivalent projectors of M are similar.

Exercise 4. *(An important consequence of Schanuel's lemma 2.8)*
1. We consider two exact sequences

$$0 \to K \to P_{n-1} \to \cdots \to P_1 \xrightarrow{u} P_0 \to M \to 0$$
$$0 \to K' \to P'_{n-1} \to \cdots \to P'_1 \xrightarrow{u'} P'_0 \to M \to 0$$

with the projective modules P_i and P'_i. Then, we obtain an isomorphism

$$K \oplus \bigoplus_{i \equiv n-1 \bmod 2} P'_i \oplus \bigoplus_{j \equiv n \bmod 2} P_j \simeq K' \oplus \bigoplus_{k \equiv n-1 \bmod 2} P_k \oplus \bigoplus_{\ell \equiv n \bmod 2} P'_\ell .$$

2. Deduce that if we have an exact sequence where the P_i's, $i \in [\![1..n]\!]$, are projective

$$0 \to P_n \to P_{n-1} \to \cdots \to P_1 \to P_0 \to M \to 0,$$

then, for every exact sequence

$$0 \to K' \to P'_{n-1} \to \cdots \to P'_1 \to P'_0 \to M \to 0,$$

where the P'_i's are projective, the module K' is also projective.

Exercise 5. Consider an exact sequence composed of finitely generated projective modules

$$0 \longrightarrow P_n \xrightarrow{u_n} P_{n-1} \xrightarrow{u_{n-1}} P_{n-2} \longrightarrow \cdots \longrightarrow P_2 \xrightarrow{u_2} P_1 \longrightarrow 0 .$$

Show that $\bigoplus_{i \text{ odd}} P_i \simeq \bigoplus_{j \text{ even}} P_j$.

Deduce that if the P_i's for $i \geqslant 2$ are stably free, similarly for P_1.

Exercise 6. Show that the following properties are equivalent.

- The ring $\mathbf{A}$ is reduced zero-dimensional.
- The finitely presented $\mathbf{A}$-modules are always finitely generated projective.
- Every module $\mathbf{A}/\langle a \rangle$ is finitely generated projective.

(In other words, show the converse for item *1* in Theorem 3.1.)

Exercise 7. *(Projectors of rank* 1*, see Proposition 7.4)*
Let $A = (a_{ij}) \in \mathbb{M}_n(\mathbf{A})$. We examine polynomial systems in the a_{ij}'s whose zeros define the subvariety $\mathbb{AG}_{n,1}(\mathbf{A})$ of $\mathbb{M}_n(\mathbf{A})$. We denote by $\mathcal{D}'_2(A)$ the ideal generated by the minors having one of the "four corners" on the diagonal (not to be mistaken with the principal minors, except when $n = 2$).

1. If A is a projector of rank $\leqslant 1$, then $\operatorname{Ann} A$ is generated by $1 - \operatorname{Tr} A$ (idempotent). In particular, a projector of rank 1 is of trace 1.

2. The equalities $\operatorname{Tr} A = 1$ and $\mathcal{D}'_2(A) = 0$ imply $A^2 = A$ and $\mathcal{D}_2(A) = 0$. In this case, A is a projector of rank 1 (but we can have $\operatorname{Tr} A = 1$ and $A^2 = A$ without having $\mathcal{D}_2(A) = 0$, e.g. for a projector of rank 3 over a ring in which $2 = 0$.) Consequently, for an arbitrary matrix A we have

$$\langle 1 - \operatorname{Tr} A \rangle + \mathcal{D}_1(A^2 - A) \subseteq \langle 1 - \operatorname{Tr} A \rangle + \mathcal{D}'_2(A) = \langle 1 - \operatorname{Tr} A \rangle + \mathcal{D}_2(A)$$

without necessarily having the left-equality.

3. We consider the polynomial $\det\big(\mathrm{I}_n + (X-1)A\big)$ (if $A \in \mathbb{AG}_n(\mathbf{A})$, it is the rank polynomial of the module $P = \operatorname{Im} A$) and we denote by $r_1(A)$ its coefficient in X. We therefore have the equality of the three following ideals, defining the subvariety $\mathbb{AG}_{n,1}(\mathbf{A})$ of $\mathbb{M}_n(\mathbf{A})$:

$$\langle 1-\operatorname{Tr} A\rangle + \mathcal{D}_2'(A) = \langle 1-\operatorname{Tr} A\rangle + \mathcal{D}_2(A) = \big\langle 1-r_1(A)\big\rangle + \mathcal{D}_1(A^2-A).$$

Specify the cardinality of each generator set.

Exercise 8. *(Projector of rank* 1 *having a regular coefficient)*
Let $A=(a_{ij})\in\mathbb{AG}_n(\mathbf{A})$ be a projector of rank 1, L_i its row i, C_j its column j.

1. Provide a direct proof of the matrix equality $C_j\cdot L_i = a_{ij}A$. By noticing that $L_i\cdot C_j = a_{ij}$, deduce the equality of ideals $\langle L_i\rangle\,\langle C_j\rangle = \langle a_{ij}\rangle$.

2. Suppose a_{ij} is regular; so $\langle L_i\rangle$ and $\langle C_j\rangle$ are invertible ideals, inverses of each other. Provide a direct proof of the exactitude in the middle of the sequence

$$\mathbf{A}^n \xrightarrow{\mathrm{I}_n - A} \mathbf{A}^n \xrightarrow{L_i} \langle L_i\rangle \to 0$$

and therefore conclude that $\langle L_i\rangle \simeq \operatorname{Im} A$.

3. Prove that the matrix A is entirely determined by L_i and C_j. More precisely, if $\mathbf{A}$ is a ring with explicit divisibility,

- compute the matrix A,
- deduce the condition for which the row L and the column C can be the row i and the column j of a projection matrix of rank 1 (we suppose that the common coefficient in position (i,j) is regular).

4. Let $C\in\operatorname{Im} A$, ${}^{\mathrm{t}}L\in\operatorname{Im}{}^{\mathrm{t}}A$ and $a=L\cdot C$. Show the matrix equality $C\cdot L = aA$ and deduce the equality of ideals $\langle L\rangle\,\langle {}^{\mathrm{t}}C\rangle = \langle a\rangle$. If a is regular, the ideals $\langle L\rangle$ and $\langle {}^{\mathrm{t}}C\rangle$ are invertible, inverses of each other, $\langle L\rangle\simeq\operatorname{Im} A$ and $\langle {}^{\mathrm{t}}C\rangle\simeq\operatorname{Im}{}^{\mathrm{t}}A$.

Exercise 9. If a *finitely generated* $\mathbf{A}$-module has its Fitting ideals generated by idempotents, it is finitely generated projective.

Exercise 10. *(Short syzygies)*
Notations, terminology. Let $(e_1,\dots,e_n)$ be the canonical bases of $\mathbf{A}^n$.
Let $x_1,\ \dots,\ x_n$ be elements of an $\mathbf{A}$-module. Let $x={}^{\mathrm{t}}[\,x_1\ \cdots\ x_n\,]$ and $x^\perp := \operatorname{Ker}({}^{\mathrm{t}}x)\subseteq\mathbf{A}^n$ the syzygy module between the x_i's.
We will say of a syzygy $z\in x^\perp$ that it is "short" if it possesses at most two nonzero coordinates, i.e. if $z\in\mathbf{A}e_i\oplus\mathbf{A}e_j$ $(1\leqslant i\neq j\leqslant n)$.

1. Let $z\in x^\perp$. Show that the condition "z is a sum of short syzygies" is a linear condition. Consequently, if z is "locally" a sum of short syzygies, it is also globally a sum of short syzygies.
2. Deduce that if $M=\sum \mathbf{A}x_i$ is a locally cyclic module, then every element of $x^\perp$ is a sum of short syzygies.
3. If every syzygy between three elements of $\mathbf{A}$ is a sum of short syzygies, then $\mathbf{A}$ is an *arithmetic ring*, i.e. every ideal $\langle x,y\rangle$ is locally principal.
4. In question *2* give a global solution by using a cyclic localization matrix $A=(a_{ij})\in\mathbb{M}_n(\mathbf{A})$ for x.

Exercise 11. *(Trivial syzygies)*
We use the notations of Exercise 10. Now $x_1, \ldots, x_n \in \mathbf{A}$.
For $z \in \mathbf{A}^n$ let $\langle z \,|\, x\rangle = \sum z_i x_i$. The module of syzygies $x^\perp$ contains the "trivial syzygies" $x_j e_i - x_i e_j$ (which are a special case of short syzygies).
In the two first questions, we show that if x is unimodular, then $x^\perp$ is generated by these trivial syzygies. We fix $y \in \mathbf{A}^n$ such that $\langle x \,|\, y\rangle = 1$.

1. Recall why $\mathbf{A}^n = \mathbf{A}y \oplus x^\perp$.
2. For $1 \leqslant i < j \leqslant n$, we define $\pi_{ij} : \mathbf{A}^n \to \mathbf{A}^n$ by
$$\pi_{ij}(z) = (z_i y_j - z_j y_i)(x_j e_i - x_i e_j),$$
so that $\operatorname{Im} \pi_{ij} \subseteq x^\perp \cap (\mathbf{A}e_i \oplus \mathbf{A}e_j)$. Show that $\pi = \sum_{i<j} \pi_{ij}$ is the projection over $x^\perp$ parallel to $\mathbf{A}y$. Deduce the result on the trivial syzygies. See also Exercise II-4.

We no longer suppose that x is unimodular. Let $M \in \mathbb{M}_n(\mathbf{A})$ be an alternating matrix.

3. Show that by letting $z = Mx$, we have $\langle x \,|\, z\rangle = 0$.
4. In which way is an alternating matrix a "sum of small alternating matrices"? Make the link with the definition of π_{ij} in question *2*.

Exercise 12. *(Projection matrices which have a free image)*
Let $P \in \mathbb{AG}_n(\mathbf{A})$ be a projector whose image is free of rank r; by Proposition 2.11 there exist $X \in \mathbf{A}^{n\times r}$, $Y \in \mathbf{A}^{r\times n}$ satisfying $YX = \mathrm{I}_r$ and $P = XY$.

1. Clarify the enlargement lemma (Lemma 2.10), in other words compute $A \in \mathbb{SL}_{n+r}(\mathbf{A})$ (and its inverse) such that
$$A^{-1}\operatorname{Diag}(0_r, P)A = \mathrm{I}_{r,n+r}. \tag{$*$}$$

2. Suppose that $X = {}^{\mathrm{t}}Y$ (so P is symmetrical).
Verify that we can impose upon A to be "orthonormal" i.e. ${}^{\mathrm{t}}A = A^{-1}$.
Conversely, if $A \in \mathbb{SL}_{n+r}(\mathbf{A})$ is orthonormal and satisfies $(*)$, then we can write $P = X\,{}^{\mathrm{t}}X$ with $X \in \mathbf{A}^{n\times r}$ and ${}^{\mathrm{t}}XX = \mathrm{I}_r$ (the matrix P is therefore symmetrical).

Exercise 13. *(Stably free modules of rank* 1*)*
Give direct proof that every stably free module of rank 1 is free (Proposition 4.4), by using the Binet-Cauchy formula (Exercise II-25).
Consider two matrices $R \in \mathbf{A}^{(n-1)\times n}$ and $R' \in \mathbf{A}^{n\times(n-1)}$ with $RR' = \mathrm{I}_{n-1}$. Show that $\operatorname{Ker} R$ is a free module. Conclude the result.

Exercise 14. *(Unimodular vectors, modules M satisfying $M \oplus \mathbf{A} \simeq \mathbf{A}^n$)*
Let x, $y \in \mathbf{A}^n$ be two vectors and $A \in \mathbb{M}_n(\mathbf{A})$ a matrix with first column x. Construct a matrix $B \in \mathbb{M}_n(\mathbf{A})$ as follows: its first row is ${}^{\mathrm{t}}y$ and its $n-1$ last rows are the $n-1$ last rows of $\widetilde{A}$, the cotransposed matrix of A.

1. Show that $\det(B) = \det(A)^{n-2}\,\langle x \,|\, y\rangle$ and that the $n-1$ last rows of B belong to $x^\perp := \operatorname{Ker} {}^{\mathrm{t}}x$.

From now on assume that $\langle x \,|\, y\rangle = 1$. We then know that the two stably free modules $x^\perp$ and $y^\perp$ are duals of one another (Facts 4.1 and 4.2); we detail this property in a matrix fashion in the case where $x^\perp$ is free.

2. Recall why $\mathbf{A}^n = \mathbf{A}x \oplus y^\perp$ and $\mathbf{A}^n = \mathbf{A}y \oplus x^\perp$.
3. Suppose that $\mathbf{A}x$ possesses a free direct complement in $\mathbf{A}^n$. Show in a matrix fashion that the same holds for $\mathbf{A}y$ by constructing an $n \times n$ invertible matrix "adapted" to the decomposition $\mathbf{A}^n = \mathbf{A}y \oplus x^\perp$.

Exercise 15. *(Symmetric principal localization matrix)*
Let $(x_1, \dots, x_n) \in \mathbf{A}^n$ possess a symmetric principal localization matrix $A \in \mathbb{M}_n(\mathbf{A})$. Let $\mathfrak{a} = \langle x_1, \dots, x_n\rangle$. By using Equality (5) of Proposition 7.4, show that $\mathfrak{a}^2$ is principal and specifically that: $\mathfrak{a}^2 = \left\langle x_1^2, \cdots, x_n^2\right\rangle = \left\langle x_1^2 + \cdots + x_n^2\right\rangle$.

Exercise 16. *(Regarding $\mathbf{A}/\mathfrak{a} \oplus \mathbf{A}/\mathfrak{b} \simeq \mathbf{A}/(\mathfrak{a} \cap \mathfrak{b}) \oplus \mathbf{A}/(\mathfrak{a} + \mathfrak{b})$)*
See also Exercise VIII-11 and Corollary XII-1.7.

1. Let $\mathfrak{a}$, $\mathfrak{b}$ be two ideals of $\mathbf{A}$ satisfying $1 \in (\mathfrak{a} : \mathfrak{b}) + (\mathfrak{b} : \mathfrak{a})$. Construct a $\theta \in \mathbb{GL}_2(\mathbf{A})$ which satisfies $\theta(\mathfrak{a} \oplus \mathfrak{b}) = (\mathfrak{a} \cap \mathfrak{b}) \oplus (\mathfrak{a} + \mathfrak{b})$. Deduce that $\mathbf{A}/\mathfrak{a} \oplus \mathbf{A}/\mathfrak{b}$ is isomorphic to $\mathbf{A}/(\mathfrak{a} \cap \mathfrak{b}) \oplus \mathbf{A}/(\mathfrak{a} + \mathfrak{b})$.

2. Let $a, b \in \mathbf{A}$, $\mathfrak{a} = \langle a\rangle$, $\mathfrak{b} = \langle b\rangle$. Suppose that there exists an $A \in \mathbb{GL}_2(\mathbf{A})$ such that $A \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} * \\ 0 \end{bmatrix}$. Show that $1 \in (\mathfrak{b} : \mathfrak{a}) + (\mathfrak{a} : \mathfrak{b})$. Find explicit d and m such that $\mathfrak{a} \cap \mathfrak{b} = \langle m\rangle$, $\mathfrak{a} + \mathfrak{b} = \langle d\rangle$, as well as a matrix equivalence between $\mathrm{Diag}(a, b)$ and $\mathrm{Diag}(m, d)$.

3. Let $a, b \in \mathbf{A}$ with $a \in \left\langle a^2\right\rangle$. Show that a, b satisfy the conditions of question *2.*

4. Let $\mathfrak{a}$, $\mathfrak{b}$ be two finitely generated ideals such that $\mathfrak{a} + \mathfrak{b}$ is locally principal. Show $1 \in (\mathfrak{a} : \mathfrak{b}) + (\mathfrak{b} : \mathfrak{a})$, $\mathfrak{a} \cap \mathfrak{b}$ is finitely generated and $\mathfrak{a}\mathfrak{b} = (\mathfrak{a} \cap \mathfrak{b})(\mathfrak{a} + \mathfrak{b})$.

The following exercises bring forth some results on the determinant, the characteristic polynomial and the fundamental polynomial.

Exercise 17. Let M be a finitely generated projective $\mathbf{A}$-module, e be an idempotent of $\mathbf{A}$, $f = 1 - e$ and φ be an endomorphism of M. It is clear that $M = eM \oplus fM$, so eM and fM are finitely generated projective. We also have $\varphi(eM) \subseteq eM$, and by letting $\varphi_e : eM \to eM$ be the endomorphism defined as such, prove that we have

$$\begin{aligned} \det(\varphi_e) = f + e\det(\varphi) \quad &\text{and} \quad \det(e\varphi) = r_0 f + e\det(\varphi) \\ \mathrm{F}_{e\varphi}(X) = \mathrm{F}_\varphi(eX) &= \mathrm{F}_{\varphi_e}(X) = f + e\,\mathrm{F}_\varphi(X) \\ \mathrm{C}_{\varphi_e}(X) &= f + e\,\mathrm{C}_\varphi(X) \\ \mathrm{R}_{eM}(X) &= f + e\,\mathrm{R}_M(X) \end{aligned}$$

Furthermore, show that $e\ \det(\varphi)$ is the determinant of φ_e as the endomorphism of the $\mathbf{A}[1/e]$-module eM.

Exercise 18. Consider the quasi-free module $M = \bigoplus_{k\in[\![1..n]\!]}(r_k\mathbf{A})^k$, where the r_k's are orthogonal idempotents. We have $M \simeq e_1\mathbf{A}\oplus\cdots\oplus e_n\mathbf{A}$ with $e_k = \sum_{j=k}^n r_j$, and $e_k \mid e_{k+1}$ for $k \in [\![1..n-1]\!]$ (cf. Lemma II-5.25, and Exercises II-10 and II-14). Let $r_0 = 1 - \sum_{i=1}^n r_i$ and $s_k = 1 - r_k$.

- Recall why $\mathrm{R}_{r_k\mathbf{A}}(X) = s_k + r_kX$.
- Show that $\mathrm{R}_M(X) = r_0 + r_1X + \cdots + r_nX^n = \prod_{k=1}^n(s_k + r_kX)^k$.
- Verify this equality using a direct computation.

Exercise 19. *(The determinant, component by component)*
Let φ be an endomorphism of a finitely generated projective module M having n generators. Let $r_h = \mathrm{e}_h(M)$ (for $h \in [\![0..n]\!]$) and $d = \det(\varphi)$. Denote by $\varphi^{(h)}$ the endomorphism of the $\mathbf{A}$-module $M^{(h)}$ induced by φ, $d_h = r_hd$, $\delta_h = \det(\varphi^{(h)})$ and $s_h = 1 - r_h$.

1. Show that we have the following equalities

$$d_0 = r_0,\ \delta_0 = 1,\ \delta_h = s_h + d_h \ \text{ and }\ d = d_0 + d_1 + \cdots + d_n = \delta_1 \times \cdots \times \delta_n.$$

2. Furthermore, show that d_h is the determinant of $\varphi^{(h)}$ in $\mathbf{A}[1/r_h]$ when we regard $\varphi^{(h)}$ as an endomorphism of the $\mathbf{A}[1/r_h]$-module $M^{(h)}$.

3. Similarly, show that we have

$$\mathrm{F}_{\varphi^{(h)}}(X) = s_h + r_h\,\mathrm{F}_\varphi(X) \quad\text{and}\quad \mathrm{C}_{\varphi^{(h)}}(X) = s_h + r_h\,\mathrm{C}_\varphi(X).$$

Exercise 20. *(Characteristic polynomial and fundamental polynomial in the case of constant rank)* Let φ be an endomorphism of a module M of constant rank h. Prove the following facts.

The characteristic polynomial of φ is monic of degree h and the fundamental polynomial of φ is of degree $\leqslant h$. The homogenized polynomials at degree h of $\mathrm{C}_\varphi(X)$ and $\mathrm{F}_\varphi(X)$ are respectively equal to $\det(X\mathrm{Id}_M - Y\varphi)$ and $\det(Y\mathrm{Id}_M + X\varphi)$. In other words we have the equalities

$$\mathrm{C}_\varphi(X) = X^h\,\mathrm{F}_\varphi(-1/X) \quad\text{and}\quad \mathrm{F}_\varphi(X) = (-X)^h\,\mathrm{C}_\varphi(-1/X).$$

Furthermore, $\det(\varphi) = (-1)^h\,\mathrm{C}_\varphi(0)$ is equal to the coefficient of X^h in $\mathrm{F}_\varphi(X)$.

Exercise 21. *(Characteristic polynomial and fundamental polynomial, general case)*
Let φ be an endomorphism of a finitely generated projective module M. Let

$$\mathrm{F}_\varphi(X) = 1 + v_1X + \cdots + v_nX^n \text{ and } \mathrm{R}_M(X) = r_0 + r_1X + \cdots + r_nX^n.$$

Then, show that we have the following equalities.

$$\begin{aligned} r_hv_k &= 0 \ \text{ for } 0 \leqslant h < k \leqslant n,\\ \mathrm{C}_\varphi(X) &= r_0 + \textstyle\sum_{1\leqslant h\leqslant n} r_h\,X^h\ \mathrm{F}_\varphi(-1/X),\\ \mathrm{F}_\varphi(-X) &= r_0 + \textstyle\sum_{1\leqslant h\leqslant n} r_h\,X^h\ \mathrm{C}_\varphi(1/X),\\ \det(\varphi - X\mathrm{Id}_M) &= \mathrm{R}_M(-1)\ \mathrm{C}_\varphi(X),\\ \det(\varphi) &= r_0 + r_1v_1 + \cdots + r_nv_n = \mathrm{R}_M(-1)\ \mathrm{C}_\varphi(0). \end{aligned}$$

Problem 1. *(Completion of unimodular vectors: a result due to Suslin)*
A vector of $\mathbf{A}^n$ is said to be *completable* if it is equal to the first column of a matrix of $\mathbb{GL}_n(\mathbf{A})$. It is then unimodular. We want to show the following result.

Let $b \in \mathbf{A}$ and $(a_1, \dots, a_n) \in \mathbf{A}^n$ such that $(\overline{a_1}, \dots, \overline{a_n})$ is completable over $\mathbf{A}/b\mathbf{A}$, then $(a_1, \dots, a_n, b^n)$ is completable (over $\mathbf{A}$).

By hypothesis, we have A, $D \in \mathbb{M}_n(\mathbf{A})$ satisfying $A\,D \equiv \mathrm{I}_n \mod b$, with $[\,a_1 \ \cdots \ a_n\,]$ as the first row of A. We want to find a matrix of $\mathbb{GL}_{n+1}(\mathbf{A})$ whose first row is $[\,a_1 \ \cdots \ a_n \ b^n\,]$. Let $a = \det(A)$.

1. Show that there exists a $C \in \mathbb{M}_n(\mathbf{A})$ such that $\begin{bmatrix} A & b\,\mathrm{I}_n \\ C & D \end{bmatrix} \in \mathbb{GL}_{2n}(\mathbf{A})$.

Now it is a matter of transforming the top-right corner $b\,\mathrm{I}_n$ of the above matrix into $B' := \mathrm{Diag}(b^n, 1, \dots, 1)$.

2. Show that we can write $B' = bE + aF$ with $E \in \mathbb{E}_n(\mathbf{A})$ and $F \in \mathbb{M}_n(\mathbf{A})$.

3. Verify that $\begin{bmatrix} A & b\,\mathrm{I}_n \\ C & D \end{bmatrix} \begin{bmatrix} \mathrm{I}_n & \widetilde{A}F \\ 0 & E \end{bmatrix} = \begin{bmatrix} A & B' \\ C & D' \end{bmatrix}$ with $D' \in \mathbb{M}_n(\mathbf{A})$.

4. Show that $\begin{bmatrix} A & B' \\ C & D' \end{bmatrix}$ is equivalent to a matrix $\begin{bmatrix} A & B' \\ C & D'' \end{bmatrix}$ where D'' has its $n-1$ last columns null. Deduce the existence of an invertible matrix whose first row is $[\,a_1 \ \cdots \ a_n \ b^n\,]$.

5. Example (Krusemeyer). If $(x, y, z) \in \mathbf{A}^3$ is unimodular, (x, y, z^2) is completable. More precisely, if $ux + vy + wz = 1$, the matrix below is suitable.

$$\begin{bmatrix} x & y & z^2 \\ v^2 & w - uv & -x - 2vz \\ -w - uv & u^2 & -y + 2uz \end{bmatrix}.$$

What is its determinant (independently from the fact that $ux + vy + wz = 1$)?

6. More generally, we have the following result (Suslin): if $(a_0, a_1, \dots, a_n)$ is unimodular, then $(a_0, a_1, a_2^2, \dots, a_n^n)$ is completable.

7. Show the following result (Suslin's $n!$ theorem): if $(a_0, a_1, \dots, a_n)$ is unimodular, then for exponents e_0, e_1, …, e_n such that $n!$ divides $e_0 \cdot e_1 \cdots e_n$, the vector $(a_0^{e_0}, a_1^{e_1}, \dots, a_n^{e_n})$ is completable.

Problem 2. *(The n-sphere when -1 is a sum of n squares, with I. Yengui)*
1. Let $\mathbf{A}$ be a ring in which -1 is a sum of 2 squares and x_0, x_1, $x_2 \in \mathbf{A}$ satisfying $x_0^2 + x_1^2 + x_2^2 = 1$.

a. Show that the vector (x_0, x_1, x_2) is completable by considering a matrix $M = \begin{bmatrix} x_0 & u & a \\ x_1 & v & b \\ x_2 & 0 & c \end{bmatrix}$ where u, v are linear forms in x_0, x_1, x_2 and a, b, c are constants.

b. Give examples of rings $\mathbf{A}$ in which -1 is a sum of 2 squares.

2. Suppose that -1 is a sum of n squares in the ring $\mathbf{A}$.

a. We use the notation $A \overset{\mathcal{G}}{\sim} B$ from page 920. Let x_0, x_1, …, x_n with $x_0^2 + \cdots + x_n^2 = 1$. Show that

$$^{\mathrm{t}}[\,x_0\ x_1\ \cdots\ x_n\,] \overset{\mathbb{E}_{n+1}}{\sim} {}^{\mathrm{t}}[\,1\ 0\ \cdots\ 0\,].$$

In particular, $^{\mathrm{t}}[\,x_0\ x_1\ \cdots\ x_n\,]$ is completable.

b. Let $m \geqslant n$, $x_0, x_1, \ldots, x_m$ and $y_{n+1}, \ldots, y_m$ satisfy $\sum\limits_{i=0}^{n} x_i^2 + \sum\limits_{j=n+1}^{m} y_j x_j = 1$. Show that $^{\mathrm{t}}[\,x_0\ x_1\ \cdots\ x_m\,] \overset{\mathbb{E}_{m+1}}{\sim} {}^{\mathrm{t}}[\,1\ 0\ \cdots\ 0\,]$.

3. Suppose that there exists an $a \in \mathbf{A}$ such that $1 + a^2$ is nilpotent. This is the case if -1 is a square in $\mathbf{A}$, or if 2 is nilpotent.

a. Let x_0, $x_1 \in \mathbf{A}$ with $x_0^2 + x_1^2 = 1$. Show that $\begin{bmatrix} x_0 & -x_1 \\ x_1 & x_0 \end{bmatrix} \in \mathbb{E}_2(\mathbf{A})$.

b. Let x_0, x_1, …,x_n and y_2, …, y_n in $\mathbf{A}$ such that $x_0^2 + x_1^2 + \sum_{i=2}^{n} x_i y_i = 1$. Show that $^{\mathrm{t}}[\,x_0\ x_1\ \cdots\ x_n\,] \overset{\mathbb{E}_{n+1}}{\sim} {}^{\mathrm{t}}[\,1\ 0\ \cdots\ 0\,]$.

c. Let $\mathbf{k}$ be a ring, $\mathbf{k}[\underline{X}, \underline{Y}] = \mathbf{k}[X_0, X_1, \ldots, X_n, Y_2, \ldots, Y_n]$ and

$$f = 1 - \big(X_0^2 + X_1^2 + \textstyle\sum_{i=2}^{n} X_i Y_i\big).$$

Let $\mathbf{A}_n = \mathbf{k}[x_0, x_1, \ldots, x_n, y_2, \ldots, y_n] = \mathbf{k}[\underline{X}, \underline{Y}]/\langle f \rangle$. Give examples for which, for all n, $^{\mathrm{t}}[\,x_0\ x_1\ \cdots\ x_n\,]$ is completable without -1 being a square in $\mathbf{A}_n$.

Some solutions, or sketches of solutions

Exercise 4. *1.* By induction on n, the $n = 1$ case being exactly Schanuel's lemma (Corollary 2.8). From each exact sequence, we construct another of length minus one

$$\begin{array}{ccccccccccc} 0 & \to & K & \to & P_{n-1} & \to & \cdots & \to & P_1 \oplus P_0' & \xrightarrow{u \oplus \mathrm{I}_{P_0}{}'} & \operatorname{Im} u \oplus P_0' & \to & 0 \\ 0 & \to & K' & \to & P_{n-1}' & \to & \cdots & \to & P_1 \oplus P_0' & \xrightarrow{u' \oplus \mathrm{I}_{P_0}} & \operatorname{Im} u' \oplus P_0 & \to & 0 \end{array}$$

But we have $\operatorname{Im} u \oplus P_0' \simeq \operatorname{Im} u' \oplus P_0$ by Schanuel's lemma applied to the two short exact sequences,

$$\begin{array}{ccccccccc} 0 & \to & \operatorname{Im} u & \to & P_0 & \to & M & \to & 0 \\ 0 & \to & \operatorname{Im} u' & \to & P_0' & \to & M & \to & 0 \end{array}$$

We can therefore apply the induction (to the two long exact sequences of length -1), which gives the desired result.

2. Immediate consequence of *1.*

Exercise 5. Let us show by induction on i that $\operatorname{Im} u_i$ is a finitely generated projective module. This is true for $i = 1$. Suppose it is true for $i \geqslant 1$; we have therefore a surjective linear map $P_i \xrightarrow{u_i} \operatorname{Im} u_i$ where $\operatorname{Im} u_i$ is finitely generated projective and thus $P_i \simeq \operatorname{Ker} u_i \oplus \operatorname{Im} u_i$. But $\operatorname{Ker} u_i = \operatorname{Im} u_{i+1}$ therefore $\operatorname{Im} u_{i+1}$ is finitely generated projective. In addition $P_i \simeq \operatorname{Im} u_i \oplus \operatorname{Im} u_{i+1}$. Then

$$\begin{aligned} P_1 \oplus P_3 \oplus P_5 \oplus \cdots &\simeq (\operatorname{Im} u_1 \oplus \operatorname{Im} u_2) \oplus (\operatorname{Im} u_3 \oplus \operatorname{Im} u_4) \oplus \cdots \\ &\simeq \operatorname{Im} u_1 \oplus (\operatorname{Im} u_2 \oplus \operatorname{Im} u_3) \oplus (\operatorname{Im} u_4 \oplus \operatorname{Im} u_5) \oplus \cdots \\ &\simeq P_2 \oplus P_4 \oplus P_6 \oplus \cdots \end{aligned}$$

Exercise 7. Let $A_1, \ldots, A_n$ be the columns of A and $t = \operatorname{Tr} A = \sum_i a_{ii}$.

1. Let us first check that $tA_j = A_j$:

by using $\begin{vmatrix} a_{ii} & a_{ij} \\ a_{ki} & a_{kj} \end{vmatrix} = 0$ and $A^2 = A$, $ta_{kj} = \sum_i a_{ii}a_{kj} = \sum_i a_{ki}a_{ij} = a_{kj}$.

Therefore $(1-t)A = 0$, then $(1-t)t = 0$, i.e. t idempotent. In addition, if $aA = 0$, then $at = 0$, i.e. $a = a(1-t)$.

2. On the localized ring at a_{ii}, two arbitrary columns A_j, A_k are multiples of A_i so $A_j \wedge A_k = 0$. Hence globally $A_j \wedge A_k = 0$, and so $\mathcal{D}_2(A) = 0$. Moreover, by using $\begin{vmatrix} a_{ik} & a_{ij} \\ a_{kk} & a_{kj} \end{vmatrix} = 0$, we have $\sum_k a_{ik}a_{kj} = \sum_k a_{ij}a_{kk} = a_{ij} \operatorname{Tr} A = a_{ij}$, i.e. $A^2 = A$.

3. The system on the right-hand side is of cardinality $1 + n^2$, the one in the middle of cardinality $1 + \binom{n}{2}^2$. To obtain the left-hand side one, we must count the minors that do not have a corner on the diagonal. Suppose $n \geqslant 3$, then there are $\binom{n}{2}\binom{n-2}{2}$ minors, and $\binom{n}{2}^2 - \binom{n}{2}\binom{n-2}{2} = (2n-3)\binom{n}{2}$ remain, hence the cardinality $1 + (2n-3)\binom{n}{2}$. For $n = 3$, each system is of cardinality 10. For $n > 3$, $1 + n^2$ is strictly less than the other two.

Exercise 8. *1.* We have $\begin{vmatrix} a_{i\ell} & a_{ij} \\ a_{k\ell} & a_{kj} \end{vmatrix} = 0$, i.e. $a_{kj}a_{i\ell} = a_{ij}a_{k\ell}$.

This is the equality $C_j \cdot L_i = a_{ij}A$. As for $L_i \cdot C_j$, this is the coefficient in position (i,j) of $A^2 = A$, i.e. a_{ij}.

2. We have $L_i \cdot A = L_i$ so $L_i \cdot (\mathrm{I}_n - A) = 0$. Conversely, for $u \in \mathbf{A}^n$ such that $\langle L_i \,|\, u\rangle = 0$, it must be shown that $u = (\mathrm{I}_n - A)(u)$, i.e. $Au = 0$, i.e. $\langle L_k \,|\, u\rangle = 0$. But $a_{ij}L_k = a_{kj}L_i$ and as a_{ij} is regular, this is immediate.

3. The equality $a_{kj}a_{i\ell} = a_{ij}a_{k\ell}$ shows that $C \cdot L = a_{ij}A$. Moreover, if $\mathbf{A}$ is with explicit divisibility, we can compute A from L and C.

If we take a row L whose coefficients are called $a_{i\ell}$ ($\ell \in [\![1..n]\!]$) and a column C whose coefficients are called a_{kj} ($k \in [\![1..n]\!]$), with the common element a_{ij} being regular, the conditions are the following:

- each coefficient of $C \cdot L$ must be divisible by a_{ij}, hence $A = \dfrac{1}{a_{ij}} C \cdot L$,
- we must have $\operatorname{Tr}(A) = a_{ij}$, i.e. $L \cdot C = a_{ij}$.

Naturally, these conditions are directly related to the invertibility of the ideal generated by the coefficients of L.

4. In the matrix equality $C \cdot L = (L \cdot C)\, A$ to be proven, each side is bilinear in (L, C). However, the equality is true if ${}^{\mathrm{t}}L$ is a column of ${}^{\mathrm{t}}A$ and C a column of A, therefore it remains true for ${}^{\mathrm{t}}L \in \operatorname{Im} {}^{\mathrm{t}}A$ and $C \in \operatorname{Im} A$. The rest is easy.

Exercise 9. M is the quotient module of a finitely generated projective module P which share the same Fitting ideals. If $P \oplus N = \mathbf{A}^n$, $M \oplus N$ is a quotient of $\mathbf{A}^n$ with the same Fitting ideals. Therefore there is no nonzero syzygy between the generators of $\mathbf{A}^n$ in the quotient $M \oplus N$. Therefore

$$M \oplus N = \mathbf{A}^n \quad \text{and} \quad P/M \simeq (P \oplus N)/(M \oplus N) = 0.$$

Exercise 10. *1.* A syzygy $z = \sum z_k e_k$ is a sum of short syzygies if and only if there exist syzygies $z_{ij} \in \mathbf{A}e_i \oplus \mathbf{A}e_j$ such that $z = \sum_{i<j} z_{ij}$. This is interpreted as follows

$$\exists \alpha_{ij}, \beta_{ij} \in \mathbf{A},\ z_{ij} = \alpha_{ij}e_i + \beta_{ij}e_j,\ \langle z_{ij} \,|\, x\rangle = 0 \quad \text{and} \quad z = \sum\nolimits_{i<j} z_{ij}.$$

This is equivalent to $z_k = \sum_{k<j} \alpha_{kj} + \sum_{i<k} \beta_{ik}$ ($k \in [\![1..n]\!]$) and $\alpha_{ij}x_i + \beta_{ij}x_j = 0$ (for $i < j$). This is indeed a system of linear equations with the "unknowns" α_{ij}, β_{ij}.

2. By reasoning locally, we can assume that the x_i's are multiples of x_1, which we write as $b_i x_1 + x_i = 0$. Hence the syzygies $r_i = b_i e_1 + e_i$ for $i \in [\![2..n]\!]$.

Let $z \in x^\perp$. Let $y = z - (z_2 r_2 + \cdots + z_n r_n)$, we have $y_i = 0$ for $i \geqslant 2$, and so y is a (very) short syzygy. Thus, $z = y + \sum_{i=2} z_i r_i$ is a sum of short syzygies.

3. Let x, $y \in \mathbf{A}$. We are looking for s, t with $s + t = 1$, $sx \in \mathbf{A}y$ and $ty \in \mathbf{A}x$. We write the syzygy $(-1, -1, 1)$ between $(x, y, x + y)$ as a sum of short syzygies

$$(-1, -1, 1) = (0, a, a') + (b, 0, b') + (c, c', 0).$$

In particular, $a' + b' = 1$, and the result follows.

4. By definition $\sum_i a_{ii} = 1$ and $\begin{vmatrix} a_{ij} & a_{ik} \\ x_j & x_k \end{vmatrix} = 0$. This provides several short syzygies $a_{ij}e_k - a_{ik}e_j$. We keep the $r_{ik} = a_{ii}e_k - a_{ik}e_i$, i.e. those that correspond to a "diagonal minor" $\begin{vmatrix} a_{ii} & a_{ik} \\ x_i & x_k \end{vmatrix}$. For $z \in \mathbf{A}^n$, let

$$y = Az \quad \text{and} \quad z' = \sum\nolimits_{i,k} z_k r_{ik} = \sum\nolimits_{i,k} z_k(a_{ii}e_k - a_{ik}e_i).$$

Then $z = z' + y$: indeed, the coefficient of e_j in z' is

$$\left(\sum\nolimits_i a_{ii}\right) z_j - \sum\nolimits_k a_{jk}z_k = z_j - (Az)_j.$$

Since $A^2 - A$ annihilates M, $z - y \in x^\perp$, so $z \in x^\perp \Rightarrow y \in x^\perp$. Each $y_i e_i$ is a (very) short syzygy since $y_i x_i = 0$. Therefore $z = z' + y = z' + \sum y_i e_i$ is a sum of short syzygies.

Exercise 11. *1.* We write $z \in \mathbf{A}^n$ in the form

$$z = \langle x \,|\, z\rangle.y + (z - \langle x \,|\, z\rangle.y),$$

which provides the decomposition $\mathbf{A}^n = \mathbf{A}y \oplus x^\perp$.

2. For $i \leqslant j$, define $z_{ij} \in \mathbf{A}$ by $z_{ij} = z_i y_j - z_j y_i$ and let

$$z' = \sum\nolimits_{i<j} z_{ij}(x_j e_i - x_i e_j) = \sum\nolimits_{i \leqslant j} z_{ij}(x_j e_i - x_i e_j).$$

For fixed k, the coefficient of e_k in the right-hand sum is

$$\begin{aligned} \sum\nolimits_{j \geqslant k} z_{kj}x_j - \sum\nolimits_{i<k} z_{ik}x_i &= \sum\nolimits_{j \geqslant k}(z_k y_j - z_j y_k)x_j - \sum\nolimits_{i<k}(z_i y_k - z_k y_i)x_i \\ &= z_k \sum\nolimits_{j=1}^n y_j x_j - y_k \sum\nolimits_{j=1}^n z_j x_j \;=\; z_k - \langle z \,|\, x\rangle y_k\,, \end{aligned}$$

which means that $z' = z - \langle z \,|\, x\rangle y$ and proves the required result.

3. If ψ is the alternating bilinear form associated with the matrix, the equality $\langle x \,|\, z\rangle = 0$ simply means that $\psi(x, x) = 0$.

4. We can express an alternating $n \times n$ matrix as a sum of $\frac{n(n-1)}{2}$ small alternating matrices. For $n = 3$, here is the alternating matrix allowing us to make the connection with question *2* (y is fixed and it is z that varies):

$$M_z = \begin{bmatrix} 0 & z_1y_2 - z_2y_1 & z_1y_3 - z_3y_1 \\ -z_1y_2 + z_2y_1 & 0 & z_2y_3 - z_3y_2 \\ -z_1y_3 + z_3y_1 & -z_2y_3 + z_3y_2 & 0 \end{bmatrix}.$$

The decomposition of M_z into small alternating matrices provides the π_{ij}'s. It must be noted that $z \mapsto M_z$, $\mathbf{A}^n \to \mathbb{M}_n(\mathbf{A})$ is a linear map and that $\pi(z) = M_z x$.

Exercise 12. *1.* We follow the method of this course. It leads to letting

$$A = \begin{bmatrix} 0_r & -Y \\ X & \mathrm{I}_n - P \end{bmatrix}, \quad A' = \begin{bmatrix} 0_r & Y \\ -X & \mathrm{I}_n - P \end{bmatrix}.$$

These matrices satisfy

$$A \begin{bmatrix} \mathrm{I}_r & 0 \\ 0 & 0_n \end{bmatrix} = \begin{bmatrix} 0_r & 0 \\ 0 & P \end{bmatrix} A, \ AA' = \mathrm{I}_{n+r}.$$

2. Immediate since we have the formulas right in front of us.

Exercise 13. The Binet-Cauchy formula gives $1 = \det(RR') = \sum \delta_i \delta'_i$ with

$$\delta_i = \det(R_{1..n-1,1..n\setminus i}) \text{ and } \delta'_i = \det(R'_{1..n\setminus i,1..n-1}).$$

Let $S = [\,\delta'_1 \ -\delta'_2 \ \cdots \ (-1)^{n-1}\delta'_n\,]$. Check that the square matrix $A = \begin{bmatrix} S \\ R \end{bmatrix}$ has determinant 1. This shows that $\operatorname{Ker} R$ is free (Proposition 4.4).
Actually let $S' = {}^{\mathrm{t}}[\,\delta_1 \ -\delta_2 \ \cdots \ (-1)^{n-1}\delta_n\,]$ and $A' = [S'\,R']$. Then $AA' = \mathrm{I}_n$, and this shows that $S' \in \mathbf{A}^n$ is a basis of $\operatorname{Ker} R$.

Exercise 14. *1.* Consider the matrix $B\,A$. By definition of B, $B\,A$ is upper triangular, with diagonal $(\langle x \,|\, y\rangle, \delta, \ldots, \delta)$ where $\delta = \det(A)$. By taking the determinant, we obtain $\det(B)\det(A) = \langle x \,|\, y\rangle\, \delta^{n-1}$. The announced algebraic identities are therefore true when δ is invertible. Since we are dealing with algebraic identities, they are always true. The second item of the question is immediate.

2. Write $z \in \mathbf{A}^n$ in the form $z = \langle y \,|\, z\rangle\, x + (z - \langle y \,|\, z\rangle\, x)$, which gives us the decomposition $\mathbf{A}^n = \mathbf{A}x \oplus y^{\perp}$.

3. The hypothesis boils down to saying that x is the first column of an invertible matrix A. Therefore y is the first row of the invertible matrix B above. The matrix ${}^{\mathrm{t}}B$ is adapted to the decomposition $\mathbf{A}^n = \mathbf{A}y \oplus x^{\perp}$.

Exercise 15. Let $x = [\,x_1 \ \cdots \ x_n\,]$. For $\alpha = {}^{\mathrm{t}}[\alpha_1, \ldots, \alpha_n]$ and $\beta = A\alpha$, the equality in question is

$$\beta\, x = \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix} \begin{bmatrix} x_1 & \cdots & x_n \end{bmatrix} = x\,\alpha\, A \quad \text{with} \quad x\,\beta = x\,\alpha.$$

Take $\alpha_i = x_i$. Since $xA = x$ and A is symmetric, we obtain $A\,{}^{\mathrm{t}}x = {}^{\mathrm{t}}x$, i.e. $\beta = {}^{\mathrm{t}}x$. Hence ${}^{\mathrm{t}}x\,x = x\,{}^{\mathrm{t}}x\,A = (x_1^2 + \cdots + x_n^2)A$.
Finally, $x_ix_j \in \left\langle x_1^2 + \cdots + x_n^2 \right\rangle$ $(i, j \in [\![1..n]\!])$.

Exercise 16. *1.* Let $\alpha \in (\mathfrak{b} : \mathfrak{a})$ and $\beta \in (\mathfrak{a} : \mathfrak{b})$ satisfy $1 = \alpha + \beta$. Then, the matrix $\theta = \begin{bmatrix} \alpha & \beta \\ -1 & 1 \end{bmatrix}$, with determinant 1 and with inverse $\theta^{-1} = \begin{bmatrix} 1 & -\beta \\ 1 & \alpha \end{bmatrix}$, is suitable. Indeed

$$\begin{bmatrix} \alpha & \beta \\ -1 & 1 \end{bmatrix} \begin{bmatrix} \mathfrak{a} \\ \mathfrak{b} \end{bmatrix} \subseteq \begin{bmatrix} \mathfrak{a} \cap \mathfrak{b} \\ \mathfrak{a} + \mathfrak{b} \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 1 & -\beta \\ 1 & \alpha \end{bmatrix} \begin{bmatrix} \mathfrak{a} \cap \mathfrak{b} \\ \mathfrak{a} + \mathfrak{b} \end{bmatrix} \subseteq \begin{bmatrix} \mathfrak{a} \\ \mathfrak{b} \end{bmatrix}.$$

On the left-hand side, the upper inclusion comes from the fact that $\alpha\mathfrak{a}+\beta\mathfrak{b} \subseteq \mathfrak{a}\cap\mathfrak{b}$, and the lower one is trivial. On the right-hand side, the upper inclusion comes from the fact that $\mathfrak{a} \cap \mathfrak{b} + \beta(\mathfrak{a} + \mathfrak{b}) \subseteq \mathfrak{a}$, and the lower one comes from the fact that $\mathfrak{a} \cap \mathfrak{b} + \alpha(\mathfrak{a} + \mathfrak{b}) \subseteq \mathfrak{b}$. Recap: we have $\theta(\mathfrak{a} \oplus \mathfrak{b}) = (\mathfrak{a} \cap \mathfrak{b}) \oplus (\mathfrak{a} + \mathfrak{b})$ with $\theta = \begin{bmatrix} 1 & \beta \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix} \in \mathbb{E}_2(\mathbf{A})$.

2. We can take A of the form $A = \begin{bmatrix} u & v \\ -b' & a' \end{bmatrix}$ with $ua' + vb' = 1$ and $a'b = b'a$.

Let $m = a'b = b'a$, $d = ua + vb$; by inverting $A \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} d \\ 0 \end{bmatrix}$, we obtain $a = da'$ and $b = db'$. It is clear that $\mathfrak{a} \cap \mathfrak{b} = \langle m \rangle$ and $\mathfrak{a} + \mathfrak{b} = \langle d \rangle$. We have $a' \in (\mathfrak{a} : \mathfrak{b})$ and $b' \in (\mathfrak{b} : \mathfrak{a})$. Therefore $1 = \alpha + \beta$ with $\alpha = vb' \in (\mathfrak{b} : \mathfrak{a})$, $\beta = ua' \in (\mathfrak{a} : \mathfrak{b})$. To explicit a matrix equivalence, it suffices to use a matrix θ from the previous question:

$$\theta \begin{bmatrix} a \\ 0 \end{bmatrix} = \begin{bmatrix} vm \\ -a \end{bmatrix} = v \begin{bmatrix} m \\ 0 \end{bmatrix} - a' \begin{bmatrix} 0 \\ d \end{bmatrix}, \quad \theta \begin{bmatrix} 0 \\ b \end{bmatrix} = \begin{bmatrix} um \\ b \end{bmatrix} = u \begin{bmatrix} m \\ 0 \end{bmatrix} + b' \begin{bmatrix} 0 \\ d \end{bmatrix}.$$

Hence the matrix equivalence: $\theta \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} = \begin{bmatrix} m & 0 \\ 0 & d \end{bmatrix} \begin{bmatrix} v & u \\ -a' & b' \end{bmatrix}$.

3. The hypothesis is $a = a^2x$ for some given x. Then, the element $e = ax$ is idempotent and $\langle a \rangle = \langle e \rangle$. We must solve $a'b = b'a$, $1 = ua' + vb'$, which is a system of linear equations in a', b', u, v.

Modulo $1 - e$, we have $ax = 1$. We take $a' = a$, $b' = b$, $u = x$, $v = 0$.

Modulo e, we have $a = 0$. We take $a' = a$, $b' = 1$, $u = 0$, $v = 1$.

Therefore globally

$$a' = a, \quad b' = axb + (1 - ax)1 = 1 - ax + axb, \quad u = ax^2, \quad v = 1 - ax.$$

4. Let $\mathfrak{a} = \langle x_1, \dots, x_n \rangle$ and $\mathfrak{b} = \langle y_1, \dots, y_m \rangle$.

We write $\mathfrak{a} + \mathfrak{b} = \langle z_1, \dots, z_{n+m} \rangle$ with $z_1 = x_1, \dots, z_{n+m} = y_m$. Let $s_1, \dots, s_{n+m}$ be comaximal such that over $\mathbf{A}_{s_i}$ we have $\mathfrak{a} + \mathfrak{b} = \langle z_i \rangle$.

In each localized ring we have $\mathfrak{a} \subseteq \mathfrak{b}$ or $\mathfrak{b} \subseteq \mathfrak{a}$, hence $\{\mathfrak{a} + \mathfrak{b}, \mathfrak{a} \cap \mathfrak{b}\} = \{\mathfrak{a}, \mathfrak{b}\}$, and

$$1 \in (\mathfrak{a} : \mathfrak{b}) + (\mathfrak{b} : \mathfrak{a}), \ \mathfrak{a}\mathfrak{b} = (\mathfrak{a} \cap \mathfrak{b})(\mathfrak{a} \oplus \mathfrak{b}) \ \text{and} \ \mathfrak{a} \cap \mathfrak{b} \text{ is finitely generated.}$$

Exercise 17. We use the notations of Lemma 8.7.

Let us take a look at the determinants of $e\varphi$ and φ_e. We have

$\det(\varphi) = \det(\mathrm{I}_n - F + H)$, $\det(e\varphi) = \det(\mathrm{I}_n - F + eH)$ and $\det(\varphi_e) = \det(\mathrm{I}_n - eF + eH)$.

We deduce that

$$e \det(\varphi_e) = \det(e\mathrm{I}_n - eF + eH) = e \det(\varphi) \text{ and}$$
$$f \det(\varphi_e) = \det(f\mathrm{I}_n - feF + feH) = \det(f\mathrm{I}_n) = f.$$

Therefore $\det(\varphi_e) = f \det(\varphi_e) + e \det(\varphi_e) = f + e \det(\varphi)$.

Similarly $e\det(e\varphi) = \det(e\mathrm{I}_n - eF + eH) = e\det(\varphi)$ and

$$f\det(e\varphi) = \det(f\mathrm{I}_n - fF + feH) = f\det(\mathrm{I}_n - F) = f\,\mathrm{R}_M(0) = f\mathrm{e}_0(M).$$

By applying $\det(\varphi_e) = f + e\det(\varphi)$ to the endomorphisms $\mathrm{Id} + X\varphi$, $X\mathrm{Id} - \varphi$ and $X\mathrm{Id}$ of the $\mathbf{A}[X]$-module $M[X]$ we obtain

$$\mathrm{F}_{\varphi_e}(X) = f + e\,\mathrm{F}_{\varphi}(X),\ \mathrm{C}_{\varphi_e}(X) = f + e\,\mathrm{C}_{\varphi}(X) \text{ and } \mathrm{R}_{eM}(X) = f + e\,\mathrm{R}_M(X).$$

Moreover, the matrix eH simultaneously represents the endomorphism $e\varphi$ of M and the endomorphism φ_e of eM. We therefore have $\mathrm{F}_{\varphi_e}(X) = \mathrm{F}_{e\varphi}(X) = \det(\mathrm{I}_n + eXH) = \mathrm{F}_{\varphi}(eX)$.

As far as the last assertion is concerned: we must look at $\det(\varphi_e)$ in $\mathbf{A}/\langle f\rangle$, we obtain $e\det(\varphi)$ modulo $f\mathbf{A}$, and this corresponds to the element $e\det(\varphi)$ of $e\mathbf{A}$.

Exercise 19. *1.* We have $\varphi^{(h)} = \varphi_{r_h}$ by applying the notation of Exercise 17. Therefore $\delta_h = s_h + d_h$. We have $\delta_0 = 1$ because $M^{(0)} = \{0\}$, and since $\delta_0 = s_0 + d_0$, this gives $d_0 = r_0$.
The equality $d = d_0 + d_1 + \cdots + d_n$ is trivial.
The equality $d = \delta_1 \times \cdots \times \delta_n$ results from item *3* of Theorem 8.1. We can also prove $d_0 + d_1 + \cdots + d_n = \delta_1 \times \cdots \times \delta_n$ by a direct computation.

2 and *3.* Already seen in Exercise 18.

Exercise 20. Recall: for $a \in \mathbf{A}$ we have $\det(a\varphi) = \mathrm{R}_M(a)\det(\varphi) = a^h\det(\varphi)$. We then place ourselves on the ring $\mathbf{A}[X, 1/X]$ and consider the module $M[X, 1/X]$. We obtain

$$X^h\,\mathrm{F}_{\varphi}(-1/X) = \det\big(X(\mathrm{Id}_M - (1/X)\varphi)\big) = \det(X\mathrm{Id}_M - \varphi) = \mathrm{C}_{\varphi}(X).$$

By replacing X by $-1/X$ in $\mathrm{C}_{\varphi}(X) = X^h\,\mathrm{F}_{\varphi}(-1/X)$ we obtain the other equality. The two polynomials are therefore of degrees $\leqslant h$. As the constant coefficient of F_{φ} is equal to 1, we also obtain that C_{φ} is monic.
For the homogenized polynomials, the same computation works.
For the determinant we notice that $\det(-\varphi) = \mathrm{C}_{\varphi}(0)$.

Exercise 21. We work over the ring $\mathbf{A}_{r_h}$ and we consider the module r_hM and the endomorphism $\varphi^{(h)}$. We obtain a module of constant rank h. Therefore $r_h\,\mathrm{F}_{\varphi}(X)$ and $r_h\,\mathrm{C}_{\varphi}(X)$ are of degrees $\leqslant h$, and $r_h\big(X^h\,\mathrm{F}_{\varphi}(-1/X)\big) = r_h\,\mathrm{C}_{\varphi}(X)$. It remains to sum up the equalities obtained in this way for $h \in [\![1..n]\!]$.
We perform the same computation for the second equality. The last two equalities were already known, except for $\det(\varphi) = r_0 + r_1v_1 + \cdots + r_nv_n$ which can be proven in the same way as the first.

Problem 1. *1.* Let C, $U \in \mathbb{M}_n(\mathbf{A})$ such that $AD = \mathrm{I}_n + bU$, $DA = \mathrm{I}_n + bC$. Then

$$\begin{bmatrix} A & b\mathrm{I}_n \\ C & D \end{bmatrix} \begin{bmatrix} D & -b\mathrm{I}_n \\ -U & A \end{bmatrix} = \begin{bmatrix} \mathrm{I}_n & 0 \\ * & \mathrm{I}_n \end{bmatrix} \in \mathbb{GL}_{2n}(\mathbf{A}).$$

2. We work modulo a by noticing that b is invertible modulo a. We can therefore, over $\mathbf{A}/a\mathbf{A}$, consider $b^{-1}B'$: it is a diagonal matrix of determinant 1, therefore it belongs to $\mathbb{E}_n(\mathbf{A}/a\mathbf{A})$ (cf. Exercise II-17), we lift it to a matrix $E \in \mathbb{E}_n(\mathbf{A})$ and we obtain $B' \equiv bE \bmod a$.

3. Immediate.

4. It suffices to use the submatrix I_{n-1} which occurs in B' to kill the coefficients of the last $n-1$ columns of D'. The square submatrix of order $n+1$ obtained from $\begin{bmatrix} A & B' \\ C & D'' \end{bmatrix}$ by deleting the rows 2 to n and the last $n-1$ columns is invertible with its first row being $[\, a_1 \ \cdots \ a_n \ b^n \,]$.

5. Modulo z, the vector $[\, x \ y \,]$ is completable in $A := \begin{bmatrix} x & y \\ -v & u \end{bmatrix}$.

We have $\det(A) = a := ux + vy \equiv 1 \bmod z$ and we can take $D = \widetilde{A}$.

We write $DA = a\,\mathrm{I}_2 = \mathrm{I}_2 - wz\mathrm{I}_2$, so $C = -w\mathrm{I}_2$. The matrix $\begin{bmatrix} A & z\mathrm{I}_2 \\ C & D \end{bmatrix}$ has determinant $(a + wz)^2$. To find E, we use the equality

$$\begin{bmatrix} z & 0 \\ 0 & z^{-1} \end{bmatrix} = \mathrm{E}_{21}(-1)\mathrm{E}_{12}(1 - z^{-1})\mathrm{E}_{21}(z)\mathrm{E}_{12}\big(z^{-1}(z^{-1} - 1)\big)$$

and the fact that modulo a, $zw \equiv 1$. The author of the exercise has obtained a matrix G that is more complicated than that of Krusemeyer. With $p = (y+u)w-u$, $q = (x-v)w+v$,

$$G = \begin{bmatrix} x & y & z^2 \\ p(w-1)v - w & -p(w-1)u & y + u(z+1) \\ -q(w-1)v & q(w-1)u - w & -x + v(z+1) \end{bmatrix}.$$

We have $\det(G) = 1+(xu+yv+zw-1)(wz+1)(yq-xp+1)$ whereas Krusemeyer's matrix has determinant $(ux + vy + wz)^2$!

6. Immediate by induction.

Problem 2. *1a.* We have $\det(M) = -(cx_1 - bx_2)u + (cx_0 - ax_2)v$.
With $u = -(cx_1 + bx_2)$, $v = cx_0 + ax_2$, we obtain $\det(M) = cx_0^2 + cx_1^2 - (a^2+b^2)x_2^2$. It suffices to take $c = 1$ and a, $b \in \mathbf{A}$ such that $-1 = a^2 + b^2$.

1b. Let us show that -1 is a sum of two squares if $\mathbf{A}$ contains a finite field. We can assume that $\mathbf{A}$ is a field of odd cardinality q.
Consider the sets $A = \{\, a^2 \mid a \in \mathbf{A} \,\}$ and $B = \{\, -1 - b^2 \mid b \in \mathbf{A} \,\}$.
They have $(q+1)/2$ elements, so $A \cap B \neq \emptyset$, which gives the result.

Now here is a more general result. If $n \not\equiv 0 \bmod 4$, then -1 is a sum of two squares in $\mathbb{Z}/n\mathbb{Z}$. The hypothesis can be written as $\gcd(n, 4) = 1, 2$ so $2 \in n\mathbb{Z} + 4\mathbb{Z}$, $2 = nu + 4v$. Let $m = -1 + nu = -4v + 1$; since $\gcd(4n, m) = 1$, the arithmetic progression $4n\mathbb{N} + m$ contains a prime number p (Dirichlet), which satisfies $p \equiv m \equiv -1 \bmod n$ and $p \equiv m \equiv 1 \bmod 4$.
By this last congruence, p is a sum of two squares, $p = a^2 + b^2$, so $-1 = a^2 + b^2$ in $\mathbb{Z}/n\mathbb{Z}$.

We deduce that if $n.1_{\mathbf{A}} = 0$ with $n \not\equiv 0 \bmod 4$ (this is the case if n is a prime number), then -1 is a sum of two squares in $\mathbf{A}$.

2a. Let $a_1, \ldots, a_n$ such that $-1 = \sum_{i=1}^n a_i^2$. We will use

$$\textstyle\sum_{i=1}^n (x_i - a_i x_0)(x_i + a_i x_0) = \sum_{i=1}^n x_i^2 - x_0^2 \sum_{i=1}^n a_i^2 = 1.$$

We have

$$\begin{bmatrix} x_0 \\ x_1 \\ \vdots \\ x_n \end{bmatrix} \overset{\mathbb{E}_{n+1}}{\sim} \begin{bmatrix} x_0 \\ x_1 + a_1x_0 \\ \vdots \\ x_n + a_nx_0 \end{bmatrix} \overset{\mathbb{E}_{n+1}}{\sim} \begin{bmatrix} x_0 + h \\ x_1 + a_1x_0 \\ \vdots \\ x_n + a_nx_0 \end{bmatrix} \qquad \begin{matrix} \text{with} \\ h = \sum_{i=1}^{n} \lambda_i(x_i + a_ix_0) \end{matrix}$$

By taking $\lambda_i = (1 - x_0)(x_i - a_ix_0)$, we obtain $h = 1 - x_0$ so $x_0 + h = 1$. It is then clear that

$${}^{\mathrm{t}}[1, x_1 + a_1x_0, \ldots, x_n + a_nx_0] \overset{\mathbb{E}_{n+1}}{\sim} {}^{\mathrm{t}}[1, 0, \ldots, 0].$$

Explicitly, by numbering the $n + 1$ rows from 0 to n (instead of 1 to $n + 1$) and by letting

$$N = \prod_{i=1}^{n} \mathrm{E}_{i,0}\big(-(x_i + a_ix_0)\big) \prod_{i=1}^{n} \mathrm{E}_{0,i}\big((1 - x_0)(x_i - a_ix_0)\big) \prod_{i=1}^{n} \mathrm{E}_{i,0}(a_i)$$
$$M = N^{-1} = \prod_{i=1}^{n} \mathrm{E}_{i,0}(-a_i) \prod_{i=1}^{n} \mathrm{E}_{0,i}\big((x_0 - 1)(x_i - a_ix_0)\big) \prod_{i=1}^{n} \mathrm{E}_{i,0}(x_i + a_ix_0),$$

we obtain a matrix $M \in \mathbb{E}_{n+1}(\mathbf{A})$ with first column ${}^{\mathrm{t}}[\, x_0 \ \cdots \ x_n \,]$.

2b. We use $\mathbf{B} = \mathbf{A}/\langle x_{n+1}, \ldots, x_m\rangle$. The morphisms $\mathbb{E}_r(\mathbf{A}) \twoheadrightarrow \mathbb{E}_r(\mathbf{B})$ are surjective. We first obtain

$${}^{\mathrm{t}}[x_0, \ldots, x_n] \overset{\mathbb{E}_{n+1}(\mathbf{B})}{\sim} {}^{\mathrm{t}}[1, 0, \ldots, 0],$$

so some $x'_0, \ldots, x'_n \in \mathbf{A}$ with in particular $x'_0 \equiv 1 \bmod \langle x_{n+1}, \ldots, x_m\rangle$ such that

$${}^{\mathrm{t}}[x_0, \ldots, x_n, x_{n+1}, \ldots, x_m] \overset{\mathbb{E}_{m+1}(\mathbf{A})}{\sim} {}^{\mathrm{t}}[x'_0, \ldots, x'_n, x_{n+1}, \ldots, x_m].$$

We easily deduce that

$${}^{\mathrm{t}}[x'_0, \ldots, x'_n, x_{n+1}, \ldots, x_m] \overset{\mathbb{E}_{m+1}(\mathbf{A})}{\sim} {}^{\mathrm{t}}[1, \ldots, x'_n, x_{n+1}, \ldots, x_m] \overset{\mathbb{E}_{m+1}(\mathbf{A})}{\sim} {}^{\mathrm{t}}[1, 0, \ldots, 0].$$

3a. We have $\begin{bmatrix} x_0 & -x_1 \\ x_1 & x_0 \end{bmatrix} \overset{\mathbb{E}_2(\mathbf{A})}{\sim} B = \begin{bmatrix} x_0 + ax_1 & -x_1 + ax_0 \\ x_1 & x_0 \end{bmatrix}$. By using the fact that $1 + a^2$ is nilpotent, we see that $x_0 + ax_1$ is invertible because

$$(x_0 + ax_1)(x_0 - ax_1) = x_0^2 + x_1^2 - (1 + a^2)x_1^2 = 1 - (1 + a^2)x_1^2.$$

The matrix $B \in \mathbb{SL}_2(\mathbf{A})$ has an invertible coefficient so it is in $\mathbb{E}_2(\mathbf{A})$.

3b. First reason modulo $\langle x_2, \ldots, x_n\rangle$, then as in question *2b.*

3c. We can take $\mathbf{k} = \mathbb{Z}/2^e\mathbb{Z}$ with $e \geqslant 2$: -1 is not a square in $\mathbf{k}$. So -1 is not a square in $\mathbf{A}_n$ either since there are morphisms $\mathbf{A}_n \to \mathbf{k}$, for example the evaluation morphism at $x_0 = 1$, $x_i = 0$ for $i \geqslant 1$, $y_j = 0$ for $j \geqslant 2$.

Bibliographic comments

Regarding Theorem 6.1 and the characterization of finitely generated projective modules by their Fitting ideals see [Northcott] Theorem 18 p. 122 and Exercise 7 p. 49. Note however that the proof given by Northcott is not entirely constructive, since he requires an abstract patching principle of the finitely generated projective modules.

We have defined the determinant of an endomorphism of a finitely generated projective module as in [97, Goldman]. The difference resides in the fact that our proofs are constructive.

A study on the feasability of the local structure theorem for finitely generated projective modules can be found in [62, Díaz-Toca&Lombardi].

Proposition 9.3 regarding $\big(\mathrm{L}_{\mathbf{A}}(M,N)\big)_S$ is a crucial result that can be found for instance in [Northcott], Exercise 9 p. 50, and in [Kunz] (Chapter IV, Proposition 1.10). This result will be generalized in Proposition VIII-5.7.

Problem 1 is due to Suslin [185].

Chapter VI

Strictly finite algebras and Galois algebras

Contents

Introduction

The chapter is devoted to a natural generalization for commutative rings of the notion of a finite algebra over a field. In constructive mathematics, to obtain the conclusions for the field case, it is often necessary to not only assume that the algebra is a finitely generated vector space, but more precisely that the field is discrete and that we know a basis of the vector space. This is what brought us to introduce the notion of a strictly finite algebra over a discrete field.

The pertinent generalization of this notion to commutative rings is given by the algebras which are finitely generated projective modules over the base ring. So we call them strictly finite algebras.

Sections 1 and 2 which only concern algebras over discrete fields can be read directly after Section III-6. Similarly for Section 7 if we start from a discrete field (certain proofs are then simplified).

Section 3 is a brief introduction to finitely presented algebras, by insisting on the case of algebras which are integral over the base ring.

The rest of the chapter is devoted to the strictly finite algebras themselves.

In Sections 5 and 6, we introduce the neighboring notions of strictly étale algebra and of separable algebra, which generalize the notion of an étale algebra over a discrete field.

In Section 7 we give a constructive presentation of the bases of the Galois algebra theory for commutative rings. This is in fact an Artin-Galois theory, since it uses the approach developed by Artin for the field case by starting directly from a finite group of automorphisms of a field, the base field only appearing as a subproduct of the constructions that ensue.

1. Étale algebras over a discrete field

In Sections 1 and 2, **K** designates a nontrivial discrete field

Recall that a **K**-algebra **B** is said to be finite (resp. strictly finite) if it is finitely generated as a **K**-vector space (resp. if **B** is a finite dimensional **K**-vector space). If **B** is a finite **K**-algebra, this does not imply that we know how to determine a basis of **B** as a **K**-vector space, nor that **B** is discrete. If it is strictly finite, however, then we know of a finite basis of **B** as a **K**-vector space. In this case, for some $x \in \mathbf{B}$, the trace, the norm, the characteristic polynomial of (multiplication by) x, as well as the minimal polynomial of x over **K** can each be computed using standard methods of linear algebra over a discrete field. Similarly every finite **K**-subalgebra of **B** is strictly finite and the intersection of two strictly finite subalgebras is strictly finite.

1.1. Definition. Let **L** be a discrete field and **A** an **L**-algebra.

1. The algebra **A** is said to be *étale (over* **L***)* if it is strictly finite and if the discriminant $\mathrm{Disc}_{\mathbf{A}/\mathbf{L}}$ is invertible.
2. An element of **A** is said to be *separable algebraic (over* **L***)* if it annihilates a separable polynomial.
3. The algebra **A** is said to be *separable algebraic (over* **L***)* if every element of **A** is separable algebraic over **L**.

When f is a monic polynomial of $\mathbf{L}[X]$, the quotient algebra $\mathbf{L}[X]/\langle f\rangle$ is étale if and only if f is separable (Proposition III-5.10).

Structure theorem for étale algebras

Proposition III-5.10 gives the following lemma.

1.2. Lemma. *Let* $\mathbf{A}$ *be a strictly finite* $\mathbf{K}$*-algebra and* $a \in \mathbf{A}$*. If the characteristic polynomial* $\mathrm{C}_{\mathbf{A}/\mathbf{K}}(a)(T)$ *is separable, then the algebra is étale and* $\mathbf{A} = \mathbf{K}[a]$*.*

In Fact 1.3, items *1* and *2* give more precise statements for certain items of Lemma IV-8.5 and of Fact IV-8.8 (concerning general reduced zero-dimensional rings), in the case of a reduced strictly finite $\mathbf{K}$-algebra.

General results on integral extensions of zero-dimensional rings are given in Section 3 from page 321 onwards.

1.3. Fact. *Let* $\mathbf{B} \supseteq \mathbf{K}$ *be a strictly finite algebra.*

1. *The algebra* $\mathbf{B}$ *is zero-dimensional. If it is reduced then for every* $a \in \mathbf{B}$ *there exists a unique idempotent* $e \in \mathbf{K}[a]$ *such that* $\langle a \rangle = \langle e \rangle$*. Furthermore, when* $e = 1$*, i.e. when* a *is invertible,* $a^{-1} \in \mathbf{K}[a]$*.*
2. *The following properties are equivalent.*
   a. $\mathbf{B}$ *is a discrete field.*
   b. $\mathbf{B}$ *is without zerodivisors:* $xy = 0 \Rightarrow (x = 0 \text{ or } y = 0)$*.*
   c. $\mathbf{B}$ *is connected and reduced.*
   d. The minimal polynomial over $\mathbf{K}$ *of any arbitrary element of* $\mathbf{B}$ *is irreducible.*
3. *If* $\mathbf{K} \subseteq \mathbf{L} \subseteq \mathbf{B}$ *and* $\mathbf{L}$ *is a strictly finite discrete field over* $\mathbf{K}$*, then* $\mathbf{B}$ *is strictly finite over* $\mathbf{L}$*. In addition,* $\mathbf{B}$ *is étale over* $\mathbf{K}$ *if and only if it is étale over* $\mathbf{L}$ *and* $\mathbf{L}$ *is étale over* $\mathbf{K}$*.*
4. *If* $(e_1, \ldots, e_r)$ *is a fundamental system of orthogonal idempotents of* $\mathbf{B}$*,* $\mathbf{B}$ *is étale over* $\mathbf{K}$ *if and only if each of the components* $\mathbf{B}[1/e_i]$ *is étale over* $\mathbf{K}$*.*
5. *If* $\mathbf{B}$ *is étale, it is reduced.*
6. *If* $\mathrm{char}(\mathbf{K}) > [\,\mathbf{B} : \mathbf{K}\,]$ *and if* $\mathbf{B}$ *is reduced, it is étale.*

D *1.* The element a of $\mathbf{B}$ is annihilated by a monic polynomial of $\mathbf{K}[T]$ that we express in the form $uT^k\big(1 - T\,h(T)\big)$ with $u \in \mathbf{K}^\times$, $k \geqslant 0$. So $\mathbf{B}$ is zero-dimensional. If it is reduced, $a\big(1 - ah(a)\big) = 0$. Then, $e = ah(a)$ satisfies $a(1-e) = 0$ and a fortiori $e(1-e) = 0$. Which allows us to conclude.

2. The equivalence of a, b and c is a special case of Lemma III-6.3. The implication $d \Rightarrow c$ is clear. Let us take a look at $b \Rightarrow d$. Let x be in $\mathbf{B}$ and $f(X)$ be its minimal polynomial over $\mathbf{K}$. If $f = gh$, with g, h monic, then $g(x)h(x) = 0$, so $g(x) = 0$ or $h(x) = 0$. For example $g(x) = 0$, and since f is the minimal polynomial, f divides g, and $h = 1$.

3. Let $(f_1, \ldots, f_s)$ be a $\mathbf{K}$-basis of $\mathbf{L}$. We can compute an $\mathbf{L}$-basis of $\mathbf{B}$ as follows. The basis starts with $e_1 = 1$. Assume we have computed elements $e_1, \ldots, e_r$ of $\mathbf{B}$ linearly independent over $\mathbf{L}$. The $\mathbf{L}e_i$'s form a direct sum in $\mathbf{B}$ and we have a $\mathbf{K}$-basis $(e_if_1, \ldots, e_if_s)$ for each $\mathbf{L}e_i$. If $rs = [\,\mathbf{B} : \mathbf{K}\,]$, we have finished. In the opposite case, we can find $e_{r+1} \in \mathbf{B}$ which is not

in $F_r = \mathbf{L}e_1 \oplus \cdots \oplus \mathbf{L}e_r$.
Then, $\mathbf{L}e_{r+1} \cap F_r = \{0\}$ (otherwise, we would express e_{r+1} as an $\mathbf{L}$-linear combination of $(e_1, \dots, e_r)$), and we iterate the process by replacing $(e_1, \dots, e_r)$ with $(e_1, \dots, e_{r+1})$.
Once we have a basis of $\mathbf{B}$ as an $\mathbf{L}$-vector space, it remains to use the transitivity formula of the discriminants (Theorem II-5.36).

4. We use the structure Theorem II-4.3 (page 37) for fundamental systems of orthogonal idempotents and the formula for the discriminant of a direct product of algebras (Proposition II-5.34).

5. Let b be a nilpotent element of $\mathbf{B}$. For all $x \in \mathbf{B}$ multiplication by bx is a nilpotent endomorphism μ_{bx} of $\mathbf{B}$. We can then find a $\mathbf{K}$-basis of $\mathbf{B}$ in which the matrix of μ_{bx} is strictly triangular, so $\mathrm{Tr}(\mu_{bx}) = \mathrm{Tr}_{\mathbf{B}/\mathbf{K}}(bx) = 0$. Thus b is in the kernel of the $\mathbf{K}$-linear map

$$tr : \mathbf{B} \to \mathrm{L}_{\mathbf{K}}(\mathbf{B}, \mathbf{K}), \ \ b \mapsto (x \mapsto \mathrm{Tr}_{\mathbf{B}/\mathbf{K}}(bx).$$

Finally, tr is an isomorphism since $\mathrm{Disc}_{\mathbf{B}/\mathbf{K}}$ is invertible, so $b = 0$.

6. With the previous notation, assume $\mathbf{B}$ is reduced and we want to show that the $\mathbf{K}$-linear map tr is an isomorphism.
It suffices to show that $\mathrm{Ker}\, tr = 0$. Suppose $tr(b) = 0$, then $\mathrm{Tr}_{\mathbf{B}/\mathbf{K}}(bx) = 0$ for every x and in particular $\mathrm{Tr}_{\mathbf{B}/\mathbf{K}}(b^n) = 0$ for all $n > 0$. Therefore the endomorphism μ_b of multiplication by b satisfies $\mathrm{Tr}(\mu_b^n) = 0$ for every $n > 0$. The formulas that link the Newton sums to the elementary symmetric functions then show that the characteristic polynomial of μ_b is equal to $T^{[\mathbf{B}:\mathbf{K}]}$ (cf. Exercise III-14). The Cayley-Hamilton theorem and the fact that $\mathbf{B}$ is reduced allow us to conclude that $b = 0$. □

1.4. Theorem. (Structure theorem for étale $\mathbf{K}$-algebras, 1)
Let $\mathbf{B}$ be an étale $\mathbf{K}$-algebra.

1. *Every ideal $\langle b_1, \dots, b_r \rangle_{\mathbf{B}}$ is generated by an idempotent e which is a member of $\langle b_1, \dots, b_r \rangle_{\mathbf{K}[b_1,\dots,b_r]}$, and the quotient algebra is étale over $\mathbf{K}$.*
2. *Let $\mathbf{A}$ be a finitely generated $\mathbf{K}$-subalgebra of $\mathbf{B}$.*
   a. *$\mathbf{A}$ is an étale $\mathbf{K}$-algebra.*
   b. *There exist an integer $r \geqslant 1$ and a fundamental system of orthogonal idempotents $(e_1, \dots, e_r)$ of $\mathbf{A}$ such that, for each $i \in [\![1..r]\!]$, $\mathbf{B}[1/e_i]$ is a free module of finite rank over $\mathbf{A}[1/e_i]$. In other words, $\mathbf{B}$ is a quasi-free module over $\mathbf{A}$.*
3. *$\mathbf{B}$ is separable algebraic over $\mathbf{K}$.*
4. *For all $b \in \mathbf{B}$, $\mathrm{C}_{\mathbf{B}/\mathbf{K}}(b)$ is a product of separable polynomials.*

D *1.* If the ideal is principal this results from Fact 1.3 item *1.* Moreover, for two idempotents e_1, e_2, we have $\langle e_1, e_2 \rangle = \langle e_1 + e_2 - e_1e_2 \rangle$. Finally, the quotient algebra is itself étale over $\mathbf{K}$ by the formula for the discriminant of a direct product algebra.

2. It suffices to prove item *b*, because the result then follows using the transitivity formula for the discriminants for each $\mathbf{K} \subseteq \mathbf{A}[1/e_i] \subseteq \mathbf{B}[1/e_i]$ and the formula for the discriminant of a direct product algebra.
To prove item *b*, we try to compute a basis of $\mathbf{B}$ over $\mathbf{A}$ by using the indicated method in the case where $\mathbf{A}$ is a discrete field for which we know of a $\mathbf{K}$-basis, given in Fact 1.3 *3*. The algorithm is in danger of struggling when $e_{r+1}\mathbf{A} \cap F_r$ is not reduced to $\{0\}$. We then have an equality $\alpha_{r+1}e_{r+1} = \sum_{i=1}^{r} \alpha_i e_i$ with all the α_i's in $\mathbf{A}$, and $\alpha_{r+1} \neq 0$ but not invertible in $\mathbf{A}$. This implies (item *1*) that we find an idempotent $e \neq 0, 1$ in $\mathbf{K}[\alpha_{r+1}] \subseteq \mathbf{A}$. We then continue with the two localizations at e and $1 - e$. Finally, we notice that the number of splits operated thus is a priori bounded by $[\,\mathbf{B} : \mathbf{K}\,]$.

3 and *4*. Easily result from *2*. □

Remark. A generalization of item *1* of the previous theorem is found in Lemmas 3.13 and 3.14. ■

We can construct step by step étale $\mathbf{K}$-algebras in virtue of the following lemma, which extends Lemma 1.2.

1.5. Lemma. *Let* $\mathbf{A}$ *be an étale* $\mathbf{K}$*-algebra and* $f \in \mathbf{A}[T]$ *be a separable monic polynomial. Then,* $\mathbf{A}[T]/\langle f \rangle$ *is an étale* $\mathbf{K}$*-algebra.*

▷ First consider $\mathbf{A}[T]/\langle f \rangle$ as a free $\mathbf{A}$-algebra of rank $\deg f$. We have $\mathrm{Disc}_{\mathbf{B}/\mathbf{A}} = \mathrm{disc}(f)$ (Proposition III-5.10 item *3*). We conclude with the transitivity formula for the discriminants. □

The two theorems that follow are corollaries.

1.6. Theorem. *Let* $\mathbf{B}$ *be a* $\mathbf{K}$*-algebra. The elements of* $\mathbf{B}$ *which are separable algebraic over* $\mathbf{K}$ *form a subalgebra* $\mathbf{A}$*. In addition, every element of* $\mathbf{B}$ *that annihilates a separable monic polynomial of* $\mathbf{A}[T]$ *is in* $\mathbf{A}$*.*

▷ Let us first show that if x is separable algebraic over $\mathbf{K}$ and y annihilates a separable monic polynomial g of $\mathbf{K}[x][Y]$, then every element of $\mathbf{K}[x, y]$ is separable algebraic over $\mathbf{K}$. If $f \in \mathbf{K}[X]$ is separable and annihilates x, then the subalgebra $\mathbf{K}[x, y]$ is a quotient $\mathbf{K}[X, Y]/\langle f(X), g(X, Y)\rangle$. This $\mathbf{K}$-algebra is étale by Lemma 1.5.
Reasoning by induction, we can iterate the previous construction. We obtain the desired result by noting that an étale $\mathbf{K}$-algebra is separable algebraic over $\mathbf{K}$, and that every quotient of such an algebra is also separable algebraic over $\mathbf{K}$. □

Here is a "strictly finite" variant. We give the proof again because the variations, although simple, point out the precautions we must take in the strictly finite case.

1.7. Theorem. (Characterization of étale $\mathbf{K}$-algebras)
Let $\mathbf{B}$ be a strictly finite $\mathbf{K}$-algebra given in the form $\mathbf{K}[x_1, \ldots, x_n]$. The following properties are equivalent.

1. *$\mathbf{B}$ is étale over $\mathbf{K}$.*
2. *The minimal polynomial over $\mathbf{K}$ of each of the x_i's is separable.*
3. *$\mathbf{B}$ is separable algebraic over $\mathbf{K}$.*

In particular, a field $\mathbf{L}$ that is a Galois extension of $\mathbf{K}$ is étale over $\mathbf{K}$.

D *1 $\Rightarrow$ 3.* By Theorem 1.4.

2 $\Rightarrow$ 1. Let us first treat the case of a strictly finite $\mathbf{K}$-algebra $\mathbf{A}[x]$ where $\mathbf{A}$ is étale over $\mathbf{K}$ and where the minimal polynomial f of x over $\mathbf{K}$ is separable. We then have a surjective homomorphism of the strictly finite $\mathbf{K}$-algebra $\mathbf{A}[T]/\langle f \rangle$ over $\mathbf{A}[x]$ and the kernel of this homomorphism (which is computed as the kernel of a linear map between finite dimensional $\mathbf{K}$-vector spaces) is finitely generated, therefore generated by an idempotent e. The $\mathbf{K}$-algebra $\mathbf{C} = \mathbf{A}[T]/\langle f \rangle$ is étale by Lemma 1.5. We deduce that $\mathbf{A}[x] \simeq \mathbf{C}/\langle e \rangle$ is étale over $\mathbf{K}$.
We can then conclude by induction on n. □

1.8. Corollary. *Let $f \in \mathbf{K}[T]$ be a monic polynomial. The universal splitting algebra $\mathrm{Adu}_{\mathbf{K},f}$ is étale if and only if f is separable.*

Remark. We have already obtained this result by direct computation of the discriminant of the universal splitting algebra (Fact III-5.11). ■

1.9. Theorem. (Primitive element theorem)
Let $\mathbf{B}$ be an étale $\mathbf{K}$-algebra.

1. *If $\mathbf{K}$ is infinite or if $\mathbf{B}$ is a discrete field, $\mathbf{B}$ is a monogenic algebra, precisely of the form $\mathbf{K}[b] \simeq \mathbf{K}[T]/\langle f \rangle$ for some $b \in \mathbf{B}$ and some separable $f \in \mathbf{K}[T]$.*
   This applies in particular to a field $\mathbf{L}$ which is a Galois extension of $\mathbf{K}$, such that the extension $\mathbf{L}/\mathbf{K}$ stems from the elementary case studied in Theorem III-6.14.
2. *$\mathbf{B}$ is a finite product of monogenic étale $\mathbf{K}$-algebras.*

D *1.* It suffices to treat the case of an algebra with two generators $\mathbf{B} = \mathbf{K}[x, z]$. We will look for a generator of $\mathbf{B}$ of the form $\alpha x + \beta z$ with α, $\beta \in \mathbf{K}$. Let f and g be the minimal polynomials of x and z over $\mathbf{K}$. We know that they are separable. Let $\mathbf{C} = \mathbf{K}[X, Z]/\langle f(X), g(Z) \rangle = \mathbf{K}[\xi, \zeta]$. It suffices to find α, $\beta \in \mathbf{K}$ such that $\mathbf{C} = \mathbf{K}[\alpha\xi + \beta\zeta]$. To obtain this result, it suffices that the characteristic polynomial of $\alpha\xi + \beta\zeta$ be separable, as we can apply Lemma 1.2. We introduce two indeterminates a and b, and we denote by $h_{a,b}(T)$ the characteristic polynomial of the multiplication by $a\xi + b\zeta$ in $\mathbf{C}[a,b]$ seen as a free $\mathbf{K}[a,b]$-algebra of finite rank. Actually

$$\mathbf{C}[a,b] \simeq \mathbf{K}[a,b][X,Z]/\langle f(X), g(Z)\rangle\,.$$

Let $d(a,b) = \mathrm{disc}_T(h_{a,b})$. We make a computation in a "double universal splitting algebra" over $\mathbf{C}[a,b]$, in which we separately factorize f and g:

$$f(X) = \textstyle\prod_{i\in[\![1..n]\!]}(X - x_i) \;\text{ and }\; g(Z) = \prod_{i\in[\![1..k]\!]}(Z - z_j).$$

We obtain

$$\pm d(a,b) = \prod_{(i,j)\neq(k,\ell)} \big(a(x_i - x_k) + b\big(z_j - z_\ell\big)\big) = (a^{n^2-n}\mathrm{disc}\,f)^{p^2}(b^{p^2-p}\mathrm{disc}\,g)^n + \dots$$

In the right-most side of the equalities above we have indicated the term of highest degree when we order the monomials in a, b according to a lexicographic order. Thus the polynomial $d(a,b)$ has at least an invertible coefficient. It suffices to choose α, β such that $d(\alpha,\beta)\in\mathbf{K}^\times$ to obtain an element $\alpha\xi+\beta\zeta$ of $\mathbf{C}$ whose characteristic polynomial is separable. This completes the proof for the case where $\mathbf{K}$ is infinite.

In the case where $\mathbf{B}$ is a discrete field we enumerate the integers of $\mathbf{K}$ until we obtain α, β in $\mathbf{K}$ with $d(\alpha,\beta)\in\mathbf{K}^\times$, or until we conclude that the characteristic is equal to a prime number p. We then enumerate the powers of the coefficients of f and of g until we obtain enough elements in $\mathbf{K}$, or until we conclude that the field $\mathbf{K}_0$ generated by the coefficients of f and g is a finite field. In this case, $\mathbf{K}_0[x,z]$ is itself a finite field and it is generated by a generator γ of its multiplicative group, so $\mathbf{K}[x,z]=\mathbf{K}[\gamma]$.

2. We use the proof that has just been given for the case where $\mathbf{B}$ is a discrete field. If we do not reach the conclusion, it means that the proof stumbled at a specific place, which reveals that $\mathbf{B}$ is not a discrete field. Since we have a strictly finite $\mathbf{K}$-algebra, this provides us with an idempotent $e\neq 0,1$ in $\mathbf{B}$.[1] Thus $\mathbf{B}\simeq\mathbf{B}[1/e]\times\mathbf{B}[1/(1-e)]$. We can then conclude by induction on $[\,\mathbf{B}:\mathbf{K}\,]$. □

Étale algebras over a separably factorial field

When every separable polynomial over $\mathbf{K}$ can be decomposed into a product of irreducible factors, the field $\mathbf{K}$ is said to be *separably factorial.*

1.10. Lemma. *A field $\mathbf{K}$ is separably factorial if and only if we have a test for the existence of a zero in $\mathbf{K}$ for an arbitrary separable polynomial of $\mathbf{K}[T]$.*

D The second condition is a priori weaker since it amounts to determining the factors of degree 1 for a separable polynomial of $\mathbf{K}[T]$. Suppose this condition is satisfied. The proof is just about the same as for Lemma III-8.14,

[1] For more details see the solution of Exercise 2.

but asks for a few additional details.
Let $f(T) = T^n + \sum_{j=0}^{n-1} a_j T^j$. We fix an integer $k \in [\![2..n-2]\!]$ and we look for the polynomials $g = T^k + \sum_{j=0}^{k-1} b_j T^j$ that divide f. We will show that there is only a finite number of (explicit) possibilities for each of the b_j's. The proof of Kronecker's theorem uses universal polynomials $Q_{n,k,r}(a_0, \ldots, a_{n-1}, X) \in \mathbb{Z}[\underline{a}, X]$, monic in X, such that $Q_{n,k,r}(\underline{a}, b_r) = 0$. These polynomials can be computed in the universal splitting algebra $\mathbf{A} = \mathrm{Adu}_{\mathbf{K},f}$ as follows. Let

$$G(T) = \prod_{i=1}^{k}(T - x_i) = T^k + \sum_{j=0}^{k-1} g_j T^j.$$

We consider the orbit $(g_{r,1}, \ldots, g_{r,\ell})$ of g_r under the action of S_n, and we obtain

$$Q_{n,k,r}(\underline{a}, X) = \prod_{i=1}^{\ell}(X - g_{r,i}).$$

We deduce that

$$\prod_{\sigma \in \mathrm{S}_n} \big(X - \sigma(g_r)\big) = Q_{n,k,r}^{n!/\ell}.$$

Therefore, by Lemma III-5.12, $\mathrm{C}_{\mathbf{A}/\mathbf{k}}(g_r)(X) = Q_{n,k,r}^{n!/\ell}(X)$. Finally, as $\mathbf{A}$ is étale over $\mathbf{K}$ (Corollary 1.8), the characteristic polynomial of g_r is a product of separable polynomials of $\mathbf{K}[T]$ by Theorem 1.4 *4*.
Thus, b_r must be looked for among the zeros of a finite number of separable polynomials: there is a finite number of possibilities, all of which are explicit. □

1.11. Theorem. (Structure theorem for étale **K**-algebras, 2)
Suppose **K** *is separably factorial. A* **K**-*algebra* **B** *is étale if and only if it is isomorphic to a finite product of étale fields over* **K**.

D Consequence of the primitive element theorem (Theorem 1.9). □

1.12. Corollary. *If* **L** *is an étale field over* **K** *and if* **K** *is separably factorial, the same goes for* **L**.

D Let $f \in \mathbf{L}[T]$ be a separable monic polynomial. The **L**-algebra $\mathbf{B} = \mathbf{L}[T]/\langle f \rangle$ is étale, therefore it is also an étale **K**-algebra. We can therefore find a fundamental system of orthogonal idempotents $(e_1, \ldots, e_n)$ such that each $\mathbf{B}[\frac{1}{e_i}]$ is connected. This is equivalent to factoring f into a product of irreducible factors. □

1.13. Corollary. *The following properties are equivalent.*

1. *Every étale* **K**-*algebra is isomorphic to a product of étale fields over* **K**.
2. *The field* **K** *is separably factorial.*
3. *Every separable polynomial possesses a field of roots which is a strictly finite extension (thus Galoisian) of* **K**.
4. *Every separable polynomial possesses a field of roots which is étale over* **K**.

D For *2* ⇒ *4* we use the fact that the universal splitting algebra for a separable polynomial is étale (Corollary 1.8) and we apply Theorem 1.11.□

1.14. Corollary. *If* $\mathbf{K}$ *is separably factorial and if* $(\mathbf{K}_i)$ *is a finite family of étale fields over* $\mathbf{K}$*, there exists a Galois extension* $\mathbf{L}$ *of* $\mathbf{K}$ *which contains a copy of each of the* $\mathbf{K}_i$*.*

D Each $\mathbf{K}_i$ is isomorphic to a $\mathbf{K}[T]/\langle f_i\rangle$ with f_i separable irreducible. We consider the lcm f of the f_i's then a splitting field of f. □

Perfect fields, separable closure and algebraic closure

For a field $\mathbf{K}$ of finite characteristic p the map $x \mapsto x^p$ is an injective ring homomorphism.

In classical mathematics a field $\mathbf{K}$ is said to be *perfect* if it is of infinite characteristic, or if, being of finite characteristic p, the morphism $x \mapsto x^p$ is an isomorphism.

In constructive mathematics, to avoid the disjunction on the characteristic in the "or" above (which cannot be made explicit), we formulate it as follows: *if* p *is a prime number such that* $p.1_{\mathbf{K}} = 0_{\mathbf{K}}$*, then the homomorphism* $\mathbf{K} \to \mathbf{K}$, $x \mapsto x^p$ *is surjective.*

The field of rationals $\mathbb{Q}$ and the finite fields (including the trivial field) are perfect.

Let $\mathbf{K}$ be a field of finite characteristic p. An overfield $\mathbf{L} \supseteq \mathbf{K}$ is called a *perfect closure* of $\mathbf{K}$ if it is a perfect field and if every element of $\mathbf{L}$, raised to a certain power p^k, is an element of $\mathbf{K}$.

1.15. Lemma. *A discrete field* $\mathbf{K}$ *of finite characteristic* p *has a perfect closure* $\mathbf{L}$*, unique up to unique isomorphism.*
Furthermore, $\mathbf{K}$ *is a detachable subset of* $\mathbf{L}$ *if and only if there exists a test for "*$\exists x \in \mathbf{K},\ y = x^p$*?" (with extraction of the* p*-th root of* y *when it exists).*

Proof idea. An element of $\mathbf{L}$ is encoded by a pair (x, k), where $k \in \mathbb{N}$ and $x \in \mathbf{K}$. This encoding represents the p^k-th root of x.
The equality in $\mathbf{L}$, $(x, k) =_{\mathbf{L}} (y, \ell)$, is defined by $x^{p^\ell} = y^{p^k}$ (in $\mathbf{K}$), such that $(x^p, k+1) =_{\mathbf{L}} (x, k)$. □

1.16. Lemma. (Algorithm for squarefree factorization)
If $\mathbf{K}$ *is a perfect discrete field, we have at our disposal an algorithm for* squarefree factorization *of the lists of polynomials of* $\mathbf{K}[X]$ *in the following sense. A squarefree factorization of a family* $(g_1, \ldots, g_r)$ *is given by*

- *a family* $(f_1, \ldots, f_s)$ *of pairwise comaximal separable polynomials,*
- *the expression of each* g_i *in the form*

$$g_i = \prod\nolimits_{k=1}^{s} f_k^{m_{k,i}} \ (m_{k,i} \in \mathbb{N}).$$

Proof idea. We start by computing a partial factorization basis for the family $(g_i)_{i\in[\![1..r]\!]}$ (see Lemma III-1.1). If some of the polynomials in the basis are of the form $h(X^p)$, we know how to express them as $g(X)^p$, and then we replace h by g. We iterate this procedure until all the polynomials of the family have a nonzero derivative. Then we introduce the derivatives of the polynomials of the family. For this new family we compute a new partial factorization basis.

We iterate the entire procedure until the original goal is reached. The details are left to the reader. □

A discrete field $\mathbf{K}$ is said to be *separably closed* if every separable monic polynomial of $\mathbf{K}[X]$ can be decomposed into a product of factors $X - x_i$ $(x_i \in \mathbf{K})$.

Let $\mathbf{K} \subseteq \mathbf{L}$ be discrete fields. We say that $\mathbf{L}$ *is a separable closure of* $\mathbf{K}$ if $\mathbf{L}$ is separably closed and separable algebraic over $\mathbf{K}$.

1.17. Lemma.

1. *A discrete field is algebraically closed if and only if it is perfect and separably closed.*
2. *If a discrete field* $\mathbf{K}$ *is perfect, every étale field over* $\mathbf{K}$ *is perfect.*
3. *If a perfect discrete field has a separable closure, it is also an algebraic closure.*

D *1.* Results from Lemma 1.16 and *3* results from *1* and *2.*

2. We consider $\mathbf{L}$ étale over $\mathbf{K}$. Let $\sigma : \mathbf{L} \to \mathbf{L} : z \mapsto z^p$.

We know that $\mathbf{L} = \mathbf{K}[x] \simeq \mathbf{K}[X]/\langle f\rangle$ where f is the minimal polynomial of x over $\mathbf{K}$. The element $y = x^p$ is a zero of the polynomial f^σ, which is separable and irreducible over $\mathbf{K}$ because σ is an automorphism of $\mathbf{K}$. We therefore obtain an isomorphism $\mathbf{K}[X]/\langle f^\sigma\rangle \to \mathbf{K}[y] \subseteq \mathbf{L}$. Thus $\mathbf{K}[y]$ and $\mathbf{L}$ are $\mathbf{K}$-vector spaces of same dimension, so $\mathbf{K}[y] = \mathbf{L}$ and σ is surjective. □

1.18. Theorem. *Let* $\mathbf{K}$ *be a separably factorial and countable discrete field.*

1. $\mathbf{K}$ *has a separable closure* $\mathbf{L}$*, and every separable closure of* $\mathbf{K}$ *is* $\mathbf{K}$*-isomorphic to* $\mathbf{L}$*.*
2. *This applies to* $\mathbf{K} = \mathbb{Q}$*,* $\mathbb{Q}(X_1,\dots,X_n)$*,* $\mathbb{F}_p$ *or* $\mathbb{F}_p(X_1,\dots,X_n)$*.*
3. *In addition if* $\mathbf{K}$ *is perfect, then* $\mathbf{L}$ *is an algebraic closure of* $\mathbf{K}$ *and every algebraic closure of* $\mathbf{K}$ *is* $\mathbf{K}$*-isomorphic to* $\mathbf{L}$*.*

D We only give a sketch of the proof of item *1.*

Recall first of all item *2* of Theorem III-6.7: if a splitting field for $f \in \mathbf{K}[X]$ exists and is strictly finite over $\mathbf{K}$, then every other splitting field for f over $\mathbf{K}$ is isomorphic to the first.

Suppose for a moment that we know how to construct a strictly finite

splitting field for every separable polynomial over $\mathbf{K}$. We enumerate all the separable monic polynomials of $\mathbf{K}[X]$ in an infinite sequence $(p_n)_{n\in\mathbb{N}}$. We call f_n the lcm of the polynomials $p_0, \ldots, p_n$. We construct successive splitting fields $\mathbf{K}_0, \ldots, \mathbf{K}_i, \ldots$ for these f_i's.
Because of the previously mentioned result, we know how to construct injective homomorphisms of $\mathbf{K}$-algebras,

$$\mathbf{K}_0 \xrightarrow{\jmath_1} \mathbf{K}_1 \xrightarrow{\jmath_2} \cdots\cdots \xrightarrow{\jmath_n} \mathbf{K}_n \xrightarrow{\jmath_{n+1}} \cdots$$

The separable closure of $\mathbf{K}$ is then the colimit of the system constructed thus. It remains to see why we know how to construct a strictly finite splitting field for every separable polynomial f over $\mathbf{K}$. If the field is infinite, the fact is given by Theorem III-6.15. In the case of a finite field, the study of finite fields directly shows how to construct a splitting field. In the most general case, we can construct a splitting field anyway by brute force, by adding the roots one after the other; we consider an irreducible factor h of f and the field $\mathbf{K}[\xi_1] = \mathbf{K}[X]/\langle h\rangle$. Over the new field $\mathbf{K}[\xi_1]$, we consider an irreducible factor $h_1(X)$ of $f_1(X) = \frac{f(X)}{X-\xi_1}$ which allows us to construct $\mathbf{K}[\xi_1, \xi_2]$ etc ...
This procedure is possible in virtue of Corollary 1.12 because the successive fields $\mathbf{K}[\xi_1]$, $\mathbf{K}[\xi_1, \xi_2]$ ... remain separably factorial. □

Remark. There exist several ways to construct an algebraic closure of $\mathbb{Q}$. The one proposed in the previous theorem depends on the chosen enumeration of the separable monic polynomials of $\mathbb{Q}[X]$ and it lacks geometric pertinence. From this point of view, the colimit that we construct is actually of significantly less interest than the special splitting fields that we can construct each time we need to. There exist other constructions, of a *geometric* nature, of algebraic closures of $\mathbb{Q}$ which are interesting however as global objects. The most renowned is the one based on the algebraic real number field to which we add an element $i = \sqrt{-1}$. For each prime number p, another very pertinent algebraic closure of $\mathbb{Q}$ is obtained via the intermediate field formed by the p-adic algebraic numbers. ■

2. Basic Galois theory (2)

This section complements Section III-6 (see also Theorems 1.7 and 1.9).

Some remainders. A Galois extension of $\mathbf{K}$ is defined as a strictly finite field over $\mathbf{K}$ which is a splitting field for a separable polynomial of $\mathbf{K}[T]$. Theorem 1.9 implies that a Galois extension always stems from the elementary case studied in Theorem III-6.14. Finally, Theorem III-6.7 says that such a splitting field is unique up to isomorphism. ■

2.1. Definition. An overfield $\mathbf{L}$ of $\mathbf{K}$ is said to be *normal* (over $\mathbf{K}$) if every $x \in \mathbf{L}$ annihilates a monic polynomial of $\mathbf{K}[T]$ which can be decomposed into a product of linear factors in $\mathbf{L}[T]$.

Remark. Note that if $\mathbf{L}$ is a strictly finite extension of $\mathbf{K}$ or more generally if $\mathbf{L}$ has a discrete basis as a $\mathbf{K}$-vector space, then the minimal polynomial of an arbitrary element of $\mathbf{K}$ exists. If the condition of the above definition is satisfied, the minimal polynomial itself can be decomposed into linear factors in $\mathbf{L}[T]$. ■

2.2. Fact. *Let $f(T) \in \mathbf{K}[T]$ be a monic polynomial and $\mathbf{L} \supseteq \mathbf{K}$ be a field of roots for f. Then, $\mathbf{L}$ is a normal extension of $\mathbf{K}$.*

D We have $\mathbf{L} = \mathbf{K}[x_1, \ldots, x_n]$ where $f(T) = \prod_{i=1}^{n}(T - x_i)$.
Let $y = h(x_1, \ldots, x_n)$ be an arbitrary element of $\mathbf{L}$. Let

$$g(X_1, \ldots, X_n, T) = \prod\nolimits_{\sigma \in \mathrm{S}_n} \big(T - h^{\sigma}(\underline{X})\big).$$

We clearly have $g(\underline{x}, y) = 0$. Moreover, $g(\underline{x}, T) \in \mathbf{K}[T]$, because each of the coefficients of $g(\underline{X})(T)$ in $\mathbf{K}[\underline{X}]$ is a symmetric polynomial in the X_i's, hence a polynomial in the elementary symmetric functions, which are specialized in elements of $\mathbf{K}$ (the coefficients of f) by the $\mathbf{K}$-homomorphism $\underline{X} \mapsto \underline{x}$.□

2.3. Theorem. (Characterization of Galois extensions)
Let $\mathbf{L}$ be a strictly finite field over $\mathbf{K}$. The following properties are equivalent.

1. *$\mathbf{L}$ is a Galois extension of $\mathbf{K}$.*
2. *$\mathbf{L}$ is étale and normal over $\mathbf{K}$.*
3. *$\mathrm{Aut}_{\mathbf{K}}(\mathbf{L})$ is finite and the Galois correspondence is bijective.*
4. *There exists a finite group $G \subseteq \mathrm{Aut}_{\mathbf{K}}(\mathbf{L})$ whose fixed field is $\mathbf{K}$.*

In this case, in item 4, we necessarily have $G = \mathrm{Gal}(\mathbf{L}/\mathbf{K})$.

D *1* $\Rightarrow$ *2.* This is Fact 2.2.
2 $\Rightarrow$ *1* and *3.* By the primitive element theorem, $\mathbf{L} = \mathbf{K}[y]$ for some y in $\mathbf{L}$. The minimal polynomial f of y over $\mathbf{K}$ is separable, and f can be completely factorized in $\mathbf{L}[T]$ because $\mathbf{L}$ is normal over $\mathbf{K}$. So $\mathbf{L}$ is a splitting field for f. Moreover, Theorem III-6.14 applies.
4 $\Rightarrow$ *2.* It suffices to show that every $x \in \mathbf{L}$ annihilates a separable polynomial of $\mathbf{K}[T]$ which can be completely factorized in $\mathbf{L}[T]$, because then the extension is normal (by definition) and étale (Theorem 1.7). Let

$$P(T) = \mathrm{Rv}_{G/H,x}(T) = \prod\nolimits_{\sigma \in G/H} \big(T - \sigma(x)\big) \quad \text{where} \quad H = \mathrm{St}(x).$$

The subscript $\sigma \in G/H$ means that we take a σ in each left coset of H in G. Hence any two left cosets have the same cardinality. The polynomial P is fixed by G, so $P \in \mathbf{K}[T]$. Moreover, $\mathrm{disc}(P) = \prod_{i,j \in \llbracket 1..k \rrbracket, i<j}(x_i - x_j)^2$ is invertible.
Finally, since the Galois correspondence is bijective, and since the fixed field of G is $\mathbf{K}$, in item *4*, we necessarily have $G = \mathrm{Gal}(\mathbf{L}/\mathbf{K})$. □

2.4. Theorem. (Galois correspondence, complement)
Let $\mathbf{L}/\mathbf{K}$ be a Galois extension with Galois group $G = \mathrm{Gal}(\mathbf{L}/\mathbf{K})$. Let H be a detachable subgroup of G, σ be an element of G, $H_\sigma = \sigma H \sigma^{-1}$.

1. *The field $\sigma(\mathbf{L}^H)$ is equal to $\mathbf{L}^{H_\sigma}$.*
2. *$\mathbf{L}^H$ is a Galois extension of $\mathbf{K}$ if and only if H is normal in G. In this case the Galois group $\mathrm{Gal}(\mathbf{L}^H/\mathbf{K})$ is canonically isomorphic to G/H.*

D *1.* Immediate computation.

2. Let $\mathbf{M} = \mathbf{L}^H$. By the primitive element theorem write $\mathbf{M} = \mathbf{K}[y]$, such that $H = \mathrm{St}(y)$. The field $\mathbf{M}$ is normal over $\mathbf{K}$ if and only if for each $\tau \in G$, we have $\tau(y) \in \mathbf{M}$, i.e. $\tau(\mathbf{M}) = \mathbf{M}$. By item *1* this means that $\tau H \tau^{-1} = H$. □

Now we add some details to Theorem III-6.14.

2.5. Theorem. (Galois correspondence, synthesis)
Let $\mathbf{L}/\mathbf{K}$ be a Galois extension. The Galois correspondence works as follows.

1. *For all $\mathbf{M} \in \mathcal{K}_{\mathbf{L}/\mathbf{K}}$, $\mathbf{L}/\mathbf{M}$ is a Galois extension with Galois group $\mathrm{Fix}(\mathbf{M})$ and $[\,\mathbf{L} : \mathbf{M}\,] = \#\mathrm{Fix}(\mathbf{M})$.*
2. *If $H_1, H_2 \in \mathcal{G}_{\mathbf{L}/\mathbf{K}}$ and $\mathbf{M}_i = \mathrm{Fix}(H_i) \in \mathcal{K}_{\mathbf{L}/\mathbf{K}}$, then*
   - *$H_1 \cap H_2$ corresponds to the $\mathbf{K}$-subalgebra generated by $\mathbf{M}_1$ and $\mathbf{M}_2$,*
   - *$\mathbf{M}_1 \cap \mathbf{M}_2$ corresponds to the subgroup generated by H_1 and H_2.*
3. *If $H_1 \subseteq H_2$, then*
   - *$\mathbf{M}_1 \supseteq \mathbf{M}_2$ and $(H_2 : H_1) = [\,\mathbf{M}_1 : \mathbf{M}_2\,]$,*
   - *$\mathbf{M}_1/\mathbf{M}_2$ is a Galois extension if and only if H_1 is normal in H_2. In this case the group $\mathrm{Gal}(\mathbf{M}_1/\mathbf{M}_2)$ is naturally isomorphic to H_2/H_1.*

3. Finitely presented algebras

Generalities

Finitely presented algebras are to systems of polynomial equations (or *polynomial systems*) what finitely presented modules are to systems of linear equations.

Here we introduce a few basic general facts regarding these algebras.

The algebras that we consider in this section are associative, commutative and unitary.

3.1. Definition. Let $\mathbf{A}$ be a $\mathbf{k}$-algebra.

1. The algebra $\mathbf{A}$ is said to be *finitely generated* if it is generated by a finite family as a $\mathbf{k}$-algebra. This boils down to saying that it is isomorphic to a quotient algebra $\mathbf{k}[X_1, \dots, X_n]/\mathfrak{a}$. We then denote it by $\mathbf{A} = \mathbf{k}[x_1, \dots, x_n]$, where x_i is the image of X_i in $\mathbf{A}$. This notation does not imply that $\mathbf{A}$ is an extension of $\mathbf{k}$.
2. The algebra $\mathbf{A}$ is said to be *finitely presented* if it is finitely presented as a $\mathbf{k}$-algebra. This boils down to saying that it is isomorphic to an algebra $\mathbf{k}[X_1, \dots, X_n]/\mathfrak{a}$, with a finitely generated ideal $\mathfrak{a} = \langle f_1, \dots, f_s\rangle$.
3. The algebra $\mathbf{A}$ is said to be *finitely presented reduced*[2] if it is finitely presented as a reduced $\mathbf{k}$-algebra. In other words if it is isomorphic to a quotient algebra $\mathbf{k}[X_1, \dots, X_n]/\sqrt{\mathfrak{a}}$ with a finitely generated ideal $\mathfrak{a}$.
4. The algebra $\mathbf{A}$ is said to be *strictly finite* if $\mathbf{A}$ is a finitely generated projective $\mathbf{k}$-module. We also say that $\mathbf{A}$ *is strictly finite over* $\mathbf{k}$. In the case of an extension, we speak of a *strictly finite extension* of $\mathbf{k}$.
5. If $\mathbf{A}$ is strictly finite we denote by
$$\mathrm{Tr}_{\mathbf{A}/\mathbf{k}}(x),\ \ \mathrm{N}_{\mathbf{A}/\mathbf{k}}(x),\ \ \mathrm{F}_{\mathbf{A}/\mathbf{k}}(x)(T)\ \text{ and }\ \mathrm{C}_{\mathbf{A}/\mathbf{k}}(x)(T),$$
the trace, the determinant, the fundamental polynomial and the characteristic polynomial of the $\mathbf{k}$-linear map $\mu_{\mathbf{A},x} \in \mathrm{End}_{\mathbf{k}}(\mathbf{A})$. Moreover, by letting $g(T) = \mathrm{C}_{\mathbf{A}/\mathbf{k}}(x)(T)$, the element $g'(x)$ is called *the different of* x.

Note that in the case where $\mathbf{k}$ is a discrete field, we indeed find the notion of a strictly finite algebra given in Definition III-6.2.

3.2. Fact. (Universal property of a finitely presented algebra)
The finitely presented algebra $\mathbf{k}[X_1, \dots, X_n]/\langle f_1, \dots, f_s\rangle = \mathbf{k}[x_1, \dots, x_n]$ *is characterized by the following property: if a* $\mathbf{k}$*-algebra* $\mathbf{k} \xrightarrow{\varphi} \mathbf{A}$ *contains elements* $y_1, \dots, y_n$ *such that the* $f_i^{\varphi}(y_1, \dots, y_n)$*'s are null, there exists a unique homomorphism of* $\mathbf{k}$*-algebras* $\mathbf{k}[x_1, \dots, x_n] \to \mathbf{A}$ *which sends the* x_i*'s to the* y_i*'s.*

Changing the generator set

3.3. Fact. *When we change the generator set for a finitely presented algebra* $\mathbf{A}$ *the ideal of relations between the new generators is again finitely generated.*

Refer to Section IV-1 to verify that what has been explained slightly informally on page 180 works well in the current case.

[2] "finitely presented reduced" expresses a single, well-defined property. Thus it is to be used and considered as a whole (like a single word) and not to be mistakenly subdivided between "finitely presented" and "reduced."

Transitivity (finitely presented algebras)

3.4. Fact. *If* $\mathbf{k} \xrightarrow{\lambda} \mathbf{A}$ *and* $\mathbf{A} \xrightarrow{\rho} \mathbf{C}$ *are two finitely presented algebras, then* $\mathbf{C}$ *is a finitely presented* $\mathbf{k}$*-algebra.*

D Let $\mathbf{A} = \mathbf{k}[\underline{y}] \simeq \mathbf{k}[\underline{Y}]/\langle g_1, \ldots, g_t\rangle$ and $\mathbf{C} = \mathbf{A}[\underline{x}] \simeq \mathbf{A}[\underline{X}]/\langle f_1, \ldots, f_s\rangle$. Let $F_1, \ldots, F_s \in \mathbf{k}[\underline{Y}, \underline{X}]$ be polynomials such that $F_i(\underline{y}, \underline{X}) = f_i(\underline{X})$.
Then, $\mathbf{C} = \mathbf{k}[\rho(\underline{y}), \underline{x}] \simeq \mathbf{k}[\underline{Y}, \underline{X}]/\langle g_1, \ldots, g_t, F_1, \ldots, F_s\rangle$. □

Subalgebras

3.5. Fact. *Let* $\mathbf{A} \subseteq \mathbf{C}$ *be two finitely generated* $\mathbf{k}$*-algebras. If* $\mathbf{C}$ *is a finitely presented* $\mathbf{k}$*-algebra it is also a finitely presented* $\mathbf{A}$*-algebra (with "the same" presentation, read in* $\mathbf{A}$*).*

D Let without loss of generality $\mathbf{C} = \mathbf{k}[x_1, \ldots, x_n] \simeq \mathbf{k}[\underline{X}]/\langle \underline{f}\rangle$ and $\mathbf{A} = \mathbf{k}[x_1, \ldots, x_r]$. We have $\mathbf{A} \simeq \mathbf{k}[X_1, \ldots, X_r]/\mathfrak{f}$ with

$$\mathfrak{f} = \langle f_1, \ldots, f_s\rangle \cap \mathbf{k}[X_1, \ldots, X_r].$$

Let us denote by $\pi : \mathbf{k}[X_1, \ldots, X_r] \to \mathbf{A}$ the passage to the quotient and for $h \in \mathbf{k}[X_1, \ldots, X_n]$, denote by $h^\pi \in \mathbf{A}[X_{r+1}, \ldots, X_n]$ its image. So

$$h^\pi = h(x_1, \ldots, x_r, X_{r+1}, \ldots, X_n).$$

Consider the homomorphism

$$\gamma : \begin{array}{l} \mathbf{A}[X_{r+1}, \ldots, X_n]/\langle f_1^\pi, \ldots, f_s^\pi\rangle \simeq \\ \mathbf{A}[X_1, \ldots, X_n]/\langle X_1 - x_1, \ldots, X_r - x_r, f_1^\pi, \ldots, f_s^\pi\rangle \end{array} \to \mathbf{C}.$$

This is the homomorphism which fixes $\mathbf{A}$ and sends X_k to x_k for $k \in [\![r+1..n]\!]$. It suffices to show that γ is injective. Every element g of $\mathbf{A}[X_{r+1}, \ldots, X_n]$ can be written in the form $g = G^\pi$ with $G \in \mathbf{k}[X_1, \ldots, X_n]$. Suppose that g modulo $\langle f_1^\pi, \ldots, f_s^\pi\rangle$ is in $\operatorname{Ker}\gamma$. We then have

$$g(x_{r+1}, \ldots, x_n) = G(x_1, \ldots, x_n) = 0.$$

Therefore $G \in \langle f_1, \ldots, f_s\rangle$, which gives us $g \in \langle f_1^\pi, \ldots, f_s^\pi\rangle$ (after transformation by π). As required. □

Remark. The condition $\mathbf{A} \subseteq \mathbf{C}$ is essential for the proof to work properly. Moreover, if must be noted that the ideal $\mathfrak{f}$ is not necessarily finitely generated. ■

The zeros of a polynomial system

Consider a polynomial system $(\underline{f}) = (f_1, \ldots, f_s)$ in $\mathbf{k}[X_1, \ldots, X_n]$, and a $\mathbf{k}$-algebra $\rho : \mathbf{k} \to \mathbf{B}$.

3.6. Definition. A *zero of the system* $(\underline{f})$ *over* $\mathbf{B}$ is an n-tuple

$$(\underline{\xi}) = (\xi_1, \ldots, \xi_n) \in \mathbf{B}^n$$

satisfying $f_i^\rho(\underline{\xi}) = 0$ for each i. The set of zeros of $(\underline{f})$ over $\mathbf{B}$ is often symbolically called the *variety of the zeros* over $\mathbf{B}$ of the polynomial system, and thus, we denote it by $\mathcal{Z}_{\mathbf{k}}(\underline{f}, \mathbf{B})$ or $\mathcal{Z}(\underline{f}, \mathbf{B})$.

Some zeros are more interesting than others: the closer the algebra $\mathbf{B}$ is to $\mathbf{k}$, the more interesting is the zero. We pay particular attention to the zeros over $\mathbf{k}$, or by default over finite $\mathbf{k}$-algebras.

Two zeros are a priori particularly disappointing. The one provided by the trivial algebra, and the zero $(x_1, \ldots, x_n)$ over the *quotient algebra* associated with the polynomial system, i.e.

$$\boxed{\mathbf{A} = \mathbf{k}[x_1, \ldots, x_n] = \mathbf{k}[X_1, \ldots, X_n]/\langle f_1, \ldots, f_s\rangle\,.}$$

Nevertheless this last algebra plays a central role for our problem because of two findings. The first is the following.

3.7. Fact. *For every* $\mathbf{k}$*-algebra* $\mathbf{B}$ *the set of zeros of* $(\underline{f})$ *over* $\mathbf{B}$ *is naturally identified with the set of homomorphisms of* $\mathbf{k}$*-algebras from* $\mathbf{A}$ *to* $\mathbf{B}$*. In particular, the zeros over* $\mathbf{k}$ *are identified with the characters of the algebra* $\mathbf{A}$*.*

Proof on an example. Let $\mathbb{Q}[x, y] = \mathbb{Q}[X, Y]/\big\langle X^2 + Y^2 - 1\big\rangle$. Taking a real point (α, β) of the circle $X^2 + Y^2 = 1$ amounts to the same thing as taking a morphism $\rho : \mathbb{Q}[x, y] \longrightarrow \mathbb{R}$ (the one which sends x and y to α and β).□

We therefore have a crucial identification, which we write as an equality

$$\boxed{\operatorname{Hom}_{\mathbf{k}}(\mathbf{A}, \mathbf{B}) = \mathcal{Z}_{\mathbf{k}}(\underline{f}, \mathbf{B}) \subseteq \mathbf{B}^n.}$$

In short the quotient algebra $\mathbf{A}$ *intrinsically* summarizes the pertinent information contained in the polynomial system $(\underline{f})$. Which is also why we say that $\mathcal{Z}_{\mathbf{k}}(\underline{f}, \mathbf{B})$ is the *variety of the zeros* of $\mathbf{A}$ over $\mathbf{B}$.

The second finding (closely related to the previous one by the way) is the following.

From a geometric point of view *two polynomial systems* $(\underline{f})$ *and* $(\underline{g})$ *in* $\mathbf{k}[\underline{X}]$ *which have the same zeros*, over any arbitrary $\mathbf{k}$-algebra, must be considered as *equivalent.* If that is the case, let $\mathbf{A}_1 = \mathbf{k}[\underline{x}]$ and $\mathbf{A}_2 = \mathbf{k}[\underline{y}]$ be the two quotient algebras (we do not give the same name to the classes of X_i's in the two quotients). Consider the canonical zero $(x_1, \ldots, x_n)$ of $(\underline{f})$ in $\mathbf{A}_1$. Since $\mathcal{Z}(\underline{f}, \mathbf{A}_1) = \mathcal{Z}(\underline{g}, \mathbf{A}_1)$, we must have $g_j(\underline{x}) = 0$ for each j. This means that $g_j(\underline{X})$ is null modulo $\big\langle \underline{f}\big\rangle$. Similarly, each f_i must be in $\big\langle \underline{g}\big\rangle$.

Let us summarize this second finding.

3.8. Fact. *Two polynomial systems* $(\underline{f})$ *and* $(\underline{g})$ *in* $\mathbf{k}[\underline{X}]$ *admit the same zeros, over any* $\mathbf{k}$*-algebra, if and only if they define the same quotient algebra.*

Example. The circles $x^2 + y^2 - 3 = 0$ and $x^2 + y^2 - 7 = 0$ cannot be distinguished by their rational points – they do not have any (since over $\mathbb{Z}$, the congruence $a^2 + b^2 \equiv 3c^2 \bmod 4$ leads to a, b, c being even), but the quotient $\mathbb{Q}$-algebras are non-isomorphic, and we can observe over $\mathbb{Q}[\sqrt{3}, \sqrt{7}]$ that they have distinct zeros "somewhere." ■

When $\mathbf{k}$ is reduced and if we focus on the zeros over the reduced $\mathbf{k}$-algebras, the algebra $\mathbf{A} = \mathbf{k}[\underline{X}]/\langle \underline{f} \rangle$ must be replaced by its reduced variant, which is a finitely presented reduced algebra

$$\mathbf{A}/\mathrm{D}_{\mathbf{A}}(0) = \mathbf{k}[X_1, \ldots, X_n]/\sqrt{\langle f_1, \ldots, f_s \rangle}\,.$$

We continue this discussion on page 558 in the subsection entitled "Nullstellensatz and equivalence of two categories."

A digression on algebraic computation

Besides their direct link to the solution of polynomial systems another reason for the importance of finitely presented algebras is the following. Each time that an algebraic computation reaches an "interesting result" in a $\mathbf{k}$-algebra $\mathbf{B}$, this computation has only involved a finite number of elements y_1, …, y_n of $\mathbf{B}$ and a finite number of relations between the y_i's, such that there exist a finitely presented $\mathbf{k}$-algebra $\mathbf{C} = \mathbf{k}[x_1, \ldots, x_n]$ and a surjective morphism $\theta : \mathbf{C} \to \mathbf{k}[y_1, \ldots, y_n] \subseteq \mathbf{B}$ which sends the x_i's to the y_i's and such that the "interesting result" has already occurred in $\mathbf{C}$ for the x_i's. In a more scholarly language: every $\mathbf{k}$-algebra is a filtering colimit of finitely presented $\mathbf{k}$-algebras.[3]

The tensor product of two k-algebras

The *direct sum* of two $\mathbf{k}$-algebras $\mathbf{A}$ and $\mathbf{B}$ in the category of $\mathbf{k}$-algebras is given by the solution of the following universal problem ("morphism" here means "homomorphism of $\mathbf{k}$-algebras").

Find a $\mathbf{k}$*-algebra* $\mathbf{C}$ *and two morphisms* $\alpha : \mathbf{A} \to \mathbf{C}$ *and* $\lambda : \mathbf{B} \to \mathbf{C}$ *such that, for every* $\mathbf{k}$*-algebra* $\mathbf{D}$ *and for every pair of morphisms* $\varphi : \mathbf{A} \to \mathbf{D}$ *and* $\psi : \mathbf{B} \to \mathbf{D}$*, there exists a unique morphism* $\gamma : \mathbf{C} \to \mathbf{D}$ *such that* $\varphi = \gamma \circ \alpha$ *and* $\psi = \gamma \circ \lambda$*.*

[3] The reader will notice that this subsection is directly copied from the analogous subsection for finitely presented modules, page 182.

$$\begin{tikzcd}
 & \mathbf{A} \arrow[dr, "\alpha"] \arrow[drr, "\varphi"] & & \\
\mathbf{k} \arrow[ur, "\beta"] \arrow[dr, "\rho"'] & & \mathbf{C} \arrow[r, dashed, "\gamma!"] & \mathbf{D} \\
 & \mathbf{B} \arrow[ur, "\lambda"] \arrow[urr, "\psi"'] & &
\end{tikzcd}$$

Note that in the category of commutative rings, the above universal property means that $\mathbf{C}$, with the two morphisms α and λ, is the *amalgamated sum* or the *push out* of the two arrows $\beta : \mathbf{k} \to \mathbf{A}$ and $\rho : \mathbf{k} \to \mathbf{B}$. In French, however, the term *carré cocartésien* is used, formed with the four arrows β, ρ, α and λ reflecting the above sketch.[4]

3.9. Theorem. *Consider two* $\mathbf{k}$*-algebras* $\mathbf{k} \xrightarrow{\rho} \mathbf{B}$ *and* $\mathbf{k} \xrightarrow{\beta} \mathbf{A}$*.*

A. (Direct sum in the category of $\mathbf{k}$-algebras)
The algebras $\mathbf{A}$ *and* $\mathbf{B}$ *admit a direct sum* $\mathbf{C}$ *in the category of* $\mathbf{k}$*-algebras. Here are different possible descriptions:*

1. *If* $\mathbf{A} = \mathbf{k}[X_1, \ldots, X_n]/\langle f_1, \ldots, f_s\rangle$, $\mathbf{C} = \mathbf{B}[X_1, \ldots, X_n]/\langle f_1^\rho, \ldots, f_s^\rho\rangle$ *with the two natural homomorphisms* $\mathbf{A} \to \mathbf{C}$ *and* $\mathbf{B} \to \mathbf{C}$*.*
2. *If in addition* $\mathbf{B} = \mathbf{k}[y_1, \ldots, y_r] \simeq \mathbf{k}[Y_1, \ldots, Y_r]/\langle g_1, \ldots, g_t\rangle$ *is itself a finitely presented* $\mathbf{k}$*-algebra, we obtain*
$$\mathbf{C} \simeq \mathbf{k}[X_1, \ldots, X_n, Y_1, \ldots, Y_r]/\langle f_1, \ldots, f_s, g_1, \ldots, g_t\rangle\,.$$
3. *Generally, we can consider the* $\mathbf{k}$*-module* $\mathbf{C} = \mathbf{B} \otimes_{\mathbf{k}} \mathbf{A}$*. It has a commutative ring structure when defining the product as*
$$(x \otimes a) \cdot (y \otimes b) = xy \otimes ab.$$
We obtain a $\mathbf{k}$*-algebra structure and we have two natural homomorphisms* $\mathbf{B} \to \mathbf{C}$, $x \mapsto x \otimes 1$ *and* $\mathbf{A} \to \mathbf{C}$, $a \mapsto 1 \otimes a$*. This makes* $\mathbf{C}$ *the direct sum of* $\mathbf{B}$ *and* $\mathbf{A}$*.*
4. *If* $\mathbf{B} = \mathbf{k}/\mathfrak{a}$, *we obtain* $\mathbf{C} \simeq \mathbf{A}/\mathfrak{b}$ *where* $\mathfrak{b} = \beta(\mathfrak{a})\mathbf{A}$*.*
5. *If* $\mathbf{B} = S^{-1}\mathbf{k}$, *we obtain* $\mathbf{C} \simeq U^{-1}\mathbf{A}$ *where* $U = \beta(S)$*.*

B. (Scalar extension)
We can regard $\mathbf{C}$ *as a* $\mathbf{B}$*-algebra. We then say that* $\mathbf{C}$ *is the* $\mathbf{B}$*-algebra obtained from* $\mathbf{A}$ *by* changing the base ring, *or by* scalar extension. *It is then logical to denote it by* $\rho_\star(\mathbf{A})$*.*

D The proof is left to the reader. □

We will be mindful of the fact that $\mathbf{k} \subseteq \mathbf{A}$ does not generally imply $\mathbf{B} \subseteq \mathbf{C}$, in particular in case *4*.

Also note that the tradition is to speak of a *tensor product of* $\mathbf{k}$*-algebras* rather than of a direct sum.

[4] The term "carré cocartésien" could be translated as "cocartesian square."

3.10. Fact. *If* $\mathbf{A}$ *and* $\mathbf{B}$ *are two* $\mathbf{k}$*-algebras, and* $(M,+)$ *is an additive group, taking an* $\mathbf{A}\otimes_{\mathbf{k}}\mathbf{B}$*-module structure over* M *is the same as taking an external law of the* $\mathbf{A}$*-module* $\mathbf{A}\times M\to M$ *and an external law of the* $\mathbf{B}$*-module* $\mathbf{B}\times M\to M$ *which both commute and "coincide over* $\mathbf{k}$*." We also say that* M *has a* $(\mathbf{A},\mathbf{B})$-bimodule structure*.*

D The explanation is the following with $\mathbf{k}\xrightarrow{\rho}\mathbf{B}$, $\mathbf{k}\xrightarrow{\alpha}\mathbf{A}$.
If we have an $\mathbf{A}\otimes_{\mathbf{k}}\mathbf{B}$-module structure over M, we have the two external laws

$$\mathbf{B}\times M\to M,\ (c,m)\mapsto c\cdot m=(1\otimes c)m,\ \text{ and}$$
$$\mathbf{A}\times M\to M,\ (b,m)\mapsto b\star m=(b\otimes 1)m.$$

Since $b\otimes c=(b\otimes 1)(1\otimes c)=(1\otimes c)(b\otimes 1)$, we must have $b\star(c\cdot m)=c\cdot(b\star m)$. If $a\in\mathbf{k}$, $a(1\otimes 1)=\alpha(a)\otimes 1=1\otimes\rho(a)$ so we must have $\rho(a)\cdot m=\alpha(a)\star m$. Thus the two laws commute and coincide over $\mathbf{k}$.
Conversely, from two external laws that commute and coincide over $\mathbf{k}$, we can define $(b\otimes c)m$ by $b\star(c\cdot m)$. □

Here is an important and easy fact regarding the scalar extension.

3.11. Fact. *Consider two* $\mathbf{k}$*-algebras* $\mathbf{k}\xrightarrow{\rho}\mathbf{k}'$ *and* $\mathbf{k}\xrightarrow{\alpha}\mathbf{A}$ *and let* $\mathbf{A}'=\rho_\star(\mathbf{A})$*. If the* $\mathbf{k}$*-algebra* $\mathbf{A}$ *is finitely generated (resp. finitely presented, finite, integral, strictly finite) the same holds for the* $\mathbf{k}'$*-algebra* $\mathbf{A}'$*.*

D The proof is left to the reader. □

Integral algebras

The Lying Over lemma

In this and the following subsection we complete what has already been said on integral algebras in Section III-8.

The following lemma expresses the constructive content of the classical Lying Over lemma of classical mathematics, which asserts that if $\mathbf{B}$ is a ring integral over a subring $\mathbf{A}$ there is always a prime ideal of $\mathbf{B}$ above a given prime ideal of $\mathbf{A}$.
Recall that we denote by $\mathrm{D}_{\mathbf{A}}(\mathfrak{a})$ the nilradical of the ideal $\mathfrak{a}$ of $\mathbf{A}$.

3.12. Lemma. (Lying Over)
Let $\mathbf{A}\subseteq\mathbf{B}$ *with* $\mathbf{B}$ *integral over* $\mathbf{A}$ *and* $\mathfrak{a}$ *be an ideal of* $\mathbf{A}$*, then* $\mathfrak{a}\mathbf{B}\cap\mathbf{A}\subseteq\mathrm{D}_{\mathbf{A}}(\mathfrak{a})$*, or (which amounts to the same thing)*

$$\mathrm{D}_{\mathbf{B}}(\mathfrak{a}\mathbf{B})\cap\mathbf{A}=\mathrm{D}_{\mathbf{A}}(\mathfrak{a}).$$

In particular, $1\in\mathfrak{a}\ \Leftrightarrow\ 1\in\mathfrak{a}\mathbf{B}$*.*

D If $x\in\mathfrak{a}\mathbf{B}$ we have $x=\sum a_ib_i$, with $a_i\in\mathfrak{a}$, $b_i\in\mathbf{B}$. The b_i's generate a finite $\mathbf{A}$-subalgebra $\mathbf{B}'$. Let G be a finite generator set (with ℓ elements) of the $\mathbf{A}$-module $\mathbf{B}'$. Let $B_i \in \mathbb{M}_\ell(\mathbf{A})$ be a matrix that expresses the multiplication by b_i over G. The multiplication by x is expressed by the matrix $\sum a_i B_i$, which has coefficients in $\mathfrak{a}$. The characteristic polynomial of this matrix, which annihilates x (because $\mathbf{B}'$ is a faithful $\mathbf{A}$-module), therefore has all of its coefficients (except for the leading coefficient) in $\mathfrak{a}$. When $x \in \mathbf{A}$, this implies $x^\ell \in \mathfrak{a}$. □

Remark. Let us indicate how we can deduce the classical Lying Over lemma in classical mathematics. Consider the case where $\mathfrak{a}$ is a prime ideal and let $S = \mathbf{A} \setminus \mathfrak{a}$. Then, $\mathfrak{a}\mathbf{B} \cap S = (\mathfrak{a}\mathbf{B} \cap \mathbf{A}) \cap S$ is empty by Lemma 3.12. By *Krull's lemma*, there exists therefore a prime ideal $\mathfrak{p}$ of $\mathbf{B}$ such that $\mathfrak{a}\mathbf{B} \subseteq \mathfrak{p}$ and $\mathfrak{p} \cap S = \emptyset$, which implies $\mathfrak{p} \cap \mathbf{A} = \mathfrak{a}$. It would also be easy to deduce, in classical mathematics, Lemma 3.12 from the Lying Over lemma. ■

Example. Here we show that the condition "$\mathbf{B}$ integral over $\mathbf{A}$" is crucial in the Lying Over lemma. Consider $\mathbf{A} = \mathbb{Z}$, $\mathbf{B} = \mathbb{Z}[1/3]$ and $\mathfrak{a} = 3\mathbb{Z}$. Then, we obtain $\mathfrak{a}\mathbf{B} = \langle 1 \rangle$, but $\mathfrak{a} \neq \langle 1 \rangle$. ■

Algebras integral over zero-dimensional rings

Here we examine the special case of algebras over zero-dimensional rings.

Algebras integral over discrete fields are an important example of zero-dimensional rings. In this situation, we give a more precise version on item *3* of Lemma IV-8.2 as follows (see also Theorem 1.4).

3.13. Lemma. *An algebra $\mathbf{A}$ integral over a discrete field $\mathbf{K}$ is zero-dimensional. More precisely, let $\mathfrak{a} = \langle a_1, \ldots, a_n \rangle = \langle \underline{a} \rangle$ be a finitely generated ideal. There exist an integer d and an idempotent $s \in a_1\mathbf{K}[\underline{a}] + \cdots + a_n\mathbf{K}[\underline{a}]$ such that $\mathfrak{a}^d = \langle s \rangle$.*

D An element x of $\mathbf{A}$ is annihilated by a monic polynomial of $\mathbf{K}[X]$ that we express as $uX^k\big(1 - X\,h(X)\big)$ where $u \in \mathbf{K}^\times$, $k \geqslant 0$ and so $x^k\big(1 - xh(x)\big) = 0$.

The idempotent e_x such that $\langle e_x \rangle = \langle x \rangle^d$ for large enough d is then equal to $\big(xh(x)\big)^k$, and d is "large enough" as soon as $d \geqslant k$.

In the case of the finitely generated ideal $\mathfrak{a} = \langle a_1, \ldots, a_n \rangle$, each idempotent e_{a_i} is an element of $a_i\mathbf{K}[a_i]$. Therefore their gcd, which is the idempotent s in the statement of the lemma, is in $a_1\mathbf{K}[\underline{a}] + \cdots + a_n\mathbf{K}[\underline{a}]$ (because the gcd of two idempotents e and f is $e \vee f = e + f - ef$). □

3.14. Lemma. *Let $\mathbf{k}$ be a zero-dimensional ring and $\mathbf{A}$ an algebra integral over $\mathbf{k}$.*

1. *The ring $\mathbf{A}$ is zero-dimensional.*
2. *More precisely, if $\mathfrak{a} = \langle a_1, \ldots, a_n \rangle$, there exist an integer d and an idempotent $s \in a_1\mathbf{k}[\underline{a}] + \cdots + a_n\mathbf{k}[\underline{a}]$ such that $\mathfrak{a}^d = \langle s \rangle$.*

3. *In particular, we obtain for each $a \in \mathbf{A}$ an equality*
$$a^d\big(1 - af(a)\big) = 0,$$
with some $f(X) \in \mathbf{k}[X]$ (so, $\big(af(a)\big)^d$ is idempotent).

NB: We do not assume that $\rho : \mathbf{k} \to \mathbf{A}$ is injective.

D It suffices to prove item *2.*

By applying the elementary local-global machinery from page 213, we extend the result of Lemma 3.13 to the case where $\mathbf{k}$ is reduced zero-dimensional. Then we extend the zero-dimensional case to the reduced zero-dimensional case by passing to the quotient via the nilradical and by using "Newton's method in algebra" (Section III-10). More precisely, let $\mathfrak{N} = \mathrm{D}_{\mathbf{A}}(0)$. By the reduced zero-dimensional case, there exist $x_1, \ldots, x_n \in \mathbf{k}[\underline{a}]$ such that
$$s = a_1x_1 + \cdots + a_nx_n, \text{ with } s^2 \equiv s \bmod \mathfrak{N} \text{ and } sa_i \equiv a_i \bmod \mathfrak{N}.$$

The element s is congruent modulo $\mathfrak{N}$ to a unique idempotent s_1, which is written as $sp(s)$ with $p(T) \in \mathbb{Z}[T]$ (Corollary III-10.4). Since $s \in \mathbf{k}[\underline{a}]$, this gives an equality $s_1 = a_1y_1 + \cdots + a_ny_n$ with $y_1, \ldots, y_n \in \mathbf{k}[\underline{a}]$. In addition, $s_1a_i \equiv sa_i \equiv a_i$ modulo $\mathfrak{N}$ for each i. Since $(1 - s_1)a_i \in \mathfrak{N}$, there exists a k_i such that $(1-s_1)a_i^{k_i} = 0$ for each i. Finally, with $k = k_1+\cdots+k_n$, we obtain $\mathfrak{a}^k = \langle s_1 \rangle$. □

Recall that Lemma IV-8.15 establishes the following reciprocal.

Let $\mathbf{k} \subseteq \mathbf{A}$, with $\mathbf{A}$ integral over $\mathbf{k}$. If $\mathbf{A}$ is a zero-dimensional ring, then $\mathbf{k}$ is a zero-dimensional ring.

A weak Nullstellensatz

The following theorem, for the implication *2* ⇒ *3* limited to the case where $\mathbf{A}$ is a discrete field, is often called the "weak Nullstellensatz" in the literature, because it can serve as a preliminary to the Nullstellensatz (in classical mathematics). It is to be distinguished from the other weak Nullstellensätze already considered in this work.

3.15. Theorem. (A weak Nullstellensatz)
Let $\mathbf{K}$ be a reduced zero-dimensional ring and $\mathbf{A}$ be a finitely generated $\mathbf{K}$-algebra. For the following properties, we have 1 ⇒ 2 ⇔ 3.

1. *$\mathbf{A}$ is a local ring.*
2. *$\mathbf{A}$ is zero-dimensional.*
3. *$\mathbf{A}$ is finite over $\mathbf{K}$.*

NB: We do not assume that $\rho : \mathbf{K} \to \mathbf{A}$ is injective.

D We already know that *3* implies *2.* Let us see that *1* or *2* implies *3.*

We can replace $\mathbf{K}$ with $\rho(\mathbf{K})$ which is also reduced zero-dimensional. We then have $\mathbf{K} \subseteq \mathbf{A} = \mathbf{K}[x_1, \ldots, x_n] = \mathbf{K}[\underline{x}]$. Our proof is by induction on n.

The $n=0$ case is trivial. Let us do the inductive step from $n-1$ to n.
If $\mathbf{A}$ is zero-dimensional, there exist a polynomial $R \in \mathbf{K}[X_1,\ldots,X_n]$ and an integer ℓ such that $x_n^\ell\big(1-x_nR(\underline{x})\big)=0$. The polynomial $X_n^\ell\big(1-X_nR(\underline{X})\big)$ has one of its coefficients equal to 1 and is therefore primitive.
If $\mathbf{A}$ is local, x_n or $1+x_n$ is invertible. Without loss of generality we assume that x_n is invertible. There exists a polynomial $R \in \mathbf{K}[X_1,\ldots,X_n]$ such that $1+x_nR(\underline{x})=0$. The polynomial $1+X_nR(\underline{X})$ has one of its coefficients equal to 1 and is therefore primitive.
In both cases, we can perform a change of variables as in Lemma III-9.4 (infinite discrete field case) or VII-1.4 (general case). We then have $\mathbf{A}=\mathbf{K}[y_1,\ldots,y_n]$, and $\mathbf{A}$ is finite over $\mathbf{A}_1=\mathbf{K}[y_1,\ldots,y_{n-1}]\subseteq\mathbf{A}$.
If $\mathbf{A}$ is zero-dimensional, Lemma IV-8.15 implies that $\mathbf{A}_1$ is zero-dimensional and we can therefore apply the induction hypothesis.
If $\mathbf{A}$ is local, item *3* of Theorem IX-1.8 implies that $\mathbf{A}_1$ is local and we can therefore apply the induction hypothesis. □

Remark. What is new for the implication *2* ⇒ *3* in Theorem 3.15, compared to Theorem IV-8.16 which uses Noether positioning, is therefore the fact that we only assume that the algebra is finitely generated instead of finitely presented. The two proofs are ultimately based on Lemma IV-8.15 and on a change of variables lemma. ■

Integral algebras over a pp-ring

We denote by $\operatorname{Reg}\mathbf{A}$ the filter of the regular elements of the ring $\mathbf{A}$, such that the total ring of fractions $\operatorname{Frac}\mathbf{A}$ is equal to $(\operatorname{Reg}\mathbf{A})^{-1}\mathbf{A}$.

3.16. Fact.
Let $\mathbf{A}$ *be a pp-ring,* $\mathbf{K}=\operatorname{Frac}\mathbf{A}$*,* $\mathbf{L}\supseteq\mathbf{K}$ *be a reduced integral* $\mathbf{K}$*-algebra and* $\mathbf{B}$ *be the integral closure of* $\mathbf{A}$ *in* $\mathbf{L}$*.*
Then, $\mathbf{B}$ *is a pp-ring and* $\operatorname{Frac}\mathbf{B}=\mathbf{L}=(\operatorname{Reg}\mathbf{A})^{-1}\mathbf{B}$.

D $\mathbf{K}$ is reduced zero-dimensional because $\mathbf{A}$ is a pp-ring (Fact IV-8.6). The ring $\mathbf{L}$ is zero-dimensional because it is integral over $\mathbf{K}$. As it is reduced, it is a pp-ring. As $\mathbf{B}$ is integrally closed in $\mathbf{L}$, every idempotent of $\mathbf{L}$ is in $\mathbf{B}$, so $\mathbf{B}$ is a pp-ring.
Consider some $x\in\mathbf{L}$ and some monic polynomial $f\in\mathbf{K}[X]$ which annihilates x. By getting rid of the denominators we obtain a polynomial

$$g(X)=a_mX^m+a_{m-1}X^{m-1}+\cdots+a_0\in\mathbf{A}[X]$$

which annihilates x, with $a_m\in\operatorname{Reg}\mathbf{A}$. Then, $y=a_mx$, integral over $\mathbf{A}$, is in $\mathbf{B}$ and $x\in(\operatorname{Reg}\mathbf{A})^{-1}\mathbf{B}$. □

Algebras that are finitely presented modules

3.17. Theorem. (When a $\mathbf{k}$-algebra is a finitely presented $\mathbf{k}$-module)

1. *For a* $\mathbf{k}$*-algebra* $\mathbf{A}$ *the following properties are equivalent.*
   - *a.* $\mathbf{A}$ *is a finitely presented* $\mathbf{k}$*-module.*
   - *b.* $\mathbf{A}$ *is finite and is a finitely presented* $\mathbf{k}$*-algebra.*
   - *c.* $\mathbf{A}$ *is finitely presented and integral over* $\mathbf{k}$*.*
2. *If these conditions are satisfied and* $\mathbf{k}$ *is coherent (resp. strongly discrete coherent), then* $\mathbf{A}$ *is coherent (resp. strongly discrete coherent).*

D *1a ⇒ 1b.* Let $\mathbf{A} = \sum_{i=1}^{m} b_i\mathbf{k}$ be a finitely presented $\mathbf{k}$-module. We must give a finite presentation of $\mathbf{A}$ as a $\mathbf{k}$-algebra. Consider the generator set $(b_1, \ldots, b_m)$. On the one hand, we take the $\mathbf{k}$-syzygies given by the presentation of $\mathbf{A}$ as a $\mathbf{k}$-module. On the other hand we express each b_ib_j as a $\mathbf{k}$-linear combination of the b_k's. Modulo these last relations, every polynomial in the b_i's with coefficients in $\mathbf{k}$ can be rewritten as a $\mathbf{k}$-linear combination of the b_i's. Therefore it evaluates to 0 in $\mathbf{A}$ if and only if (as a polynomial) it is in the ideal generated by all the relations we have given.
1b ⇔ 1c. Clear.
1b ⇒ 1a. Suppose that $\mathbf{A}$ is finite over $\mathbf{k}$ with

$$\mathbf{A} = \mathbf{k}[x_1, \ldots, x_n] = \mathbf{k}[\underline{X}]/\langle \underline{f} \rangle\,.$$

For each i, let $t_i(X_i) \in \mathbf{k}[X_i]$ be a monic polynomial such that $t_i(x_i) = 0$, and $\delta_i = \deg\, t_i$. We have

$$\mathbf{A} = \mathbf{k}[\underline{X}]/\langle t_1, \ldots, t_n, h_1, \ldots, h_s \rangle\,,$$

where the h_j's are the reduced f_j's modulo $\langle t_1, \ldots, t_n \rangle$.
The "monomials" $\underline{x}^{\underline{d}} = x_1^{d_1} \cdots x_n^{d_n}$ where $d_1 < \delta_1, \ldots,\ d_n < \delta_n$ (which we denote by $\underline{d} < \underline{\delta}$) form a basis for the algebra $\mathbf{k}[\underline{X}]/\langle \underline{t} \rangle$ and a generator set G of the $\mathbf{k}$-module $\mathbf{A}$. An arbitrary $\mathbf{k}$-syzygy between these generators is obtained when we write $\sum_{j=1}^{s} g_j(\underline{x})h_j(\underline{x}) = 0$, on the condition that we express it as a $\mathbf{k}$-linear combination of elements of G. We can naturally limit ourselves to the g_j's that are of degree $< \delta_i$ in each variable X_i. If we fix an index $j \in [\![1..s]\!]$ and a monomial $\underline{x}^{\underline{d}}$ with $\underline{d} < \underline{\delta}$, we obtain a $\mathbf{k}$-syzygy between the elements of G by rewriting $\underline{X}^{\underline{d}}\, h_j(\underline{X})$ modulo $\langle t_1, \ldots, t_n \rangle$ and by saying that the linear combination of the elements of G obtained as such is null. These syzygies generate the $\mathbf{k}$-syzygy module between the elements of G.

2. If $\mathbf{k}$ is coherent (resp. strongly discrete coherent), then we know that $\mathbf{A}$ is coherent (resp. strongly discrete coherent) as a $\mathbf{k}$-module (since it is finitely presented). Let $(b_i)_{i=1}^{m}$ be a generator set of $\mathbf{A}$ as a $\mathbf{k}$-module and $v = (v_1, \ldots, v_n) \in \mathbf{A}^n$. The ideal $\langle v_1, \ldots, v_n \rangle$ is the $\mathbf{k}$-module finitely generated by the v_ib_j's, so it is detachable if $\mathbf{k}$ is strongly discrete.
Moreover, an $\mathbf{A}$-syzygy for v can be rewritten as a $\mathbf{k}$-syzygy between the

v_ib_j's. Therefore a generator set of the $\mathbf{k}$-syzygy module between the v_ib_j's gives on a reread a generator set of the $\mathbf{A}$-syzygy module between the v_i's.□

Integral algebra over an integrally closed ring

Here we generalize Proposition III-8.17.

3.18. Theorem. *Let* $\mathbf{A}$ *be an integrally closed ring,* $\mathbf{K}$ *be its quotient field,* $\mathbf{L}$ *be a strictly finite overfield of* $\mathbf{K}$ *and* $\mathbf{B}$ *be the integral closure of* $\mathbf{A}$ *in* $\mathbf{L}$*. For* $z \in \mathbf{L}$*, let* $\mu_{\mathbf{L},z} \in \mathrm{End}_{\mathbf{K}}(\mathbf{L})$ *be multiplication by* z*, and* $\nu_z(X)$ *and* $\chi_z(X)$ *be the minimal polynomial and the characteristic polynomial of* $\mu_{\mathbf{L},z}$ *(they are elements of* $\mathbf{K}[X]$*).*

1. *For* $z \in \mathbf{L}$*, we have* $z \in \mathbf{B} \iff \nu_z \in \mathbf{A}[X] \iff \chi_z \in \mathbf{A}[X]$*. In particular, for* $z \in \mathbf{B}$*,* $\mathrm{N}_{\mathbf{L}/\mathbf{K}}(z)$ *and* $\mathrm{Tr}_{\mathbf{L}/\mathbf{K}}(z) \in \mathbf{A}$*.*

We now suppose that $\mathbf{L}$ *is étale over* $\mathbf{K}$*, i.e. that* $\mathrm{Disc}_{\mathbf{L}/\mathbf{K}} \in \mathbf{K}^\times$*.*

2. *Let* x *be an element of* $\mathbf{B}$ *such that* $\mathbf{K}[x] = \mathbf{L}$*. Let* $\Delta_x = \mathrm{disc}(\chi_x)$*.*
   a. $\mathbf{A}[x] \simeq \mathbf{A}[X]/\langle\chi_x\rangle$*, free* $\mathbf{A}$*-module of rank* $[\,\mathbf{L} : \mathbf{K}\,]$*.*
   b. *We have* $\mathbf{A}[x][1/\Delta_x] = \mathbf{B}[1/\Delta_x]$*, integrally closed ring.*
   c. *If* $\mathbf{A}$ *is a gcd domain, if* $\Delta_x = d^2b$ *and* b *is squarefree then* $\mathbf{A}[x][1/d] = \mathbf{B}[1/d]$ *and it is an integrally closed ring.*
3. *Let* $\mathcal{B}$ *be a basis of* $\mathbf{L}$ *over* $\mathbf{K}$ *contained in* $\mathbf{B}$ *and* $M \subseteq \mathbf{B}$ *be the* $\mathbf{A}$*-module with basis* $\mathcal{B}$*.*
   a. *The element* $\Delta = \mathrm{disc}_{\mathbf{L}/\mathbf{K}}(\mathcal{B})$ *is in* $\mathbf{A}$*.*
   b. *For all* $x \in \mathbf{B}$*,* $\Delta x \in M$*, in other words* $M \subseteq \mathbf{B} \subseteq \frac{1}{\Delta}M$*.*
   c. *If* $\mathbf{A}$ *is a gcd domain, for all* $x \in \mathbf{B}$*, there exists a* $\delta \in \mathbf{A}$ *such that* δ^2 *divides* Δ *and* $\delta x \in M$*.*
      If in addition $\Delta = d^2b$ *with* b *being squarefree,* $M \subseteq \mathbf{B} \subseteq \frac{1}{d}M$*.*

D *1.* If $z \in \mathbf{B}$, it annihilates a monic polynomial $h(X) \in \mathbf{A}[X]$, and the polynomial ν_z divides h in $\mathbf{K}[X]$. As ν_z is monic and $\mathbf{A}$ is integrally closed, we obtain $\nu_z \in \mathbf{A}[X]$ by Lemma III-8.10.

Moreover in $\mathbf{K}[X]$, ν_z divides χ_z and χ_z divides a power of ν_z, so, still by Lemma III-8.10, $\nu_z \in \mathbf{A}[X]$ is equivalent to $\chi_z \in \mathbf{A}[X]$.

2a. Clear: $(1, x, \dots, x^{[\mathbf{L}:\mathbf{K}]-1})$ is both a basis of $\mathbf{A}[x]$ over $\mathbf{A}$ and of $\mathbf{L}$ over $\mathbf{K}$. Note that by hypothesis $\chi_x = \nu_x$.

2b. Consider the special case of *3b.* where $M = \mathbf{A}[x]$.

We obtain $\mathbf{B}[1/\Delta_x] = \mathbf{A}[x][1/\Delta_x]$, and since $\mathbf{B}$ is integrally closed, the same goes for $\mathbf{B}[1/\Delta_x]$.

2c. Special case of *3c.* with $M = \mathbf{A}[x]$, reasoning as in *3c.*

3a. Immediate consequence of *1.*

3b. Let $\mathcal{B} = (b_1, \dots, b_n)$ and $x = \sum_i x_ib_i$ with $x_i \in \mathbf{K}$. Consider for example the coefficient x_1, assumed nonzero. The n-tuple $\mathcal{B}' = (x, b_2, \dots, b_n)$ is a $\mathbf{K}$-basis of $\mathbf{L}$ contained in $\mathbf{B}$. The matrix of $\mathcal{B}'$ over $\mathcal{B}$ has as its determinant x_1. Therefore $x_1^2\Delta = x_1^2 \operatorname{disc}(\mathcal{B}) = \operatorname{disc}(\mathcal{B}') \in \mathbf{A}$. A fortiori $(x_1\Delta)^2 \in \mathbf{A}$, and since $\mathbf{A}$ is integrally closed, $x_1\Delta \in \mathbf{A}$. Thus all the coordinates over $\mathcal{B}$ of Δx are in $\mathbf{A}$.

3c. When $\mathbf{A}$ is a gcd domain, we express the element x_1 as a reduced fraction $x_1 = a_1/\delta_1$. Then, since $x_1^2\Delta \in \mathbf{A}$, δ_1^2 divides $a_1^2\Delta$, and since $\gcd(a_1, \delta_1) = 1$, the element δ_1^2 divides Δ. We proceed in the same way for each $x_i = a_i/\delta_i$. If δ is the lcm of the δ_i's, δ^2 is the lcm of the δ_i^2's, so it divides Δ, and $\delta x \in M$. □

4. Strictly finite algebras

The dual module and the trace

If P and Q are finitely generated projective $\mathbf{k}$-modules, we have a canonical isomorphism $\theta_{P,Q} : P^\star \otimes_{\mathbf{k}} Q \to \mathrm{L}_{\mathbf{k}}(P, Q)$.

When the context is clear we can identify $\alpha \otimes x \in P^\star \otimes_{\mathbf{k}} Q$ with the corresponding $\mathbf{k}$-linear map $y \mapsto \alpha(y)x$.

In particular, a coordinate system of P, $\big((x_1, \dots, x_n), (\alpha_1, \dots, \alpha_n)\big)$, is characterized by the equality

$$\sum\nolimits_{i=1}^{n} \alpha_i \otimes x_i = \mathrm{Id}_P. \tag{1}$$

Dually we have, modulo the identification of P with $(P^\star)^\star$,

$$\sum\nolimits_{i=1}^{n} x_i \otimes \alpha_i = \mathrm{Id}_{P^\star}. \tag{2}$$

This equation means that for every $\gamma \in P^\star$ we have $\gamma = \sum_{i=1}^{n} \gamma(x_i)\alpha_i$.

4.1. Definition and notation. Let $\mathbf{A}$ be a $\mathbf{k}$-algebra.
The dual $\mathbf{A}^\star$ of the $\mathbf{k}$-module $\mathbf{A}$ has an $\mathbf{A}$-module structure via the external law $(a, \alpha) \mapsto a \centerdot \alpha \overset{\text{def}}{=} \alpha \circ \mu_a$, i.e. $(a \centerdot \alpha)(x) = \alpha(ax)$.

Facts V-2.9 and/or V-8.9 give the following result.

4.2. Fact. *Let $\big((x_1, \dots, x_n), (\alpha_1, \dots, \alpha_n)\big)$ be a coordinate system for the strictly finite $\mathbf{k}$-algebra $\mathbf{A}$, then the $\mathbf{k}$-linear map $\mu_{\mathbf{A},a}$ is represented in this system by the matrix $\big(\alpha_i(ax_j)\big)_{i,j \in [\![1..n]\!]}$ and we have*

$$\mathrm{Tr}_{\mathbf{A}/\mathbf{k}} = \sum\nolimits_{i=1}^{n} x_i \centerdot \alpha_i, \quad \big(i.e.\ \forall a \in \mathbf{A},\ \mathrm{Tr}_{\mathbf{A}/\mathbf{k}}(a) = \sum\nolimits_{i=1}^{n} \alpha_i(ax_i)\big). \tag{3}$$

Norm and cotransposed element

We introduce the notion of a *cotransposed element* in a strictly finite algebra. It suffices to build upon what was said in the case of a free algebra of finite rank on page 129. If $\mathbf{A}$ is strictly finite over $\mathbf{k}$ we can indentify $\mathbf{A}$ with a commutative $\mathbf{k}$-subalgebra of $\mathrm{End}_{\mathbf{k}}(A)$, where A designates the $\mathbf{k}$-module $\mathbf{A}$ deprived of its multiplicative structure, by means of the multiplication homomorphism $x \mapsto \mu_{A,x} = \mu_x$. Then, since $\widetilde{\mu_x} = G(\mu_x)$ for a polynomial $G \in \mathbf{k}[T]$ (item *6* of Theorem V-8.1), we can define $\widetilde{x}$ by the equality $\widetilde{x} = G(x)$, or (what amounts to the same thing) $\widetilde{\mu_x} = \mu_{\widetilde{x}}$. If more precision is necessary we will use the notation $\mathrm{Adj}_{\mathbf{A}/\mathbf{k}}(x)$. This element $\widetilde{x}$ is called *the cotransposed element of* x. The equality $\widetilde{\mu_x}\, \mu_x = \det(\mu_x)\mathrm{Id}_{\mathbf{A}}$ then gives

$$x\ \mathrm{Adj}_{\mathbf{A}/\mathbf{k}}(x) = \mathrm{N}_{\mathbf{A}/\mathbf{k}}(x). \tag{4}$$

4.3. Lemma. *Let $\mathbf{k} \xrightarrow{\rho} \mathbf{A}$ be a strictly finite algebra, $x \in \mathbf{A}$ and $y \in \mathbf{k}$.*

1. *We have $x \in \mathbf{A}^\times$ if and only if $\mathrm{N}_{\mathbf{A}/\mathbf{k}}(x) \in \mathbf{A}^\times$.*
   In this case $x^{-1} = \widetilde{x}/\mathrm{N}_{\mathbf{A}/\mathbf{k}}(x)$.
2. *x is regular in $\mathbf{A}$ if and only if $\mathrm{N}_{\mathbf{A}/\mathbf{k}}(x)$ is regular in $\mathbf{k}$. In this case $\widetilde{x}$ is also regular.*
3. *$\rho(\mathbf{k})$ is a direct summand in $\mathbf{A}$.*

Let $e = \mathrm{e}_0(\mathbf{A})$ (such that $\langle e\rangle_{\mathbf{k}} = \mathrm{Ann}_{\mathbf{k}}(\mathbf{A})$).

4. *We have $\rho(y) \in \mathbf{A}^\times$ if and only if $y \in (\mathbf{k}/\langle e\rangle)^\times$.*
5. *$\rho(y)$ is regular in $\mathbf{A}$ if and only if y is regular in $\mathbf{k}/\langle e\rangle$.*

NB. If $\mathbf{A}$ is a faithful $\mathbf{k}$-module, i.e. if ρ is injective, we identify $\mathbf{k}$ with $\rho(\mathbf{k})$. Then, $\mathbf{k}$ is a direct summand in $\mathbf{A}$, and an element y of $\mathbf{k}$ is invertible (resp. regular) in $\mathbf{k}$ if and only if it is invertible (resp. regular) in $\mathbf{A}$.

D *1.* In a finitely generated projective module an endomorphism (here μ_x) is a bijection if and only if its determinant is invertible.

2. In a finitely generated projective module an endomorphism is injective if and only if its determinant is regular.

Items *3*, *4* and *5* can be proven after localization at comaximal elements of $\mathbf{k}$. By the local structure theorem we are reduced to the case where $\mathbf{A}$ is free of finite rank, say k. If $k = 0$, then $e = 1$, so $\mathbf{A}$ and $\mathbf{k}/\langle e\rangle$ are trivial and everything is clear (even if it is a little unsettling). Let us examine the case where $k \geqslant 1$, hence $e = 0$, and let us identify $\mathbf{k}$ with $\rho(\mathbf{k})$.

Items *4* and *5* then result from items *1* and *2* because $\mathrm{N}_{\mathbf{A}/\mathbf{k}}(y) = y^k$.

For item *3*, we consider a basis $(b_1, \dots, b_k)$ of $\mathbf{A}$ over $\mathbf{k}$ and elements a_1, …, $a_k \in \mathbf{k}$ such that $\sum_i a_i b_i = 1$. We have $\mathrm{N}_{\mathbf{A}/\mathbf{k}}(\sum_i a_i b_i) = 1$. Moreover, for $y_1, \dots, y_k \in \mathbf{k}$, $\mathrm{N}_{\mathbf{A}/\mathbf{k}}(\sum_i y_i b_i)$ is expressed as a homogeneous polynomial of degree k in $\mathbf{k}[\underline{y}]$ (see the remark on page 129), and so

$$\mathrm{N}_{\mathbf{A}/\mathbf{k}}(\textstyle\sum_i a_i b_i) = \sum_i a_i \beta_i = 1$$

for suitable $\beta_i \in \mathbf{k}$.
Let us consider the element $\beta \in \mathrm{End}_{\mathbf{k}}(\mathbf{A})$ defined by $\beta(\sum_i x_i b_i) = \sum_i x_i \beta_i$. Then, $\beta(1) = 1$, so $\beta(z) = z$ for $z \in \mathbf{k}$, $\mathrm{Im}\,\beta = \mathbf{k}$ and $\beta \circ \beta = \beta$. □

Transitivity and rank

When $\mathbf{A}$ is of constant rank n, we write $[\,\mathbf{A} : \mathbf{k}\,] = n$. This generalizes the notation already defined in the free algebra case, and this will be generalized further in Chapter X (notation X-3.6). In this subsection, m and n are integers.

4.4. Fact. *Let* $\mathbf{A}$ *be a strictly finite* $\mathbf{k}$*-algebra,* M *be a finitely generated projective* $\mathbf{A}$*-module and* $\mathbf{B}$ *be a strictly finite* $\mathbf{A}$*-algebra.*

1. M *is also a finitely generated projective* $\mathbf{k}$*-module.*
2. *Suppose* $\mathrm{rk}_{\mathbf{A}} M = m$ *and let* $f(T) = \mathrm{R}_{\mathbf{k}}(\mathbf{A}) \in \mathbb{B}(\mathbf{k})[T]$ *be the rank polynomial of* $\mathbf{A}$ *as a* $\mathbf{k}$*-module, then* $\mathrm{R}_{\mathbf{k}}(M) = f^m(T) = f(T^m)$*.*
3. $\mathbf{B}$ *is strictly finite over* $\mathbf{k}$ *and* $\mathrm{Tr}_{\mathbf{B}/\mathbf{k}} = \mathrm{Tr}_{\mathbf{A}/\mathbf{k}} \circ \mathrm{Tr}_{\mathbf{B}/\mathbf{A}}$.

D *1.* Assume that $\mathbf{A} \oplus E \simeq \mathbf{k}^r$ ($\mathbf{k}$-modules) and $M \oplus N \simeq \mathbf{A}^s$ ($\mathbf{A}$-modules). Then $M \oplus N \oplus E^s \simeq \mathbf{k}^{rs}$ ($\mathbf{k}$-modules). We can state this again with coordinate systems in the following form: if $\big((x_1, \ldots, x_n), (\alpha_1, \ldots, \alpha_n)\big)$ is a coordinate system for the $\mathbf{k}$-module $\mathbf{A}$ and $\big((y_1, \ldots, y_m), (\beta_1, \ldots, \beta_m)\big)$ is a coordinate system for the $\mathbf{A}$-module M, then $\big((x_i y_j), (\alpha_i \circ \beta_j)\big)$ is a coordinate system for the $\mathbf{k}$-module M.
2. Left to the reader (who can rely on the previous description of the coordinate system, or consult the proof of Lemma X-3.8).
3. We work with coordinate systems as in item *1* and we apply Fact 4.2 regarding the trace. □

4.5. Theorem. *Let* $\mathbf{k} \subseteq \mathbf{A} \subseteq \mathbf{B}$ *be rings. Suppose that* $\mathbf{B}$ *is strictly finite over* $\mathbf{A}$*. Then*

1. *the ring* $\mathbf{B}$ *is strictly finite over* $\mathbf{k}$ *if and only if* $\mathbf{A}$ *is strictly finite over* $\mathbf{k}$*,*
2. *if* $[\,\mathbf{A} : \mathbf{k}\,] = n$ *and* $[\,\mathbf{B} : \mathbf{A}\,] = m$*, then* $[\,\mathbf{B} : \mathbf{k}\,] = mn$*,*
3. *if* $[\,\mathbf{B} : \mathbf{k}\,] = mn$ *and* $[\,\mathbf{B} : \mathbf{A}\,] = m$*, then* $[\,\mathbf{A} : \mathbf{k}\,] = n$*.*

D *1.* If $\mathbf{B}$ is strictly finite over $\mathbf{k}$, then $\mathbf{A}$ is strictly finite over $\mathbf{k}$; this results from $\mathbf{A}$ being a direct summand in $\mathbf{B}$ (Lemma 4.3 item *3*), which is a finitely generated projective $\mathbf{k}$-module.
The converse implication is in Lemma 4.4.

2 and *3.* Result from item *2* of Fact 4.4: if $f = T^n$ then $f^m(T) = T^{mn}$; if $f = \sum_k r_k T^k$ is a multiplicative polynomial such that $f^m(T) = T^{mn}$ then $f = T^n$, since $f^m(T) = f(T^m) = \sum_k r_k T^{km}$. □

Remark. More general transitivity formulas (in the case of nonconstant rank) are given in Section X-3 in the subsection entitled "Transitivity formulas" on page 551 (in particular, see Corollary X-3.9 and Theorem X-3.10). ∎

5. Dualizing linear forms, strictly étale algebras

5.1. Definition. *(Non-degenerate symmetric bilinear form, dualizing linear form, strictly étale algebra)*
Let M be a $\mathbf{k}$-module and $\mathbf{A}$ be a $\mathbf{k}$-algebra.

1. If $\phi : M \times M \to \mathbf{k}$ is a symmetric bilinear form, it is associated with the $\mathbf{k}$-linear map $\varphi : M \to M^\star$ defined by $\varphi(x) = \phi(x, \bullet) = \phi(\bullet, x)$.
   We say that ϕ is *non-degenerate* if φ is an isomorphism.
2. If $\lambda \in \mathrm{L}_\mathbf{k}(\mathbf{A}, \mathbf{k}) = \mathbf{A}^\star$, it is associated with the symmetric $\mathbf{k}$-bilinear form over $\mathbf{A}$, denoted by $\Phi_{\mathbf{A}/\mathbf{k},\lambda} = \Phi_\lambda$ and defined by $\Phi_\lambda(x, y) = \lambda(xy)$.
   We say that the linear form λ is *dualizing* if Φ_λ is non-degenerate.
   We call a *Frobenius algebra* an algebra for which there exists a dualizing linear form.
3. If $\mathbf{A}$ is strictly finite over $\mathbf{k}$ the form $\Phi_{\mathrm{Tr}_{\mathbf{A}/\mathbf{k}}}$ is called the *trace form.*
4. The algebra $\mathbf{A}$ is said to be *strictly étale* over $\mathbf{k}$ if it is strictly finite and if the trace is dualizing, i.e. the trace form is non-degenerate.

Remark. If $\mathbf{A}$ is free with basis $(\underline{e}) = (e_1, \ldots, e_n)$ over $\mathbf{k}$, the matrix of ϕ and that of φ coincide (for the suitable bases). Moreover, ϕ is non-degenerate if and only if $\mathrm{Disc}_{\mathbf{A}/\mathbf{k}} = \mathrm{disc}_{\mathbf{A}/\mathbf{k}}(\underline{e})$ is invertible. Note that when $\mathbf{k}$ is a discrete field we once again find Definition 1.1 for an étale algebra.[5] ∎

Dualizing forms

5.2. Theorem. (Characterization of the dualizing forms in the strictly finite case)
Let $\mathbf{A}$ be a $\mathbf{k}$-algebra and $\lambda \in \mathbf{A}^\star$. For $x \in \mathbf{A}$, let $x^\star = x \centerdot \lambda \in \mathbf{A}^\star$.

1. *If $\mathbf{A}$ is strictly finite and if λ is dualizing, then for every generator set $(x_i)_{i \in [\![1..n]\!]}$, there exists a system $(y_i)_{i \in [\![1..n]\!]}$ such that we have*
$$\sum\nolimits_{i=1}^{n} y_i^\star \otimes x_i = \mathrm{Id}_\mathbf{A}, \quad \textit{i.e.} \quad \forall x \in \mathbf{A},\ x = \sum\nolimits_{i=1}^{n} \lambda(xy_i)x_i. \quad (5)$$
   Moreover, if $\mathbf{A}$ is faithful, λ is surjective.

[5] We have not given the general definition of an étale algebra. It so happens that the étale algebras over discrete fields are always strictly étale (at least in classical mathematics, this is in relation to Theorem 6.14), but that it is no longer the case for an arbitrary commutative ring, hence the necessity to introduce the terminology "strictly étale" here.

2. *Conversely, if there exist two systems* $(x_i)_{i\in[\![1..n]\!]}$, $(y_i)_{i\in[\![1..n]\!]}$ *such that* $\sum_i y_i^\star \otimes x_i = \mathrm{Id}_{\mathbf{A}}$, *then*
   - $\mathbf{A}$ *is strictly finite,*
   - *the form* λ *is dualizing,*
   - *and we have the equality* $\sum_i x_i^\star \otimes y_i = \mathrm{Id}_{\mathbf{A}}$.
3. *If* $\mathbf{A}$ *is strictly finite, the following properties are equivalent.*
   a. λ *is dualizing.*
   b. λ *is a basis of the* $\mathbf{A}$*-module* $\mathbf{A}^\star$ *(which is therefore free of rank* 1*).*
   c. λ *generates the* $\mathbf{A}$*-module* $\mathbf{A}^\star$, *i.e.* $\mathbf{A} \centerdot \lambda = \mathbf{A}^\star$.

D *1.* On the one hand $y \mapsto y^\star$ is an isomorphism of $\mathbf{A}$ over $\mathbf{A}^\star$, and on the other hand every generator set is the first component of a coordinate system. Let us take a look at the surjectivity. As $\mathbf{A}$ is faithful we can assume that $\mathbf{k} \subseteq \mathbf{A}$. Let $\mathfrak{a}$ be the ideal of $\mathbf{k}$ generated by the $\lambda(y_i)$'s. Equality (5) gives the membership $1 = \sum_i \lambda(y_i)x_i \in \mathfrak{a}\mathbf{A}$. As $\mathbf{A}$ is integral over $\mathbf{k}$, the Lying Over (Lemma 3.12) shows that $1 \in \mathfrak{a}$.

2. Equality (5) gives $\alpha = \sum_i \alpha(x_i)y_i^\star$ for $\alpha \in \mathbf{A}^\star$. This proves that $y \mapsto y^\star$ is surjective. Moreover, if $x^\star = 0$, then we have $\lambda(xy_i) = 0$, then $x = 0$. Thus λ is dualizing.
Finally, the equality $\alpha = \sum_i \alpha(x_i)y_i^\star$ with $\alpha = x^\star$ gives $x^\star = \sum_i \lambda(x_i x)y_i^\star$, and since $z \mapsto z^\star$ is a $\mathbf{k}$-isomorphism, $x = \sum_i \lambda(x_i x)y_i$.

3. *a* $\Leftrightarrow$ *b.* "λ is dualizing" means that $x \mapsto x^\star$ is an isomorphism, i.e. that λ is an $\mathbf{A}$-basis of $\mathbf{A}^\star$. The implication $c \Rightarrow a$ results from item *2* because a coordinate system is given by $\big((x_i), (y_i^\star)\big)$. □

Examples. See Exercises 10 to 12 and Problem 2.

1) If $f \in \mathbf{k}[X]$ is monic, the algebra $\mathbf{k}[x] = \mathbf{k}[X]/\langle f(X)\rangle$ is a Frobenius algebra (Exercise 11).

2) The algebra $\mathbf{k}[x, y] = \mathbf{k}[X, Y]/\big\langle X^2, Y^2, XY\big\rangle$ is not a Frobenius algebra (Exercise 12). ■

Scalar extension

5.3. Fact. (Stability of the dualizing forms by scalar extension)
Consider two $\mathbf{k}$*-algebras* $\mathbf{k}'$ *and* $\mathbf{A}$ *and let* $\mathbf{A}' = \mathbf{k}' \otimes_{\mathbf{k}} \mathbf{A}$.
If the form $\alpha \in \mathrm{L}_{\mathbf{k}}(\mathbf{A}, \mathbf{k})$ *is dualizing, so is the form* $\alpha' \in \mathrm{L}_{\mathbf{k}'}(\mathbf{A}', \mathbf{k}')$ *obtained by scalar extension.*
Consequently, scalar extension preserves the Frobenius property of an algebra.

Transitivity for dualizing forms

5.4. Fact. *Let* $\mathbf{A}$ *be a strictly finite* $\mathbf{k}$*-algebra,* $\mathbf{B}$ *be a strictly finite* $\mathbf{A}$*-algebra,* $\beta \in \mathrm{L}_{\mathbf{A}}(\mathbf{B}, \mathbf{A})$ *and* $\alpha \in \mathrm{L}_{\mathbf{k}}(\mathbf{A}, \mathbf{k})$.

1. *If* α *and* β *are dualizing, so is* $\alpha \circ \beta$.
2. *If* $\alpha \circ \beta$ *is dualizing and* β *is surjective (for instance* $\mathbf{B}$ *is faithful and* β *is dualizing), then* α *is dualizing.*

D If $\big((a_i), (\alpha_i)\big)$ is a coordinate system of $\mathbf{A}/\mathbf{k}$ and $\big((b_j), (\beta_j)\big)$ is a coordinate system of $\mathbf{B}/\mathbf{A}$, then $\big((a_i b_j), (\alpha_i \circ \beta_j)\big)$ is a coordinate system of $\mathbf{B}/\mathbf{k}$.

1. For $a \in \mathbf{A}$, $b \in \mathbf{B}$, $\eta \in \mathrm{L}_{\mathbf{k}}(\mathbf{A}, \mathbf{k})$ and $\epsilon \in \mathrm{L}_{\mathbf{A}}(\mathbf{B}, \mathbf{A})$ we can easily verify that $ab \centerdot (\eta \circ \epsilon) = (a \centerdot \eta) \circ (b \centerdot \epsilon)$.
Since α is dualizing, we have $u_i \in \mathbf{A}$ such that $u_i \centerdot \alpha = \alpha_i$ for $i \in [\![1..n]\!]$.
Since β is dualizing, we have $v_j \in \mathbf{B}$ such that $v_j \centerdot \beta = \beta_j$ for $j \in [\![1..m]\!]$.
Then, $u_i v_j \centerdot (\alpha \circ \beta) = \alpha_i \circ \beta_j$, and this shows that $\alpha \circ \beta$ is dualizing.

2. Let $\alpha' \in \mathrm{L}_{\mathbf{k}}(\mathbf{A}, \mathbf{k})$, which we aim to express in the form $a \centerdot \alpha$. Note that for every $b_0 \in \mathbf{B}$, we have $\big(b_0 \centerdot (\alpha' \circ \beta)\big)|_{\mathbf{A}} = \beta(b_0) \centerdot \alpha'$; in particular, if $\beta(b_0) = 1$, then $\big(b_0 \centerdot (\alpha' \circ \beta)\big)|_{\mathbf{A}} = \alpha'$. Since $\alpha \circ \beta$ is dualizing, there exists a $b \in \mathbf{B}$ such that $\alpha' \circ \beta = b \centerdot (\alpha \circ \beta)$. By multiplying this equality by $b_0 \centerdot$, we obtain, by restricting to $\mathbf{A}$, $\alpha' = \big((b_0 b) \centerdot (\alpha \circ \beta)\big)|_{\mathbf{A}} = \beta(b_0 b) \centerdot \alpha$. □

Strictly étale algebras

The following theorem is an immediate corollary of Theorem 5.2.

5.5. Theorem. (Characterization of strictly étale algebras) *Let* $\mathbf{A}$ *be a strictly finite* $\mathbf{k}$*-algebra. For* $x \in \mathbf{A}$*, let* $x^\star = x \centerdot \mathrm{Tr}_{\mathbf{A}/\mathbf{k}} \in \mathbf{A}^\star$.

1. *If* $\mathbf{A}$ *is strictly étale, then for every generator set* $(x_i)_{i \in [\![1..n]\!]}$*, there exists a system* $(y_i)_{i \in [\![1..n]\!]}$ *such that we have*
$$\sum\nolimits_{i=1}^{n} y_i^\star \otimes x_i = \mathrm{Id}_{\mathbf{A}}, \quad \textit{i.e.} \quad \forall x \in \mathbf{A},\ x = \sum\nolimits_{i=1}^{n} \mathrm{Tr}_{\mathbf{A}/\mathbf{k}}(x y_i) x_i. \quad (6)$$
Such a pair $\big((x_i), (y_i)\big)$ *is called a* trace system of coordinates*.*
In addition, if $\mathbf{A}$ *is faithful,* $\mathrm{Tr}_{\mathbf{A}/\mathbf{k}}$ *is surjective.*
2. *Conversely, if we have a pair* $\big((x_i)_{i \in [\![1..n]\!]}, (y_i)_{i \in [\![1..n]\!]}\big)$ *that satisfies* (6)*, then* $\mathbf{A}$ *is strictly étale, and we have* $\sum_i x_i^\star \otimes y_i = \mathrm{Id}_{\mathbf{A}}$.
3. *The following properties are equivalent.*
   - *a.* $\mathrm{Tr}_{\mathbf{A}/\mathbf{k}}$ *is dualizing (i.e.* $\mathbf{A}$ *is strictly étale).*
   - *b.* $\mathrm{Tr}_{\mathbf{A}/\mathbf{k}}$ *is a basis of the* $\mathbf{A}$*-module* $\mathbf{A}^\star$ *(which is therefore free of rank* 1*).*
   - *c.* $\mathrm{Tr}_{\mathbf{A}/\mathbf{k}}$ *generates the* $\mathbf{A}$*-module* $\mathbf{A}^\star$.

Scalar extension

The following fact extends Facts 3.11 and 5.3.

5.6. Fact. *Consider two* $\mathbf{k}$*-algebras* $\mathbf{k}'$ *and* $\mathbf{A}$ *and let* $\mathbf{A}' = \mathbf{k}' \otimes_{\mathbf{k}} \mathbf{A}$*.*

1. *If* $\mathbf{A}$ *is strictly étale over* $\mathbf{k}$*, then* $\mathbf{A}'$ *is strictly étale over* $\mathbf{k}'$*.*
2. *If* $\mathbf{k}'$ *is strictly finite and contains* $\mathbf{k}$*, and if* $\mathbf{A}'$ *is strictly étale over* $\mathbf{k}'$*, then* $\mathbf{A}$ *is strictly étale over* $\mathbf{k}$*.*

D *1.* Left to the reader.

2. First assume that $\mathbf{A}$ is free over $\mathbf{k}$. Let $\Delta = \mathrm{Disc}_{\mathbf{A}/\mathbf{k}} = \mathrm{disc}_{\mathbf{A}/\mathbf{k}}(\underline{e}) \in \mathbf{k}$ for a basis $\underline{e}$ of $\mathbf{A}$ over $\mathbf{k}$. By scalar extension we obtain the equality $\Delta = \mathrm{Disc}_{\mathbf{A}'/\mathbf{k}'} \in \mathbf{k}'$. If Δ is invertible in $\mathbf{k}'$ it is invertible in $\mathbf{k}$ by Lemma 4.3. In the general case we reduce it back to the previous case by localization at comaximal elements of $\mathbf{k}$. □

Transitivity for strictly étale algebras

5.7. Fact. *Let* $\mathbf{A}$ *be a strictly finite* $\mathbf{k}$*-algebra and* $\mathbf{B}$ *be a strictly finite* $\mathbf{A}$*-algebra.*

1. *If* $\mathbf{A}$ *is strictly étale over* $\mathbf{k}$*, then* $\mathbf{B}$ *is strictly étale over* $\mathbf{k}$*.*
2. *If* $\mathbf{B}$ *is strictly étale over* $\mathbf{k}$ *and faithful over* $\mathbf{A}$*, then* $\mathbf{A}$ *is strictly étale over* $\mathbf{k}$*.*

D Results from Facts 5.4 and 4.4. □

Separability and nilpotency

5.8. Theorem. *Let* $\mathbf{A}$ *be a strictly étale* $\mathbf{k}$*-algebra.*

1. *If* $\mathbf{k}$ *is reduced, then so is* $\mathbf{A}$*.*
2. *The ideal* $\mathrm{D}_{\mathbf{A}}(0)$ *is generated by the image of* $\mathrm{D}_{\mathbf{k}}(0)$ *in* $\mathbf{A}$*.*
3. *If* $\mathbf{k}'$ *is a reduced* $\mathbf{k}$*-algebra,* $\mathbf{A}' = \mathbf{k}' \otimes_{\mathbf{k}} \mathbf{A}$ *is reduced.*

D *1.* We reason more or less as for the case where $\mathbf{k}$ is a discrete field (Fact 1.3). First suppose that $\mathbf{A}$ is free over $\mathbf{k}$. Let $a \in \mathrm{D}_{\mathbf{A}}(0)$.

For all $x \in \mathbf{A}$ multiplication by ax is a nilpotent endomorphism μ_{ax} of $\mathbf{A}$. Its matrix is nilpotent so the coefficients of its characteristic polynomial are nilpotent (see for example Exercise II-2), therefore null since $\mathbf{k}$ is reduced. In particular, $\mathrm{Tr}_{\mathbf{A}/\mathbf{k}}(ax) = 0$. Thus a is in the kernel of the $\mathbf{k}$-linear map $tr : a \mapsto \big(x \mapsto \mathrm{Tr}_{\mathbf{A}/\mathbf{k}}(ax)\big)$. However, tr is an isomorphism by hypothesis so $a = 0$.

In the general case we reduce it to the case where $\mathbf{A}$ is free over $\mathbf{k}$ by the local structure theorem for finitely generated projective modules (taking into account Fact 5.6 *1*).

Item *3* results from *1* and from Fact 5.6 *1*. Item *2* results from *3*, when we consider $\mathbf{k}' = \mathbf{k}_{\mathrm{red}}$. □

The same technique proves the following lemma.

5.9. Lemma. *If $\mathbf{A}$ is strictly finite over $\mathbf{k}$ and if $a \in \mathbf{A}$ is nilpotent, the coefficients of $\mathrm{F}_{\mathbf{A}/\mathbf{k}}(a)(T)$ are nilpotent (except the constant coefficient).*

Tensor products

If ϕ and ϕ' are two symmetric bilinear forms over M and M', we define a symmetric bilinear form over $M \otimes_{\mathbf{k}} M'$, denoted $\phi \otimes \phi'$, by

$$(\phi \otimes \phi')(x \otimes x', y \otimes y') = \phi(x, y)\phi'(x', y').$$

5.10. Proposition. (Tensor product of two non-degenerate forms)
Let M, M' be two finitely generated projective $\mathbf{k}$-modules and $\mathbf{A}$, $\mathbf{A}'$ two strictly finite $\mathbf{k}$-algebras.

1. *If ϕ over M and ϕ' over M' are two non-degenerate symmetric bilinear forms, so is $\phi \otimes \phi'$.*
2. *If $\lambda \in \mathbf{A}^\star$ and $\lambda' \in \mathbf{A}'^\star$ are two dualizing $\mathbf{k}$-linear forms, so is $\lambda \otimes \lambda' \in (\mathbf{A} \otimes_{\mathbf{k}} \mathbf{A}')^\star$.*

D *1.* The canonical $\mathbf{k}$-linear map $M^\star \otimes_{\mathbf{k}} M'^\star \to (M \otimes_{\mathbf{k}} M')^\star$ is an isomorphism since M, M' are finitely generated projective. Let $\varphi : M \to M^\star$ be the isomorphism associated with ϕ, and $\varphi' : M' \to M'^\star$ be the one associated with ϕ'. The morphism associated with $\phi \otimes \phi'$ is composed of two isomorphisms, so it is an isomorphism

$$\begin{tikzcd}
M \otimes_{\mathbf{k}} M' \arrow[rr] \arrow[dr, "\varphi\otimes\varphi'"'] & & (M \otimes_{\mathbf{k}} M')^\star \\
& M^\star \otimes_{\mathbf{k}} M'^\star \arrow[ur, "\text{can. iso.}"'] &
\end{tikzcd}$$

2. Results from $\Phi_{\lambda\otimes\lambda'} = \Phi_\lambda \otimes \Phi_{\lambda'}$. □

The previous proposition and Lemma V-8.10 give the following result.

5.11. Corollary. *Let $\mathbf{A}$ and $\mathbf{C}$ be two strictly finite $\mathbf{k}$-algebras. Then*

$$\Phi_{\mathrm{Tr}_{(\mathbf{A}\otimes_{\mathbf{k}}\mathbf{C})/\mathbf{k}}} = \Phi_{\mathrm{Tr}_{\mathbf{A}/\mathbf{k}}} \otimes \Phi_{\mathrm{Tr}_{\mathbf{C}/\mathbf{k}}}.$$

In particular, $\mathbf{A} \otimes_{\mathbf{k}} \mathbf{C}$ is strictly étale if $\mathbf{A}$ and $\mathbf{C}$ are strictly étale. (For the precise computation of the discriminant, see Exercise 7.)

Integral elements, idempotents, diagonalization

The following theorem is a subtle consequence of the remarkable Lemma III-8.5. It will be useful in the context of Galois theory for Theorem VII-6.4.

5.12. Theorem. *Let $\rho : \mathbf{k} \to \mathbf{k}'$ be an injective ring homomorphism with $\mathbf{k}$ integrally closed in $\mathbf{k}'$, and $\mathbf{A}$ be a strictly étale $\mathbf{k}$-algebra. By scalar extension we obtain $\mathbf{A}' = \rho_\star(\mathbf{A}) \simeq \mathbf{k}' \otimes_{\mathbf{k}} \mathbf{A}$ strictly étale over $\mathbf{k}'$.*

1. *The homomorphism $\mathbf{A} \to \mathbf{A}'$ is injective.*
2. *The ring $\mathbf{A}$ is integrally closed in $\mathbf{A}'$.*
3. *Every idempotent of $\mathbf{A}'$ is in $\mathbf{A}$.*

D Item *3* is a special case of item *2*.

1. Apply the local structure theorem for finitely generated projective modules and the local-global principle II-6.7 for exact sequences.

2. We can identify $\mathbf{k}$ with a subring of $\mathbf{k}'$ and $\mathbf{A}$ with a subring of $\mathbf{A}'$. Recall that $\mathbf{A}$ is finite, therefore integral over $\mathbf{k}$. It suffices to treat the case where $\mathbf{A}$ is free over $\mathbf{k}$ (local structure theorem for finitely generated projective modules and local-global principle III-8.9 for integral elements). Let $(\underline{e}) = (e_1, \dots, e_n)$ be a basis of $\mathbf{A}$ over $\mathbf{k}$ and $(\underline{h})$ the dual basis with respect to the trace form. If $n = 0$ or $n = 1$ the result is obvious.
Suppose $n \geqslant 2$. Note that $(\underline{e})$ is also a basis of $\mathbf{A}'$ over $\mathbf{k}'$. In addition, since, for $a \in \mathbf{A}$, the endomorphisms $\mu_{\mathbf{A},a}$ and $\mu_{\mathbf{A}',a}$ have the same matrix over $(\underline{e})$, the trace form over $\mathbf{A}'$ is an extension of the trace form over $\mathbf{A}$ and $(\underline{h})$ remains the dual basis relative to the trace form in $\mathbf{A}'$. Let $x = \sum_i x_i e_i$ be an integral element of $\mathbf{A}'$ over $\mathbf{A}$ ($x_i \in \mathbf{k}'$). We must prove that the x_i's are in $\mathbf{k}$, or (which amounts to the same thing) integral over $\mathbf{k}$. However, xh_i is integral over $\mathbf{k}$. The matrix of $\mu_{\mathbf{A}',xh_i}$ is therefore an integral element of $\mathbb{M}_n(\mathbf{k}')$ over $\mathbf{k}$. Therefore the coefficients of its characteristic polynomial are integral over $\mathbf{k}$ (Lemma III-8.5), so in $\mathbf{k}$, and in particular $x_i = \mathrm{Tr}_{\mathbf{A}'/\mathbf{k}'}(xh_i) \in \mathbf{k}$. □

5.13. Lemma. *The cartesian product $\mathbf{k}^n$ is a strictly étale $\mathbf{k}$-algebra. The discriminant of the canonical basis is equal to 1. If $\mathbf{k}$ is a nontrivial connected ring, this $\mathbf{k}$-algebra has exactly n characters and $n!$ automorphisms (those that we spot at first sight).*

D The assertion regarding the discriminant is clear (Proposition II-5.34). We obviously have as the characters the n natural projections $\pi_i : \mathbf{k}^n \to \mathbf{k}$ over each of the factors, and as the $\mathbf{k}$-automorphisms the $n!$ automorphisms obtained by permuting the coordinates. Let e_i be the idempotent defined by $\operatorname{Ker} \pi_i = \langle 1 - e_i \rangle$. If $\pi : \mathbf{k}^n \to \mathbf{k}$ is a character, the $\pi(e_i)$'s form a fundamental system of orthogonal idempotents of $\mathbf{k}$. Since $\mathbf{k}$ is nontrivial and connected, all but one are null, $\pi(e_j) = 1$ for example. Then, $\pi = \pi_j$, because they are $\mathbf{k}$-linear maps that coincide over the e_i's. Finally, as a consequence every $\mathbf{k}$-automorphism of $\mathbf{k}^n$ permutes the e_i's. □

5.14. Definition. *(Diagonal algebras)*

1. A $\mathbf{k}$-algebra is said to be *diagonal* if it is isomorphic to a product algebra $\mathbf{k}^n$ for some $n \in \mathbb{N}$. In particular, it is strictly étale.
2. Let $\mathbf{A}$ be a strictly étale $\mathbf{k}$-algebra and $\mathbf{L}$ be a $\mathbf{k}$-algebra. We say that $\mathbf{L}$ *diagonalizes* $\mathbf{A}$ if $\mathbf{L} \otimes_{\mathbf{k}} \mathbf{A}$ is a diagonal $\mathbf{L}$-algebra.

5.15. Fact. (Monogenic diagonal algebras)
Let $f \in \mathbf{k}[X]$ be a monic polynomial of degree n and $\mathbf{A} = \mathbf{k}[X]/\langle f \rangle$.

1. *The $\mathbf{k}$-algebra $\mathbf{A}$ is diagonal if and only if f is separable and can be decomposed into linear factors in $\mathbf{k}[X]$.*
2. *In this case, if $\mathbf{k}$ is nontrivial connected, f admits exactly n zeros in $\mathbf{k}$, and the decomposition of f is unique up to the order of the factors.*
3. *A $\mathbf{k}$-algebra $\mathbf{L}$ diagonalizes $\mathbf{A}$ if and only if* $\mathrm{disc}(f)$ *is invertible in $\mathbf{L}$ and f can be decomposed into linear factors in $\mathbf{L}[X]$.*

D *1.* If f is separable and can be completely factorized, we have an isomorphism $\mathbf{A} \simeq \mathbf{k}^n$ by the Lagrange interpolation theorem (Exercise III-1). Let us show the converse. Every character $\mathbf{k}[X] \to \mathbf{k}$ is an evaluation homomorphism, so every character $\mathbf{A} \to \mathbf{k}$ is the evaluation at a zero of f in $\mathbf{k}$. Thus the isomorphism given in the hypothesis is of the form

$$\overline{g} \mapsto \big(g(x_1), \ldots, g(x_n)\big) \quad (x_i \in \mathbf{k} \text{ and } f(x_i) = 0).$$

Then let g_i satisfy $g_i(x_i) = 1$ and, for $j \neq i$, $g_i(x_j) = 0$. For $j \neq i$, the element $x_i - x_j$ divides $g_i(x_i) - g_i(x_j) = 1$, so $x_i - x_j$ is invertible. This implies that $f = \prod_{i=1}^{n}(X - x_i)$ (again by Lagrange).

2. With the previous notations we must show that the only zeros of f in $\mathbf{k}$ are the x_i's. A zero of f corresponds to a character $\pi : \mathbf{A} \to \mathbf{k}$. We therefore must prove that $\mathbf{k}^n$ does not admit any other character than the projections over each factor. However, this has been proven in Lemma 5.13.

3. Apply item *1* to the $\mathbf{L}$-algebra $\mathbf{L} \otimes_{\mathbf{k}} \mathbf{A} \simeq \mathbf{L}[X]/\langle f \rangle$. □

Remarks.

1) Item *2* requires $\mathbf{k}$ to be connected.

2) (Exercise left to the reader) If $\mathbf{k}$ is a discrete field and if A is a matrix of $\mathbb{M}_n(\mathbf{k})$, saying that $\mathbf{L}$ diagonalizes $\mathbf{k}[A]$ means that this matrix is "diagonalizable" in $\mathbb{M}_n(\mathbf{L})$, in the (weak) sense that $\mathbf{L}^n$ is a direct sum of the eigen-subspaces of A.

3) The decomposition of a ring $\mathbf{A}$ into a finite product of nonzero connected rings, when possible, is unique up to the order of the factors. Each connected factor, isomorphic to a localized ring $\mathbf{A}[1/e]$, corresponds in fact to an *indecomposable* idempotent e.[6] This can be understood to be a consequence

[6] The idempotent e is said to be indecomposable if the equality $e = e_1 + e_2$ with e_1, e_2 being idempotents and $e_1 e_2 = 0$ implies $e_1 = 0$ or $e_2 = 0$.

of the structure theorem for finite Boolean algebras (see Theorem VII-3.3). We can also obtain the result by reasoning with a fundamental system of orthogonal idempotents as in the proof of Lemma 5.13.

4) In item *2*, the “nontrivial” hypothesis gives a more common statement. Without this hypothesis we would have said in the first part of the sentence: every zero of f is given by one of the x_i’s corresponding to the assumed decomposition of f into linear factors.

5) For the most part the previous fact is a more abstract reformulation of the Lagrange interpolation theorem. ■

5.16. Proposition. *Let* $\mathbf{K}$ *be a separably factorial discrete field and* $\mathbf{B}$ *be a strictly finite* $\mathbf{K}$*-algebra. Then,* $\mathbf{B}$ *is étale if and only if it is diagonalized by an overfield of* $\mathbf{K}$ *étale over* $\mathbf{K}$.

D Suppose $\mathbf{B}$ is étale. It is isomorphic to a product of fields $\mathbf{K}_i$ étale over $\mathbf{K}$ (Theorem 1.11) and there exists a field $\mathbf{L}$ étale over $\mathbf{K}$, which is a Galois extension that contains a copy of each $\mathbf{K}_i$ (Corollary 1.14). We easily see that $\mathbf{L}$ diagonalizes $\mathbf{B}$.

Suppose that a field $\mathbf{L}$ étale over $\mathbf{K}$ diagonalizes $\mathbf{B}$. Then, $\mathrm{Disc}_{\mathbf{B}/\mathbf{K}}$ is invertible in $\mathbf{L}$ therefore in $\mathbf{K}$, so $\mathbf{B}$ is étale. □

6. Separable algebras, separability idempotent

The results in this section will be used in Section 7 devoted to Galois algebras, but only for Theorem 7.19 which establishes the Galois correspondence in the connected case. Moreover, they are also very useful when studying modules of differentials. Here we will limit ourselves to speaking of derivations.

6.1. Definitions and notations. Let $\mathbf{A}$ be a $\mathbf{k}$-algebra.

1. The algebra $\mathbf{A} \otimes_{\mathbf{k}} \mathbf{A}$, called the *enveloping algebra* of $\mathbf{A}$, is denoted by $\mathbf{A}^{\mathrm{e}}_{\mathbf{k}}$.
2. This $\mathbf{k}$-algebra possesses two natural $\mathbf{A}$-algebra structures, respectively given by the homomorphisms $g_{\mathbf{A}/\mathbf{k}} : a \mapsto a \otimes 1$ (left-structure) and $d_{\mathbf{A}/\mathbf{k}} : a \mapsto 1 \otimes a$ (right-structure). We will use the following abbreviated notation for the two corresponding $\mathbf{A}$-module structures. For $a \in \mathbf{A}$ and $\gamma \in \mathbf{A}^{\mathrm{e}}_{\mathbf{k}}$,
$$a \cdot \gamma \,=\, g_{\mathbf{A}/\mathbf{k}}(a)\gamma \,=\, (a \otimes 1)\gamma \quad \text{and} \quad \gamma \cdot a \,=\, d_{\mathbf{A}/\mathbf{k}}(a)\gamma \,=\, \gamma(1 \otimes a).$$
3. We will denote by $\mathrm{J}_{\mathbf{A}/\mathbf{k}}$ (or J if the context is clear) the ideal of $\mathbf{A}^{\mathrm{e}}_{\mathbf{k}}$ generated by the elements of the form $a \otimes 1 - 1 \otimes a = a \cdot 1_{\mathbf{A}^{\mathrm{e}}_{\mathbf{k}}} - 1_{\mathbf{A}^{\mathrm{e}}_{\mathbf{k}}} \cdot a$.
4. We also introduce the following $\mathbf{k}$-linear maps
$$\Delta_{\mathbf{A}/\mathbf{k}} : \mathbf{A} \to \mathrm{J}_{\mathbf{A}/\mathbf{k}}, \quad a \mapsto a \otimes 1 - 1 \otimes a. \tag{7}$$
$$\mu_{\mathbf{A}/\mathbf{k}} \,:\, \mathbf{A}^{\mathrm{e}}_{\mathbf{k}} \to \mathbf{A},\ a \otimes b \mapsto ab \quad \text{(multiplication)} \tag{8}$$

5. In the case where $\mathbf{A}$ is a finitely generated $\mathbf{k}$-algebra, $\mathbf{A} = \mathbf{k}[x_1, \ldots, x_n]$, the same holds for $\mathbf{A}^{\mathrm{e}}_{\mathbf{k}}$ and we have the following possible description of the previous objects.
   - $\mathbf{A}^{\mathrm{e}}_{\mathbf{k}} = \mathbf{k}[y_1, \ldots, y_n, z_1, \ldots, z_n] = \mathbf{k}[\underline{y}, \underline{z}]$ with $y_i = x_i \otimes 1$, $z_i = 1 \otimes x_i$.
   - For $a = a(\underline{x}) \in \mathbf{A}$, and $h(\underline{y}, \underline{z}) \in \mathbf{k}[\underline{y}, \underline{z}]$, we have
     - $g_{\mathbf{A}/\mathbf{k}}(a) = a(\underline{y})$, $d_{\mathbf{A}/\mathbf{k}}(a) = a(\underline{z})$,
     - $a \cdot h = a(\underline{y})h(\underline{y}, \underline{z})$, $h \cdot a = a(\underline{z})h(\underline{y}, \underline{z})$,
     - $\Delta_{\mathbf{A}/\mathbf{k}}(a) = a(\underline{y}) - a(\underline{z})$,
     - and $\mu_{\mathbf{A}/\mathbf{k}}(h) = h(\underline{x}, \underline{x})$.
   - $\mathrm{J}_{\mathbf{A}/\mathbf{k}}$ is the ideal of $\mathbf{k}[\underline{y}, \underline{z}]$ generated by the $(y_i - z_i)$'s.
6. Finally, in the case where $\mathbf{A} = \mathbf{k}[X_1, \ldots, X_n]/\langle f_1, \ldots, f_s\rangle = \mathbf{k}[\underline{x}]$, in other words when $\mathbf{A}$ is a finitely presented $\mathbf{k}$-algebra, the same holds for $\mathbf{A}^{\mathrm{e}}_{\mathbf{k}}$ (see Theorem 3.9).
$$\mathbf{A}^{\mathrm{e}}_{\mathbf{k}} = \mathbf{k}[Y_1, \ldots, Y_n, Z_1, \ldots, Z_n]/\big\langle \underline{f}(\underline{Y}), \underline{f}(\underline{Z})\big\rangle = \mathbf{k}[\underline{y}, \underline{z}].$$

Note that $\mu_{\mathbf{A}/\mathbf{k}}(a \cdot \gamma) = a\mu_{\mathbf{A}/\mathbf{k}}(\gamma) = \mu_{\mathbf{A}/\mathbf{k}}(\gamma \cdot a)$ for $\gamma \in \mathbf{A}^{\mathrm{e}}_{\mathbf{k}}$ and $a \in \mathbf{A}$.

Towards the separability idempotent

6.2. Fact.

1. *The map* $\mu_{\mathbf{A}/\mathbf{k}}$ *is a character of* $\mathbf{A}$*-algebras (for the two structures).*
2. *We have* $\mathrm{J}_{\mathbf{A}/\mathbf{k}} = \mathrm{Ker}(\mu_{\mathbf{A}/\mathbf{k}})$. *So* $\mathbf{A} \simeq \mathbf{A}^{\mathrm{e}}_{\mathbf{k}}\big/\mathrm{J}_{\mathbf{A}/\mathbf{k}}$ *and*
$$\mathbf{A}^{\mathrm{e}}_{\mathbf{k}} = (\mathbf{A} \otimes 1) \oplus \mathrm{J}_{\mathbf{A}/\mathbf{k}} = (1 \otimes \mathbf{A}) \oplus \mathrm{J}_{\mathbf{A}/\mathbf{k}},$$
and $\mathrm{J}_{\mathbf{A}/\mathbf{k}}$ *is the left- (or right-)* $\mathbf{A}$*-module generated by* $\mathrm{Im}\,\Delta_{\mathbf{A}/\mathbf{k}}$.
3. *In the case where* $\mathbf{A} = \mathbf{k}[X_1, \ldots, X_n]/\langle f_1, \ldots, f_s\rangle = \mathbf{k}[\underline{x}]$ *we obtain*
$$\mathbf{k}[\underline{y}, \underline{z}] = \mathbf{k}[\underline{y}] \oplus \langle y_1 - z_1, \ldots, y_n - z_n\rangle = \mathbf{k}[\underline{z}] \oplus \langle y_1 - z_1, \ldots, y_n - z_n\rangle\,.$$

D The inclusion $\mathrm{J}_{\mathbf{A}/\mathbf{k}} \subseteq \mathrm{Ker}(\mu_{\mathbf{A}/\mathbf{k}})$ is clear. Denoting $\Delta_{\mathbf{A}/\mathbf{k}}$ by Δ, we have
$$\textstyle\sum_i a_i \otimes b_i = \big(\sum_i a_i b_i\big) \otimes 1 - \sum_i a_i \cdot \Delta(b_i) = 1 \otimes \big(\sum_i a_i b_i\big) - \sum_i \Delta(a_i) \cdot b_i.$$
We deduce that $\mathrm{Ker}(\mu_{\mathbf{A}/\mathbf{k}})$ is the (left- or right-) $\mathbf{A}$-module generated by $\mathrm{Im}\,\Delta$ and therefore that it is contained in $\mathrm{J}_{\mathbf{A}/\mathbf{k}}$.
The result follows by IV-2.7. □

Example. For $\mathbf{A} = \mathbf{k}[X]$, we have $\mathbf{A}^{\mathrm{e}}_{\mathbf{k}} \simeq \mathbf{k}[Y, Z]$ with the homomorphisms
$$\begin{aligned} h(X) &\mapsto h(Y) && \text{(on the left-hand side) and} \\ h(X) &\mapsto h(Z) && \text{(on the right-hand side),} \end{aligned}$$
so $h \cdot g = h(Y)g$ and $g \cdot h = h(Z)g$. We also have
$$\Delta_{\mathbf{A}/\mathbf{k}}(h) = h(Y) - h(Z),\ \mu_{\mathbf{A}/\mathbf{k}}\big(g(Y, Z)\big) = g(X, X) \text{ and } \mathrm{J}_{\mathbf{A}/\mathbf{k}} = \langle Y - Z\rangle\,.$$
We see that $\mathrm{J}_{\mathbf{A}/\mathbf{k}}$ is free with $Y - Z$ as its basis over $\mathbf{A}^{\mathrm{e}}_{\mathbf{k}}$, and as a left-$\mathbf{A}$-module, it is free with basis $\big((Y - Z)Z^n\big)_{n\in\mathbb{N}}$. ■

6.3. Fact. *We write Δ to denote $\Delta_{\mathbf{A}/\mathbf{k}}$.*

1. *For $a, b \in \mathbf{A}$ we have $\Delta(ab) = \Delta(a) \cdot b + a \cdot \Delta(b)$. More generally,*
$$\begin{aligned}\Delta(a_1 \cdots a_n) \;=\; & \Delta(a_1) \cdot a_2 \cdots a_n + a_1 \cdot \Delta(a_2) \cdot a_3 \cdots a_n + \cdots \\ & + a_1 \cdots a_{n-2} \cdot \Delta(a_{n-1}) \cdot a_n + a_1 \cdots a_{n-1} \cdot \Delta(a_n).\end{aligned}$$
2. *If $\mathbf{A}$ is a finitely generated $\mathbf{k}$-algebra, generated by $(x_1, \ldots, x_r)$, $\mathrm{J}_{\mathbf{A}/\mathbf{k}}$ is a finitely generated ideal of $\mathbf{A}^{\mathrm{e}}_{\mathbf{k}}$, generated by $(\Delta(x_1), \ldots, \Delta(x_r))$.*
3. *Over the ideal $\mathrm{Ann}(\mathrm{J}_{\mathbf{A}/\mathbf{k}})$, the two structures of $\mathbf{A}$-modules, on the left- and right-hand sides, coincide. In addition, for $\alpha \in \mathrm{Ann}(\mathrm{J}_{\mathbf{A}/\mathbf{k}})$ and $\gamma \in \mathbf{A}^{\mathrm{e}}_{\mathbf{k}}$, we have*
$$\gamma\alpha = \mu_{\mathbf{A}/\mathbf{k}}(\gamma) \cdot \alpha = \alpha \cdot \mu_{\mathbf{A}/\mathbf{k}}(\gamma). \tag{9}$$

D *1.* Immediate computation. Item *2* results from it since $\mathrm{J}_{\mathbf{A}/\mathbf{k}}$ is the ideal generated by the image of Δ, and since for every "monomial" in the generators, for example $x^3y^4z^2$, $\Delta(x^3y^4z^2)$, is equal to a linear combination (with coefficients in $\mathbf{A}^{\mathrm{e}}_{\mathbf{k}}$) of the images of the generators $\Delta(x)$, $\Delta(y)$ and $\Delta(z)$.

3. The ideal $\mathfrak{a} = \mathrm{Ann}(\mathrm{J}_{\mathbf{A}/\mathbf{k}})$ is an $\mathbf{A}^{\mathrm{e}}_{\mathbf{k}}$-module, so it is stable for the two $\mathbf{A}$-module laws. Let us show that these two structures coincide. If $\alpha \in \mathfrak{a}$, for every $a \in \mathbf{A}$ we have $0 = \alpha(a \cdot 1 - 1 \cdot a) = a \cdot \alpha - \alpha \cdot a$.
Equality (9) stems from the fact that $\gamma - \mu_{\mathbf{A}/\mathbf{k}}(\gamma) \cdot 1$ and $\gamma - 1 \cdot \mu_{\mathbf{A}/\mathbf{k}}(\gamma)$ are in $\mathrm{Ker}\, \mu_{\mathbf{A}/\mathbf{k}} = \mathrm{J}_{\mathbf{A}/\mathbf{k}}$. □

6.4. Lemma. *The ideal $\mathrm{J}_{\mathbf{A}/\mathbf{k}}$ is generated by an idempotent if and only if*
$$1 \in \mu_{\mathbf{A}/\mathbf{k}}\big(\mathrm{Ann}(\mathrm{J}_{\mathbf{A}/\mathbf{k}})\big).$$
Moreover, if $1 = \mu_{\mathbf{A}/\mathbf{k}}(\varepsilon)$ with $\varepsilon \in \mathrm{Ann}(\mathrm{J}_{\mathbf{A}/\mathbf{k}})$, then ε is an idempotent, and we have
$$\mathrm{Ann}(\mathrm{J}_{\mathbf{A}/\mathbf{k}}) = \langle \varepsilon \rangle \;\; \textit{and}\; \mathrm{J}_{\mathbf{A}/\mathbf{k}} = \langle 1 - \varepsilon \rangle\,,$$
such that ε is uniquely determined.

D We omit the $\mathbf{A}/\mathbf{k}$ subscript. If $\mathrm{J} = \langle \varepsilon \rangle$ with an idempotent ε, we obtain the equalities $\mathrm{Ann}(\mathrm{J}) = \langle 1 - \varepsilon \rangle$ and $\mu(1 - \varepsilon) = 1$.
Conversely, suppose that $1 = \mu(\varepsilon)$ with $\varepsilon \in \mathrm{Ann}(\mathrm{J})$. Then $\mu(1 - \varepsilon) = 0$, so $1 - \varepsilon \in \mathrm{J}$, then $(1 - \varepsilon)\varepsilon = 0$, i.e. ε is idempotent.
The equality $1 = (1 - \varepsilon) + \varepsilon$ implies that $\mathrm{Ann}(\mathrm{J}) = \langle \varepsilon \rangle$ and $\mathrm{J} = \langle 1 - \varepsilon \rangle$. □

Bézout matrix of a polynomial system

Let $f_1, \ldots, f_s \in \mathbf{k}[X_1, \ldots, X_n] = \mathbf{k}[\underline{X}]$.

We define the *Bézout matrix* of the system $(\underline{f}) = (f_1, \ldots, f_s)$ in the variables $(Y_1, \ldots, Y_n, Z_1, \ldots, Z_n)$ by

$$\mathrm{BZ}_{\underline{Y},\underline{Z}}(\underline{f}) = (b_{ij})_{i\in[\![1..s]\!], j\in[\![1..n]\!]}, \quad \text{where}$$

$$b_{ij} = \frac{f_i(Z_{1..j-1}, Y_j, Y_{j+1..n}) - f_i(Z_{1..j-1}, Z_j, Y_{j+1..n})}{Y_j - Z_j}.$$

Thus for $n = 2$, $s = 3$:

$$\mathrm{BZ}_{\underline{Y},\underline{Z}}(f_1, f_2, f_3) = \begin{bmatrix} \frac{f_1(Y_1,Y_2)-f_1(Z_1,Y_2)}{Y_1-Z_1} & \frac{f_1(Z_1,Y_2)-f_1(Z_1,Z_2)}{Y_2-Z_2} \\ \frac{f_2(Y_1,Y_2)-f_2(Z_1,Y_2)}{Y_1-Z_1} & \frac{f_2(Z_1,Y_2)-f_2(Z_1,Z_2)}{Y_2-Z_2} \\ \frac{f_3(Y_1,Y_2)-f_3(Z_1,Y_2)}{Y_1-Z_1} & \frac{f_3(Z_1,Y_2)-f_3(Z_1,Z_2)}{Y_2-Z_2} \end{bmatrix}.$$

For $n = 3$, the i^{th} row of the Bézout matrix is

$$\begin{bmatrix} \frac{f_i(Y_1,Y_2,Y_3)-f_i(Z_1,Y_2,Y_3)}{Y_1-Z_1} & \frac{f_i(Z_1,Y_2,Y_3)-f_i(Z_1,Z_2,Y_3)}{Y_2-Z_2} & \frac{f_i(Z_1,Z_2,Y_3)-f_i(Z_1,Z_2,Z_3)}{Y_3-Z_3} \end{bmatrix}.$$

We have the equality

$$\mathrm{BZ}_{\underline{Y},\underline{Z}}(\underline{f}) \cdot \begin{bmatrix} Y_1 - Z_1 \\ \vdots \\ Y_n - Z_n \end{bmatrix} = \begin{bmatrix} f_1(\underline{Y}) - f_1(\underline{Z}) \\ \vdots \\ f_s(\underline{Y}) - f_s(\underline{Z}) \end{bmatrix} \tag{$\star$}$$

In addition $\mathrm{BZ}_{\underline{X},\underline{X}}(\underline{f}) = \mathrm{JAC}_{\underline{X}}(\underline{f})$, the Jacobian matrix of $(f_1, \ldots, f_s)$.

Now consider a finitely generated $\mathbf{k}$-algebra

$$\mathbf{A} = \mathbf{k}[x_1, \ldots, x_n] = \mathbf{k}[\underline{x}],$$

with polynomials f_i satisfying $f_i(\underline{x}) = 0$ for every i. Its enveloping algebra is $\mathbf{A}^{\mathrm{e}}_{\mathbf{k}} = \mathbf{k}[y_1, \ldots, y_n, z_1, \ldots, z_n]$ (using the notation from the beginning of the section).

Then the matrix $\mathrm{BZ}_{\underline{y},\underline{z}}(\underline{f}) \in \mathbb{M}_{s,n}(\mathbf{A}^{\mathrm{e}}_{\mathbf{k}})$ has as its image under $\mu_{\mathbf{A}/\mathbf{k}}$ the Jacobian matrix $\mathrm{JAC}_{\underline{x}}(f_1, \ldots, f_s) \in \mathbb{M}_{s,n}(\mathbf{A})$.

For a minor D of order n of $\mathrm{BZ}_{\underline{y},\underline{z}}(\underline{f})$, Equality ($\star$) shows that $D\,(y_j - z_j) = 0$ for $j \in [\![1..n]\!]$. In other words $D \in \mathrm{Ann}(\mathrm{J}_{\mathbf{A}/\mathbf{k}})$. The Bézout matrix therefore allows us to construct elements of the ideal $\mathrm{Ann}(\mathrm{J}_{\mathbf{A}/\mathbf{k}})$.

In addition, $\delta := \mu_{\mathbf{A}/\mathbf{k}}(D)$ is the corresponding minor in $\mathrm{JAC}_{\underline{x}}(\underline{f})$.

Let us give an application of this theory to the special case when the transposed matrix ${}^{\mathrm{t}}\mathrm{JAC}_{\underline{x}}(\underline{f}) : \mathbf{A}^s \to \mathbf{A}^n$ is surjective, i.e. $1 \in \mathcal{D}_n(\mathrm{JAC}_{\underline{x}}(\underline{f}))$. We therefore have an equality $1 = \sum_{I\in\mathcal{P}_{n,s}} u_I \delta_I$ in $\mathbf{A}$, where δ_I is the minor of the extracted matrix of $\mathrm{JAC}_{\underline{x}}(\underline{f})$ on the rows $i \in I$. By letting $\varepsilon = \sum_{I\in\mathcal{P}_{n,s}} u_I D_I \in \mathbf{A}^{\mathrm{e}}_{\mathbf{k}}$, we obtain $\mu_{\mathbf{A}/\mathbf{k}}(\varepsilon) = 1$ with $\varepsilon \in \mathrm{Ann}(\mathrm{J}_{\mathbf{A}/\mathbf{k}})$.

Recap: ε is what we call the separability idempotent of $\mathbf{A}$, and $\mathbf{A}$ is a separable algebra, notions which will be defined later (Definition 6.10).

Therefore, if $\mathbf{A}$ is a finitely presented $\mathbf{k}$-algebra $\mathbf{k}[\underline{X}]/\langle \underline{f}\rangle$ and if the linear map ${}^{\mathrm{t}}\mathrm{JAC}_{\underline{x}}(\underline{f}) : \mathbf{A}^s \to \mathbf{A}^n$ is surjective, then $\mathbf{A}$ is separable.
More generally, for a finitely presented algebra $\mathbf{A} = \mathbf{k}[\underline{X}]/\langle \underline{f}\rangle$, we will see that $\mathrm{Coker}\left({}^{\mathrm{t}}\mathrm{JAC}_{\underline{x}}(\underline{f})\right)$ and $\mathrm{J}_{\mathbf{A}/\mathbf{k}}/\mathrm{J}^2_{\mathbf{A}/\mathbf{k}}$ are isomorphic $\mathbf{A}$-modules (Theorem 6.7).

Derivations

6.5. Definition. Let $\mathbf{A}$ be a $\mathbf{k}$-algebra and M be an $\mathbf{A}$-module.
We call a $\mathbf{k}$-*derivation of* $\mathbf{A}$ *in* M, a $\mathbf{k}$-linear map $\delta : \mathbf{A} \to M$ which satisfies the Leibniz equality

$$\delta(ab) = a\delta(b) + b\delta(a).$$

We denote by $\mathrm{Der}_{\mathbf{k}}(\mathbf{A}, M)$ the $\mathbf{A}$-module of the $\mathbf{k}$-derivations of $\mathbf{A}$ in M. A derivation with values in $\mathbf{A}$ is “simply” called a derivation of $\mathbf{A}$. When the context is clear, $\mathrm{Der}(\mathbf{A})$ is an abbreviation for $\mathrm{Der}_{\mathbf{k}}(\mathbf{A}, \mathbf{A})$.

Note that $\delta(1) = 0$ because $1^2 = 1$, and so $\delta|_{\mathbf{k}} = 0$.

6.6. Theorem and definition. (Universal derivation)
The context is that of Definition 6.1.

1. *Over* J/J^2 *the two* $\mathbf{A}$*-module structures (on the left- and right-hand sides) coincide.*
2. *The composite map* $\mathrm{d} : \mathbf{A} \to \mathrm{J}/\mathrm{J}^2$*, defined by* $\mathrm{d}(a) = \overline{\Delta(a)}$*, is a* $\mathbf{k}$*-derivation.*
3. *It is a universal* $\mathbf{k}$*-derivation in the following sense.*
   For every $\mathbf{A}$*-module* M *and every* $\mathbf{k}$*-derivation* $\delta : \mathbf{A} \to M$*, there exists a unique* $\mathbf{A}$*-linear map* $\theta : \mathrm{J}/\mathrm{J}^2 \to M$ *such that* $\theta \circ \mathrm{d} = \delta$*.*

$$\begin{tikzcd}
\mathbf{A} \arrow[d, "\mathrm{d}"'] \arrow[rd, "\delta"] & & \mathbf{k}\text{-}\textit{derivations} \\
\mathrm{J}/\mathrm{J}^2 \arrow[r, dashed, "\theta\,!"'] & M & \mathbf{A}\text{-}\textit{linear maps.}
\end{tikzcd}$$

The $\mathbf{A}$*-module* J/J^2*, denoted by* $\Omega_{\mathbf{A}/\mathbf{k}}$*, is called the* module of (Kähler) differentials of $\mathbf{A}$.

D Items *1* and *2* are left to the reader.
3. The uniqueness is clear, let us show the existence.

We define the $\mathbf{k}$-linear map $\tau : \mathbf{A} \otimes_{\mathbf{k}} \mathbf{A} \to M$

$$\begin{tikzcd}
\mathbf{A} \arrow[d, "\Delta"'] \arrow[dr, "\delta"] & \\
\mathbf{A} \otimes_{\mathbf{k}} \mathbf{A} \arrow[r, "\tau"'] & M
\end{tikzcd} \qquad \tau(a \otimes b) = -a\,\delta(b).$$

The diagram commutes and τ is $\mathbf{A}$-linear on the left-hand side.
It remains to see that $\tau(\mathrm{J}^2) = 0$, because θ is then defined by restriction and passage to the quotient of τ. We verify that $\tau(\Delta(a)\Delta(b)) = b\delta(a) + a\delta(b) - \delta(ab) = 0$. □

We now consider the case of a finitely presented algebra

$$\mathbf{A} = \mathbf{k}[X_1, \dots, X_n]/\langle f_1, \dots, f_s \rangle = \mathbf{k}[\underline{x}].$$

We use the notations in 6.1. Recall that the Jacobian matrix of the polynomial system is defined as

$$\mathrm{JAC}_{\underline{X}}(\underline{f}) \;=\; \begin{array}{c|cccc|}
 & X_1 & X_2 & \cdots & X_n \\
f_1 & \frac{\partial f_1}{\partial X_1} & \frac{\partial f_1}{\partial X_2} & \cdots & \frac{\partial f_1}{\partial X_n} \\
f_2 & \frac{\partial f_2}{\partial X_1} & \frac{\partial f_2}{\partial X_2} & \cdots & \frac{\partial f_2}{\partial X_n} \\
f_i & \vdots & & & \vdots \\
 & \vdots & & & \vdots \\
f_s & \frac{\partial f_s}{\partial X_1} & \frac{\partial f_s}{\partial X_2} & \cdots & \frac{\partial f_s}{\partial X_n}
\end{array}\,.$$

In the following theorem, we denote by $\mathrm{Ja} = {}^{\mathrm{t}}\mathrm{JAC}_{\underline{X}}(\underline{f}) : \mathbf{A}^s \to \mathbf{A}^n$ the linear map defined by the transposed matrix, and by $(e_1, \dots, e_n)$ the canonical basis of $\mathbf{A}^n$. We define

$$\begin{aligned}
\delta : \mathbf{A} \to \mathrm{Coker}(\mathrm{Ja}) \quad &: \quad g(\underline{x}) \mapsto \textstyle\sum_{i=1}^n \frac{\partial g}{\partial X_i}(\underline{x})\,\overline{e_i}, \\
\lambda : \mathbf{A}^n \to \mathrm{J}/\mathrm{J}^2 \quad &: \quad e_i \mapsto \mathrm{d}(x_i) = \overline{y_i - z_i}.
\end{aligned}$$

6.7. Theorem. (Universal derivation via the Jacobian)

1. *The map δ is a $\mathbf{k}$-derivation with $\delta(x_i) = \overline{e_i}$.*
2. *The $\mathbf{A}$-linear map λ induces by passage to the quotient an isomorphism $\overline{\lambda} : \mathrm{Coker}(\mathrm{Ja}) \to \mathrm{J}/\mathrm{J}^2$.*

Consequently, δ is also a universal derivation.

$$\begin{tikzcd}
 & \mathrm{Coker}(\mathrm{Ja}) \arrow[dd, "\overline{\lambda}"] & \delta(x_i) \arrow[dd, leftrightarrow] \\
\mathbf{A} \arrow[ur, "\delta"] \arrow[dr, "\mathrm{d}"'] & & \\
 & \mathrm{J}/\mathrm{J}^2 & \mathrm{d}(x_i)
\end{tikzcd}$$

D *1.* Left to the reader.

2. We start by showing the inclusion $\mathrm{Im}(\mathrm{Ja}) \subseteq \mathrm{Ker}\,\lambda$, i.e. for each k,

$$\lambda\big(\textstyle\sum_{i=1}^{n} \frac{\partial f_k}{\partial X_i}(\underline{x})\, e_i\big) = 0.$$

For $g \in \mathbf{k}[\underline{X}]$ we use Taylor's theorem at order 1:

$$g(\underline{y}) \equiv g(\underline{z}) + \textstyle\sum_{i=1}^{n} \frac{\partial g}{\partial X_i}(\underline{z})\,(y_i - z_i) \bmod \mathrm{J}^2.$$

For $g = f_k$ we have $f_k(\underline{y}) = f_k(\underline{z}) = 0$, so $\sum_{i=1}^{n} \frac{\partial f_k}{\partial X_i}(\underline{z})\,(y_i - z_i) \in \mathrm{J}^2$. This proves the above equality by taking into account the $\mathbf{A}$-module law over J/J^2. This shows that λ passes to the quotient, with

$$\overline{\lambda} : \delta(x_i) = \overline{e_i} \mapsto \mathrm{d}(x_i) = \overline{y_i - z_i}.$$

Moreover, since δ is a $\mathbf{k}$-derivation, the universal property of the derivation $\mathrm{d} : \mathbf{A} \to \mathrm{J}/\mathrm{J}^2$ gives us an $\mathbf{A}$-linear factorization

$$\mathrm{J}/\mathrm{J}^2 \to \mathrm{Coker}(\mathrm{Ja}) \;:\; \mathrm{d}(x_i) \mapsto \delta(x_i).$$

It is clear that the two mappings are inverses of each other. □

Separability idempotent of a strictly étale algebra

Let $\mathbf{A}$ be a strictly finite $\mathbf{k}$-algebra. For $a \in \mathbf{A}$, let $a^\star = a \centerdot \mathrm{Tr}_{\mathbf{A}/\mathbf{k}}$. We have a canonical $\mathbf{k}$-linear map $\mathbf{A}^{\mathrm{e}}_{\mathbf{k}} \to \mathrm{End}_{\mathbf{k}}(\mathbf{A})$, composed of the linear map $\mathbf{A}^{\mathrm{e}}_{\mathbf{k}} \to \mathbf{A}^\star \otimes_{\mathbf{k}} \mathbf{A}$, $a \otimes b \mapsto a^\star \otimes b$, and of the natural isomorphism $\mathbf{A}^\star \otimes_{\mathbf{k}} \mathbf{A} \to \mathrm{End}_{\mathbf{k}}(\mathbf{A})$.

If $\mathbf{A}$ is strictly étale these linear maps are all isomorphisms. Then, if $\big((x_i), (y_i)\big)$ is a trace system of coordinates, the element $\sum_i x_i \otimes y_i$ is independent of the choice of the system because its image in $\mathrm{End}_{\mathbf{k}}(\mathbf{A})$ is $\mathrm{Id}_{\mathbf{A}}$. In particular, $\sum_i x_i \otimes y_i = \sum_i y_i \otimes x_i$.

The following theorem identifies the characteristic properties of this element $\sum_i x_i \otimes y_i$. These properties lead to the notion of a separable algebra.

6.8. Theorem. (Separability idempotent of a strictly étale algebra)
Let $\mathbf{A}$ be a strictly étale $\mathbf{k}$-algebra and $\big((x_i), (y_i)\big)$ be a trace system of coordinates of $\mathbf{A}$. Then, the element $\varepsilon = \sum_i x_i \otimes y_i \in \mathbf{A}^{\mathrm{e}}_{\mathbf{k}}$ satisfies the conditions of Lemma 6.4. In particular, ε is idempotent and we have

$$\sum\nolimits_i x_i y_i = 1, \quad a \cdot \varepsilon = \varepsilon \cdot a \quad \forall a \in \mathbf{A}.$$

NB: We prove the converse (for strictly finite algebras) a little later (Theorem 6.13).

Proof in the Galoisian case (to be read after Theorem 7.11).
Let $(\mathbf{k}, \mathbf{A}, G)$ be a Galois algebra. Since the result to be proven is independent of the trace system of coordinates, we can suppose that the families (x_i) and (y_i) are two systems of elements of $\mathbf{A}$ satisfying the conditions of item *2* of Artin's theorem 7.11.

Saying that $\mu(\varepsilon) = 1$ consists in saying that $\sum_i x_i y_i = 1$, which is what $\big((x_i), (y_i)\big)$ satisfies. To show that $\sum_i ax_i \otimes y_i = \sum_i x_i \otimes ay_i$, it suffices to apply ψ_G; we let $(g_\sigma)_\sigma$ be the image of the left-hand side, and $(d_\sigma)_\sigma$ be the image of the right-hand side. We obtain, by letting δ be the Kronecker symbol,

$$g_\sigma = \textstyle\sum_i ax_i\sigma(y_i) = a\delta_{\sigma,\mathrm{Id}}, \qquad d_\sigma = \sum_i x_i\sigma(ay_i) = \sigma(a)\delta_{\sigma,\mathrm{Id}}.$$

We indeed have the equality since the components of the two families (d_σ) and (g_σ) are null except at the index $\sigma = \mathrm{Id}$, at which their (common) value is a.

Note that ε is equal to the element $\varepsilon_{\mathrm{Id}}$ introduced in Lemma 7.10. Its image under φ_G is the idempotent e_{Id}, which confirms that ε is idempotent. □

(General) Proof in the strictly étale case.

We write Tr for $\mathrm{Tr}_{\mathbf{A}/\mathbf{k}}$ and let $m_\varepsilon : \mathbf{A}^{\mathrm{e}}_{\mathbf{k}} \to \mathbf{A}^{\mathrm{e}}_{\mathbf{k}}$ be multiplication by ε. We have

$$\mathrm{Tr}(ab) = \textstyle\sum_i \mathrm{Tr}(ay_i)\,\mathrm{Tr}(bx_i), \qquad a, b \in \mathbf{A}. \tag{$\star$}$$

Indeed, this easily results from the equality $a = \sum_i \mathrm{Tr}(ay_i)x_i$.

We rewrite ($\star$) as the equality of two $\mathbf{k}$-linear forms, $\mathbf{A}^{\mathrm{e}}_{\mathbf{k}} \to \mathbf{k}$:

$$\mathrm{Tr}_{\mathbf{A}/\mathbf{k}} \circ \mu_{\mathbf{A}/\mathbf{k}} = \mathrm{Tr}_{\mathbf{A}^{\mathrm{e}}_{\mathbf{k}}/\mathbf{k}} \circ m_\varepsilon. \tag{$*$}$$

Let us show that $\varepsilon \in \mathrm{Ann}(\mathrm{J})$. Let $z \in \mathbf{A}^{\mathrm{e}}_{\mathbf{k}}$, $z' \in \mathrm{J}$. By evaluating the equality ($*$) at zz', we obtain

$$\mathrm{Tr}_{\mathbf{A}/\mathbf{k}}\,\big(\mu_{\mathbf{A}/\mathbf{k}}(zz')\big) = \mathrm{Tr}_{\mathbf{A}^{\mathrm{e}}_{\mathbf{k}}/\mathbf{k}}(\varepsilon zz').$$

But $\mu_{\mathbf{A}/\mathbf{k}}(zz') = \mu_{\mathbf{A}/\mathbf{k}}(z)\mu_{\mathbf{A}/\mathbf{k}}(z') = 0$ because $z' \in \mathrm{J} = \mathrm{Ker}\,\mu_{\mathbf{A}/\mathbf{k}}$. We deduce that $\mathrm{Tr}_{\mathbf{A}^{\mathrm{e}}_{\mathbf{k}}/\mathbf{k}}(\varepsilon zz') = 0$ for every $z \in \mathbf{A}^{\mathrm{e}}_{\mathbf{k}}$. As $\mathrm{Tr}_{\mathbf{A}^{\mathrm{e}}_{\mathbf{k}}/\mathbf{k}}$ is non-degenerate we obtain $\varepsilon z' = 0$. Thus $\varepsilon \in \mathrm{Ann}(\mathrm{J})$.

It remains to show that $\mu_{\mathbf{A}/\mathbf{k}}(\varepsilon) = 1$, i.e. $s = \sum_i x_i y_i = 1$.

The equality $\mathrm{Tr}(x) = \sum_i \mathrm{Tr}(xx_iy_i)$ (Fact V-8.9) says that $\mathrm{Tr}\,\big((1-s)x\big) = 0$ for all $x \in \mathbf{A}$, thus $s = 1$. □

Separable algebras

6.9. Theorem. *For a* $\mathbf{k}$*-algebra* $\mathbf{A}$ *the following properties are equivalent.*

1. $\mathbf{A}$ *is projective as an* $\mathbf{A}^{\mathrm{e}}_{\mathbf{k}}$*-module.*
2. $\mathrm{J}_{\mathbf{A}/\mathbf{k}}$ *is generated by an idempotent of* $\mathbf{A}^{\mathrm{e}}_{\mathbf{k}}$.
3. $\mathrm{J}_{\mathbf{A}/\mathbf{k}}$ *is finitely generated and idempotent.*
4. $1 \in \mu_{\mathbf{A}/\mathbf{k}}\big(\mathrm{Ann}(\mathrm{J}_{\mathbf{A}/\mathbf{k}})\big)$.
5. *There exist an* $n \in \mathbb{N}$ *and* $x_1, \ldots, x_n, y_1, \ldots, y_n \in \mathbf{A}$ *such that* $\sum_i x_i y_i = 1$ *and for every* $a \in \mathbf{A}$, $\sum_i ax_i \otimes y_i = \sum_i x_i \otimes ay_i$.

In this case we denote by $\varepsilon_{\mathbf{A}/\mathbf{k}}$ *the unique idempotent which generates the ideal* $\mathrm{Ann}(\mathrm{J}_{\mathbf{A}/\mathbf{k}})$.

When $\mathbf{A}$ *is a finitely generated* $\mathbf{k}$*-algebra, another equivalent property is*

6. $\Omega_{\mathbf{A}/\mathbf{k}} = 0$.[7]

D Since $\mathbf{A} \simeq \mathbf{A}^{\mathrm{e}}_{\mathbf{k}}/\mathrm{J}_{\mathbf{A}/\mathbf{k}}$, items *1* and *2* are equivalent under Lemma V-7.5 regarding the cyclic projective modules. Items *2* and *3* are equivalent under Lemma II-4.6 on finitely generated idempotent ideals. Lemma 6.4 gives the equivalence of *2* and *4*.

3 ⇔ *6.* If $\mathbf{A}$ is a finitely generated $\mathbf{k}$-algebra, then $\mathrm{J}_{\mathbf{A}/\mathbf{k}}$ is a finitely generated ideal of $\mathbf{A}^{\mathrm{e}}_{\mathbf{k}}$, therefore condition *3* can be reduced to: $\mathrm{J}_{\mathbf{A}/\mathbf{k}}$ is idempotent, i.e. $\Omega_{\mathbf{A}/\mathbf{k}} = 0$.

Finally, *5* is the concrete form of *4*. □

6.10. Definition. We call an algebra that satisfies the equivalent properties stated in Theorem 6.9 a *separable algebra*. The idempotent $\varepsilon_{\mathbf{A}/\mathbf{k}} \in \mathbf{A}^{\mathrm{e}}_{\mathbf{k}}$ is called *the separability idempotent* of $\mathbf{A}$.

Comment. It should be noted that Bourbaki uses a notion of separable extension for fields that is quite different to the above definition. In classical mathematics, algebras over a field $\mathbf{K}$ "separable in the sense of Definition 6.10" are the algebras that are "finite and separable in the Bourbaki sense" (see Theorem 6.14). Many authors follow Bourbaki at least for the algebraic extensions of fields, whether they are finite or not. In the case of an algebraic $\mathbf{K}$-algebra over a discrete field $\mathbf{K}$, the definition à la Bourbaki means that every element of the algebra is a zero of a separable monic polynomial of $\mathbf{K}[T]$. ■

6.11. Fact. (Stability of separable algebras by scalar extension)
Let $\imath : \mathbf{k} \to \mathbf{A}$ and $\rho : \mathbf{k} \to \mathbf{k}'$ be two $\mathbf{k}$-algebras and $\mathbf{A}' = \rho_\star(\mathbf{A})$. We have a canonical isomorphism $\rho_\star(\mathbf{A}^{\mathrm{e}}_{\mathbf{k}}) \to {\mathbf{A}'}^{\mathrm{e}}_{\mathbf{k}'}$ and the diagram below commutes

$$\begin{tikzcd}
\mathbf{A}^{\mathrm{e}}_{\mathbf{k}} \arrow[r, "\rho^{\mathrm{e}}_{\mathbf{k}}"] \arrow[d, "\mu_{\mathbf{A}/\mathbf{k}}"] & {\mathbf{A}'}^{\mathrm{e}}_{\mathbf{k}'} \arrow[d, "\mu_{\mathbf{A}'/\mathbf{k}'}"] \\
\mathbf{A} \arrow[r, "\rho"] & \mathbf{A}'
\end{tikzcd}$$

In particular, a separable algebra remains separable by scalar extension.

D The proof is left to the reader. □

Now we prove the converse of Theorem 6.8, which requires a preliminary lemma.

[7] By Theorem 6.7, if $\mathbf{A} = \mathbf{k}[X_1, \ldots, X_n]/\langle f_1, \ldots, f_s\rangle = \mathbf{k}[\underline{x}]$, $\Omega_{\mathbf{A}/\mathbf{k}} = 0$ means that the matrix $\mathrm{Ja}(\underline{x})$ (the transposed of the Jacobian matrix) is surjective, i.e. $1 \in \mathcal{D}_n(\mathrm{JAC}_{\underline{X}}(\underline{f})(\underline{x}))$.

6.12. Lemma. *Let* $\mathbf{A}$ *be a strictly finite* $\mathbf{k}$*-algebra and* $\mathbf{A}^{\mathrm{e}}_{\mathbf{k}}$ *its enveloping algebra.*

1. $\mathbf{A}^{\mathrm{e}}_{\mathbf{k}}$ *is a strictly finite left* $\mathbf{A}$*-algebra whose trace is given by* $\gamma_{\mathrm{l}} \circ (\mathrm{Id}_{\mathbf{A}} \otimes \mathrm{Tr}_{\mathbf{A}/\mathbf{k}})$ *(where* $\gamma_{\mathrm{l}} : \mathbf{A} \otimes_{\mathbf{k}} \mathbf{k} \to \mathbf{A}$ *is the canonical isomorphism), i.e. for* $\alpha = \sum_i a_i \otimes b_i$*:*
$$\mathrm{Tr}_{(\mathbf{A}^{\mathrm{e}}_{\mathbf{k}}/\mathbf{A})_{\mathrm{l}}}(\alpha) = \textstyle\sum_i a_i \, \mathrm{Tr}_{\mathbf{A}/\mathbf{k}}(b_i).$$
Similarly, $\mathbf{A}^{\mathrm{e}}_{\mathbf{k}}$ *is a strictly finite right* $\mathbf{A}$*-algebra whose trace is given by* $\gamma_{\mathrm{r}} \circ (\mathrm{Tr}_{\mathbf{A}/\mathbf{k}} \otimes \mathrm{Id}_{\mathbf{A}})$*, i.e.* $\mathrm{Tr}_{(\mathbf{A}^{\mathrm{e}}_{\mathbf{k}}/\mathbf{A})_{\mathrm{r}}}(\alpha) = \sum_i \mathrm{Tr}_{\mathbf{A}/\mathbf{k}}(a_i) b_i$*.*
2. *Over* $\mathrm{Ann}(\mathrm{J}_{\mathbf{A}/\mathbf{k}})$*, the* $\mathbf{A}$*-linear forms* $\mathrm{Tr}_{(\mathbf{A}^{\mathrm{e}}_{\mathbf{k}}/\mathbf{A})_{\mathrm{l}}}$*,* $\mathrm{Tr}_{(\mathbf{A}^{\mathrm{e}}_{\mathbf{k}}/\mathbf{A})_{\mathrm{r}}}$ *and* $\mu_{\mathbf{A}/\mathbf{k}}$ *coincide, i.e. if* $\alpha = \sum_i a_i \otimes b_i \in \mathrm{Ann}(\mathrm{J}_{\mathbf{A}/\mathbf{k}})$*,*
$$\textstyle\sum_i a_i b_i = \sum_i a_i \, \mathrm{Tr}_{\mathbf{A}/\mathbf{k}}(b_i) = \sum_i \mathrm{Tr}_{\mathbf{A}/\mathbf{k}}(a_i) b_i.$$

D *1.* This is a general structural result: the trace is preserved by scalar extension (see Fact V-8.8). In other words if $\mathbf{k}'$ is a $\mathbf{k}$-algebra, $\mathbf{k}' \otimes_{\mathbf{k}} \mathbf{A}$ is a strictly finite $\mathbf{k}'$-algebra whose trace is $\gamma \circ (\mathrm{Id}_{\mathbf{k}'} \otimes \mathrm{Tr}_{\mathbf{A}/\mathbf{k}})$ where $\gamma : \mathbf{k}' \otimes_{\mathbf{k}} \mathbf{k} \to \mathbf{k}'$ is the canonical isomorphism.

2. Generally, under the hypotheses that E is a finitely generated projective $\mathbf{A}$-module, $x \in E$, $\nu \in E^{\star}$ and $u = \theta_E(\nu \otimes x) \in \mathrm{End}_{\mathbf{A}}(E)$, we obtain the equality $\mathrm{Tr}_E(u) = \nu(x)$ (see Fact V-8.9).
We apply this to $E = \mathbf{A}^{\mathrm{e}}_{\mathbf{k}}$, $x = \alpha \in E$ and $\nu = \mu_{\mathbf{A}/\mathbf{k}} \in E^{\star}$, by noting then that $u = \theta_E(\nu \otimes \alpha) = \mu_{\mathbf{A}^{\mathrm{e}}_{\mathbf{k}},\alpha}$. Indeed, by item *3* of Fact 6.3, we have for $\gamma \in \mathbf{A}^{\mathrm{e}}_{\mathbf{k}}$, $\gamma\alpha = \mu_{\mathbf{A}/\mathbf{k}}(\gamma) \cdot \alpha = \theta_E(\nu \otimes \alpha)(\gamma)$. □

6.13. Theorem. (Strictly étale algebras and separable algebras)
Every separable and strictly finite $\mathbf{k}$*-algebra* $\mathbf{A}$ *is strictly étale. More precisely, if* $\varepsilon_{\mathbf{A}/\mathbf{k}} = \sum x_i \otimes y_i \in \mathbf{A}^{\mathrm{e}}_{\mathbf{k}}$ *is the separability idempotent of* $\mathbf{A}$*, then* $\big((x_i), (y_i)\big)$ *is a trace system of coordinates of* $\mathbf{A}/\mathbf{k}$*.*
In brief, a strictly finite algebra is separable if and only if it is strictly étale.

NB: Precisely, the link between the two notions is obtained by the relation linking the separability idempotent and the coordinate systems, as is apparent in the direct Theorem 6.8 and in the converse theorem.

D Let $x \in \mathbf{A}$, then $(x \otimes 1)\varepsilon_{\mathbf{A}/\mathbf{k}} = \sum_i x x_i \otimes y_i$ is in $\mathrm{Ann}(\mathrm{J}_{\mathbf{A}/\mathbf{k}})$, so by Lemma 6.12, we have $\sum_i x x_i y_i = \sum_i \mathrm{Tr}_{\mathbf{A}/\mathbf{k}}(x_i x) y_i$.
As $\sum_i x_i y_i = 1$, this gives $x = \sum_i \mathrm{Tr}_{\mathbf{A}/\mathbf{k}}(x_i x) y_i$. The result follows by the characterization of strictly étale algebras given in Fact 5.5. □

The following theorem strengthens the previous theorem and shows that the existence of a separability idempotent is a very strong condition of finiteness.

6.14. Theorem. *Let* $\mathbf{A}$ *be a separable* $\mathbf{k}$*-algebra.*
Suppose that $\mathbf{A}$ *has a* coordinate system *in the following sense. We have a discrete set* I*, a family* $(a_i)_{i\in I}$ *in* $\mathbf{A}$ *and a family* $(\alpha_i)_{i\in I}$ *in the dual* $\mathbf{k}$*-module* $\mathbf{A}^\star = \mathrm{L}_\mathbf{k}(\mathbf{A},\mathbf{k})$*, such that for all* $x \in \mathbf{A}$ *we have*

$$x = \textstyle\sum_{i\in J_x} \alpha_i(x)a_i.$$

Here J_x *is a finite subset of* I*, and every* $\alpha_i(x)$ *for* $i \in I \setminus J_x$ *is null.*
Then, $\mathbf{A}$ *is strictly finite, therefore strictly étale.*
This is the case, for example, if $\mathbf{k}$ *is a discrete field and if* $\mathbf{A}$ *is a finitely presented* $\mathbf{k}$*-algebra.*

D Regarding the special case, the quotient algebra has a finite or countable basis of monomials, by the theory of Gröbner bases.
Let $\varepsilon = \sum_{k=1}^r b_k \otimes c_k$ be the separability idempotent. We have $\varepsilon\cdot x = x\cdot\varepsilon$ for every $x \in \mathbf{A}$, and $\sum_{k=1}^r b_k c_k = 1$.
For $\alpha \in \mathbf{A}^\star$ and $x \in \mathbf{A}$, by applying $1\otimes\alpha$ to $x\cdot\varepsilon = \varepsilon\cdot x$ we obtain

$$\textstyle\sum_k x b_k \alpha(c_k) = \sum_k b_k\alpha(xc_k).$$

By denoting by J the finite subset $J = \bigcup J_{c_k}$, we obtain for each k

$$c_k = \sum\nolimits_{i\in J} \alpha_i(c_k)a_i.$$

We then write

$$x = \sum_{k\in[\![1..r]\!]} x b_k c_k = \sum_{k\in[\![1..r]\!],i\in J} x b_k\alpha_i(c_k)a_i = \sum_{i\in J,k\in[\![1..r]\!]} \alpha_i(c_k x)b_k a_i.$$

This now gives a finite coordinate system for $\mathbf{A}$, with the elements $b_k a_i$ and the forms $x \mapsto \alpha_i(c_k x)$ for $(i,k) \in J\times[\![1..r]\!]$. □

Comment. Note that, when we have a coordinate system for a module, the module is projective in the usual sense. The definition of a coordinate system for a module M amounts to saying that M is isomorphic to a direct summand of the module $\mathbf{A}^{(I)}$. The latter module, freely generated by I, is projective because I is discrete.
In classical mathematics, every projective module has a coordinate system, because all the sets are discrete, so the previous theorem applies: every separable $\mathbf{k}$-algebra which is a projective $\mathbf{k}$-module is strictly finite. By the same token *every separable algebra over a discrete field or over a reduced zero-dimensional ring is strictly finite.* ■

In the case of a finitely presented algebra over a discrete field, Theorems 6.9 and 6.14 give the following result.

6.15. Corollary. *For* $f_1, \ldots, f_s \in \mathbf{k}[X_1,\ldots,X_n]$ *when* $\mathbf{k}$ *is a discrete field, the following properties are equivalent.*

1. *The quotient algebra* $\mathbf{A} = \mathbf{k}[\underline{x}]$ *is strictly étale.*
2. *The quotient algebra is separable.*

3. The matrix $\mathrm{Ja}(\underline{x})$*, transposed of the Jacobian matrix of the polynomial system, is surjective.*

We will now show that a separable algebra looks a lot like a diagonal algebra, including when the base ring is arbitrary.

Consider the diagonal $\mathbf{k}$-algebra $\mathbf{k}^n$. Let $(e_1, \dots, e_n)$ be its canonical basis and $p_i : \mathbf{k}^n \to \mathbf{k}$ be the coordinate form in relation to e_i. Then we have

$$e_i \in \mathbb{B}(\mathbf{k}^n),\ p_i \in \mathrm{Hom}_{\mathbf{k}}(\mathbf{k}^n, \mathbf{k}),\ p_i(e_i) = 1 \text{ and } xe_i = p_i(x)e_i\ \forall x \in \mathbf{k}^n.$$

In a way, we are about to generalize the above result to separable algebras.

6.16. Lemma. (Characters of a separable algebra)
Let $\mathbf{A}$ *be a separable* $\mathbf{k}$*-algebra with* $\mathbf{k} \subseteq \mathbf{A}$*.*

1. *Let* $\imath : \mathbf{k} \to \mathbf{A}$ *be the canonical injection. If* $\varphi \in \mathrm{Hom}_{\mathbf{k}}(\mathbf{A}, \mathbf{k})$*,* $\imath \circ \varphi$ *is a projector with image* $\mathbf{k}.1$*, so*
$$\mathbf{A} = \mathbf{k}.1 \oplus \mathrm{Ker}\,\varphi \quad \textit{and} \quad \mathrm{Im}(\mathrm{Id}_{\mathbf{A}} - \imath \circ \varphi) = \mathrm{Ker}\,\varphi.$$
In fact the ideal $\mathrm{Ker}\,\varphi$ *is generated by an idempotent of* $\mathbf{A}$*. We will denote by* ε_φ *the complementary idempotent.*
2. *For* φ*,* $\varphi' \in \mathrm{Hom}_{\mathbf{k}}(\mathbf{A}, \mathbf{k})$*, we have* $\varphi'(\varepsilon_\varphi) = \varphi(\varepsilon_{\varphi'})$*.*
This element, denoted by $e_{\{\varphi,\varphi'\}}$*, is an idempotent of* $\mathbf{k}$ *and we have*
$$\varepsilon_\varphi \varepsilon_{\varphi'} = e_{\{\varphi,\varphi'\}}\varepsilon_\varphi = e_{\{\varphi,\varphi'\}}\varepsilon_{\varphi'} = \varphi(\varepsilon_\varphi\varepsilon_{\varphi'}) = \varphi'(\varepsilon_\varphi\varepsilon_{\varphi'}),$$
$$\langle \mathrm{Im}(\varphi - \varphi')\rangle_{\mathbf{k}} = \left\langle 1 - e_{\{\varphi,\varphi'\}}\right\rangle_{\mathbf{k}} \ \textit{and}\ \mathrm{Ann}_{\mathbf{k}}(\varphi - \varphi') = \left\langle e_{\{\varphi,\varphi'\}}\right\rangle_{\mathbf{k}}.$$
3. *Consequently we have the equivalences*
$$e_{\{\varphi,\varphi'\}} = 1 \iff \varepsilon_\varphi = \varepsilon_{\varphi'} \iff \varphi = \varphi',\ \textit{and}$$
$$e_{\{\varphi,\varphi'\}} = 0 \iff \varepsilon_\varphi\varepsilon_{\varphi'} = 0.$$
4. *If* $\mathbf{k}$ *is connected, two idempotents* ε_φ*, (for* $\varphi \in \mathrm{Hom}_{\mathbf{k}}(\mathbf{A}, \mathbf{k})$*), are equal or orthogonal.*

D Let $\varepsilon_{\mathbf{A}/\mathbf{k}} = \sum x_i \otimes y_i$. We know that $a \cdot \varepsilon_{\mathbf{A}/\mathbf{k}} = \varepsilon_{\mathbf{A}/\mathbf{k}} \cdot a$ for every $a \in \mathbf{A}$, that $\sum x_i \otimes y_i = \sum y_i \otimes x_i$ and that $\sum_i x_i y_i = 1$.

1. The first assertion is valid for every character of every algebra $\mathbf{A}$. It remains to see that $\mathrm{Ker}\,\varphi$ is generated by an idempotent. We consider the homomorphism of $\mathbf{k}$-algebras $\nu = \mu_{\mathbf{A}/\mathbf{k}} \circ (\varphi \otimes \mathrm{Id}_{\mathbf{A}}) : \mathbf{A}^{\mathrm{e}}_{\mathbf{k}} \to \mathbf{A}$, and the element $\varepsilon = \nu(\varepsilon_{\mathbf{A}/\mathbf{k}})$. Thus $\varepsilon = \sum_i \varphi(x_i)y_i$ is an idempotent and we obtain the equalities

$$\varphi(\varepsilon) = \textstyle\sum_i \varphi(x_i)\varphi(y_i) = \varphi(\sum_i x_i y_i) = \varphi(1) = 1.$$

Therefore $1 - \varepsilon \in \mathrm{Ker}\,\varphi$.

By applying ν to the equality $\sum_i ax_i \otimes y_i = \sum_i x_i \otimes ay_i$, we obtain $\varphi(a)\varepsilon = a\varepsilon$. Therefore $a \in \mathrm{Ker}\,\varphi$ implies $a = (1 - \varepsilon)a$, and $\mathrm{Ker}\,\varphi = \langle 1 - \varepsilon\rangle$.

2. We have, for $a \in \mathbf{A}$,

$$\varphi'(a)\varphi'(\varepsilon_\varphi) = \varphi'(a\varepsilon_\varphi) = \varphi'(\varphi(a)\varepsilon_\varphi) = \varphi(a)\varphi'(\varepsilon_\varphi). \qquad (\star)$$

For $a = \varepsilon_{\varphi'}$, we obtain $\varphi'(\varepsilon_\varphi) = \varphi(\varepsilon_{\varphi'})\varphi'(\varepsilon_\varphi)$. By symmetry, $\varphi(\varepsilon_{\varphi'}) = \varphi'(\varepsilon_\varphi)$. Denote by e this idempotent of $\mathbf{k}$. By definition, we have $a\varepsilon_\varphi =$

$\varphi(a)\varepsilon_\varphi$. By making $a = \varepsilon_{\varphi'}$, we obtain $\varepsilon_{\varphi'}\varepsilon_\varphi = e\varepsilon_\varphi$.

Finally, let $\mathfrak{a} = \langle \mathrm{Im}(\varphi - \varphi') \rangle$. The relation $(\star)$ shows that $\mathfrak{a}e = 0$. Moreover $1 - e = (\varphi - \varphi')(\varepsilon_\varphi) \in \mathfrak{a}$. Therefore $\mathfrak{a} = \langle 1 - e \rangle_{\mathbf{k}}$ and $\mathrm{Ann}_{\mathbf{k}}(\mathfrak{a}) = \langle e \rangle_{\mathbf{k}}$.

3 and *4*. Result from the previous item. □

6.17. Lemma. (Separable subalgebra of a diagonal extension)
Let $\mathbf{k}$ *be a* nontrivial connected *ring,* $\mathbf{B} = \mathbf{k}^n$*,* $p_i : \mathbf{B} \to \mathbf{k}$ *be the* i^{th} *canonical projection,* e_i *be the idempotent defined by* $\mathrm{Ker}\, p_i = \langle 1 - e_i \rangle$ $(i \in [\![1..n]\!])$. *For a finite subset* I *of* $[\![1..n]\!]$ *we let* $e_I = \sum_{i \in I} e_i$.
Let $\mathbf{A}$ *be a separable* $\mathbf{k}$*-algebra with* $\mathbf{k} \subseteq \mathbf{A} \subseteq \mathbf{k}^n$ *and* π_i *be the restriction of* p_i *to* $\mathbf{A}$ *for* $i \in [\![1..n]\!]$.

1. *We consider the equivalence relation over* $[\![1..n]\!]$ *defined by* $\pi_i = \pi_j$*. The corresponding partition* $\mathcal{P}$ *is a finite set of finite subsets of* $[\![1..n]\!]$*. For* $J \in \mathcal{P}$ *we denote by* π_J *the common value of the* π_j*'s for* $j \in J$.
2. $\mathbf{A}$ *is a free* $\mathbf{k}$*-module with basis* $\{\, e_J \mid J \in \mathcal{P} \,\}$.
3. $\mathbf{A}^\star$ *is a free* $\mathbf{k}$*-module with basis* $\{\, \pi_J \mid J \in \mathcal{P} \,\} = \mathrm{Hom}_{\mathbf{k}}(\mathbf{A}, \mathbf{k})$.

D *1.* As $\mathbf{k}$ is nontrivial and connected, every idempotent of $\mathbf{B}$ is of the form e_I for a unique finite subset I of $[\![1..n]\!]$.

Let $i \in [\![1..n]\!]$. By Lemma 6.16 there exists one and only one idempotent ε_i of $\mathbf{A}$ such that $\pi_i(\varepsilon_i) = 1$ and $a\varepsilon_i = \pi_i(a)\varepsilon_i$ for every $a \in \mathbf{A}$. This idempotent is also an idempotent of $\mathbf{B}$ so of the form e_{J_i} for a finite subset J_i of $[\![1..n]\!]$. Since $\pi_i(\varepsilon_i) = p_i(e_{J_i}) = 1$, we have $i \in J_i$, and the union of the J_i's is $[\![1..n]\!]$. Two distinct J_i are disjoint by the last item of Lemma 6.16. The J_i's therefore form a finite partition formed of finite subsets of $[\![1..n]\!]$. If $\pi_i = \pi_j$, then $\varepsilon_i = \varepsilon_j$ so $J_i = J_j$. If $J_i = J_j$, then $\varepsilon_i = \varepsilon_j$ and $\pi_i(\varepsilon_j) = 1$. Item *2* of Lemma 6.16 gives $1 \in \mathrm{Ann}_{\mathbf{A}}(\pi_i - \pi_j)$, so $\pi_i = \pi_j$.

2. Results from item *1.*

3. Let $\varphi \in \mathrm{Hom}_{\mathbf{k}}(\mathbf{A}, \mathbf{k})$. The $\varphi(e_J)$'s are idempotents of $\mathbf{k}$. As $\mathbf{k}$ is connected, we have $\varphi(e_J) = 0$ or 1. But the $(e_J)_{J \in \mathcal{P}}$'s form a fundamental system of orthogonal idempotents, therefore there is only one $J \in \mathcal{P}$ for which $\varphi(e_J) = 1$ and consequently $\varphi = \pi_J$. The rest is immediate. □

7. Galois algebras, general theory

The theory developed by Artin considers a finite group G of automorphisms of a discrete field $\mathbf{L}$, calls $\mathbf{K}$ the subfield of the fixed points of G and proves that $\mathbf{L}$ is a Galois extension of $\mathbf{K}$, with G as the Galois group.

In the current section we give the generalization of Artin's theory for commutative rings instead of discrete fields. A good idea of "how this can work" is already given by the following significant small example, which shows that the hypothesis "discrete field" is not required.

A small example to start off

Let $\mathbf{A}$ be a commutative ring, $\sigma \in \mathrm{Aut}(\mathbf{A})$ be an automorphism of order 3, and G be the group that it generates. Suppose that there exists an $x \in \mathbf{A}$ such that $\sigma(x) - x \in \mathbf{A}^{\times}$. Let $\mathbf{k} = \mathbf{A}^G$ be the subring of fixed points. Then, $(1, x, x^2)$ is a basis of $\mathbf{A}$ over $\mathbf{k}$. Indeed, let V be the Vandermonde matrix

$$V = \begin{bmatrix} 1 & x & x^2 \\ 1 & \sigma(x) & \sigma(x^2) \\ 1 & \sigma^2(x) & \sigma^2(x^2) \end{bmatrix} = \begin{bmatrix} 1 & x_0 & x_0^2 \\ 1 & x_1 & x_1^2 \\ 1 & x_2 & x_2^2 \end{bmatrix} \quad \text{with} \quad x_i = \sigma^i(x).$$

Let $\varepsilon = \sigma(x) - x$. Then, $\det(V) = (x_1 - x_0)(x_2 - x_1)(x_2 - x_0)$ is invertible:

$$\det(V) = \big(\sigma(x) - x\big) \cdot \sigma\big(\sigma(x) - x\big) \cdot \sigma^2\big(x - \sigma(x)\big) = -\varepsilon\sigma(\varepsilon)\sigma^2(\varepsilon).$$

For $y \in \mathbf{A}$, we want to write $y = \lambda_0 + \lambda_1 x + \lambda_2 x^2$ with each $\lambda_i \in \mathbf{k}$. We then necessarily have

$$\begin{bmatrix} y \\ \sigma(y) \\ \sigma^2(y) \end{bmatrix} = \begin{bmatrix} 1 & x & x^2 \\ 1 & \sigma(x) & \sigma(x^2) \\ 1 & \sigma^2(x) & \sigma^2(x^2) \end{bmatrix} \begin{bmatrix} \lambda_0 \\ \lambda_1 \\ \lambda_2 \end{bmatrix}.$$

However, the above system of linear equations has one and only one solution in $\mathbf{A}$. Since the solution is unique, $\sigma(\lambda_i) = \lambda_i$, i.e. $\lambda_i \in \mathbf{k}$ $(i = 0, 1, 2)$. Finally, $(1, x, x^2)$ is indeed a $\mathbf{k}$-basis of $\mathbf{A}$. ■

Galois correspondence, obvious facts

This can be considered as a resumption of Proposition III-6.10.

7.1. Fact. (Galois correspondence, obvious facts)
Consider a finite group G of automorphisms of a ring $\mathbf{A}$. We use the notations defined in III-6.8. In particular, $\mathbf{A}^H = \mathrm{Fix}_{\mathbf{A}}(H)$ for a subgroup H of G. Let $\mathbf{k} = \mathbf{A}^G$.

1. *If $H \subseteq H'$ are two subgroups of G, then $\mathbf{A}^H \supseteq \mathbf{A}^{H'}$, and if H is the subgroup generated by $H_1 \cup H_2$, then $\mathbf{A}^H = \mathbf{A}^{H_1} \cap \mathbf{A}^{H_2}$.*
2. *$H \subseteq \mathrm{Stp}(\mathbf{A}^H)$ for every subgroup H of G.*
3. *If $\sigma \in G$ and H is a subgroup of G then*
$$\sigma(\mathbf{A}^H) = \mathbf{A}^{\sigma H \sigma^{-1}}.$$
4. *If $\mathbf{C} \subseteq \mathbf{C}'$ are two $\mathbf{k}$-subalgebras of $\mathbf{A}$, then $\mathrm{Stp}(\mathbf{C}) \supseteq \mathrm{Stp}(\mathbf{C}')$, and if $\mathbf{C}$ is the $\mathbf{k}$-subalgebra generated by $\mathbf{C}_1 \cup \mathbf{C}_2$, then*
$$\mathrm{Stp}(\mathbf{C}) = \mathrm{Stp}(\mathbf{C}_1) \cap \mathrm{Stp}(\mathbf{C}_2).$$
5. *$\mathbf{C} \subseteq \mathbf{A}^{\mathrm{Stp}(\mathbf{C})}$ for every $\mathbf{k}$-subalgebra $\mathbf{C}$ of $\mathbf{A}$.*
6. *After any "go-come-go motion," we end up with the resulting set of the first "go":*
$$\mathbf{A}^H = \mathbf{A}^{\mathrm{Stp}(\mathbf{A}^H)} \quad \textit{and} \quad \mathrm{Stp}(\mathbf{C}) = \mathrm{Stp}\left(\mathbf{A}^{\mathrm{Stp}(\mathbf{C})}\right).$$

D The last item is a direct consequence of the previous ones, which are immediate. Likewise for all the "dualities" of this type. □

A natural definition

Let $\mathcal{G} = \mathcal{G}_G$ be the set of finite (i.e. detachable) subgroups of G, and $\mathcal{A} = \mathcal{A}_G$ be the set of subrings of $\mathbf{A}$ which are of the form $\mathrm{Fix}(H)$ for some $H \in \mathcal{G}$. Consider the restrictions of Fix and Stp to the sets $\mathcal{G}$ and $\mathcal{A}$. We are interested in determining under which conditions we thus obtain two inverse bijections between $\mathcal{G}$ and $\mathcal{A}$, and in giving a nice characterization of subalgebras belonging to $\mathcal{A}$. In the case where $\mathbf{A}$ is a discrete field, Artin's theory shows that we find ourselves in the classical Galois situation: $\mathbf{A}$ is a Galois extension of the subfield $\mathbf{k} = \mathbf{A}^G$, G is the Galois group of this extension and $\mathcal{A}$ is the set of all the strictly finite subextensions of $\mathbf{A}$.

This "Artin-Galois" theory has then been generalized to an arbitrary commutative ring $\mathbf{A}$, where certain conditions are imposed on the group G and on the $\mathbf{k}$-subalgebras of $\mathbf{A}$.

Actually, we want the corresponding notion of a Galois algebra to be sufficiently stable. In particular, when we replace $\mathbf{k}$ by a nontrivial quotient $\mathbf{k}/\mathfrak{a}$ and $\mathbf{A}$ by $\mathbf{A}/\mathfrak{a}\mathbf{A}$, we wish to maintain the notion of a Galois algebra. Therefore two automorphisms of $\mathbf{A}$ present in G must not be able to become a single automorphism upon passage to the quotient.

This leads to the following definition.

7.2. Definition. *(Well-separated maps, separating automorphisms, Galois algebras)*

1. Two maps σ, σ' from a set E to a ring $\mathbf{A}$ are said to be *well-separated* if
$$\langle\, \sigma(x) - \sigma'(x) \;;\; x \in E \,\rangle_{\mathbf{A}} = \langle 1 \rangle\,.$$
2. An automorphism τ of $\mathbf{A}$ is said to be *separating* if it is well-separated from $\mathrm{Id}_{\mathbf{A}}$.
3. A finite group G that operates on $\mathbf{A}$ is said to be *separating* if the elements $\sigma \neq 1_G$ of G are separating (it amounts to the same to say that every pair of distinct elements of G gives two well-separated automorphisms).

   We will also say that G operates *in a separating way* on $\mathbf{A}$.
4. A *Galois algebra* is by definition a triple $(\mathbf{k}, \mathbf{A}, G)$, where $\mathbf{A}$ is a ring, G is a finite group operating on $\mathbf{A}$ in a separating way, and $\mathbf{k} = \mathrm{Fix}(G)$.

Comments.

1) As for the definition of a Galois algebra, we did not want to forbid a finite group operating on the trivial ring, and consequently we do not define G as a group of automorphisms of $\mathbf{A}$, but as a finite group operating on $\mathbf{A}$.[8] In fact, the definition implies that G always operates faithfully on $\mathbf{A}$ (and thus can be identified with a subgroup of $\mathrm{Aut}(\mathbf{A})$) except in the case where

[8] The unique automorphism of the trivial ring is separating, and every finite group operates on the trivial ring in order to make it a Galois algebra.

the ring is trivial. This presents several advantages.
On the one hand, a Galois algebra remains Galoisian, *with the same group G*, for every scalar extension; it is possible that we do not know if a scalar extension $\mathbf{k} \to \mathbf{k}'$, appearing in the middle of a proof, is trivial or not.
On the other hand, the fact of not changing groups is more convenient for any scalar extension anyway.

2) We have imposed the condition $\mathbf{k} \subseteq \mathbf{A}$, which is not in the usual categorical style. The readers will be able to restore a more categorical definition, if they wish, by saying by saying that the morphism $\mathbf{k} \to \mathbf{A}$ establishes an isomorphism between $\mathbf{k}$ and $\mathbf{A}^G$. This will sometimes be necessary, for example in item *2* of Fact 7.3. ■

Examples.
1) If $\mathbf{L}/\mathbf{K}$ is a Galois extension of discrete fields, then the triple

$$\big(\mathbf{K}, \mathbf{L}, \mathrm{Gal}(\mathbf{L}/\mathbf{K})\big)$$

is a Galois algebra.

2) We will show a little further (Theorem VII-4.10) that for a separable monic polynomial $f \in \mathbf{k}[T]$, the triple $(\mathbf{k}, \mathrm{Adu}_{\mathbf{k},f}, \mathrm{S}_n)$ is a Galois algebra.

3) An automorphism σ of a local ring $\mathbf{A}$ is separating if and only if there exists some $x \in \mathbf{A}$ such that $x - \sigma(x)$ is invertible. ■

The notions of a separating automorphism and of a Galois algebra have been developed in order to satisfy the following fundamental facts.

7.3. Fact.

1. *A separating automorphism σ of a ring $\mathbf{A}$ provides by scalar extension $\rho : \mathbf{A} \to \mathbf{B}$ a separating automorphism $\rho_\star(\sigma)$ of $\mathbf{B}$.*
2. *If $(\mathbf{k}, \mathbf{A}, G)$ is a Galois algebra and if $\rho : \mathbf{k} \to \mathbf{k}'$ is a ring homomorphism, then $(\mathbf{k}', \rho_\star(\mathbf{A}), G)$ is a Galois algebra.*

D Item *1*, as well as item *2* in the case of a scalar extension by localization, are easy and left to the reader.
The proof of the general case for item *2* will have to wait until Theorem 7.13. □

7.4. Concrete local-global principle. (Galois algebras)
Let G be a finite group operating on a $\mathbf{k}$-algebra $\mathbf{A}$ with $\mathbf{k} \subseteq \mathbf{A}$.
Let S_1, …, S_n be comaximal monoids of $\mathbf{k}$.
Then, $(\mathbf{k}, \mathbf{A}, G)$ is a Galois algebra if and only if each triple $(\mathbf{k}_{S_i}, \mathbf{A}_{S_i}, G)$ is a Galois algebra.

D The proof is left to the reader. □

Dedekind's lemma

Let $\mathbf{A}$ be a commutative ring. Consider the m^{th} power $\mathbf{A}$-algebra $\mathbf{A}^m$. Its elements will be ragarded as column vectors and the laws are the product laws

$$\begin{bmatrix} a_1 \\ \vdots \\ a_m \end{bmatrix} \star \begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix} = \begin{bmatrix} a_1 \star b_1 \\ \vdots \\ a_m \star b_m \end{bmatrix}, \quad a \begin{bmatrix} a_1 \\ \vdots \\ a_m \end{bmatrix} = \begin{bmatrix} aa_1 \\ \vdots \\ aa_m \end{bmatrix}.$$

7.5. Lemma. *Let C be a finite subset of $\mathbf{A}^m$ which "separates the rows"; i.e. $\langle x_i - x_j\,;\, x \in C\rangle_{\mathbf{A}} = \langle 1\rangle$ (for $i \neq j \in [\![1..m]\!]$). Then, the $\mathbf{A}$-algebra generated by C is equal to $\mathbf{A}^m$.*

D The fundamental remark is that in the $\mathbf{A}$-module generated by $1_{\mathbf{A}^m}$ and $x = {}^{\text{t}}[\, x_1 \cdots x_m \,]$ there are the vectors

$x - x_2\, 1_{\mathbf{A}^m} = {}^{\text{t}}[\, x_1 - x_2 \;\, 0 \;\, * \cdots * \,]$ and $-x + x_1\, 1_{\mathbf{A}^m} = {}^{\text{t}}[\, 0 \;\, x_1 - x_2 \;\, * \cdots * \,]$.

Therefore, when we suppose that the ideal generated by the $x_1 - x_2$'s contains 1, this implies that in the $\mathbf{A}$-module generated by C there is a vector $g^{1,2}$ of the type ${}^{\text{t}}[\, 1 \; 0 \; g_3^{1,2} \cdots g_m^{1,2} \,]$ and a vector $g^{2,1}$ of the type ${}^{\text{t}}[\, 0 \; 1 \; g_3^{2,1} \cdots g_m^{2,1} \,]$. The general case is similar replacing 1 and 2 with two integers $i \neq j \in [\![1..m]\!]$.

We deduce that ${}^{\text{t}}[\, 1 \; 0 \; 0 \cdots 0 \,] = g^{1,2} \cdot g^{1,3} \cdots g^{1,m}$ is in the $\mathbf{A}$-algebra generated by C. Similarly, each vector of the canonical basis of $\mathbf{A}^m$ will be in the $\mathbf{A}$-algebra generated by C. We actually get that $\mathbf{A}^m$ is the image of a matrix whose columns are the products of at most m columns in C. □

7.6. Notations. *(Context of Dedekind's lemma)*

- $\mathbf{A}$ is a commutative ring.
- $(M, \cdot, 1)$ is a monoid.
- $\tau = (\tau_1, \tau_2, \ldots, \tau_m)$ is a list of m homomorphisms, pairwise well-separated, of $(M, \cdot, 1)$ in $(\mathbf{A}, \cdot, 1)$.
- For $z \in M$ we denote by $\tau(z)$ the element of $\mathbf{A}^m$ defined by
$$\tau(z) = {}^{\text{t}}[\, \tau_1(z) \cdots \tau_m(z) \,].$$

7.7. Theorem. (Dedekind's lemma)
Using the notations in 7.6 there exist $y_1, \ldots, y_r \in M$ such that the matrix

$$[\, \tau(y_1) \mid \cdots \mid \tau(y_r) \,] = \big(\tau_i(y_j)\big)_{i \in [\![1..m]\!], j \in [\![1..r]\!]}$$

is surjective.

Weak form. *In particular, $\tau_1, \ldots, \tau_m$ are $\mathbf{A}$-linearly independent.*

D This is deduced from Lemma 7.5 by noting that, since $\tau(xy) = \tau(x)\tau(y)$, the $\mathbf{A}$-algebra generated by the $\tau(x)$ coincide with the $\mathbf{A}$-module generated by the $\tau(x)$. □

Remarks.
1) Let $F = \big(\tau_i(y_j)\big)_{ij} \in \mathbf{A}^{m\times r}$. The linear independence of the rows means that $\mathcal{D}_m(F)$ is faithful, whereas the surjectivity of F means that $\mathcal{D}_m(F)$ contains 1. Sometimes, Dedekind's lemma is called "Artin's theorem" or the "independence of characters lemma," when one has in view the case where $\mathbf{A}$ is a discrete field. In fact, it is only when $\mathbf{A}$ is a zero-dimensional ring that we can deduce "$\mathcal{D}_m(F) = \langle 1\rangle$" from "$\mathcal{D}_m(F)$ is faithful."

2) The integer r can be controlled from the data in the problem. ∎

Artin's theorem and first consequences

7.8. Definition and notation. Let $\mathbf{A}$ be a $\mathbf{k}$-algebra with $\mathbf{k} \subseteq \mathbf{A}$.

1. We can equip the $\mathbf{k}$-module $\mathrm{L}_\mathbf{k}(\mathbf{A},\mathbf{A})$ with an $\mathbf{A}$-module structure by the external law
$$(y,\varphi) \mapsto \big(x \mapsto y\varphi(x)\big), \quad \mathbf{A} \times \mathrm{L}_\mathbf{k}(\mathbf{A},\mathbf{A}) \to \mathrm{L}_\mathbf{k}(\mathbf{A},\mathbf{A})\,.$$
We then denote this $\mathbf{A}$-module by $\mathrm{Lin}_\mathbf{k}(\mathbf{A},\mathbf{A})$.

Let $G = \{\sigma_1 = \mathrm{Id}, \sigma_2, \ldots, \sigma_n\}$ be a finite group operating (by $\mathbf{k}$-automorphisms) on $\mathbf{A}$.

2. The $\mathbf{A}$-linear map $\iota_G : \prod_{\sigma\in G} \mathbf{A} \to \mathrm{Lin}_\mathbf{k}(\mathbf{A},\mathbf{A})$ is defined by
$$\iota_G\big((a_\sigma)_{\sigma\in G}\big) = \textstyle\sum_{\sigma\in G} a_\sigma \sigma\,.$$
3. The $\mathbf{k}$-linear map $\psi_G : \mathbf{A}^{\mathrm{e}}_\mathbf{k} \to \prod_{\sigma\in G} \mathbf{A}$ is defined by
$$\psi_G(a\otimes b) = \big(a\sigma(b)\big)_{\sigma\in G}\,.$$
This is a homomorphism of $\mathbf{A}$-algebras (on the left-hand side).

7.9. Fact. *With the above notations, and the left-structure for the $\mathbf{A}$-module $\mathbf{A}^{\mathrm{e}}_\mathbf{k}$, we have the following results.*

1. *Saying that ι_G is an isomorphism means that $\mathrm{Lin}_\mathbf{k}(\mathbf{A},\mathbf{A})$ is a free $\mathbf{A}$-module whose G is a basis.*
2. *If $\mathbf{A}$ is strictly étale of constant rank over $\mathbf{k}$, saying that $\mathbf{A}^{\mathrm{e}}_\mathbf{k}$ is a free $\mathbf{A}$-module of finite rank means that $\mathbf{A}$ diagonalizes itself.*
3. *Saying that ψ_G is an isomorphism means precisely the following.*
The $\mathbf{A}$-module $\mathbf{A}^{\mathrm{e}}_\mathbf{k}$ is free of rank $\#G$, with a basis $\mathcal{B}$ such that, after scalar extension from $\mathbf{k}$ to $\mathbf{A}$, the linear map $\mu_{\mathbf{A},a}$, which has become $\mu_{\mathbf{A}^{\mathrm{e}}_\mathbf{k},1\otimes a}$, is now diagonal over the basis $\mathcal{B}$, with matrix
$$\mathrm{Diag}\,\big(\sigma_1(a), \sigma_2(a), \ldots, \sigma_n(a)\big)$$
for any $a \in \mathbf{A}$.

7.10. Lemma.
Let $G = \{\sigma_1 = \mathrm{Id}, \sigma_2, \ldots, \sigma_n\}$ be a finite group operating on a ring $\mathbf{A}$ and let $\mathbf{k} = \mathbf{A}^G$. For $y \in \mathbf{A}$, let $y^\star$ be the element of $\mathbf{A}^\star$ defined by $x \mapsto \mathrm{Tr}_G(xy)$. The following properties are equivalent.

1. *$(\mathbf{k}, \mathbf{A}, G)$ is a Galois algebra.*
2. *There exist $x_1, \ldots, x_r, y_1, \ldots, y_r$ in $\mathbf{A}$ such that for every $\sigma \in G$ we have*
$$\sum\nolimits_{i=1}^r x_i\sigma(y_i) = \begin{cases} 1 & \textit{if } \sigma = \mathrm{Id} \\ 0 & \textit{otherwise}. \end{cases} \tag{10}$$

In this case we have the following results.

3. *For $z \in \mathbf{A}$, we have $z = \sum_{i=1}^r \mathrm{Tr}_G(zy_i)\, x_i = \sum_{i=1}^r \mathrm{Tr}_G(zx_i)\, y_i$.*
In other words, $\mathbf{A}$ is a finitely generated projective $\mathbf{k}$-module and
$$\big((x_1, \ldots, x_r), (y_1^\star, \ldots, y_r^\star)\big) \quad \textit{and} \quad \big((y_1, \ldots, y_r), (x_1^\star, \ldots, x_r^\star)\big)$$
are coordinate systems.
4. *The form $\mathrm{Tr}_G : \mathbf{A} \to \mathbf{k}$ is dualizing and surjective.*
5. *For $\sigma \in G$, let $\varepsilon_\sigma = \sum_i \sigma(x_i) \otimes y_i \in \mathbf{A}^{\mathrm{e}}_{\mathbf{k}}$. Then, $(\varepsilon_\sigma)_{\sigma\in G}$ is an $\mathbf{A}$-basis "on the left-hand side" of $\mathbf{A}^{\mathrm{e}}_{\mathbf{k}}$. In addition, for a, $b \in \mathbf{A}$, We have*
$$b \otimes a = \sum\nolimits_\sigma b\sigma(a)\varepsilon_\sigma,$$
and the image of this basis $(\varepsilon_\sigma)_\sigma$ under $\psi_G : \mathbf{A}^{\mathrm{e}}_{\mathbf{k}} \to \prod_{\tau\in G} \mathbf{A}$ is the canonical $\mathbf{A}$-basis $(e_\sigma)_{\sigma\in G}$ of $\prod_{\tau\in G} \mathbf{A}$. Consequently, ψ_G is an isomorphism of $\mathbf{A}$-algebras.

▷ *1 ⇒ 2.* By Dedekind's lemma, there exist an integer r and elements $x_1, \ldots, x_r, y_1, \ldots, y_r \in \mathbf{A}$ such that

$$\sum_{i=1}^r x_i \begin{bmatrix} \sigma_1(y_i) \\ \sigma_2(y_i) \\ \vdots \\ \sigma_n(y_i) \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix},$$

meaning, for $\sigma \in G$, precisely Equations (10).

2 ⇒ 1. For $\sigma \neq \mathrm{Id}$, we have $\sum_{i=1}^r x_i\big(y_i - \sigma(y_i)\big) = 1$, which proves that σ is separating.

3. For $z \in \mathbf{A}$, we have the equalities

$$\begin{aligned} \sum\nolimits_{i=1}^r \mathrm{Tr}_G(zy_i)\, x_i \;=\; \sum\nolimits_{i=1}^r \sum\nolimits_{j=1}^n \sigma_j(zy_i)x_i \;= \\ \sum\nolimits_{j=1}^n \sigma_j(z)\big(\sum\nolimits_{i=1}^r \sigma_j(y_i)x_i\big) \;=\; \sigma_1(z)\cdot 1 + \sum\nolimits_{j=2}^n \sigma_j(z)\cdot 0 \;=\; z. \end{aligned}$$

3 ⇒ 4. By item *1* of Theorem 5.2.

5. We have $\psi_G(\varepsilon_\sigma) = \big(\sum_i \sigma(x_i)\tau(y_i)\big)_\tau = e_\sigma$. Let us now show the equality with respect to $b \otimes a$. Given the chosen $\mathbf{A}$-module structure on the left-hand side, we can assume that $b = 1$. Then

$$\begin{aligned}\textstyle\sum_\sigma \sigma(a)\varepsilon_\sigma &= \textstyle\sum_\sigma \sigma(a)\sum_i \sigma(x_i)\otimes y_i = \sum_i \mathrm{Tr}_G(ax_i)\otimes y_i \\ &= \textstyle\sum_i 1\otimes \mathrm{Tr}_G(ax_i)y_i = 1\otimes\sum_i \mathrm{Tr}_G(ax_i)y_i = 1\otimes a.\end{aligned}$$

This shows that $(\varepsilon_\sigma)_\sigma$ is a generator set of the $\mathbf{A}$-module $\mathbf{A}^{\mathrm{e}}_{\mathbf{k}}$. As its image under ψ_G is the canonical $\mathbf{A}$-basis of $\prod_{\tau\in G}\mathbf{A}$, this system is free over $\mathbf{A}$. The rest follows from this. □

Remark. Here is an alternative proof of the surjectivity of the trace (item *4*). For $z = 1$, $1 = \sum_{i=1}^r t_i x_i$ with $t_i = \mathrm{Tr}_G(y_i) \in \mathrm{Tr}_G(\mathbf{A}) \subseteq \mathbf{k}$. Let us introduce the "normic" polynomial $N(T_1,\ldots,T_r)$:

$$N(T_1,\ldots,T_r) = \mathrm{N}_G\big(\textstyle\sum_{i=1}^r T_i x_i\big) = \prod_{\sigma\in G}\big(T_1\sigma(x_1)+\cdots+T_r\sigma(x_r)\big).$$

It is a homogeneous polynomial of degree $n \geqslant 1$, invariant under G, therefore with coefficients in $\mathbf{k}$: $N(\underline{T}) = \sum_{|\alpha|=n}\lambda_\alpha \underline{T}^\alpha$ with $\lambda_\alpha \in \mathbf{k}$. Consequently, for u_1, …, $u_r \in \mathbf{k}$, we have $N(u_1,\ldots,u_r) \in \mathbf{k}u_1+\cdots+\mathbf{k}u_r$. In particular

$$1 = \mathrm{N}_G(1) = \mathrm{N}_G\big(\textstyle\sum_{i=1}^r t_i x_i\big) = N(t_1,\ldots,t_r) \in \mathbf{k}t_1+\cdots+\mathbf{k}t_r \subseteq \mathrm{Tr}_G(\mathbf{A}). \quad ■$$

7.11. Theorem. (Artin's theorem, Galois algebras version)
Let $(\mathbf{k},\mathbf{A},G)$ be a Galois algebra (notations in 7.8).

1. *The $\mathbf{k}$-module $\mathbf{A}$ is projective of constant rank $\#G$, and $\mathbf{k}$ is a direct summand in $\mathbf{A}$.*
2. *There exist x_1, …, x_r and y_1, …, y_r such that for all σ, $\tau \in G$ we have*

$$\forall \sigma,\tau\in G \qquad \sum_{i=1}^r \tau(x_i)\sigma(y_i) = \begin{cases} 1 & \text{if } \sigma=\tau \\ 0 & \text{otherwise.}\end{cases} \tag{11}$$

3. *The form Tr_G is dualizing.*
4. *The map $\psi_G : \mathbf{A}^{\mathrm{e}}_{\mathbf{k}} \to \prod_{\sigma\in G}\mathbf{A}$ is an isomorphism of $\mathbf{A}$-algebras. In particular, $\mathbf{A}$ diagonalizes itself.*
5. *a. $\mathrm{C}_G(x)(T) = \mathrm{C}_{\mathbf{A}/\mathbf{k}}(x)(T)$, $\mathrm{Tr}_G = \mathrm{Tr}_{\mathbf{A}/\mathbf{k}}$ and $\mathrm{N}_G = \mathrm{N}_{\mathbf{A}/\mathbf{k}}$,*
   b. $\mathbf{A}$ is strictly étale over $\mathbf{k}$.
6. *If $\mathbf{A}$ is a discrete field, it is a Galois extension of $\mathbf{k}$, and we have $G = \mathrm{Gal}(\mathbf{A}/\mathbf{k})$.*

D In this proof, for $x \in \mathbf{A}$, we let $\mathrm{Tr}(x) = \mathrm{Tr}_G(x)$, and $x^\star$ is the $\mathbf{k}$-linear form $z \mapsto \mathrm{Tr}(zx)$.

Lemma 7.10 proves items *1* (besides the rank question), *3* and *4*. It also proves item *2*, because (11) clearly results from (10).
Note that $\mathbf{k}$ is a direct summand in $\mathbf{A}$ by item *3* of Lemma 4.3.[9]

Let us see that $\mathbf{A}$ is indeed of constant rank n. Item *4* shows that, after scalar extension from $\mathbf{k}$ to $\mathbf{A}$, the $\mathbf{k}$-module $\mathbf{A}$ becomes free of rank $\#G$.

[9] Or more directly, by the surjectivity of the trace (which results from Theorem 5.5 *1*. Indeed, let $x_0 \in \mathbf{A}$ such that $\mathrm{Tr}(x_0) = 1$. We have $\mathbf{A} = \mathbf{k}\cdot 1 \oplus \mathrm{Ker}\,x_0^\star$, because every $y \in \mathbf{A}$ can be written as $y = x_0^\star(y)\cdot 1 + (y - x_0^\star(y)\cdot 1)$ with $y - x_0^\star(y)\cdot 1 \in \mathrm{Ker}\,x_0^\star$.

Thus **A** is indeed of constant rank n over **k**; the rank polynomial of the **k**-module **A** “does not change” under the scalar extension $\mathbf{k} \to \mathbf{A}$ (injective), it is therefore itself equal to T^n.[10]

5a (and so *5b*) Since ψ_G is an isomorphism of **A**-algebras (item *4*), **A** diagonalizes itself. We then deduce from Fact 7.9 item *3*, the equality

$$\mathrm{C}_G(x)(T) = \mathrm{C}_{\mathbf{A}/\mathbf{k}}(x)(T).$$

This is true for the polynomials in $\mathbf{A}[T]$, therefore also in $\mathbf{k}[T]$.

6. First of all, the ring **k** is zero-dimensional by Lemma IV-8.15. It is therefore a discrete field, because it is connected and reduced. The extension is étale. It is normal, because every $x \in \mathbf{A}$ annihilates $\mathrm{C}_G(x)(T)$, and this polynomial can be decomposed into a product of linear factors in $\mathbf{A}[T]$. □

Remark. The computation that follows can clarify things, despite it not being necessary.

Note that by item *3* of Lemma 7.10, the **k**-module **A** is the image of the projection matrix

$$P = (p_{ij})_{i,j\in\llbracket 1..r\rrbracket} = \big(y_i^\star(x_j)\big)_{i,j\in\llbracket 1..r\rrbracket} = \big(\operatorname{Tr}(y_ix_j)\big)_{i,j\in\llbracket 1..r\rrbracket}.$$

Also recall Equation (11): $\sum_{i=1}^r \tau(x_i)\sigma(y_i) = \begin{cases} 1 & \text{if } \sigma=\tau \\ 0 & \text{otherwise}\end{cases}.$

Then let

$$X = \begin{bmatrix} \sigma_1(x_1) & \sigma_1(x_2) & \cdots & \sigma_1(x_r) \\ \sigma_2(x_1) & \sigma_2(x_2) & \cdots & \sigma_2(x_r) \\ \vdots & \vdots & & \vdots \\ \sigma_n(x_1) & \sigma_n(x_2) & \cdots & \sigma_n(x_r) \end{bmatrix} \quad \text{and}$$

$$Y = \begin{bmatrix} \sigma_1(y_1) & \sigma_1(y_2) & \cdots & \sigma_1(y_r) \\ \sigma_2(y_1) & \sigma_2(y_2) & \cdots & \sigma_2(y_r) \\ \vdots & \vdots & & \vdots \\ \sigma_n(y_1) & \sigma_n(y_2) & \cdots & \sigma_n(y_r) \end{bmatrix}.$$

By Equation (11), we have $X\,{}^{\mathrm{t}}Y = \mathrm{I}_n$ and $P = {}^{\mathrm{t}}YX$.

By Proposition V-2.11, this means that the **k**-module **A**, becomes free of rank n, with for basis the n rows of Y, after scalar extension from **k** to **A**. In other words, the **A**-module $\mathbf{A}^{\mathrm{e}}_{\mathbf{k}}$, seen as an image of the matrix P “with coefficients in **A**” is a free **A**-submodule of rank n of $\mathbf{A}^r$, and it is a direct summand. ■

[10] Actually, its coefficients are transformed into “themselves,” viewed in **A**.

7.12. Corollary. (Free Galois algebra)
Let $(\mathbf{k}, \mathbf{A}, G)$ *be a free Galois algebra, and* $n = \#G$. *If* $\underline{b} = (b_1, \dots, b_n)$ *in* $\mathbf{A}$, *we define* $M_{\underline{b}} \in \mathbb{M}_n(\mathbf{A})$ *by* $M_{\underline{b}} = \big(\sigma_i(b_j)\big)_{i,j\in[\![1..n]\!]}$.

Then, for two systems $\underline{b}$, $\underline{b}'$ *of* n *elements of* $\mathbf{A}$ *we obtain*

$$ {}^{\mathrm{t}}M_{\underline{b}}\, M_{\underline{b}'} = \mathrm{Tr}_G(b_i b'_j)_{i,j\in[\![1..n]\!]}. $$

Consequently, we obtain the following results.

- $\det(M_{\underline{b}})^2 = \mathrm{disc}(b_1, \dots, b_n)$.
- *The system* $(b_1, \dots, b_n)$ *is a* $\mathbf{k}$*-basis of* $\mathbf{A}$ *if and only if the matrix* $M_{\underline{b}}$ *is invertible.*
- *In this case, if* $\underline{b}'$ *is the dual basis of* $\underline{b}$ *with respect to the trace-valued bilinear form, then the matrices* $M_{\underline{b}}$ *and* $M_{\underline{b}'}$ *are inverses of one another.*

Remark. In the situation where $\mathbf{A}$ is a discrete field, Dedekind's lemma in its original form asserts that the "Dedekind matrix" $M_{\underline{b}}$ is invertible when $(\underline{b})$ is a basis of $\mathbf{A}$ as a $\mathbf{k}$-vector space. ■

7.13. Theorem. (Scalar extension for Galois algebras)
Let $(\mathbf{k}, \mathbf{A}, G)$ *be a Galois algebra,* $\rho : \mathbf{k} \to \mathbf{k}'$ *be an algebra and* $\mathbf{A}' = \rho_\star(\mathbf{A})$.

1. *The group* G *operates naturally over* $\mathbf{A}'$ *and* $(\mathbf{k}', \mathbf{A}', G)$ *is a Galois algebra.*
2. *The "Galois theory" of* $(\mathbf{k}', \mathbf{A}', G)$ *is deduced by scalar extension of that of* $(\mathbf{k}, \mathbf{A}, G)$, *in the following sense: for each finite subgroup* H *of* G, *the natural homomorphism* $\rho_\star(\mathbf{A}^H) \to \mathbf{A}'^H$ *is an isomorphism.*

D *1.* We easily see that G acts on $\mathbf{A}'$ in a separating way. It remains to show that $\mathbf{k}'$ is the subring of G-invariant elements of $\mathbf{A}'$.
Let $\mathrm{Tr} = \mathrm{Tr}_G$. We see Tr as a $\mathbf{k}$-endomorphism of $\mathbf{A}$, which by scalar extension gives the $\mathbf{k}'$-endomorphism $\mathrm{Id}_{\mathbf{k}'} \otimes \mathrm{Tr}$ of $\mathbf{A}'$.
Let $y \in \mathbf{A}'^G$. For $z \in \mathbf{A}'$, since y is G-invariant, we have the equality

$$ (\mathrm{Id}_{\mathbf{k}'} \otimes \mathrm{Tr})(yz) = y\,(\mathrm{Id}_{\mathbf{k}'} \otimes \mathrm{Tr})(z). $$

By taking $z_0 = 1_{\mathbf{k}'} \otimes x_0$, where $x_0 \in \mathbf{A}$ satisfies $\mathrm{Tr}(x_0) = 1$, we obtain the desired membership

$$ y = (\mathrm{Id}_{\mathbf{k}'} \otimes \mathrm{Tr})(yz_0) \in \mathbf{k}' \otimes_{\mathbf{k}} \mathbf{k} = \mathbf{k}'. $$

2. Results from item *1.* Indeed, consider the Galois algebra $(\mathbf{A}^H, \mathbf{A}, H)$ and the scalar extension $\varphi : \mathbf{A}^H \to \mathbf{k}' \otimes_{\mathbf{k}} \mathbf{A}^H = \rho_\star(\mathbf{A}^H)$. We obtain the equality $\varphi_\star(\mathbf{A}) = \mathbf{A}'$. So $\big(\rho_\star(\mathbf{A}^H), \mathbf{A}', H\big)$ is a Galois algebra and $\mathbf{A}'^H = \rho_\star(\mathbf{A}^H)$.□

In the following theorem, we could have expressed the hypothesis by saying that the finite group G operates over the ring $\mathbf{A}$, and that $\mathbf{k}$ is a subring of $\mathbf{A}^H$.

7.14. Theorem. (Characterizations of Galois algebras)
Let G be a finite group operating over a $\mathbf{k}$-algebra $\mathbf{A}$ with $\mathbf{k} \subseteq \mathbf{A}$. The following properties are equivalent.

1. *$(\mathbf{k}, \mathbf{A}, G)$ is a Galois algebra (in particular, $\mathbf{k} = \mathbf{A}^G$).*
2. *$\mathbf{k} = \mathbf{A}^G$, and there exist $x_1, \ldots, x_r, y_1, \ldots, y_r$ in $\mathbf{A}$ such that we have for every $\sigma \in G$*
$$\textstyle\sum_{i=1}^r x_i\sigma(y_i) = \begin{cases} 1 & \text{if } \sigma = \mathrm{Id} \\ 0 & \text{otherwise.} \end{cases}$$
3. *$\mathbf{k} = \mathbf{A}^G$, $\mathbf{A}$ is finite over $\mathbf{k}$, and for every finite generator set $(a_j)_{j\in J}$ of $\mathbf{A}$ as a $\mathbf{k}$-module, there exists a family $(b_j)_{j\in J}$ in $\mathbf{A}$ such that we have for all σ, $\tau \in G$*
$$\textstyle\sum_{j\in J} \tau(a_j)\sigma(b_j) = \begin{cases} 1 & \text{if } \sigma = \tau \\ 0 & \text{otherwise.} \end{cases}$$
4. *$\mathbf{k} = \mathbf{A}^G$, and $\psi_G : \mathbf{A}^{\mathrm{e}}_{\mathbf{k}} \to \prod_{\sigma\in G} \mathbf{A}$ is an isomorphism of $\mathbf{A}$-algebras.*
5. *$\mathbf{A}$ is strictly finite over $\mathbf{k}$, and G is a basis of $\mathrm{Lin}_{\mathbf{k}}(\mathbf{A}, \mathbf{A})$.*

D We have already seen *1* ⇔ *2* and *1* ⇒ *4* (Lemma 7.10).
The implication *3* ⇒ *2* is clear.

2 ⇒ *3*. We express x_i in terms of a_j: $x_i = \sum_j u_{ij}a_j$ with $u_{ij} \in \mathbf{k}$. Then,
$$\textstyle\sum_j \sigma\big(\sum_i u_{ij}y_i\big)a_j = \sum_{j,i} u_{ij}\sigma(y_i)a_j = \sum_i \sigma(y_i)x_i = \delta_{\mathrm{Id},\sigma},$$
hence the result by taking $b_j = \sum_i u_{ij}y_i$.

2 ⇒ *5*. Let us first note that if $\varphi \in \mathrm{Lin}_{\mathbf{k}}(\mathbf{A}, \mathbf{A})$ is written as $\varphi = \sum_\sigma a_\sigma\sigma$, then by evaluating at y_i, by multiplying by $\tau(x_i)$ and by summing over the i's, we get
$$\textstyle\sum_i \varphi(y_i)\tau(x_i) = \sum_{i,\sigma} a_\sigma\sigma(y_i)\tau(x_i) = a_\tau.$$
This shows on the one hand that G is $\mathbf{A}$-free. On the other hand, this leads to believe that every $\varphi \in \mathrm{Lin}_{\mathbf{k}}(\mathbf{A}, \mathbf{A})$ is written as $\varphi = \sum_\sigma a_\sigma\sigma$ with $a_\sigma = \sum_i \varphi(y_i)\sigma(x_i)$. Let us verify this by evaluating $\varphi' := \sum_\sigma a_\sigma\sigma$ at $x \in \mathbf{A}$,
$$\textstyle\varphi'(x) = \sum_{i,\sigma} \varphi(y_i)\sigma(x_i)\sigma(x) = \sum_i \mathrm{Tr}_G(x_ix)\varphi(y_i) = \varphi(\sum_i \mathrm{Tr}_G(x_ix)y_i) = \varphi(x).$$

5 ⇒ *2*. Since $\mathbf{k} \subseteq \mathbf{A}$, we have an inclusion $\mathbf{A}^\star \hookrightarrow \mathrm{Lin}_{\mathbf{k}}(\mathbf{A}, \mathbf{A})$. Let us first show that $\mathbf{A}^G \subseteq \mathbf{k}$ (we will then have the equality). Each $\sigma \in G$ is $\mathbf{A}^G$-linear so, since G generates $\mathrm{Lin}_{\mathbf{k}}(\mathbf{A}, \mathbf{A})$ as an $\mathbf{A}$-module, each element φ of $\mathrm{Lin}_{\mathbf{k}}(\mathbf{A}, \mathbf{A})$ is $\mathbf{A}^G$-linear. In particular, each $\alpha \in \mathbf{A}^\star$ is $\mathbf{A}^G$-linear. Let $\big((x_i), (\alpha_i)\big)$ be a coordinate system of the $\mathbf{k}$-module $\mathbf{A}$. As $\mathbf{A}$ is a faithful $\mathbf{k}$-module, by Proposition V-8.11, there exists a family (z_i) in $\mathbf{A}$ such that $1 = \sum_i \alpha_i(z_i)$. Then, if $x \in \mathbf{A}^G$, $x = \sum_i \alpha_i(z_i)x = \sum_i \alpha_i(z_ix)$ belonging to $\mathbf{k}$.

Let us then show that for each $\alpha \in \mathbf{A}^\star$, there exists a unique $a \in \mathbf{A}$ such that $\alpha = \sum_{\sigma\in G} \sigma(a)\sigma$, i.e. such that α is the $\mathbf{k}$-linear form $x \mapsto \mathrm{Tr}_G(ax)$.

Since G is an $\mathbf{A}$-basis of $\mathrm{Lin}_{\mathbf{k}}(\mathbf{A},\mathbf{A})$, we have $\alpha = \sum_\sigma a_\sigma \sigma$ with $a_\sigma \in \mathbf{A}$. Let $a = a_{\mathrm{Id}}$. By writing, for $\tau \in G$, $\tau \circ \alpha = \alpha$, we obtain $\tau(a_\sigma) = a_{\sigma\tau}$, in particular $a_\tau = \tau(a)$, hence the desired equality $\alpha = \sum_{\sigma\in G} \sigma(a)\sigma$. In passing, we have just proven that the $\mathbf{k}$-linear map

$$\mathbf{A} \to \mathbf{A}^\star,\ a \mapsto \mathrm{Tr}_G(a\bullet)$$

is an isomorphism of $\mathbf{k}$-modules. We can therefore define a system (y_i) by the equalities $\alpha_i = \mathrm{Tr}_G(y_i\bullet)$. Then, for $x \in \mathbf{A}$ we obtain

$$x = \textstyle\sum_i \alpha_i(x)x_i = \sum_{i,\sigma} \sigma(y_i x)x_i = \sum_\sigma \big(\sum_i x_i\sigma(y_i)\big)\sigma(x),$$

i.e. $\mathrm{Id} = \sum_\sigma \big(\sum_i x_i\sigma(y_i)\big)\sigma$. But as G is $\mathbf{A}$-free, the expression of $\mathrm{Id} \in G$ is reduced to Id, so $\sum_i x_i\sigma(y_i) = 1$ if $\sigma = \mathrm{Id}$, 0 otherwise.

NB: Since $\sum_i x_iy_i = 1$, we have the equalities

$$\mathrm{Tr}(x) = \textstyle\sum_i \alpha_i(x_ix) = \sum_{i,\sigma} \sigma(x_iy_i)\sigma(x) = \sum_\sigma \sum_i \sigma(x_iy_i)\sigma(x) = \mathrm{Tr}_G(x).$$

4 ⇒ *2.* Let $z = \sum_i x_i \otimes y_i$ be the element of $\mathbf{A}^{\mathrm{e}}_{\mathbf{k}}$ defined by: $\psi_G(z)$ is the element of $\prod_{\sigma\in G} \mathbf{A}$ every component of which is null, except that of index Id which is equal to 1. This means precisely that $\sum_i x_i\sigma(y_i) = 1$ if $\sigma = \mathrm{Id}$ and 0 otherwise. □

The case of free Galois algebras is described in the following corollary, which is an immediate consequence of the previous more general results.

7.15. Corollary. (Characterizations of free Galois algebras)
Let G be a finite group operating on a $\mathbf{k}$-algebra $\mathbf{A}$ with $\mathbf{k} \subseteq \mathbf{A}$.
Assume that $\mathbf{A}$ is free over $\mathbf{k}$, of rank $n = |G|$, with $\underline{x} = (x_1, \dots, x_n)$ as its basis. The following properties are equivalent.

1. *$(\mathbf{k}, \mathbf{A}, G)$ is a Galois algebra (in particular, $\mathbf{k} = \mathbf{A}^G$).*
2. *The matrix $M_{\underline{x}} = \big(\sigma_i(x_j)\big)_{i,j\in[\![1..n]\!]}$ is invertible (we have indexed the group G by $[\![1..n]\!]$).*
3. *The form Tr_G is dualizing.*
4. *$\mathbf{k} = \mathbf{A}^G$, and there exist $y_1, \dots, y_n$ in $\mathbf{A}$ such that we have for every $\sigma \in G$*
$$\textstyle\sum_{i=1}^n x_i\sigma(y_i) = \begin{cases} 1 & \textit{if}\ \sigma = \mathrm{Id} \\ 0 & \textit{otherwise.}\end{cases}$$
5. *The group G is an $\mathbf{A}$-basis of $\mathrm{Lin}_{\mathbf{k}}(\mathbf{A},\mathbf{A})$.*
6. *$\mathbf{k} = \mathbf{A}^G$, and $\psi_G : \mathbf{A}^{\mathrm{e}}_{\mathbf{k}} \to \prod_{\sigma\in G} \mathbf{A}$ is an isomorphism of $\mathbf{A}$-algebras.*

In this case we have the following results.

7. *In items 4 and 3,*
   - *we obtain the y_i's as the solution of $M_{\underline{x}}.{}^{\mathrm{t}}[\,y_1\ \cdots\ y_n\,] = {}^{\mathrm{t}}[\,1\,0\cdots\,0\,]$, where $M_{\underline{x}}$ is defined as in item 2, with $\sigma_1 = Id$,*
   - *$(y_1^\star, \dots, y_n^\star)$ is the dual basis of $(x_1, \dots, x_n)$.*

8. *Item 6 can be specified as follows.*
   For $\sigma \in G$, we let $\varepsilon_\sigma = \sum_i \sigma(x_i) \otimes y_i \in \mathbf{A}^{\mathrm{e}}_{\mathbf{k}}$. Then, $(\varepsilon_\sigma)_{\sigma\in G}$ is an $\mathbf{A}$-basis for the left-structure of $\mathbf{A}^{\mathrm{e}}_{\mathbf{k}}$. In addition, for a, $b \in \mathbf{A}$, we have
   $$b \otimes a = \textstyle\sum_\sigma b\sigma(a)\varepsilon_\sigma$$
   and the image of this basis $(\varepsilon_\sigma)_\sigma$ under $\psi_G : \mathbf{A}^{\mathrm{e}}_{\mathbf{k}} \to \prod_{\tau\in G} \mathbf{A}$ is the canonical $\mathbf{A}$-basis $(e_\sigma)_{\sigma\in G}$ of $\prod_{\tau\in G} \mathbf{A}$.

Finally, we underline the following items, in which we do not suppose that $\mathbf{A}$ is free over $\mathbf{A}^G$.

- *When $\mathbf{A}$ is a discrete field (historical background of Artin's theorem), if a group G operates faithfully over $\mathbf{A}$, the algebra $(\mathbf{A}^G, \mathbf{A}, G)$ is always Galoisian, $\mathbf{A}^G$ is a discrete field and $\mathbf{A}$ is free of rank n over $\mathbf{A}^G$.*
- *When $\mathbf{A}$ is a residually discrete local ring, the algebra $(\mathbf{A}^G, \mathbf{A}, G)$ is Galoisian if and only if G operates faithfully over the residual field $\mathbf{A}/\operatorname{Rad}\mathbf{A}$. In this case, $\mathbf{A}^G$ is a residually discrete local ring and $\mathbf{A}$ is free of rank n over $\mathbf{A}^G$.*

Naturally, we strongly encourage the reader to give a more direct and shorter proof of the previous corollary. It is also possible to deduce the general results of the particular results stated in the case where $\mathbf{A}$ is a residually discrete local ring, which could themselves be deduced from the discrete fields case.

7.16. Theorem. (The Galois correspondence for a Galois algebra) *Let $(\mathbf{k}, \mathbf{A}, G)$ be a nontrivial Galois algebra, and H be a finite subgroup of G.*

1. *The triple $(\mathbf{A}^H, \mathbf{A}, H)$ is a Galois algebra, $\mathbf{A}^H$ is strictly étale over $\mathbf{k}$, of constant rank $[\mathbf{A}^H : \mathbf{k}] = |\, G : H \,|$.*
2. *If $H' \supseteq H$ is a finite subgroup of G, $\mathbf{A}^H$ is strictly finite over $\mathbf{A}^{H'}$, of constant rank $[\mathbf{A}^H : \mathbf{A}^{H'}] = |\, H' : H \,|$.*
3. *We have $H = \operatorname{Stp}(\mathbf{A}^H)$.*
4. *The map $\operatorname{Fix}_{\mathbf{A}}$ restricted to the finite subgroups of G is injective.*
5. *If H is normal in G, $(\mathbf{k}, \mathbf{A}^H, G/H)$ is a Galois algebra.*

D *1.* Since H is a separating group of automorphisms of $\mathbf{A}$, $(\mathbf{A}^H, \mathbf{A}, H)$ is a Galois algebra. So $\mathbf{A}$ is a strictly finite $\mathbf{A}^H$-algebra of constant rank $\#H$. Therefore $\mathbf{A}^H$ is strictly finite over $\mathbf{k}$, of constant rank equal to $|\, G : H \,|$ (Theorem 4.5). In addition, it is strictly étale by Fact 5.7.

2. We apply Theorem 4.5.

3. The inclusion $H \subseteq \operatorname{Stp}(\mathbf{A}^H)$ is obvious. Let $\sigma \in \operatorname{Stp}(\mathbf{A}^H)$ and H' be the subgroup generated by H and σ. We have $|\, H' : H \,| = [\mathbf{A}^H : \mathbf{A}^{H'}]$, but $\mathbf{A}^H = \mathbf{A}^{H'}$, therefore $H' = H$ and $\sigma \in H$.

4. Results from *3.*

5. First of all, for $\sigma \in G$, we have $\sigma(\mathbf{A}^H) = \mathbf{A}^H$. If we let $\overline{\sigma}$ be the restriction of σ to $\mathbf{A}^H$, we obtain a morphism of groups $G \to \mathrm{Aut}_{\mathbf{k}}(\mathbf{A}^H)$, $\sigma \mapsto \overline{\sigma}$, whose kernel is H by item *3.* The quotient group G/H is therefore realized as a subgroup of $\mathrm{Aut}_{\mathbf{k}}(\mathbf{A}^H)$.

Let $x \in \mathbf{A}$ satisfy $\mathrm{Tr}_H(x) = 1$, $(a_1, \ldots, a_r)$ be a generator set of $\mathbf{A}$ as a $\mathbf{k}$-module, and $b_1, \ldots, b_r$ be some elements such that for all σ, $\tau \in G$ we have $\sum_{i=1}^r \tau(a_i)\sigma(b_i) = \begin{cases} 1 & \text{if } \sigma = \tau \\ 0 & \text{otherwise.} \end{cases}$ We then define, for $i \in [\![1..r]\!]$, the elements of $\mathbf{A}^H$, $a_i' = \mathrm{Tr}_H(xa_i)$, and $b_i' = \mathrm{Tr}_H(b_i)$.

We easily verify that for $\sigma \in G$ we have

$$\textstyle\sum_{i=1}^r a_i'\sigma(b_i') = \begin{cases} 1 & \text{if } \sigma \in H \\ 0 & \text{otherwise.} \end{cases}$$

Thus, when applying item *2* of Theorem 7.14, $(\mathbf{k}, \mathbf{A}^H, \mathrm{G}/H)$ is a Galois algebra. □

Theorem 7.16 above establishes the Galois correspondence between finite subgroups of G on the one hand and "certain" strictly étale $\mathbf{k}$-subalgebras of $\mathbf{A}$ on the other. An exact bijective correspondence will be established in the following subsection when $\mathbf{A}$ is connected.

However, beforehand we give a few additional results.

7.17. Proposition. *Let $(\mathbf{k}, \mathbf{A}, G)$ be a Galois algebra and H be a finite subgroup of G.*

1. *$\mathbf{A}$ diagonalizes $\mathbf{A}^H$.*
2. *For $b \in \mathbf{A}^H$, the characteristic polynomial of b (over $\mathbf{k}$, in $\mathbf{A}^H$) is given by $\mathrm{C}_{\mathbf{A}^H/\mathbf{k}}(b)(T) = \prod_{\sigma \in G/H} \big(T - \sigma(b)\big)$ (the subscript $\sigma \in G/H$ means that we take exactly one σ from each left coset of H, and we note that $\sigma(b)$ does not depend on the chosen representative σ).*

D Recall that $\mathbf{A}$ diagonalizes itself, as the isomorphism $\psi_G : \mathbf{A}^{\mathrm{e}}_{\mathbf{k}} \to \prod_{\sigma \in G} \mathbf{A}$ shows. We consider this product as the algebra of functions $\mathcal{F}(G, \mathbf{A})$. It is provided with a natural action of G on the left-hand side as follows

$$\sigma \in G,\ w \in \mathcal{F}(G, \mathbf{A}) : \sigma \cdot w \in \mathcal{F}(G, \mathbf{A}) \text{ defined by } \tau \mapsto w(\tau\sigma).$$

Similarly G acts on the left-hand side over the $\mathbf{A}$-algebra $\mathbf{A}^{\mathrm{e}}_{\mathbf{k}} = \mathbf{A} \otimes_{\mathbf{k}} \mathbf{A}$ via $\mathrm{Id} \otimes G$. We then verify that ψ_G is a G-morphism, i.e. that for $\tau \in G$, the following diagram commutes.

$$\begin{tikzcd}
\mathbf{A} \otimes_{\mathbf{k}} \mathbf{A} \arrow[r, "\psi_G"] \arrow[d, "\mathrm{Id}\otimes\tau"] & \mathcal{F}(G, \mathbf{A}) = \prod_{\sigma \in G} \mathbf{A} \arrow[d, "w \mapsto \tau \cdot w"] \\
\mathbf{A} \otimes_{\mathbf{k}} \mathbf{A} \arrow[r, "\psi_G"] & \mathcal{F}(G, \mathbf{A}) = \prod_{\sigma \in G} \mathbf{A}
\end{tikzcd}$$

1. Consider the commutative diagram

$$\begin{tikzcd}
\mathbf{A} \otimes_{\mathbf{k}} \mathbf{A}^H \arrow[r, "\varphi_H"] \arrow[d] & \mathcal{F}(G/H, \mathbf{A}) = \prod_{\sigma \in G/H} \mathbf{A} \arrow[d] \\
\mathbf{A} \otimes_{\mathbf{k}} \mathbf{A} \arrow[r, "\psi_G", "\sim"'] & \mathcal{F}(G, \mathbf{A}) = \prod_{\sigma \in G} \mathbf{A}
\end{tikzcd}$$

On the right-hand side, the vertical arrow is injective, and it identifies $\mathcal{F}(G/H, \mathbf{A})$ with the subset $\mathcal{F}(G, \mathbf{A})^H$ of $\mathcal{F}(G, \mathbf{A})$ (constant functions over the left cosets of H in G).
On the left, the vertical arrow (corresponding to the injection $\mathbf{A}^H \hookrightarrow \mathbf{A}$) is also an injection because $\mathbf{A}^H$ is a direct summand in $\mathbf{A}$ viewed as an $\mathbf{A}^H$-module. Finally, φ_H is defined by $a \otimes b \mapsto \big(a\sigma(b)\big)_{\sigma \in G/H}$.
Then, φ_H is an isomorphism of $\mathbf{A}$-algebras. Indeed, φ_H is injective, and for the surjectivity, it suffices to see that $(\mathbf{A} \otimes_{\mathbf{k}} \mathbf{A})^{\mathrm{Id} \otimes H} = \mathbf{A} \otimes_{\mathbf{k}} \mathbf{A}^H$. This is given by Theorem 7.13 for the Galois algebra $(\mathbf{A}^H, \mathbf{A}, H)$ and the scalar extension $\mathbf{A}^H \hookrightarrow \mathbf{A}$.

2. This results from item *1* and from the following lemma. □

7.18. Lemma. *Let* $\mathbf{A}$ *and* $\mathbf{B}$ *be two* $\mathbf{k}$*-algebras where* $\mathbf{B}$ *is strictly finite of constant rank* n*. Assume that* $\mathbf{A}$ *diagonalizes* $\mathbf{B}$ *by means of an isomorphism*

$$\psi : \mathbf{A} \otimes_{\mathbf{k}} \mathbf{B} \longrightarrow \mathbf{A}^n$$

given by "coordinates" denoted by $\psi_i : \mathbf{B} \to \mathbf{A}$*.*
Then, for $b \in \mathbf{B}$*, we have an equality*

$$\mathrm{C}_{\mathbf{B}/\mathbf{k}}(b)(T) = \prod_{i=1}^{n} \big(T - \psi_i(b)\big),$$

if we transform the left-hand side (which is an element of $\mathbf{k}[T]$*) into an element of* $\mathbf{A}[T]$ *via* $\mathbf{k} \to \mathbf{A}$*.*

D Immediate by the computation of the characteristic polynomial of an element in a diagonal algebra. □

The Galois correspondence when A is connected

The reader is invited to revisit Lemma 6.17.

7.19. Theorem. *If* $(\mathbf{k}, \mathbf{A}, G)$ *is a nontrivial Galois algebra and if* $\mathbf{A}$ *is* connected*, the Galois correspondence establishes a decreasing bijection between*

- *on the one hand, the set of detachable subgroups of* G*,*
- *and on the other hand, the set of* $\mathbf{k}$*-subalgebras of* $\mathbf{A}$ *which are separable.*

The latter set is also that of the subalgebras of $\mathbf{A}$ *which are strictly étale over* $\mathbf{k}$*.*

D Let $\mathbf{k} \subseteq \mathbf{A}' \subseteq \mathbf{A}$ with $\mathbf{A}'$ separable. By letting $H = \mathrm{Stp}(\mathbf{A}')$, we must show that $\mathbf{A}' = \mathbf{A}^H$. We of course have $\mathbf{A}' \subseteq \mathbf{A}^H$.
Consider the product $\mathbf{A}$-algebra $\mathbf{C} = \prod_{\sigma \in G} \mathbf{A} \simeq \mathbf{A}^n$ with $n = \#G$.
Let $p_\sigma : \mathbf{C} \to \mathbf{A}$ be the projection defined by $p_\sigma\big((a_\tau)_\tau\big) = a_\sigma$. Recall the isomorphism of $\mathbf{A}$-algebras $\psi_G : \mathbf{A} \otimes_{\mathbf{k}} \mathbf{A} \to \mathbf{C}$, $a \otimes b \mapsto \big(a\sigma(b)\big)_{\sigma \in G}$.
Since $\mathbf{A}$ is a finitely generated projective $\mathbf{k}$-module, the canonical morphism $\mathbf{A} \otimes_{\mathbf{k}} \mathbf{A}' \to \mathbf{A} \otimes_{\mathbf{k}} \mathbf{A}$ is injective. By composing it with ψ_G, we obtain an injective morphism of $\mathbf{A}$-algebras $\mathbf{A} \otimes_{\mathbf{k}} \mathbf{A}' \to \mathbf{C}$. In the above notation, we will identify $\mathbf{A} \otimes_{\mathbf{k}} \mathbf{A}'$ with its image $\mathbf{B}$ in $\mathbf{C} \simeq \mathbf{A}^n$.
Since $\mathbf{A}'$ is a separable $\mathbf{k}$-algebra, $\mathbf{B}$ is a separable $\mathbf{A}$-algebra. We can therefore apply Lemma 6.17. If we denote by π_σ the restriction of p_σ to $\mathbf{B}$, we must identify the equivalent relation over G defined by $\pi_\sigma = \pi_{\sigma'}$. For $a' \in \mathbf{A}'$, $1 \otimes a'$ corresponds by ψ_G to $\big(\tau(a')\big)_\tau$, so $\pi_\sigma(1 \otimes a') = \sigma(a')$. Consequently, $\pi_\sigma = \pi_{\sigma'}$ if and only if σ and σ' coincide over $\mathbf{A}'$ or, by definition of H, if and only if $\sigma^{-1}\sigma' \in H$, i.e. $\sigma H = \sigma' H$. We deduce that the equivalence classes are the left cosets of H in G. With the notations of Lemma 6.17, we therefore have $\mathbf{B} = \bigoplus_J \mathbf{A} e_J$, where J describes G/H. By using the $\mathbf{A}$-basis $(e_J)_J$ of $\mathbf{B}$, we then see that $\mathbf{B} = \mathbf{C}^H$.
It remains to “return” to $\mathbf{A}$. Via the inverse image under ψ_G, we have

$$(\mathbf{A} \otimes_{\mathbf{k}} \mathbf{A})^{\mathrm{Id} \otimes H} = \mathbf{A} \otimes_{\mathbf{k}} \mathbf{A}' \,.$$

In particular, $\mathbf{A} \otimes_{\mathbf{k}} \mathbf{A}^H \subseteq \mathbf{A} \otimes_{\mathbf{k}} \mathbf{A}'$. By applying $\mathrm{Tr}_G \otimes \mathrm{Id}_{\mathbf{A}}$ to this inclusion and by using the fact that $\mathrm{Tr}_G : \mathbf{A} \to \mathbf{k}$ is surjective, we obtain the inclusion

$$\mathbf{k} \otimes_{\mathbf{k}} \mathbf{A}^H \subseteq \mathbf{k} \otimes_{\mathbf{k}} \mathbf{A}', \text{ i.e.} \quad \mathbf{A}^H \subseteq \mathbf{A}' \,.$$

Thus $\mathbf{A}^H = \mathbf{A}'$, as required.

Finally, since the $\mathbf{k}$-algebras $\mathbf{A}^H$ are strictly étale and the strictly étale algebras are separable, it is clear that the separable $\mathbf{k}$-subalgebras of $\mathbf{A}$ coincide with the strictly étale $\mathbf{k}$-subalgebras. □

Remark. The theory of Galois algebras does not really require the use of separable algebras, even for the previous theorem that we can state with only strictly étale subalgebras of $\mathbf{A}$. For a proof of the theorem without using separable algebras, see Exercises 18 and 19. Nevertheless the theory of separable algebras, noteworthy in itself, sheds an interesting light on the Galois algebras. ■

Quotients of Galois algebras

7.20. Proposition. (Quotient of a Galois algebra by an invariant ideal)
Let $(\mathbf{k}, \mathbf{C}, G)$ *be a Galois algebra,* $\mathfrak{c}$ *be a* G*-invariant ideal of* $\mathbf{C}$ *and* $\mathfrak{a} = \mathfrak{c} \cap \mathbf{k}$.

1. *The triple* $(\mathbf{k}/\mathfrak{a}\,, \mathbf{C}/\mathfrak{c}\,, G)$ *is a Galois algebra.*

2. *This Galois algebra is naturally isomorphic to that obtained from* $(\mathbf{k}, \mathbf{C}, G)$ *by means of the scalar extension* $\mathbf{k} \to \mathbf{k}/\mathfrak{a}$.

D *1.* The group G operates on $\mathbf{C}/\mathfrak{c}$ because $\mathfrak{c}$ is (globally) invariant. Let us show that the natural injective homomorphism $\mathbf{k}/\mathfrak{a} \to (\mathbf{C}/\mathfrak{c})^G$ is surjective. If $x \in \mathbf{C}$ is G-invariant modulo $\mathfrak{c}$, we must find an element of $\mathbf{k}$ equal to x modulo $\mathfrak{c}$. Consider $x_0 \in \mathbf{C}$ satisfying $\mathrm{Tr}_G(x_0) = 1$; then $\mathrm{Tr}_G(xx_0)$ satisfies:

$$x = \textstyle\sum_{\sigma \in G} x\sigma(x_0) \equiv \sum_{\sigma \in G} \sigma(x)\sigma(x_0) = \mathrm{Tr}_G(xx_0) \bmod \mathfrak{c}\,.$$

Thus $(\mathbf{C}/\mathfrak{c})^G = \mathbf{k}/\mathfrak{a}$. Finally, it is clear that G operates in a separating way over $\mathbf{C}/\mathfrak{c}$.

2. The scalar extension $\mathbf{k} \to \mathbf{k}/\mathfrak{a}$ gives $(\mathbf{k}/\mathfrak{a}, \mathbf{C}/\mathfrak{a}\mathbf{C}, G)$ (Galois algebra), with $\mathfrak{a}\mathbf{C} \subseteq \mathfrak{c}$. We must verify that $\mathfrak{c} = \mathfrak{a}\mathbf{C}$.
The projection $\pi : \mathbf{C}/\mathfrak{a}\mathbf{C} \to \mathbf{C}/\mathfrak{c}$ is a $\mathbf{k}/\mathfrak{a}$-linear surjective map between projective modules, so $\mathbf{C}/\mathfrak{a}\mathbf{C} \simeq \mathbf{C}/\mathfrak{c} \oplus \mathrm{Ker}\,\pi$. As the two modules have the same constant rank $\#G$, the rank polynomial of $\mathrm{Ker}\,\pi$ is equal to 1, therefore $\mathrm{Ker}\,\pi = 0$ (Theorem V-8.4). □

In the definition that follows, we do not need to suppose that $(\mathbf{k}, \mathbf{C}, G)$ is a Galois algebra.

7.21. Definition. Let G be a finite group that operates on a $\mathbf{k}$-algebra $\mathbf{C}$.

1. An idempotent of $\mathbf{C}$ is said to be *Galoisian* if its orbit under G is a fundamental system of orthogonal idempotents (this requires that this orbit is a finite set, or, equivalently, that the subgroup $\mathrm{St}_G(e)$ is detachable).
2. An ideal of $\mathbf{C}$ is said to be *Galoisian* when it is generated by the complementary idempotent of a Galoisian idempotent e.
3. In this case, the group $\mathrm{St}_G(e)$ operates on the algebra $\mathbf{C}[1/e] \simeq \mathbf{C}/\langle 1-e \rangle$, and $\big(\mathbf{k}, \mathbf{C}[1/e], \mathrm{St}_G(e)\big)$ is called a *Galois quotient* of $(\mathbf{k}, \mathbf{C}, G)$.

7.22. Fact. *With the hypotheses of Definition 7.21, if* $\{e_1, \ldots, e_r\}$ *is the orbit of* e*, the natural* $\mathbf{k}$*-linear map* $\mathbf{C} \to \prod_{i=1}^r \mathbf{C}[1/e_i]$ *is an isomorphism of* $\mathbf{k}$*-algebras. Moreover, the* $\mathrm{St}_G(e_i)$*'s are pairwise conjugated by elements of* G *that permute the* $\mathbf{k}$*-algebras* $\mathbf{C}[1/e_i]$ *(they are therefore pairwise isomorphic). In particular* $\mathbf{C} \simeq \mathbf{C}[1/e]^r$.

7.23. Theorem. (Galois quotients of Galois algebras)
Every Galois quotient of a Galois algebra is a Galois algebra.

D See Theorem VII-4.3 (Galois quotients of pre-Galois algebras). □

Exercises and problems

Exercise 1. We recommend that the proofs which are not given, or are sketched, or left to the reader, etc, be done. But in particular, we will cover the following cases.

- Prove Theorem 3.9 (page 319).
- Prove Fact 3.11 (page 320).
- Prove the local-global principle 7.4 for Galois algebras.
- Verify Fact 7.9 (page 353).

Exercise 2. Give a detailed proof of item *2* of Theorem 1.9.

Exercise 3. Consider the product $\mathbf{A}$-algebra $\mathbf{B} = \mathbf{A}^n$.

1. Under what condition does some $x \in \mathbf{B}$ satisfy $\mathbf{B} = \mathbf{A}[x]$?
In this case, prove that $(1, x, \dots, x^{n-1})$ is an $\mathbf{A}$-basis of $\mathbf{B}$.

2. If $\mathbf{A}$ is a discrete field, under what condition does $\mathbf{B}$ admit a primitive element?

Exercise 4. Let $\mathbf{K}$ be a nontrivial discrete field, $\mathbf{B}$ be a reduced strictly finite $\mathbf{K}$-algebra and v be an indeterminate.
Consider the $\mathbf{L}$-algebra $\mathbf{B}(v) \overset{\text{def}}{=} \mathbf{K}(v) \otimes_{\mathbf{K}} \mathbf{B}$. Prove the following results.

1. $\mathbf{B}(v)$ is strictly finite over $\mathbf{K}(v)$.

2. If $\mathbf{B}$ is étale over $\mathbf{K}$, $\mathbf{B}(v)$ is étale over $\mathbf{K}(v)$.

3. Every idempotent of $\mathbf{B}(v)$ is in fact in $\mathbf{B}$.

Exercise 5. If $\mathbf{K}$ is a separably factorial discrete field, so is $\mathbf{K}(v)$, where v is an indeterminate.
NB: we do not assume that $\mathbf{K}$ is finite or infinite.

Exercise 6. *(The rings of integers of the extension $\mathbb{Q}(\sqrt{a}) \subset \mathbb{Q}(\sqrt{a}, \sqrt{2})$)*
Let $\mathbf{K} \subseteq \mathbf{L}$ be two number fields and $\mathbf{A} \subseteq \mathbf{B}$ be their rings of integers; here we give an elementary example where $\mathbf{B}$ is not a free $\mathbf{A}$-module.

1. Let $d \in \mathbb{Z}$ be squarefree. Determine the ring of integers of $\mathbb{Q}(\sqrt{d})$.

Let $a \in \mathbb{Z}$ squarefree with $a \equiv 3 \bmod 4$. Let $\mathbf{K} = \mathbb{Q}(\sqrt{a})$, $\mathbf{L} = \mathbf{K}(\sqrt{2})$, and $\beta = \sqrt{2}\frac{1+\sqrt{a}}{2}$. We define $\sigma \in \mathrm{Aut}(\mathbf{L}/\mathbf{K})$ and $\tau \in \mathrm{Aut}\big(\mathbf{L}/\mathbb{Q}(\sqrt{2})\big)$, by

$$\sigma(\sqrt{2}) = -\sqrt{2} \quad\text{and}\quad \tau(\sqrt{a}) = -\sqrt{a}.$$

2. Verify that $\beta \in \mathbf{B}$ and compute $(\sigma\tau)(\beta)$.

3. We want to show that $(1, \sqrt{2}, \sqrt{a}, \beta)$ (which is a $\mathbb{Q}$-basis of $\mathbf{L}$) is a $\mathbb{Z}$-basis of $\mathbf{B}$. Let $z = r + s\sqrt{2} + t\sqrt{a} + u\beta \in \mathbf{B}$ with r, s, t, $u \in \mathbb{Q}$.
Considering $(\sigma\tau)(z)$, show that $u \in \mathbb{Z}$ then that r, s, $t \in \mathbb{Z}$.

4. Express $\mathbf{B}$ as a finitely generated projective $\mathbf{A}$-module. Verify that it is isomorphic to its dual.

Exercise 7. *(Discriminant of the tensor product)*
Let $\mathbf{A}$, $\mathbf{A}'$ be two free $\mathbf{k}$-algebras of ranks n, n', $(\underline{x}) = (x_i)$ be a family of n elements of $\mathbf{A}$, $(\underline{x}') = (x'_j)$ be a family of n' elements of $\mathbf{A}'$. Let $\mathbf{B} = \mathbf{A} \otimes_{\mathbf{k}} \mathbf{A}'$ and $(\underline{x} \otimes \underline{x}')$ be the family $(x_i \otimes x'_j)$ of nn' elements of $\mathbf{B}$. Prove the equality

$$\mathrm{Disc}_{\mathbf{B}/\mathbf{k}}(\underline{x} \otimes \underline{x}') = \mathrm{Disc}_{\mathbf{A}/\mathbf{k}}(\underline{x})^{n'}\ \mathrm{Disc}_{\mathbf{A}'/\mathbf{k}}(\underline{x}')^{n}.$$

Exercise 8. *(Normal basis of a cyclic extension)*
Let $\mathbf{L}$ be a discrete field, $\sigma \in \mathrm{Aut}(\mathbf{L})$ of order n and $\mathbf{K} = \mathbf{L}^{\sigma}$ be the field of invariants under σ. Prove that there exists an $x \in \mathbf{L}$ such that $\big(x, \sigma(x), \cdots, \sigma^{n-1}(x)\big)$ is a $\mathbf{K}$-basis of $\mathbf{L}$; we then speak of a *normal basis* of $\mathbf{L}/\mathbf{K}$ (defined by x).

Exercise 9. *(Homography of order 3 and universal equation with Galois group* A_3*)*
We denote by A_n the subgroup of even permutations of S_n. Let $\mathbf{L} = \mathbf{k}(t)$ where $\mathbf{k}$ is a discrete field and t is indeterminate.

1. Check that $A = \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix}$ is of order 3 in $\mathbb{PGL}_2(\mathbf{k})$ and explain the origin of this matrix.

We denote by $\sigma \in \mathrm{Aut}_{\mathbf{k}}\big(\mathbf{k}(t)\big)$ the automorphism of order 3 associated with A (see Problem 1, we have $\sigma(f) = f(\frac{-1}{t+1})$), and $G = \langle \sigma \rangle$.

2. Compute $g = \mathrm{Tr}_G(t)$ and show that $\mathbf{k}(t)^G = \mathbf{k}(g)$.
3. Let a be an indeterminate over $\mathbf{k}$ and $f_a(T) = T^3 - aT^2 - (a+3)T - 1 \in \mathbf{k}(a)[T]$. Prove that f_a is irreducible, with Galois group A_3.
4. Prove that the polynomial $f_a(X)$ is a "generic polynomial with Galois group A_3" in the following sense: if $\mathbf{L}/\mathbf{K}$ is a Galois extension with Galois group A_3 ($\mathbf{L}$ being a discrete field), there exists a primitive element of $\mathbf{L}/\mathbf{K}$ whose minimal polynomial is $f_\alpha(X)$ for some value of $\alpha \in \mathbf{K}$.

Exercise 10. *(Algebra of a finite commutative group)*
Let $\mathbf{k}$ be a commutative ring, G be a commutative group of order n and $\mathbf{A} = \mathbf{k}[G]$ be the *algebra of the group* G, i.e. $\mathbf{A}$ admits G as a $\mathbf{k}$-basis and the product in $\mathbf{A}$ of two elements of G is their product in G.[11]

1. Determine $\mathrm{Ann}(\mathrm{J}_{\mathbf{A}/\mathbf{k}})$, its image under $\mu_{\mathbf{A}/\mathbf{k}}$ and the trace form over $\mathbf{A}$.
2. Prove that the following properties are equivalent.
   - n is invertible in $\mathbf{k}$.
   - $\mathbf{A}$ is strictly étale.
   - $\mathbf{A}$ is separable.
3. Prove that $\mathbf{k}[G]$ is a Frobenius algebra.

[11] The definition works also for *the algebra* $\mathbf{k}[M]$ *of a monoid* M.

Exercise 11. *(A finite monogenic algebra is a Frobenius algebra)*
Let $f = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbf{k}[X]$ and $\mathbf{A} = \mathbf{k}[X]/\langle f \rangle = \mathbf{k}[x]$. Consider the linear form $\lambda : \mathbf{A} \to \mathbf{k}$ defined by $x^{n-1} \mapsto 1$ and $x^i \mapsto 0$ for $i < n-1$. We will show that λ is dualizing and that $\mathrm{Tr}_{\mathbf{A}/\mathbf{k}} = f'(x) \centerdot \lambda$.
To that effect, we append an indeterminate Y. The system $(1, x, \ldots, x^{n-1})$ is a basis of $\mathbf{A}[Y]/\mathbf{k}[Y]$. Let $\widetilde{\lambda} : \mathbf{A}[Y] \to \mathbf{k}[Y]$ be the extension of λ and define the $\mathbf{k}[Y]$-linear map $\varphi : \mathbf{A}[Y] \to \mathbf{k}[Y]$, by $\varphi(x^i) = Y^i$ for $i \in [\![0..n-1]\!]$.

1. Prove that $\qquad \forall g \in \mathbf{A}[Y], \quad f(Y)\widetilde{\lambda}(g) = \varphi\big((Y-x)g\big) \qquad (*)$
2. We define the (triangular Horner) basis $(b_0, \ldots, b_{n-1})$ of $\mathbf{A}/\mathbf{k}$ by
$$\begin{aligned} b_0 &= x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_2x + a_1, \\ b_1 &= x^{n-2} + a_{n-1}x^{n-3} + \cdots + a_3x + a_2\,, \end{aligned}$$
and so on: $b_i = x^{n-i-1} + \cdots + a_{i+1}$ and $b_{n-1} = 1$. We have
$$f'(Y) = \frac{f(Y) - f(x)}{Y - x} = \frac{f(Y)}{Y - x} = b_{n-1}Y^{n-1} + \cdots + b_1Y + b_0.$$
Applying Equality $(*)$ to $g_i = x^i f'(Y)$, show that $(b_0 \centerdot \lambda, \ldots, b_{n-1} \centerdot \lambda)$ is the dual basis of $(1, x, \ldots, x^{n-1})$. Conclude the result.
3. Prove that $\mathrm{Tr}_{\mathbf{A}/\mathbf{k}} = f'(x) \centerdot \lambda$.

Exercise 12. *(Frobenius algebras: elementary examples and counterexamples)*
Throughout the exercise, $\mathbf{k}$ is a commutative ring.

1. Let $f_1, \ldots, f_n \in \mathbf{k}[T]$ be monic polynomials. Prove that the quotient $\mathbf{k}$-algebra $\mathbf{k}[X_1, \ldots, X_n]/\langle f_1(X_1), \ldots, f_n(X_n)\rangle$ is Frobenius and free of finite rank.

2. Let $\mathbf{A} = \mathbf{k}[X, Y]\big/\langle X, Y\rangle^2 = \mathbf{k}[x, y]$. Describe $\mathbf{A}^\star$ as a finitely presented $\mathbf{A}$-module. Deduce that $\mathbf{A}$ is not a Frobenius algebra.

3. Consider the analogous question to the previous one with $\mathbf{A} = \mathbf{k}[X, Y]/\langle X, Y\rangle^n$ for $n \geqslant 2$ and $\mathbf{B} = \mathbf{k}[X, Y]\big/\big\langle X^2, XY^{n+1}, Y^{n+2}\big\rangle$ for $n \geqslant 0$.

Exercise 13. *(The ideal $\mathrm{J}_{\mathbf{A}/\mathbf{k}}$ for a monogenic $\mathbf{k}$-algebra $\mathbf{A}$)*
Let $\mathbf{A} = \mathbf{k}[x]$ be a monogenic $\mathbf{k}$-algebra and $\mathbf{A}^{\mathrm{e}}_{\mathbf{k}} = \mathbf{A} \otimes_{\mathbf{k}} \mathbf{A}$ be its enveloping algebra. Let $y = x \otimes 1$, $z = 1 \otimes x$, such that $\mathbf{A}^{\mathrm{e}}_{\mathbf{k}} = \mathbf{k}[y, z]$. We know that $\mathrm{J}_{\mathbf{A}/\mathbf{k}} = \langle y - z\rangle$. Suppose $f(x) = 0$ for some $f \in \mathbf{k}[X]$ (not necessarily monic) and consider the symmetric polynomial $f^{\Delta}(Y, Z) = \big(f(Y) - f(Z)\big)/(Y - Z)$. It satisfies the equality $f^{\Delta}(X, X) = f'(X)$.

1. Let $\delta = f^{\Delta}(y, z)$. Prove that $\delta \in \mathrm{Ann}(\mathrm{J}_{\mathbf{A}/\mathbf{k}})$ and that $\delta^2 = f'(y)\delta = f'(z)\delta$.

2. Suppose that $1 \in \langle f, f'\rangle$.
2a. Prove that $\mathbf{A}$ is separable: make the separability idempotent explicit.
2b. Prove that $\mathrm{J}_{\mathbf{A}/\mathbf{k}} = \big\langle f^{\Delta}(y, z)\big\rangle$ and that $f^{\Delta}(y, z) = f'(y)\varepsilon_{\mathbf{A}/\mathbf{k}} = f'(z)\varepsilon_{\mathbf{A}/\mathbf{k}}$.

Remark. $\mathbf{A}$ is not necessarily strictly finite.

Exercise 14. *(Complete intersection, Jacobian, Bézoutian and separability)*
In this exercise, the number of indeterminates is equal to the number of polynomials. We define the *Bézoutian* of $(f_1,\dots,f_n)$ where each $f_i \in \mathbf{k}[\underline{X}] = \mathbf{k}[X_1,\dots,X_n]$ by

$$\beta_{\underline{Y},\underline{Z}}(\underline{f}) = \det \mathrm{BZ}_{\underline{Y},\underline{Z}}(\underline{f}),$$

so that $\beta_{\underline{X},\underline{X}}(\underline{f}) = \mathrm{Jac}_{\underline{X}}(\underline{f})$.

We denote by $\mathbf{A} = \mathbf{k}[x_1,\dots,x_n]$ a finitely generated $\mathbf{k}$-algebra and $\mathbf{A}^{\mathrm{e}}_{\mathbf{k}} = \mathbf{k}[\underline{y},\underline{z}]$ its enveloping algebra. Suppose that $f_i(\underline{x}) = 0$ for all i.

1. In the case where $\mathrm{Jac}_{\underline{x}}(f_1,\dots,f_n) \in \mathbf{A}^{\times}$, provide a direct proof of the fact that $\mathbf{A}$ is a separable algebra.

2. We define in $\mathbf{A}^{\mathrm{e}}_{\mathbf{k}}$

$$\varepsilon = \mathrm{Jac}_{\underline{y}}(\underline{f})^{-1}\beta_{\underline{y},\underline{z}}(\underline{f}) = \beta_{\underline{y},\underline{z}}(\underline{f})\,\mathrm{Jac}_{\underline{z}}(\underline{f})^{-1}.$$

Verify that $\beta_{\underline{y},\underline{z}}(\underline{f})$ and ε are generators of $\mathrm{Ann}(\mathrm{J}_{\mathbf{A}/\mathbf{k}})$ and that ε is the separability idempotent of $\mathbf{A}$.

3. Give examples.

Exercise 15. *(Separation of morphisms over a separable algebra)*
Let $\mathbf{k}$ be a commutative ring and $\mathbf{A}$, $\mathbf{B}$ be two $\mathbf{k}$-algebras with $\mathbf{A}$ separable. For any arbitrary function $f : \mathbf{A} \to \mathbf{B}$, we define $\mathrm{Ann}_{\mathbf{B}}(f) = \mathrm{Ann}_{\mathbf{B}}\langle f(\mathbf{A})\rangle$.

1. Prove that to every morphism $\varphi \in \mathrm{Hom}_{\mathbf{k}}(\mathbf{A},\mathbf{B})$ is attached a pair of finite families $(a_i)_{i\in I}$, $(b_i)_{i\in I}$, with $a_i \in \mathbf{A}$, $b_i \in \mathbf{B}$, satisfying the following properties:

- $\sum_i b_i\varphi(a_i) = 1$
- $\sum_i \varphi(a)b_i \otimes a_i = \sum_i b_i \otimes aa_i$ for every $a \in \mathbf{A}$.

2. If the pair of families $(a'_j)_j$, $(b'_j)_j$ is attached to the morphism $\varphi' \in \mathrm{Hom}_{\mathbf{k}}(\mathbf{A},\mathbf{B})$, show that

$$\textstyle\sum_i b_i\varphi'(a_i) = \sum_j b'_j\varphi(a'_j),$$

and that the latter element, denoted by e, is an idempotent of $\mathbf{B}$ having the following property of "separation of morphisms"

$$\mathrm{Ann}_{\mathbf{B}}(\varphi - \varphi') = \langle e\rangle_{\mathbf{B}}\,, \qquad \langle \mathrm{Im}(\varphi - \varphi')\rangle_{\mathbf{B}} = \langle 1 - e\rangle_{\mathbf{B}}\,.$$

3. Let φ_1, $\dots$, $\varphi_n \in \mathrm{Hom}_{\mathbf{k}}(\mathbf{A},\mathbf{B})$ and, for i, $j \in [\![1..n]\!]$, $e_{ij} = e_{ji}$ be the idempotent defined by $\mathrm{Ann}_{\mathbf{B}}(\varphi_i - \varphi_j) = \langle e_{ij}\rangle_{\mathbf{B}}$; in particular, $e_{ii} = 1$. We say that a matrix $A \in \mathbb{M}_{n,m}(\mathbf{B})$ is a *Dedekind evaluation matrix* for the n morphisms φ_1, $\dots$, φ_n if each column of A is of the form ${}^{\mathrm{t}}[\,\varphi_1(a)\ \cdots\ \varphi_n(a)\,]$ for some $a \in \mathbf{A}$ (depending on the column). Prove the existence of a Dedekind evaluation matrix whose image contains the vectors ${}^{\mathrm{t}}[\,e_{1i}\ \cdots\ e_{ni}\,]$. In particular, if $\mathrm{Ann}_{\mathbf{B}}(\varphi_i - \varphi_j) = 0$ for $i \neq j$, such a matrix is surjective.

Exercise 16. *(Another proof of Artin's theorem, item 2)*
The context is that of Theorem 7.11: $(\mathbf{k},\mathbf{A},G)$ is a Galois algebra and we want to show the existence of a_1, $\dots$, a_r, b_1, $\dots$, $b_r \in \mathbf{A}$ such that for every $\sigma \in G$

we have
$$\sum\nolimits_{i=1}^{r} a_i\sigma(b_i) = \begin{cases} 1 & \text{if } \sigma = \mathrm{Id} \\ 0 & \text{otherwise.} \end{cases}$$

For $\tau \in \mathrm{G}$, $\tau \neq \mathrm{Id}$, show that there exist m_τ and $x_{1,\tau}, \ldots, x_{m_\tau,\tau}, y_{1,\tau}, \ldots, y_{m_\tau,\tau}$ in $\mathbf{A}$ such that
$$\sum\nolimits_{j=1}^{m_\tau} x_{j,\tau}\tau(y_{j,\tau}) = 0, \qquad \sum\nolimits_{j=1}^{m_\tau} x_{j,\tau}y_{j,\tau} = 1.$$

Conclude the result.

Exercise 17. *(Galois algebras: a few elementary examples)*
Let $(e_1, \ldots, e_n)$ be the canonical basis of $\mathbf{k}^n$. We make S_n act on $\mathbf{k}^n$ by permutation of the coordinates: $\sigma(e_i) = e_{\sigma(i)}$ for $\sigma \in \mathrm{S}_n$.

1. Let $G \subset \mathrm{S}_n$ be a transitive subgroup of cardinality n.

- *a.* Prove that $(\mathbf{k}, \mathbf{k}^n, G)$ is a Galois algebra.
- *b.* Give examples.

2. Let $\mathbf{B} = \mathbf{k}(e_1 + e_2) \oplus \mathbf{k}(e_3 + e_4) \subset \mathbf{k}^4$ and $G = \langle(1, 2, 3, 4)\rangle$.
Determine $\mathrm{Stp}_{\mathrm{S}_4}(\mathbf{B})$ and $H = \mathrm{Stp}_G(\mathbf{B})$. Do we have $\mathbf{B} = (\mathbf{k}^4)^H$?

3. Let $(\mathbf{k}, \mathbf{A}, G)$ be a Galois algebra. The group G operates naturally on $\mathbf{A}[X]$.

- *a.* Prove that $(\mathbf{k}[X], \mathbf{A}[X], G)$ is a Galois algebra.
- *b.* Let $\mathbf{B} = X\mathbf{A}[X] + \mathbf{k}$ ($\mathbf{B}$ therefore consists of the polynomials of $\mathbf{A}[X]$ whose constant coefficient is in $\mathbf{k}$). Then, $\mathbf{B}$ is a $\mathbf{k}$-subalgebra of $\mathbf{A}[X]$ which is not of the form $\mathbf{A}[X]^H$ except in a special case.

Exercise 18. Let $\mathbf{k} \subseteq \mathbf{B} \subseteq \mathbf{C}$ with $\mathbf{B}$ strictly étale over $\mathbf{k}$ and $\mathbf{C}$ strictly finite over $\mathbf{k}$. Suppose that $\mathrm{rk}_{\mathbf{k}}(\mathbf{B}) = \mathrm{rk}_{\mathbf{k}}(\mathbf{C})$ (i.e. $\mathbf{C}$ and $\mathbf{B}$ have the same rank polynomial over $\mathbf{k}$). Then prove that $\mathbf{B} = \mathbf{C}$.

Exercise 19. Base yourself on Exercise 18 and prove the Galois correspondence (Theorem 7.19) between the finite subgroups of G and the strictly étale $\mathbf{k}$-subalgebras of $\mathbf{A}$ when $\mathbf{A}$ is connected.

Exercise 20. *(Galois algebras: globally invariant ideals)*
Let $(\mathbf{A}, \mathbf{B}, G)$ be a Galois algebra. We say that an ideal $\mathfrak{c}$ of $\mathbf{B}$ is *globally invariant* if $\sigma(\mathfrak{c}) = \mathfrak{c}$ for every $\sigma \in G$.

1. Prove that $\mathfrak{c}$ is generated by invariant elements, i.e. by elements of $\mathbf{A}$.

2. More precisely, consider the two transformations between ideals of $\mathbf{A}$ and ideals of $\mathbf{B}$: $\mathfrak{a} \mapsto \mathfrak{a}\mathbf{B}$ and $\mathfrak{c} \mapsto \mathfrak{c} \cap \mathbf{A}$. Prove that they establish a non-decreasing bijective correspondence between ideals of $\mathbf{A}$ and globally invariant ideals of $\mathbf{B}$.

Problem 1. *(Lüroth's theorem)*
Let $\mathbf{L} = \mathbf{k}(t)$ where $\mathbf{k}$ is a discrete field and t an indeterminate. If $g = u/v \in \mathbf{L}$ is a nonconstant irreducible fraction ($u, v \in \mathbf{k}[t]$, coprime), we define the *height* of g (with respect to t) by $\mathrm{height}_t(g) \overset{\mathrm{def}}{=} \max\big(\deg_t(u), \deg_t(v)\big)$.

1. *(Direct part of Lüroth's theorem)* Let $\mathbf{K} = \mathbf{k}(g) \subseteq \mathbf{L}$. Prove that $\mathbf{L}/\mathbf{K}$ is an algebraic extension of degree $d = \text{height}(g)$. More precisely, t is algebraic over $\mathbf{K}$ and its minimal polynomial is, up to multiplicative factor in $\mathbf{K}^\times$, equal to $u(T) - gv(T)$. Thus, every nonconstant coefficient of $\text{Min}_{\mathbf{K},t}(T)$, $a \in \mathbf{K} = \mathbf{k}(g)$ is of the form $a = \frac{\alpha g + \beta}{\gamma g + \delta}$ with $\alpha\delta - \beta\gamma \in \mathbf{k}^\times$, and $\mathbf{k}(a) = \mathbf{k}(g)$.
2. Let $f \in \mathbf{L}$ be an arbitrary element. Give an explicit formula using the resultants to express f as a $\mathbf{K}$-linear combination of $(1, t, \ldots, t^{d-1})$.
3. If h is another element of $\mathbf{L} \setminus \mathbf{k}$ show that
$$\text{height}\big(g(h)\big) = \text{height}(g)\text{height}(h).$$
Prove that every $\mathbf{k}$-algebra homomorphism $\mathbf{L} \to \mathbf{L}$ is of the form $f \mapsto f(h)$ for some $h \in \mathbf{L} \setminus \mathbf{k}$. Deduce a precise description of $\text{Aut}_{\mathbf{k}}(\mathbf{L})$ by means of fractions of height 1.
4. We denote by $\mathbb{PGL}_n(\mathbf{A})$ the quotient group $\mathbb{GL}_n(\mathbf{A})/\mathbf{A}^\times$ (where $\mathbf{A}^\times$ is identified with the subgroup of invertible homotheties via $a \mapsto a\text{I}_n$). To a matrix
$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathbb{GL}_2(\mathbf{A}),$$
we associate the $\mathbf{A}$-automorphism[12]
$$\varphi_A : \mathbf{A}(t) \to \mathbf{A}(t), \quad t \mapsto \tfrac{at+b}{ct+d}.$$
We have $\varphi_A \circ \varphi_B = \varphi_{BA}$ and $\varphi_A = \text{Id} \Leftrightarrow A = \lambda\text{I}_2$ ($\lambda \in \mathbf{A}^\times$). Thus $A \mapsto \varphi_A$ defines an injective homomorphism $\mathbb{PGL}_2(\mathbf{A})^{\text{op}} \to \text{Aut}_{\mathbf{A}}\big(\mathbf{A}(t)\big)$.
Prove that in the discrete field case we obtain an isomorphism.
5. *(Converse part of Lüroth's theorem)* Let $g_1, \ldots, g_r \in \mathbf{L} \setminus \mathbf{k}$. Prove that $\mathbf{k}(g_1, \ldots, g_r) = \mathbf{k}(g)$ for a suitable g. It suffices to treat the $n = 2$ case. We show that $\mathbf{L}$ is strictly finite over $\mathbf{K}_1 = \mathbf{k}(g_1, g_2)$. We must then have $\mathbf{K}_1 = \mathbf{k}(g)$ for any nonconstant coefficient g of $\text{Min}_{\mathbf{K}_1,t}(T)$.
NB: Since $\mathbf{L}$ is a finite dimensional $\mathbf{k}(g_1)$-vector space, every subfield of $\mathbf{L}$ strictly containing $\mathbf{k}$ is, in classical mathematics, finitely generated, therefore of the form $\mathbf{k}(g)$. Our formulation of the converse part of Lüroth's theorem give the constructive meaning of this assertion.

Problem 2. *(Differential operators and Frobenius algebras)*
In the first questions, $\mathbf{k}$ is a commutative ring. The *Hasse derivative* of order m of a polynomial of $\mathbf{k}[X]$ is formally defined by $f^{[m]} = \frac{1}{m!} f^{(m)}$. Similarly, for $\alpha \in \mathbb{N}^n$, we define $\partial^{[\alpha]}$ over $\mathbf{k}[\underline{X}] = \mathbf{k}[X_1, \ldots, X_n]$ by
$$\partial^{[\alpha]} f = \frac{1}{\alpha!} \frac{\partial^\alpha f}{\partial X^\alpha} \quad \text{with} \quad \alpha! = \alpha_1! \cdots \alpha_n!, \quad f \in \mathbf{k}[\underline{X}].$$
We then have $\partial^{[\alpha]}(fg) = \sum_{\beta+\gamma=\alpha} \partial^{[\beta]}(f)\, \partial^{[\gamma]}(g)$. We denote by $\delta^{[\alpha]} : \mathbf{k}[\underline{X}] \to \mathbf{k}$ the linear form $f \mapsto \partial^{[\alpha]}(f)(0)$. Thus, $f = \sum_\alpha \delta^{[\alpha]}(f) X^\alpha$. We deduce, by letting

[12] We denote by $\mathbf{A}(t)$ the Nagata ring of $\mathbf{A}$ which is obtained from $\mathbf{A}[t]$ by inverting the primitive polynomials.

$\alpha \leqslant \beta$ for $X^\alpha \mid X^\beta$,

$$X^\alpha \centerdot \delta^{[\beta]} = \begin{cases} \delta^{[\beta-\alpha]} & \text{if } \alpha \leqslant \beta \\ 0 & \text{otherwise,} \end{cases} \qquad \partial^{[\alpha]}(X^\beta) = \begin{cases} X^{\beta-\alpha} & \text{if } \alpha \leqslant \beta \\ 0 & \text{otherwise.} \end{cases}$$

Let $g = \sum_\beta b_\beta X^\beta$. Evaluating the *differential polynomial* $\sum_\beta b_\beta \partial^{[\beta]}$ at $(\underline{0})$, we obtain a linear form $\delta_g : \mathbf{k}[\underline{X}] \to \mathbf{k}$, $\delta_g = \sum_\beta b_\beta \delta^{[\beta]}$, then an ideal $\mathfrak{a}_g$ of $\mathbf{k}[\underline{X}]$

$$\mathfrak{a}_g = \{\, f \in \mathbf{k}[\underline{X}] \mid f \centerdot \delta_g = 0 \,\} \overset{\text{def}}{=} \{\, f \in \mathbf{k}[\underline{X}] \mid \delta_g(fu) = 0 \ \forall u \in \mathbf{k}[\underline{X}] \,\}.$$

We thus obtain a Frobenius $\mathbf{k}$-algebra $\mathbf{k}[\underline{X}]/\mathfrak{a}_g$ (with δ_g dualizing).

1. Let $f = \sum_\alpha a_\alpha X^\alpha$, $g = \sum_\beta b_\beta X^\beta$. We let $\partial_f : \mathbf{k}[\underline{X}] \to \mathbf{k}[\underline{X}]$ be the differential operator associated with f, i.e. $\partial_f = \sum_\alpha a_\alpha \partial^{[\alpha]}$. Check the following relation between the operator ∂_f and the linear form δ_g

$$\textstyle\sum_\gamma (f \centerdot \delta_g)(X^\gamma) X^\gamma = \partial_f(g) = \sum_{\alpha \leqslant \beta} a_\alpha b_\beta X^{\beta-\alpha}.$$

Deduce that $f \centerdot \delta_g = 0 \iff \partial_f(g) = 0$.

Now we must note that the law $f * g = \partial_f(g)$ provides the additive group $\mathbf{k}[\underline{X}]$ with a $\mathbf{k}[\underline{X}]$-module structure (in particular because $\partial_{f_1 f_2} = \partial_{f_1} \circ \partial_{f_2}$). But as $X^\alpha * X^\beta = X^{\beta-\alpha}$ or 0, certain authors use $X^{-\alpha}$ instead of X^α; they provide $\mathbf{k}[\underline{X}]$ with a $\mathbf{k}[\underline{X}^{-1}]$-module structure. Other authors permute $\underline{X}$ and $\underline{X}^{-1}$; they provide $\mathbf{k}[\underline{X}^{-1}]$ with a $\mathbf{k}[\underline{X}]$-module structure such that the ideal $\mathfrak{a}_g$ (annihilator of $g \in \mathbf{k}[\underline{X}^{-1}]$) is an ideal of a polynomial ring with indeterminates with exponents $\geqslant 0$. In the latter formalism, a polynomial f with indeterminates with exponents $\geqslant 0$ therefore acts on a polynomial g having its indeterminates with exponents $\leqslant 0$ to provide a polynomial $f * g$ having indeterminates with exponents $\leqslant 0$ (by deleting the monomials containing an exponent > 0). Thus, if $g = X^{-2} + Y^{-2} + Z^{-2}$, the ideal $\mathfrak{a}_g$ of $\mathbf{k}[X, Y, Z]$ contains for example XY, $X^2 - Y^2$ and every homogeneous polynomial of degree $\geqslant 3$.

2. Let $d \geqslant 1$. Study the special case of the Newton sum $g = \sum_i X_i^{-d}$, i.e. $\delta_g : f \mapsto \sum_i \frac{1}{d!} \frac{\partial^d f}{\partial X_i^d}(0)$, the sum of the coefficients over $X_1^d, \ldots, X_n^d$.

In the remainder, we fix $g = \sum_\beta b_\beta X^\beta$, or according to taste, $g = \sum_\beta b_\beta X^{-\beta}$.

3. Prove that we have an inclusion $\mathfrak{b} \subseteq \mathfrak{a}_g$ for some ideal $\mathfrak{b} = \langle X_1^{e_1}, \cdots, X_n^{e_n} \rangle$ with integers $e_i \geqslant 1$. In particular, $\mathbf{k}[\underline{X}]/\mathfrak{b}$ is a free $\mathbf{k}$-module of finite rank and $\mathbf{k}[\underline{X}]/\mathfrak{a}_g$ is a finitely generated $\mathbf{k}$-module.

4. Define a $\mathbf{k}$-linear map $\varphi : \mathbf{k}[\underline{X}]/\mathfrak{b} \to \mathbf{k}[\underline{X}]$ such that $\operatorname{Ker}\varphi = \mathfrak{a}_g/\mathfrak{b}$. We can therefore compute $\mathfrak{a}_g$ if we know how to solve linear systems over $\mathbf{k}$.

5. Suppose that $\mathbf{k}$ is a discrete field and so $\mathbf{A} := \mathbf{k}[\underline{X}]/\mathfrak{a}_g$ is a finite dimensional $\mathbf{k}$-vector space. Prove that $(\mathbf{A}, \delta_g)$ is a Frobenius $\mathbf{k}$-algebra.

Problem 3. *(Hilbert's theorem* 90*, additive version)*
Let $(\mathbf{k}, \mathbf{A}, G)$ be a Galois algebra where $G = \langle \sigma \rangle$ is cyclic of order n.

1. Considering an element $z \in \mathbf{A}$ of trace 1, we will show that

$$\mathbf{A} = \mathrm{Im}(\mathrm{Id}_{\mathbf{A}} - \sigma) \oplus \mathbf{k}z, \qquad \mathrm{Im}(\mathrm{Id}_{\mathbf{A}} - \sigma) = \mathrm{Ker}\,\mathrm{Tr}_G\,.$$

Consequently $\mathrm{Im}(\mathrm{Id}_{\mathbf{A}} - \sigma)$ is a stably free $\mathbf{k}$-module of rank $n-1$. You can use the family of endomorphisms $(c_i)_{i \in [\![0..n]\!]}$,

$$c_0 = 0,\; c_1(x) = x,\; c_2(x) = x + \sigma(x),\; \ldots,\; c_i(x) = \textstyle\sum_{j=0}^{i-1} \sigma^j(x),\; \ldots$$

2. For $x \in \mathbf{A}$ prove that to be of the form $y - \sigma(y)$, it is necessary and sufficient that $\mathrm{Tr}_G(x) = 0$.

3. More generally, let $(c_\tau)_{\tau \in G}$ be a family in $\mathbf{A}$. Prove that there exists an element y such that $c_\tau = y - \tau(y)$ if and only if the family satisfies the following additive cocycle condition: for all τ_1, $\tau_2 \in G$: $c_{\tau_1\tau_2} = \tau_1(c_{\tau_2}) + c_{\tau_1}$.

4. Assume that n is a prime number p and that $p = 0$ in $\mathbf{k}$. Prove the existence of some $y \in \mathbf{A}$ such that $\sigma(y) = y + 1$.
Deduce that $(1, y, \ldots, y^{p-1})$ is a $\mathbf{k}$-basis of $\mathbf{A}$ and that the characteristic polynomial of y is of the form $Y^p - Y - \lambda$ with $\lambda \in \mathbf{k}$.
We therefore have $\mathbf{A} = \mathbf{k}[y] \simeq \mathbf{k}[Y]/\langle Y^p - Y - \lambda\rangle$ (Artin-Schreier extension).

5. Give a converse of the previous item.

Problem 4. *(Galois algebras: study of an example)* Consider a ring $\mathbf{B}$ in which 2 is invertible, with x, $y \in \mathbf{B}$ and $\sigma \in \mathrm{Aut}(\mathbf{B})$ of order 2 satisfying $x^2 + y^2 = 1$, $\sigma(x) = -x$ and $\sigma(y) = -y$. We can take as an example the ring $\mathbf{B}$ of continuous functions over the unit circle $x^2 + y^2 = 1$ and for σ the involution $f \mapsto \{(x, y) \mapsto f(-x, -y)\}$. Let $\mathbf{A} = \mathbf{B}^{\langle\sigma\rangle}$ (subring of the “even functions”).

1. Prove that $(\mathbf{A}, \mathbf{B}, \langle\sigma\rangle)$ is a Galois algebra.
Consequently, $\mathbf{B}$ is a projective $\mathbf{A}$-module of constant rank 2.

2. Let $E = \mathbf{A}x + \mathbf{A}y$ (submodule of the “odd functions”).
Check that $\mathbf{B} = \mathbf{A} \oplus E$ and that E is a projective $\mathbf{A}$-module of constant rank 1.

3. Let $x_1 = 1$, $x_2 = x$, $x_3 = y$ such that (x_1, x_2, x_3) is a generator set of the $\mathbf{A}$-module $\mathbf{B}$. Make y_1, y_2, $y_3 \in \mathbf{B}$ explicit as in Lemma 7.10, i.e. $\big((x_i)_{i \in [\![1..3]\!]}, (y_i)_{i \in [\![1..3]\!]}\big)$ is a trace system of coordinates.
Deduce a projection matrix $P \in \mathbb{M}_3(\mathbf{A})$ of rank 2 with $\mathbf{B} \simeq_{\mathbf{A}} \mathrm{Im}\,P$.

4. Let $R = \begin{bmatrix} x & -y \\ y & x \end{bmatrix} \in \mathbb{SL}_2(\mathbf{B})$. Prove that this “rotation” R induces an isomorphism of $\mathbf{A}$-modules between E^2 and $\mathbf{A}^2$

$$\begin{bmatrix} f \\ g \end{bmatrix} \mapsto R \begin{bmatrix} f \\ g \end{bmatrix} = \begin{bmatrix} xf - yg \\ yf + xg \end{bmatrix}.$$

Consequently (next question), $E \otimes_{\mathbf{A}} E \simeq \mathbf{A}$; verify that $f \otimes g \mapsto fg$ realizes an isomorphism of $\mathbf{A}$-modules of $E \otimes_{\mathbf{A}} E$ over $\mathbf{A}$.

5. For some $\mathbf{A}$-module M ($\mathbf{A}$ arbitrary), let

$$M^{2\otimes} = M \otimes_{\mathbf{A}} M,\; M^{3\otimes} = M \otimes_{\mathbf{A}} M \otimes_{\mathbf{A}} M,\; \text{etc}\ldots$$

Let E be an $\mathbf{A}$-module satisfying $E^n \simeq \mathbf{A}^n$ for some $n \geqslant 1$. Prove that E is a projective $\mathbf{A}$-module of constant rank 1 and that $E^{n\otimes} \simeq \mathbf{A}$.

6. Let $\mathfrak{a}$ be the ideal of $\mathbf{A}$ defined by $\mathfrak{a} = \langle xy, x^2 \rangle$. Check that $\mathfrak{a}^2 = x^2\mathbf{A}$ (so if x is regular, $\mathfrak{a}$ is an invertible ideal of $\mathbf{A}$), that $\mathfrak{a}\mathbf{B}$ is principal and finally, that $\mathfrak{a}$, regarded as an $\mathbf{A}$-submodule of $\mathbf{B}$, is equal to xE.

7. Let $\mathbf{k}$ be a nontrivial ring with $2 \in \mathbf{k}^\times$ and $\mathbf{B} = \mathbf{k}[X,Y]\big/\langle X^2 + Y^2 - 1\rangle$. We write $\mathbf{B} = \mathbf{k}[x, y]$. We can apply the above by taking σ as defined by $\sigma(x) = -x$ and $\sigma(y) = -y$. Suppose that $\alpha^2 + \beta^2 = 0 \Rightarrow \alpha = \beta = 0$ in $\mathbf{k}$ (for example if $\mathbf{k}$ is a discrete field and -1 is not a square in $\mathbf{k}$).

- *a.* Prove that $\mathbf{B}^\times = \mathbf{k}^\times$; illustrate the importance of the hypothesis "of reality" made about $\mathbf{k}$.
- *b.* Prove that $\mathfrak{a}$ is not principal and so E is not a free $\mathbf{A}$-module. Deduce that $\mathbf{B}$ is not a free $\mathbf{A}$-module.

8. Let $\mathbf{B}$ be the ring of (real) continuous functions over the unit circle $x^2 + y^2 = 1$ and σ the involution $f \mapsto \{(x, y) \mapsto f(-x, -y)\}$. Prove that $\mathfrak{a}$ is not principal and that $\mathbf{B}$ is not a free $\mathbf{A}$-module.

Some solutions, or sketches of solutions

Exercise 2. We have $\mathbf{B} = \mathbf{K}[x_1, \dots, x_n]$, with $[\mathbf{B} : \mathbf{K}] = m$. We will perform a computation that shows that the $\mathbf{K}$-algebra $\mathbf{B}$ is monogenic or contains an idempotent $e \neq 0, 1$. In the second case, $\mathbf{B} \simeq \mathbf{B}_1 \times \mathbf{B}_2$, with $[\mathbf{B}_i : \mathbf{K}] = m_i < m$, $m_1 + m_2 = m$, which allows us to conclude by induction on m.
If we are able to treat the $n = 2$ case, we are done, because $\mathbf{K}[x_1, x_2]$ is étale over $\mathbf{K}$, so either we replace $\mathbf{K}[x_1, x_2]$ with $\mathbf{K}[y]$ for some y, or we find an idempotent $e \neq 0, 1$ within it. The proof of item *1* of Theorem 1.9 shows that an étale $\mathbf{K}$-algebra $\mathbf{K}[x, z]$ is monogenic if $\mathbf{K}$ contains an infinite sequence of distinct elements. It uses a polynomial $d(a, b)$ which, evaluated in $\mathbf{K}$ must give an invertible element. If we do not have any information on the existence of an infinite sequence of distinct elements of $\mathbf{K}$, we enumerate the integers of $\mathbf{K}$ until we obtain α, β in $\mathbf{K}$ with $d(\alpha, \beta) \in \mathbf{K}^\times$, or until we conclude that the characteristic is equal to a prime number p. We then enumerate the powers of the coefficients of f and of g (the minimal polynomials of x and z over $\mathbf{K}$) until we obtain α, β in $\mathbf{K}$ with $d(\alpha, \beta) \in \mathbf{K}^\times$, or until we conclude that the field $\mathbf{K}_0$ generated by the coefficients of f and g is a finite field. In this case, $\mathbf{K}_0[x, z]$ is a reduced finite $\mathbf{K}_0$-algebra. It is a reduced finite ring, so either it is a finite field, of the form $\mathbf{K}_0[\gamma]$, and $\mathbf{K}[x, z] = \mathbf{K}[\gamma]$, or it contains an idempotent $e \neq 0, 1$.

Remark. The reader will be able to verify that the proof transformation that we put the "$\mathbf{B}$ is a discrete field" case through is precisely the implementation of the elementary local-global machinery of reduced zero-dimensional rings. In fact the same machinery also applies to the discrete field $\mathbf{K}$ and provides the following result: a strictly étale algebra over a reduced zero-dimensional ring $\mathbf{K}$ (Definition 5.1) is a finite product of strictly étale $\mathbf{K}$-algebras. ■

Exercise 3. *1.* We write $x = (x_1, \dots, x_n) = \sum_{i=1}^{n} x_i e_i$ and identify $\mathbf{A}$ with a subring of $\mathbf{B}$ by $1 \mapsto (1, \dots, 1)$. By writing $e_i \in \mathbf{A}[x]$, we obtain that the elements $x_i - x_j$ are invertible for $j \neq i$. Conversely, if $x_i - x_j$ is invertible for all $i \neq j$, we have $\mathbf{B} = \mathbf{A}[x] = \mathbf{A} \oplus \mathbf{A}x \oplus \cdots \oplus \mathbf{A}x^{n-1}$ (Lagrange interpolation, Vandermonde determinant).

2. If and only if $\#\mathbf{A} \geqslant n$.

Exercise 4. *1* and *2.* If $(a_1, \dots, a_\ell)$ is a basis of $\mathbf{B}$ over $\mathbf{K}$, it is also a basis of $\mathbf{B}(v)$ over $\mathbf{K}(v)$.

3. Let b/p be an idempotent of $\mathbf{B}(v)$: we have $b^2 = bp$. If $p(0) = 0$, then $b(0)^2 = 0$, and since $\mathbf{B}$ is reduced, $b(0) = 0$. We can then divide b and p by v. Thus, we can assume that $p(0) \in \mathbf{K}^\times$. By dividing b and p by $p(0)$ we are reduced to the case where $p(0) = 1$. We then see that $b(0)$ is idempotent. We denote it by b_0 and let $e_0 = 1 - b_0$. Let us write $e_0 b = vc$. We multiply the equality $b^2 = bp$ by $e_0 = e_0^2$ and we obtain $v^2c^2 = vcp$. So $vc(p - vc) = 0$, and since the polynomial $p - vc$ has 1 as its constant term, so is regular, this gives us $c = 0$. Therefore $b = b_0 b$. Let us reason modulo e_0 for a moment: we have $b_0 \equiv 1$ so b is primitive and the equality $b^2 = bp$ is simplified to $b \equiv p \bmod e_0$. This gives the equality $b = b_0 b = b_0 p$ in $\mathbf{B}(v)$ and so $b/p = b_0$.

Exercise 6.

1. Classical: it is $\mathbb{Z}[\sqrt{d}]$ if $d \equiv 2$ or $3 \bmod 4$ and $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ if $d \equiv 1 \bmod 4$.

2. We have $\mathbf{A} = \mathbb{Z}[\sqrt{a}]$. We have $\beta^2 = \frac{a+1}{2} + \sqrt{a} \in \mathbf{A}$, therefore β is integral over $\mathbf{A}$, then over $\mathbb{Z}$. Actually, $(\beta^2 - \frac{a+1}{2})^2 = a$ and β is a root of $X^4 - (a+1)X^2 + (\frac{a-1}{2})^2$. We thus find $(\sigma\tau)(\beta) = \beta - \sqrt{2}$.

3. We find $(\sigma\tau)(z) = r - (s+u)\sqrt{2} + u\beta$ then $z + (\sigma\tau)(z) = 2r + u\sqrt{2a}$. This last element of $\mathbb{Q}(\sqrt{2a})$ is integral over $\mathbb{Z}$, hence in $\mathbb{Z}[\sqrt{2a}]$ because $2a \equiv 2 \bmod 4$. Hence $u \in \mathbb{Z}$ (and $2r \in \mathbb{Z}$). We replace z with $z - u\beta$ which is integral over $\mathbb{Z}$, i.e. $z = r + s\sqrt{2} + t\sqrt{a}$. We have $\sigma(z) = r - s\sqrt{2} + t\sqrt{a}$, $\tau(z) = r + s\sqrt{2} - t\sqrt{a}$; by using $z + \sigma(z)$ and $z + \tau(z)$, we see that $2r$, $2s$, $2t \in \mathbb{Z}$. Let us use

$$z\sigma(z) = x + 2rt\sqrt{a},\ z\tau(z) = y + 2rs\sqrt{2},\ \text{with } x = r^2 - 2s^2 + at^2,\ y = r^2 + 2s^2 - at^2.$$

We therefore have x, $y \in \mathbb{Z}$ then $x + y = 2r^2 \in \mathbb{Z}$, $x - y = 2at^2 - (2s)^2 \in \mathbb{Z}$, so $2at^2 \in \mathbb{Z}$. From $2r$, $2r^2 \in \mathbb{Z}$, we deduce $r \in \mathbb{Z}$. Similarly, from $2t$, $2at^2 \in \mathbb{Z}$ (using that a is odd), we see that $t \in \mathbb{Z}$, and then finally $s \in \mathbb{Z}$. Phew!

Thanks to the $\mathbb{Z}$-basis of $\mathbf{B}$, we obtain $\mathrm{Disc}_{\mathbf{B}/\mathbb{Z}} = 2^8 a^2$.

4. We have $\mathbf{B} = \mathbb{Z} \oplus \mathbb{Z}\sqrt{a} \oplus \mathbb{Z}\sqrt{2} \oplus \mathbb{Z}\beta = \mathbf{A} \oplus E$ with $E = \mathbb{Z}\sqrt{2} \oplus \mathbb{Z}\beta$.

We also have $2E = \sqrt{2}\,\mathfrak{a}$ with $\mathfrak{a} = 2\,\mathbb{Z} \oplus \mathbb{Z}(\sqrt{a} - 1) = \left\langle 2, \sqrt{a} - 1 \right\rangle_{\mathbf{A}}$. This proves on the one hand that E is an $\mathbf{A}$-module, and on the other that it is isomorphic to the ideal $\mathfrak{a}$ of $\mathbf{A}$. Consequently, E is a projective $\mathbf{A}$-module of constant rank 1. The expression $\mathbf{B} = \mathbf{A} \oplus E$ certifies that $\mathbf{B}$ is a finitely generated projective $\mathbf{A}$-module, written as a direct sum of a free $\mathbf{A}$-module of rank 1 and of a projective module of constant rank 1. In general, the ideal $\mathfrak{a}$ is not principal, so E is not a free $\mathbf{A}$-module. Here is a small sample of values of $a \equiv 3 \bmod 4$; we have underlined those values for which the ideal $\mathfrak{a}$ is principal:

$$-33,\ -29,\ -21,\ -17,\ -13,\ -5,\ \underline{-1},\ \underline{3},\ \underline{7},\ \underline{11},\ 15,\ \underline{19},\ \underline{23},\ \underline{31},\ 35.$$

In the case where $\mathfrak{a}$ is not principal, $\mathbf{B}$ is not a free $\mathbf{A}$-module. Otherwise, E would be stably free of rank 1, therefore free (see Exercise V-13). Finally, we always have $\mathfrak{a}^2 = 2\mathbf{A}$ (see below), so $\mathfrak{a} \simeq \mathfrak{a}^{-1} \simeq \mathfrak{a}^\star$. Consequently $\mathbf{B} \simeq_{\mathbf{A}} \mathbf{B}^\star$.
Justification of $\mathfrak{a}^2 = 2\mathbf{A}$: always in the same context ($a \equiv 3 \bmod 4$ so $\mathbf{A} = \mathbb{Z}[\sqrt{a}\,]$), we have for $m \in \mathbb{Z}$

$$\left\langle m, 1+\sqrt{a}\right\rangle \left\langle m, 1-\sqrt{a}\right\rangle = \gcd(a-1, m)\,\mathbf{A}.$$

Indeed, the left ideal is generated by $\left(m^2, m(1 \pm \sqrt{a}), 1-a\right)$, each one a multiple of the gcd. This ideal contains $2m = m(1+\sqrt{a}) + m(1-\sqrt{a})$, so it contains the element $\gcd(m^2, 2m, 1-a) = \gcd(m, 1-a)$, (the equality is due to $a \equiv 3 \bmod 4$). For $m = 2$, we have $\left\langle 2, 1+\sqrt{a}\right\rangle = \left\langle 2, 1-\sqrt{a}\right\rangle = \mathfrak{a}$ and $\gcd(a-1, 2) = 2$.

Exercise 7. We consider $\mathbf{B} = \mathbf{A} \otimes_{\mathbf{k}} \mathbf{A}'$ as an $\mathbf{A}$-algebra, a scalar extension to $\mathbf{A}$ of the $\mathbf{k}$-algebra $\mathbf{A}'$; it is free of rank n'. We therefore have at our disposal a stack of free algebras $\mathbf{k} \to \mathbf{A} \to \mathbf{B}$ and the transitivity formula of the discriminant provides

$$\mathrm{Disc}_{\mathbf{B}/\mathbf{k}}\left(\underline{x} \otimes \underline{x}'\right) = \mathrm{Disc}_{\mathbf{A}/\mathbf{k}}\left(\underline{x}\right)^{n'} \cdot \mathrm{N}_{\mathbf{A}/\mathbf{k}}\left(\mathrm{Disc}_{\mathbf{B}/\mathbf{A}}\left(1 \otimes \underline{x}'\right)\right).$$

But $\mathrm{Disc}_{\mathbf{B}/\mathbf{A}}\left(1 \otimes \underline{x}'\right) = \mathrm{Disc}_{\mathbf{A}'/\mathbf{k}}\left(\underline{x}'\right)$. As it is an element of $\mathbf{k}$, its norm $\mathrm{N}_{\mathbf{A}/\mathbf{k}}$ has the value $\mathrm{Disc}_{\mathbf{A}'/\mathbf{k}}\left(\underline{x}'\right)^n$. Ultimately we obtain the equality

$$\mathrm{Disc}_{\mathbf{B}/\mathbf{k}}\left(\underline{x} \otimes \underline{x}'\right) = \mathrm{Disc}_{\mathbf{A}/\mathbf{k}}\left(\underline{x}\right)^{n'}\ \mathrm{Disc}_{\mathbf{A}'/\mathbf{k}}\left(\underline{x}'\right)^n.$$

Exercise 8. We will use the following classical result on linear algebras. Let E be a finite dimensional $\mathbf{K}$-vector space and $u \in \mathrm{End}_{\mathbf{K}}(E)$. If d is the degree of the minimal polynomial of u, there exists an $x \in E$ such that the elements x, $u(x)$, …, $u^{d-1}(x)$ are $\mathbf{K}$-linearly independent.
Here $[\,\mathbf{L} : \mathbf{K}\,] = n$, and $\mathrm{Id}_{\mathbf{L}}$, σ, …, σ^{n-1} are $\mathbf{K}$-linearly independent, so the minimal polynomial of σ is $X^n - 1$, of degree n. We apply the above result.

Exercise 9. *1.* A is the companion matrix of the polynomial $X^2 - X + 1 = \Phi_6(X)$, so $A^3 = -\mathrm{I}_2$ in $\mathbb{GL}_2(\mathbf{k})$ and $A^3 = 1$ in $\mathbb{PGL}_2(\mathbf{k})$.

2. We know by Artin's theorem that $\mathbf{k}(t)/\mathbf{k}(t)^G$ is a Galois extension with Galois group A_3. The computation gives

$$g = t + \sigma(t) + \sigma^2(t) = \tfrac{t^3 - 3t - 1}{t(t+1)}.$$

We obviously have $g \in \mathbf{k}(t)^G$ and $t^3 - gt^2 - (g+3)t - 1 = 0$. Therefore, (direct part of Lüroth's theorem, Problem 1) $[\,\mathbf{k}(t) : \mathbf{k}(g)\,] = 3$, and $\mathbf{k}(t)^G = \mathbf{k}(g)$.

3. Since $\mathbf{k}(a) \simeq \mathbf{k}(g)$ and $f_g(t) = 0$, the extension $\mathbf{k}(a) \to \mathbf{k}[T]/\langle f_a\rangle$ is a copy of the extension $\mathbf{k}(g) \to \mathbf{k}(t)$.

4. Let σ be a generator of $\mathrm{Aut}(\mathbf{L}/\mathbf{K})$. This question amounts to saying that we can find some $t \in \mathbf{L} \setminus \mathbf{K}$ such that $\sigma(t) = \frac{-1}{t+1}$ $(*)$. Since t must be of norm 1, we seek it of the form $t = \frac{\sigma(u)}{u}$. The computation then shows that $(*)$ is satisfied under the condition that $u \in \mathrm{Ker}(\mathrm{Tr}_G)$. It remains to show that there exists some $u \in \mathrm{Ker}(\mathrm{Tr}_G)$ such that $\frac{\sigma(u)}{u} \notin \mathbf{K}$. This amounts to saying that the restriction of σ to $E = \mathrm{Ker}(\mathrm{Tr}_G)$ is not a homothety. However, $E \subseteq \mathbf{L}$ is a $\mathbf{K}$-linear subspace of dimension 2, stable under σ. By Exercise 8, the $\mathbf{K}$-vector space $\mathbf{L}$ admits a generator for the endomorphism σ. This linear algebra property remains true for every stable subspace by σ.

Exercise 10. The elements $g \otimes h$ form a $\mathbf{k}$-basis of $\mathbf{A}^{\mathrm{e}}_{\mathbf{k}}$.
Let $z = \sum_{g,h} a_{g,h} g \otimes h$ with $a_{g,h} \in \mathbf{k}$. Then, $z \in \mathrm{Ann}(\mathrm{J}_{\mathbf{A}/\mathbf{k}})$ if and only if we have $g' \cdot z = z \cdot g'$ for every $g' \in G$. We obtain $a_{g,h} = a_{1,gh}$, so z is a $\mathbf{k}$-linear combination of the $z_k \overset{\mathrm{def}}{=} \sum_{gh=k} g \otimes h$.
Conversely, we see that $z_k \in \mathrm{Ann}(\mathrm{J}_{\mathbf{A}/\mathbf{k}})$ and we have $z_k = k \cdot z_1 = z_1 \cdot k$.
So $\mathrm{Ann}(\mathrm{J}_{\mathbf{A}/\mathbf{k}})$ is the $\mathbf{k}$-module generated by the z_k's, and it is the $\mathbf{A}$-module (or the ideal of $\mathbf{A}^{\mathrm{e}}_{\mathbf{k}}$) generated by $z_1 = \sum_g g \otimes g^{-1}$.
The image under $\mu_{\mathbf{A}/\mathbf{k}}$ of $\mathrm{Ann}(\mathrm{J}_{\mathbf{A}/\mathbf{k}})$ is the ideal $n\mathbf{A}$. Regarding the trace, we have $\mathrm{Tr}_{\mathbf{A}/\mathbf{k}}(g) = 0$ if $g \neq 1$. Therefore $\mathrm{Tr}_{\mathbf{A}/\mathbf{k}}\big(\sum_g a_g g\big) = n a_1$.
If $a = \sum_g a_g g$ and $b = \sum_g b_g g$, then $\mathrm{Tr}_{\mathbf{A}/\mathbf{k}}(ab) = n \sum_g a_g b_{g^{-1}}$.
The equivalences of item *2* are therefore clear, and in the case where $n \in \mathbf{k}^{\times}$, the separability idempotent is $n^{-1} \sum_g g \otimes g^{-1}$.

3. Let $\lambda : \mathbf{k}[G] \to \mathbf{k}$ be the linear form "coordinate over 1." For g, $h \in G$, we have $\lambda(gh) = 0$ if $h \neq g^{-1}$, and 1 otherwise. So, λ is dualizing and $(g^{-1})_{g \in G}$ is the dual basis of $(g)_{g \in G}$ with respect to λ. We have $\mathrm{Tr}_{\mathbf{k}[G]/\mathbf{k}} = n \cdot \lambda$.

Exercise 11. *1.* It suffices to do it for $g \in \{1, x, \ldots, x^{n-1}\}$, which is a basis of $\mathbf{A}[Y]$ over $\mathbf{k}[Y]$. The right-hand side of $(*)$ with $g = x^i$ is

$$h_i = \varphi\big((Y - x)x^i\big) = \varphi(Yx^i - x^{i+1}) = Y^{i+1} - \varphi(x^{i+1}).$$

If $i < n - 1$, we have $\varphi(x^{i+1}) = Y^{i+1}$, so $h_i = 0$. For $i = n - 1$, we have

$$\varphi(x^n) = -\varphi(a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}) = -(a_0 + a_1 Y + \cdots + a_{n-1} Y^{n-1}),$$

and $h_n(Y) = f(Y)$, which gives the result.

2. For $i < n$, we have

$$f(Y)\widetilde{\lambda}\big(x^i f'(Y)\big) = \varphi\big((Y - x)x^i f'(Y)\big) = \varphi\big(x^i f(Y)\big) = Y^i f(Y), \text{ i.e.}$$
$$\widetilde{\lambda}\big(x^i f'(Y)\big) = \textstyle\sum_{j<n} \lambda(x^i b_j) Y^j = Y^i.$$

Therefore $(b_j \bullet \lambda)(x^i) = \lambda(x^i b_j) = \delta_{ij}$. Thus, λ is dualizing.

3. For two dual bases (e_i), (α_i), we have $\mathrm{Tr}_{\mathbf{A}/\mathbf{k}} = \sum e_i \bullet \alpha_i$. With the two dual bases $(1, x, \ldots, x^{n-1})$ and $(b_0 \bullet \lambda, b_1 \bullet \lambda, \ldots, b_{n-1} \bullet \lambda)$ we obtain

$$\mathrm{Tr}_{\mathbf{A}/\mathbf{k}} = b_0 \bullet \lambda + x b_1 \bullet \lambda + \cdots + x^{n-1} b_{n-1} \bullet \lambda = f'(x) \bullet \lambda.$$

Exercise 12. *1.* The $\mathbf{k}$-algebra $\mathbf{A} := \mathbf{k}[X_1, \ldots, X_n]/\langle f_1(X_1), \ldots, f_n(X_n)\rangle$ is the tensor product of the $\mathbf{k}[X_i]/\langle f_i(X_i)\rangle$ which are Frobenius algebras, so $\mathbf{A}$ is a Frobenius algebra. Precision with $d_i = \deg(f_i)$. The $\mathbf{k}$-algebra $\mathbf{A}$ is free of rank $d_1 \cdots d_n$, the monomials $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ with $\alpha_i < d_i$ for every i form a $\mathbf{k}$-basis, and the linear form "coordinate over $x_1^{d_1-1} \cdots x_n^{d_n-1}$" is dualizing.

2. Let δ_0, δ_x, δ_y be three linear forms over $\mathbf{k}[X, Y]$ defined by

$$\delta_0(f) = f(0), \quad \delta_x(f) = f'_X(0), \quad \delta_y(f) = f'_Y(0).$$

Viewed as linear forms over $\mathbf{A}$ they define a $\mathbf{k}$-basis of $\mathbf{A}^{\star}$, a dual basis of the $\mathbf{k}$-basis $(1, x, y)$ of $\mathbf{A}$. We have

$$x \bullet \delta_x = y \bullet \delta_y = \delta_0,$$

and so $\mathbf{A}^\star = \mathbf{A} \bullet \delta_x + \mathbf{A} \bullet \delta_y$. Let us show that $G = \begin{bmatrix} x \\ -y \end{bmatrix}$ is a presentation matrix of $\mathbf{A}^\star$ for (δ_x, δ_y). We must observe that for u, v in $\mathbf{A}$ we have the implication

$$u \bullet \delta_x + v \bullet \delta_y = 0 \implies \begin{bmatrix} u \\ v \end{bmatrix} \in \mathbf{A} \begin{bmatrix} x \\ -y \end{bmatrix}.$$

By multiplying $u \bullet \delta_x + v \bullet \delta_y = 0$ by x, we obtain $u \bullet \delta_0 + (xv) \bullet \delta_y = 0$; we evaluate at 1 and we put $x := 0$ to obtain $u(0, y) = 0$, i.e. $u \in \mathbf{A}x$. Similarly, $v \in \mathbf{A}y$. If we write $u = xr$, $v = ys$, we obtain $r \bullet \delta_0 + s \bullet \delta_0 = 0$, i.e. $r + s = 0$, as required.

The determinantal ideal $\mathcal{D}_1(G) = \langle x, y \rangle$ is nonzero, with a null square, so it cannot be generated by an idempotent. Consequently, the $\mathbf{A}$-module $\mathbf{A}^\star$ is not projective. A fortiori, it is not free.

Exercise 13. *1.* We have $(y - z) f^\Delta(y, z) = 0$ so $\delta := f^\Delta(y, z) \in \mathrm{Ann}(\mathrm{J})$. We then know that for $\alpha \in \mathbf{A}^{\mathrm{e}}_{\mathbf{k}}$, we have $\alpha\delta = \mu_{\mathbf{A}/\mathbf{k}}(\alpha) \cdot \delta = \delta \cdot \mu_{\mathbf{A}/\mathbf{k}}(\alpha)$. We apply this result to $\alpha = \delta$ by noticing that $\mu_{\mathbf{A}/\mathbf{k}}(\delta) = f'(x)$.

2. We write $f(Y) - f(Z) = (Y - Z)f'(Y) - (Y - Z)^2 g(Y, Z)$, which gives us in the algebra $\mathbf{A}^{\mathrm{e}}_{\mathbf{k}}$ the equality $(y - z)f'(y) = (y - z)^2 g(y, z)$. We write the equality $1 = uf + vf'$ in $\mathbf{A}[X]$. Then $f'(y)v(y) = 1$, so $y - z = (y - z)^2 v(y) g(y, z)$.

When $a = a^2 b$, the element ab is idempotent and $\langle a \rangle = \langle ab \rangle$. Therefore $\mathrm{J} = \langle e \rangle$ with the idempotent $e = (y - z)v(y)g(y, z)$.

We have $f^\Delta(Y, Z) = f'(Y) - (Y - Z)g(Y, Z)$, so

$$f^\Delta(y, z) = f'(y) - (y - z)g(y, z) = f'(y)\big(1 - (y - z)v(y)g(y, z)\big) = f'(y)(1 - e).$$

Exercise 14. *1.* Let $f'_{ij} = \partial f_i / \partial X_j$ and we write, in $\mathbf{k}[\underline{Y}, \underline{Z}]$,

$$f_i(\underline{Y}) - f_i(\underline{Z}) - \textstyle\sum_j (Y_j - Z_j) f'_{ij}(\underline{Y}) =: -g_i(\underline{Y}, \underline{Z}) \in \langle Y_1 - Z_1, \ldots, Y_n - Z_n \rangle^2.$$

In $\mathbf{A}^{\mathrm{e}}_{\mathbf{k}}$, by letting $A = \mathrm{JAC}_{\underline{y}}(f_1, \ldots, f_n)$ we obtain

$$A \begin{bmatrix} y_1 - z_1 \\ \vdots \\ y_n - z_n \end{bmatrix} = \begin{bmatrix} g_1(\underline{y}, \underline{z}) \\ \vdots \\ g_n(\underline{y}, \underline{z}) \end{bmatrix} \quad \text{with} \quad g_i(\underline{y}, \underline{z}) \in \langle y_1 - z_1, \ldots, y_n - z_n \rangle^2 = \mathrm{J}^2_{\mathbf{A}/\mathbf{k}}.$$

By inverting A, we obtain $y_i - z_i \in \mathrm{J}^2_{\mathbf{A}/\mathbf{k}}$, i.e. $\mathrm{J}_{\mathbf{A}/\mathbf{k}} = \mathrm{J}^2_{\mathbf{A}/\mathbf{k}}$.

2. As $\mu_{\mathbf{A}/\mathbf{k}}\big(\beta_{\underline{y},\underline{z}}(\underline{f})\big) = \mathrm{Jac}_{\underline{x}}(\underline{f})$, we have $\mu_{\mathbf{A}/\mathbf{k}}(\varepsilon) = 1$.

As $\varepsilon \in \mathrm{Ann}(\mathrm{J}_{\mathbf{A}/\mathbf{k}})$, ε is the idempotent generator of $\mathrm{Ann}(\mathrm{J}_{\mathbf{A}/\mathbf{k}})$.

Finally, $\beta_{\underline{y},\underline{z}}(\underline{f})$, which is associated with ε, is also a generator of $\mathrm{Ann}(\mathrm{J}_{\mathbf{A}/\mathbf{k}})$.

3. Let f_1, …, f_n be in $\mathbf{k}[\underline{X}]$ and $\delta = \mathrm{Jac}_{\underline{X}}(\underline{f})$. Let us invert δ with an indeterminate T. Then, in $\mathbf{k}[\underline{X}, T]$ we obtain

$$\mathrm{JAC}_{\underline{X},T}(\underline{f}, \delta T - 1) = \begin{array}{c} \\ f_1 \\ \vdots \\ f_n \\ \delta T - 1 \end{array} \begin{array}{c} \begin{array}{cccc} \partial_{X_1} & \cdots & \partial_{X_n} & \partial_T \end{array} \\ \left[\begin{array}{ccc|c} & & & 0 \\ & \mathrm{JAC}_{\underline{X}}(\underline{f}) & & \vdots \\ & & & 0 \\ \star & \cdots & \star & \delta \end{array}\right] \end{array}$$

and so $\mathrm{Jac}_{\underline{X},T}(\underline{f}, \delta T - 1) = \delta^2$. Let

$$\mathbf{A} = \mathbf{k}[\underline{X}] \big/ \big\langle \underline{f} \big\rangle \quad \text{and} \quad \mathbf{B} = \mathbf{A}[\delta^{-1}] = \mathbf{k}[\underline{X}, T] \big/ \big\langle \underline{f}, 1 - \delta T \big\rangle.$$

Then the Jacobian of the system $(\underline{f}, \delta T - 1)$ which defines $\mathbf{B}$ is invertible in $\mathbf{B}$ and so $\mathbf{B}$ is a separable algebra.

Exercise 15. The $\mathbf{B}$-algebra $\mathbf{B} \otimes_{\mathbf{k}} \mathbf{A}$ is separable. We have a transformation (universal property of the scalar extension)

$$\mathrm{Hom}_{\mathbf{k}}(\mathbf{A}, \mathbf{B}) \to \mathrm{Hom}_{\mathbf{B}}(\mathbf{B} \otimes_{\mathbf{k}} \mathbf{A}, \mathbf{B}),\ \psi \mapsto \overline{\psi},$$

defined by $\overline{\psi}(b \otimes a) = b\psi(a)$.

1. We then consider the idempotent $\varepsilon_{\overline{\varphi}} \in \mathbf{B} \otimes_{\mathbf{k}} \mathbf{A}$ of Lemma 6.16, and we write it in the form $\varepsilon_{\overline{\varphi}} = \sum_{i \in I} b_i \otimes a_i$.

2. Directly results from Lemma 6.16: the idempotent e is none other than $e_{\{\overline{\varphi}, \overline{\varphi'}\}}$.

3. Since the horizontal juxtaposition of Dedekind evaluation matrices is a Dedekind evaluation matrix, it suffices to show that there exists one, say A_1, whose image contains the vector $v := {}^{\mathrm{t}}[\, e_{11} \ \cdots \ e_{n1} \,]$.

Let $\big((a_j)_{j \in [\![1..m]\!]}, (b_j)_{j \in [\![1..m]\!]}\big)$ be the pair attached to φ_1. We put in column j of A_1 the vector ${}^{\mathrm{t}}[\, \varphi_1(a_j) \ \cdots \ \varphi_n(a_j) \,]$. We then have $A_1 \, {}^{\mathrm{t}}[\, b_1 \ \cdots \ b_m \,] = v$.

Exercise 16. By hypothesis, for each $\tau \in G \setminus \{\mathrm{Id}\}$ there exist $n_\tau \in \mathbb{N}$ and $x_{1,\tau}, \ldots, x_{n_\tau,\tau}, y_{1,\tau}, \ldots, y_{n_\tau,\tau} \in \mathbf{A}$ such that $1 = \sum_{j=1}^{n_\tau} x_{j,\tau}\big(y_{j,\tau} - \tau(y_{j,\tau})\big)$. Let $s_\tau = \sum_{j=1}^{n_\tau} x_{j,\tau}\tau(y_{j,\tau})$ such that $\sum_{j=1}^{n_\tau} x_{j,\tau}y_{j,\tau} = 1 + s_\tau$, then we define $x_{n_\tau+1,\tau} = -s_\tau$ and $y_{n+1,\sigma} = 1$. Then, with $m_\tau = 1 + n_\tau$

$$\textstyle\sum_{j=1}^{m_\tau} x_{j,\tau}\tau(y_{j,\tau}) = s_\tau - s_\tau = 0, \qquad \sum_{j=1}^{m_\tau} x_{j,\tau}y_{j,\tau} = 1 + s_\tau - s_\tau = 1.$$

Fixing $\sigma \in G$, we obtain the product

$$\textstyle\prod_{\tau \in G \setminus \{\mathrm{Id}\}} \sum_{j=1}^{m_\tau} x_{j,\tau}\sigma(y_{j,\tau}) = \begin{cases} 1 & \text{if } \sigma = \mathrm{Id} \\ 0 & \text{otherwise.} \end{cases}$$

The development of the product provides two families (a_i) and (b_i) indexed by the same set (each a_i is the product of some $x_{j,\tau}$'s and b_i is the product of the corresponding $y_{j,\tau}$'s) satisfying

$$\textstyle\sum_{i=1}^{r} a_i\sigma(b_i) = \begin{cases} 1 & \text{if } \sigma = \mathrm{Id} \\ 0 & \text{otherwise.} \end{cases}$$

Exercise 17. *1.* As G acts transitively over $[\![1..n]\!]$, we have $(\mathbf{k}^n)^G = \mathbf{k}$. In addition, G being of cardinality n, a permutation $\sigma \in G \setminus \{\mathrm{Id}\}$ has no fixed point. We deduce that $\sum_{\sigma \in G} e_i\sigma(e_i) = 0$ if $\sigma \in G \setminus \{\mathrm{Id}\}$, and 1 otherwise.

By taking $x_i = y_i = e_i$, the conditions of Lemma 7.10 are satisfied and $(\mathbf{k}, \mathbf{k}^n, G)$ is a Galois algebra.

The map $G \to [\![1..n]\!]$, $\sigma \mapsto \sigma(1)$, is a bijection. The action of G on $[\![1..n]\!]$ is necessarily isomorphic to the action of G on itself by translations. If n is fixed, we can take for G the group generated by an n-cycle.

2. We have $\mathrm{Stp}_{\mathrm{S}_4}(\mathbf{B}) = \langle (1,2), (3,4) \rangle$ and $H = \mathrm{Stp}_G(\mathbf{B}) = \{\mathrm{Id}\}$; so $(\mathbf{k}^4)^H = \mathbf{k}^4$.

3. The first item is immediate. Suppose $\mathbf{B} = \mathbf{A}[X]^H$ and let $a \in \mathbf{A}$.

Then $aX \in \mathbf{B}$, so aX is invariant under H, i.e. a is invariant under H.

Recap: $\mathbf{A} = \mathbf{A}^H$ so $H = \{\mathrm{Id}\}$ then $\mathbf{A}[X] = X\mathbf{A}[X] + \mathbf{k}$, i.e. $\mathbf{A} = \mathbf{k}$ and $G = \{\mathrm{Id}\}$.

Besides this very special case, $\mathbf{B}$ is not of the form $\mathbf{A}[X]^H$.

Exercise 18. Assume without loss of generality that $\mathbf{B}$ and $\mathbf{C}$ are free of rank $n \in \mathbb{N}$: it indeed suffices to check the conclusion after localization at comaximal elements and we have the local structure theorem for finitely generated projective modules readily available. If $n = 0$ then $\mathbf{k}$ is trivial, we can therefore assume that $1 \leqslant n$. Consider a basis $\mathcal{C} = (c_1, \dots, c_n)$ of $\mathbf{C}$ and a basis $\mathcal{B} = (b_1, \dots, b_n)$ of $\mathbf{B}$ (over $\mathbf{k}$), and write the matrix $B \in \mathbb{M}_n(\mathbf{k})$ of $\mathcal{B}$ over $\mathcal{C}$. The fact that the b_i's form a basis implies that B is injective, i.e. $\delta = \det B$ is regular (Theorem II-5.22). Moreover, $\delta\mathbf{C} \subseteq \mathbf{B}$.

Let us compare $\mathrm{Tr}_{\mathbf{B}/\mathbf{k}}(x)$ and $\mathrm{Tr}_{\mathbf{C}/\mathbf{k}}(x)$ for some $x \in \mathbf{B}$. Consider $\mathbf{k}' = \mathbf{k}[1/\delta] \supseteq \mathbf{k}$. The two $\mathbf{k}'$-algebras obtained by scalar extension, $\mathbf{B}[1/\delta]$ and $\mathbf{C}[1/\delta]$, are the same, and the trace is well-behaved under scalar extension, so $\mathrm{Tr}_{\mathbf{B}/\mathbf{k}}(x)$ and $\mathrm{Tr}_{\mathbf{C}/\mathbf{k}}(x)$ are equal because they are equal in $\mathbf{k}'$. But then

$$\mathrm{disc}\, \mathbf{B}/\mathbf{k} = \mathrm{disc}_{\mathbf{B}/\mathbf{k}}(\mathcal{B}) = \mathrm{disc}_{\mathbf{C}/\mathbf{k}}(\mathcal{B}) = \delta^2\, \mathrm{disc}_{\mathbf{C}/\mathbf{k}}(c_1, \dots, c_n).$$

Finally, since $\mathrm{disc}\, \mathbf{B}/\mathbf{k}$ is invertible, so is δ and $\mathbf{B} = \mathbf{C}$.

Exercise 19. First of all, note that since $\mathbf{k}$ is connected, all the finitely generated projective modules over $\mathbf{k}$ are of constant rank. Also recall that the Galois correspondence is already established when $\mathbf{k}$ is a discrete field.

We must show that if $\mathbf{k} \subseteq \mathbf{B} \subseteq \mathbf{A}$ with $\mathbf{B}$ strictly étale, then

$$\mathbf{B} = \mathbf{C} \overset{\mathrm{def}}{=} \mathrm{Fix}\left(\mathrm{Stp}(\mathbf{B})\right).$$

By Lemma 18, it suffices to show that $\mathbf{B}$ and $\mathbf{C}$ have the same rank. In classical mathematics we conclude by noting that after scalar extension to any field, $\mathbf{B}$ and $\mathbf{C}$ have the same rank since the Galois correspondence is established for fields. Via a dynamic rereading of this classical argument we obtain a constructive proof. This is linked to the formal Nullstellensatz (Theorem III-9.9).

Exercise 20. Let (x_i), (y_i) be two systems of elements of $\mathbf{B}$ as in Lemma 7.10.

1. We know that for $x \in \mathbf{B}$, $x = \sum_i \mathrm{Tr}_G(xy_i)x_i$. If $x \in \mathfrak{b}$, then $xy_i \in \mathfrak{b}$, and as $\mathfrak{b}$ is globally invariant, $\mathrm{Tr}_G(xy_i) \in \mathfrak{b}$.

Recap : $\mathfrak{b}$ is generated by the invariant elements $\mathrm{Tr}_G(xy_i)$ for $x \in \mathfrak{b}$.

2. Let $\mathfrak{a}$ be an ideal of $\mathbf{A}$; it is clear that $\mathfrak{a}\mathbf{B}$ is globally invariant.

We must show that $\mathfrak{a}\mathbf{B} \cap \mathbf{A} = \mathfrak{a}$. This comes from the fact that $\mathbf{A}$ is a direct summand in $\mathbf{B}$ (as an $\mathbf{A}$-module). Indeed, let $\mathbf{B} = \mathbf{A} \oplus E$, so $\mathfrak{a}\mathbf{B} = \mathfrak{a} \oplus \mathfrak{a}E$. If $x \in \mathfrak{a}\mathbf{B} \cap \mathbf{A}$, we write $x = y + z$ with $y \in \mathfrak{a}$ and $z \in \mathfrak{a}E \subseteq E$; we then have x, $y \in \mathbf{A}$, so $z \in \mathbf{A}$, and as $z \in E$, $z = 0$. Consequently, $x = y \in \mathfrak{a}$.

Conversely, if $\mathfrak{b} \subseteq \mathbf{B}$ is globally invariant, we must show that $(\mathfrak{b} \cap \mathbf{A})\mathbf{B} = \mathfrak{b}$; but this is what has been shown in the previous question.

Problem 2. Generally, the linear form δ_g is passed on to the quotient modulo the ideal $\mathfrak{a}_g$ that it defines. In addition, if $\delta_g(\overline{u}\,\overline{v}) = 0$ over $\mathbf{A} = \mathbf{k}[\underline{X}]/\mathfrak{a}_g$ for every $\overline{v}$, then $\delta_g(uv) = 0$ for every v, so $u \in \mathfrak{a}_g$, i.e. $\overline{u} = 0$. Therefore $\mathrm{Ann}_{\mathbf{A}}(\delta_g) = 0$.

For $i \in [\![1..n]\!]$, let $\delta_i^m = \delta_{X_i^m}$ (coordinate over X_i^m).

In particular, $\delta_i(f) = \frac{\partial f}{\partial X_i}(0)$, and we define $\delta_0 : \mathbf{k}[\underline{X}] \to \mathbf{k}$ by $\delta_0(f) = f(0)$.

1. Easy computation.

2. We verify that $f * g = 0$ if and only if $f_m * g = 0$ for every homogeneous component f_m of f. In other words the ideal $\mathfrak{a}_g$ is homogeneous (this is always

the case if g is homogeneous).
It is also clear that for $i \neq j$, $X_iX_j * g = 0$, and for $|\alpha| > d$, $X^\alpha * g = 0$. If $f = \sum_i a_i X_i^m + \cdots$ is homogeneous of degree $m \leqslant d$, we have $f * g = \sum_i a_i X_i^{-(d-m)}$.
If $m < d$, we therefore have $f * g = 0$ if and only if $a_i = 0$, $\forall i$, i.e. if $f \in \langle X_iX_j, i \neq j\rangle$.
If $m = d$, we have $f * g = 0$ if and only if $\sum_i a_i = 0$, i.e. if $f \in \langle X_iX_j, i \neq j\rangle + \left\langle X_i^d - X_1^d, i \in [\![2..n]\!]\right\rangle$, because $\sum_i a_iX_i^d = \sum_i a_i(X_i^d - X_1^d)$.
Recap: we have obtained a generator set of $\mathfrak{a}_g$ consisting of $\frac{n(n-1)}{2}$ homogeneous polynomials of degree 2 and of $n-1$ homogeneous polynomials of degree d

$$\mathfrak{a}_g = \langle X_iX_j, i < j\rangle + \left\langle X_i^d - X_1^d, i \in [\![2..n]\!]\right\rangle .$$

Let $\mathbf{A} = \mathbf{k}[\underline{X}]/\mathfrak{a}_g = \mathbf{k}[x_1, \ldots, x_n]$. Then

$$1, \quad x_1,\ \ldots,\ x_n, \quad x_1^2,\ \ldots,\ x_n^2, \quad \ldots \quad x_1^{d-1},\ \ldots,\ x_n^{d-1}, \quad x_1^d$$

is a $\mathbf{k}$-basis of $\mathbf{A}$ of cardinality $(d-1)n + 2$. The $\mathbf{k}$-dual basis of $\mathbf{A}^\star$ is

$$\delta_0, \quad \delta_1,\ \ldots,\ \delta_n, \quad \delta_1^2,\ \ldots,\ \delta_n^2, \quad \ldots \quad \delta_1^{d-1},\ \ldots,\ \delta_n^{d-1}, \quad \delta_g$$

and we have

$$x_i^m \centerdot \delta_g = \delta_i^{d-m} \text{ for } m \in [\![1..d-1]\!], \quad x_i^d \centerdot \delta_g = \delta_0.$$

Therefore $\mathbf{A}^\star = \mathbf{A} \centerdot \delta_g$ and δ_g is dualizing.

3. If we take e_i strictly greater than the exponent of X_i in the set of monomials of g, we have $X_i^{e_i} * g = 0$.

4. Let $f \in \mathbf{k}[\underline{X}]$. We have seen that $f \centerdot \delta_g = 0$ if and only if $\partial_f(g) = 0$.
So the $\mathbf{k}$-linear map $\mathbf{k}[\underline{X}] \to \mathbf{k}[\underline{X}]$, $f \mapsto \partial_f(g)$, passes to the quotient modulo $\mathfrak{b}$ to define a $\mathbf{k}$-linear map $\varphi : \mathbf{k}[\underline{X}]/\mathfrak{b} \to \mathbf{k}[\underline{X}]$.

5. The $\mathbf{k}$-linear map $\mathbf{A} \to \mathbf{A}^\star$, $f \mapsto f \centerdot \delta_g$, is injective and as $\mathbf{A}$ and $\mathbf{A}^\star$ are $\mathbf{k}$-vector spaces of the same finite dimension, it is an isomorphism.

Problem 3. *1.* As if by magic we let $\theta(x) = \sum_{i=0}^{n-1} \sigma^i(z)c_i(x)$ (thanks to Hilbert). We will check that

$$\sigma\big(\theta(x)\big) = \theta(x) + \mathrm{Tr}_G(x)z - x \quad \text{or} \quad x = (\mathrm{Id}_\mathbf{A} - \sigma)\big(\theta(x)\big) + \mathrm{Tr}_G(x)z.$$

So, $(\mathrm{Id}_\mathbf{A} - \sigma) \circ \theta$ and $x \mapsto \mathrm{Tr}_G(x)z$ are two orthogonal projectors with sum $\mathrm{Id}_\mathbf{A}$, hence $\mathbf{A} = \mathrm{Im}(\mathrm{Id}_\mathbf{A} - \sigma) \oplus \mathbf{k}z$. For the verification, write c_i for $c_i(x)$ and $y = \theta(x)$. We have $\sigma(c_i) = c_{i+1} - x$, $c_n = \mathrm{tr}_G(x)$ and

$$\begin{aligned} \sigma(y) &= \textstyle\sum_{i=0}^{n-1}(c_{i+1} - x)\sigma^{i+1}(z) = \sum_{i=0}^{n-1} c_{i+1}\sigma^{i+1}(z) - \sum_{i=0}^{n-1} x\sigma^{i+1}(z) \\ &= (y + \mathrm{Tr}_G(x)z) - x\,\mathrm{Tr}_G(z) = y + \mathrm{Tr}_G(x)z - x. \end{aligned}$$

Since $\mathrm{Tr}_G(z) = 1$, z is a basis of $\mathbf{k}z$ (if $az = 0$, then $0 = \mathrm{Tr}_G(az) = a$), so $\mathrm{Im}(\mathrm{Id}_\mathbf{A} - \sigma)$ is indeed stably free of rank $n-1$.

2. It is clear that $\mathrm{Im}(\mathrm{Id}_\mathbf{A} - \sigma) \subseteq \mathrm{Ker}\,\mathrm{Tr}_G$. The other inclusion results from the previous item.

3. The reader can verify this by letting $y = \sum_\tau c_\tau \tau(z)$. There is a link with question *1*: for fixed x with $\mathrm{Tr}_G(x) = 0$, the family $\big(c_i(x)\big)$ is an additive 1-cocycle under the condition that $[\![0..n-1]\!]$ and G are identified via $i \leftrightarrow \sigma^i$.

4. The element -1 has null trace, hence the existence of $y \in \mathbf{A}$ such that $-1 = y - \sigma(y)$. We then have, for every $i \in \mathbb{Z}$, $\sigma^i(y) = y + i$, and $\sigma^j(y) - \sigma^i(y) = j - i$ is invertible for $i \not\equiv j \bmod p$.
Let $y_i = \sigma^i(y)$, ($i \in [\![0..p-1]\!]$). The Vandermonde matrix of $(y_0, y_1, \ldots, y_{p-1})$ is invertible and consequently $(1, y, \ldots, y^{p-1})$ is a $\mathbf{k}$-basis of $\mathbf{A}$. Let $\lambda = y^p - y$. Then $\lambda \in \mathbf{k}$ since

$$\sigma(\lambda) = \sigma(y)^p - \sigma(y) = (y+1)^p - (y+1) = y^p - y = \lambda.$$

The characteristic polynomial of y is $(Y - y_0)(Y - y_1) \cdots (Y - y_{p-1})$ and this polynomial is equal to $f(Y) = Y^p - Y - \lambda$ (because the y_i's are roots of f and $y_i - y_j$ is invertible for $i \neq j$).

5. Let $\mathbf{k}$ be a ring with $p =_{\mathbf{k}} 0$. Fix $\lambda \in \mathbf{k}$ and let $\mathbf{A} = \mathbf{k}[Y]/\langle f \rangle = \mathbf{k}[y]$, where $f(Y) = Y^p - Y - \lambda$. Then, $y + 1$ is a root of f, and we can define $\sigma \in \mathrm{Aut}(\mathbf{A}/\mathbf{k})$ by $\sigma(y) = y + 1$. The element σ is of order p and the reader will check that $(\mathbf{k}, \mathbf{A}, \langle\sigma\rangle)$ is a Galois algebra.

Problem 4. *1.* Consider the ideal $\langle x - \sigma(x), y - \sigma(y) \rangle \overset{\text{def}}{=} \langle 2x, 2y \rangle$. Since 2 is invertible, it is the ideal $\langle x, y \rangle$, and it contains 1 because $x^2 + y^2 = 1$. Thus, $\langle\sigma\rangle$ is separating.

2. For all $f \in \mathbf{B}$, we have $f = (xf)x + (yf)y$. If f is odd i.e. if $\sigma(f) = -f$, we have xf, $yf \in \mathbf{A}$, so $f \in \mathbf{A}x + \mathbf{A}y$ and $E = \{\, f \in \mathbf{B} \,|\, \sigma(f) = -f \,\}$. The equality $\mathbf{B} = \mathbf{A} \oplus E$ stems from the equality $f = \frac{f+\sigma(f)}{2} + \frac{f-\sigma(f)}{2}$ for $f \in \mathbf{B}$.
Other proof. We know that there exists a $b_0 \in \mathbf{B}$ of trace 1 and that the kernel of the linear form $\mathbf{B} \to \mathbf{A}$ defined by $b \mapsto \mathrm{Tr}(b_0 b)$ is a complementary subspace of $\mathbf{A}$ in $\mathbf{B}$. Here we can take $b_0 = 1/2$, again we find E as a complementary subspace.

3. This is a matter of finding y_1, y_2, $y_3 \in \mathbf{B}$ such that $\sum_{i=1}^{3} x_i \tau(y_i) = 1$ for $\tau = \mathrm{Id}$ and 0 otherwise. We notice that

$$1 \cdot 1 + x \cdot x + y \cdot y = 2, \quad \text{and} \quad 1 \cdot \sigma(1) + x \cdot \sigma(x) + y \cdot \sigma(y) = 0,$$

hence we obtain a solution when taking $y_i = x_i/2$. Letting $X = \begin{bmatrix} 1 & x & y \\ \frac{1}{2} & -\frac{x}{2} & -\frac{y}{2} \end{bmatrix}$, we have $X\,{}^{\mathrm{t}}X = \mathrm{I}_2$ and ${}^{\mathrm{t}}XX = P$ with $P = \begin{bmatrix} 1 & 0 & 0 \\ 0 & x^2 & xy \\ 0 & xy & y^2 \end{bmatrix}$. The matrix P is a projector of rank 2 whose image is isomorphic to the $\mathbf{A}$-module $\mathbf{B}$.

Note: we deduce that E is isomorphic to the image of the projector $\begin{bmatrix} x^2 & xy \\ xy & y^2 \end{bmatrix}$ and that $\mathbf{B} \otimes_{\mathbf{A}} E$ is isomorphic to $\mathbf{B}$ as a $\mathbf{B}$-module.

4. Easy.

5. The isomorphism $E^n \simeq \mathbf{A}^n$ proves that E is a projective module of constant rank 1. Applying $\bigwedge^n$ we obtain $E^{n\otimes} \simeq \mathbf{A}$.
Note: for more details see Section X-1, the proof of Proposition X-1.2, Equality (1) on page 538 and Equality (5) on page 572.

6. The equality $1 = x^2 + y^2$ implies $\mathfrak{a}^2 = \left\langle x^2y^2, x^3y, x^4 \right\rangle = x^2 \left\langle y^2, xy, x^2 \right\rangle = x^2\mathbf{A}$, and $\mathfrak{a}\mathbf{B} = xy\mathbf{B} + x^2\mathbf{B} = x(y\mathbf{B} + x\mathbf{B}) = x\mathbf{B}$. In $\mathbf{B}$, $\mathfrak{a} = x(y\mathbf{A} + x\mathbf{A}) = xE$. Therefore if x is regular, $\mathfrak{a} \simeq_{\mathbf{A}} E$ via the multiplication by x.

7a. We have $\mathbf{k}[x] \simeq \mathbf{k}[X]$ and $\mathbf{A} = \mathbf{k}[x^2, xy, y^2]$. We consider $\mathbf{B}$ as a free $\mathbf{k}[x]$-module of rank 2, with basis $(1, y)$, and we let $\mathrm{N} : \mathbf{B} \to \mathbf{k}[x]$ be the norm.
For a, $b \in \mathbf{k}[x]$ we obtain

$$\mathrm{N}(a + by) = (a + by)(a - by) = a^2 + (x^2 - 1)b^2.$$

As $\mathrm{N}(x) = x^2$, x is regular (Lemma 4.3 item *2*). Moreover, $a + by \in \mathbf{B}^\times$ if and only if $a^2 + (x^2 - 1)b^2 \in \mathbf{k}^\times$. Suppose b has formal degree $m \geqslant 0$ and a has formal degree $n \geqslant 0$. Then, $(x^2 - 1)b^2 = \beta^2 x^{2m+2} + \ldots$ and $a^2 = \alpha^2 x^{2n} + \ldots$ Since $a^2 + (x^2 - 1)b^2 \in \mathbf{k}^\times$, we obtain

- if $n > m + 1$, $\alpha^2 = 0$ so $\alpha = 0$ and a can be rewritten with formal degree $< n$,
- if $n < m + 1$, $\beta^2 = 0$ so $\beta = 0$ and
  - if $m = 0$, $b = 0$ and $a = \alpha \in \mathbf{k}^\times$, or
  - if $m > 0$, b can be rewritten with formal degree $< m$,
- if $n = m + 1$ (which implies $n > 0$), $\alpha^2 + \beta^2 = 0$ so $\alpha = \beta = 0$ and a can be rewritten with formal degree $< n$.

We conclude by induction on $m + n$ that if $a + by \in \mathbf{B}^\times$, then $b = 0$ and $a \in \mathbf{k}^\times$.
We notice that if $-1 = i^2$ in $\mathbf{k}$, then $(x + iy)(x - iy) = 1$ and we obtain an inverse $x + iy$ which is not a constant.

7b. Let us show that $\mathfrak{a}$ is not principal. As $\mathfrak{a} \simeq_{\mathbf{A}} E$, it will follow that E is not a free $\mathbf{A}$-module, and $\mathbf{B}$ is not free either, because otherwise E would be stably free of rank 1, therefore free.
Suppose $\mathfrak{a} = a\mathbf{A}$ with $a \in \mathbf{A}$. By extending to $\mathbf{B}$, we obtain $\mathfrak{a}\mathbf{B} = a\mathbf{B}$. But we have seen that $\mathfrak{a}\mathbf{B} = x\mathbf{B}$, and since x is regular, $x = ua$ with $u \in \mathbf{B}^\times = \mathbf{k}^\times$. This would imply $x \in \mathbf{A}$, which is not the case because $\mathbf{k}$ is nontrivial.

8. We reuse the preceding proof to show that $\mathfrak{a}$ is not principal, but here $\mathbf{B}^\times$ no longer consists of only constants, for example the (continuous) function $(x, y) \mapsto x^2 + 1$ is invertible. From the point where $x = ua$ and $u \in \mathbf{B}^\times$, we reason as follows. Since u is an invertible element of $\mathbf{B}$, its absolute value is bounded below by an element > 0, and u is everywhere > 0, or everywhere < 0. As x is odd and a even, a and x are identically zero; a contradiction.

Bibliographic comments

A constructive study of strictly finite (not necessarily commutative) associative algebras over a discrete field can be found in [163, Richman] and in [MRR, Chapitre IX].

Proposition 1.13 is found in [MRR] which introduces the terminology of *separably factorial field.* See also [162, Richman].

Lemma 1.16 for squarefree factorization over a perfect discrete field admits a subtle generalization in the form of an “algorithm for separable factorization” over an arbitrary discrete field; see [MRR, th. IV.6.3, p. 162] and [125, Lecerf].

The notions of a Galois algebra and of a separable algebra were introduced by Auslander & Goldman in [3, 1960]. The core of the theory of Galois algebras is found in Chase, Harrison & Rosenberg's paper [30, 1968]. A book that presents this theory is [Demeyer & Ingraham]. Almost every argument in [30] is already of an elementary and constructive nature.

The result given in Exercise 18 is due to Ferrero and Paques in [85].

Problem 2 is inspired by Chapter 21 (Duality, Canonical Modules, and Gorenstein Rings) of [Eisenbud] and in particular by Exercises 21.6 and 21.7.

Chapter VII

The dynamic method

Nullstellensatz
Splitting field
Galois theory

Contents

Introduction

The first section of this chapter gives general constructive versions of the Nullstellensatz for a polynomial system over a discrete field (we will be able to compare Theorems 1.5 (page 392), 1.8 (page 394) and 1.9 (page 394), to Theorems III-9.5 (page 140) and III-9.7 (page 142)). We also give a simultaneous Noether positioning theorem (Theorem 1.7).

This is a significant example of a reformulation of a result from classical mathematics *in a more general framework*: classical mathematics admits that every field has an algebraic closure. This means it does not have to deal with the problem of the exact meaning of Hilbert's Nullstellensatz when such an algebraic closure is not available. But the question does get asked, and we can offer a perfectly reasonable answer: the algebraic closure is not really necessary. Rather than looking for the zeros of a polynomial system in an algebraic closure, we can look for them in finite algebras over the field given at the start.

We then tackle another problem: that of constructively interpreting the classical discourse on the algebraic closure of a field. The problem might seem to largely involve the use of Zorn's lemma, which is necessary for the construction of the global object. Actually, a more delicate problem arises well beforehand, at the moment the splitting field of an individual polynomial is constructed.

The theorem from classical mathematics stating that every separable polynomial of $\mathbf{K}[T]$ has a strictly finite splitting field over $\mathbf{K}$ (in which case the Galois theory applies), is only valid from a constructive point of view under hypotheses regarding the possibility of factorizing the separable polynomials (cf. [MRR] and in this work Theorem III-6.15 on the one hand and Corollary VI-1.13 on the other). Our goal here is to give a constructive Galois theory for an arbitrary separable polynomial in the absence of such hypotheses.

The counterpart is that we must not consider the splitting field of a polynomial as a usual "static" object, but as a "dynamic" object. This phenomenon is inevitable, because we must manage the ambiguity that results from the impossibility of knowing the Galois group of a polynomial by an infallible method. Moreover, the disorientation produced by this shift to a dynamic perspective is but one example of the general lazy evaluation method: *nothing comes of over-exhausting ourselves to know the whole truth when a partial truth is sufficient for the stakes of the ongoing computation.*

In Section 2, we give a heuristic approach to the dynamic method, which forms a cornerstone of the new methods in constructive algebra.

Section 3, dedicated to Boolean algebras, is a short introduction to the problems that will have to be dealt with in the context of a universal splitting algebra over a discrete field when it is not connected.

Section 4 continues the theory of universal splitting algebra already started in Section III-4. Without assuming that the polynomial is separable, the universal splitting algebra has several interesting properties that are preserved upon passage to a "Galois quotient." When summarizing these properties we have been brought to introduce the notion of a *pre-Galois algebra.*

Section 5 gives a constructive and dynamic approach to the splitting field of a polynomial over a discrete field, without a separability hypothesis regarding the polynomial.

The dynamic Galois theory of a separable polynomial over a discrete field is developed in Section 6.

The current chapter can be read immediately after Sections III-6 and VI-2, bypassing Chapters IV and V, if we restrict the universal splitting algebra to the discrete fields case (which would in fact simplify some of the proofs). However, it seemed natural to us to develop the material with respect to the universal splitting algebra in a more general framework, which requires the notion of a projective module of constant rank over an arbitrary commutative ring.

1. The Nullstellensatz without algebraic closure

In this chapter, which is dedicated to the question "how can we constructively recover the results from classical mathematics that are based on the existence of an algebraic closure, even when it is missing?," it seemed logical to have a new look at the Nullstellensatz and the Noether position (Theorem III-9.5) in this new framework.

The case of an infinite basis field

We claim that Theorem III-9.5 can be copied virtually word-for-word, by simply deleting the reference to an algebraically closed field that contains **K**.

We no longer necessarily see the zeros of the polynomial system considered in finite extensions of the discrete field **K**, but we construct strictly finite nonzero **K**-algebras (i.e. that are finite dimensional **K**-vector spaces) which account for these zeros; in classical mathematics the zeros are in the quotient fields of these **K**-algebras, and such quotient fields are easily seen to exist by applying **LEM** since it suffices to consider a strict ideal that is of maximal dimension as a **K**-vector space.

1.1. Theorem. (Weak Nullstellensatz and Noether position, 2)
Let $\mathbf{K}$ *be an infinite discrete field and* $(f_1,\dots,f_s)=(\underline{f})$ *be a polynomial system in the algebra* $\mathbf{K}[\underline{X}]=\mathbf{K}[X_1,\dots,X_n]$ $(n\geqslant 1)$*. Let* $\mathfrak{f}=\left\langle \underline{f}\right\rangle_{\mathbf{K}[\underline{X}]}$ *and* $\mathbf{A}=\mathbf{K}[\underline{X}]/\mathfrak{f}$*.*

Weak Nullstellensatz.

Either $\mathbf{A}=0$*, or there exists a nonzero quotient of* $\mathbf{A}$ *which is a strictly finite* $\mathbf{K}$*-algebra.*

Noether postion.

More precisely, we have a well-defined integer $r\in[\![-1..n]\!]$ *with the following properties.*

1. *Either* $r=-1$ *and* $\mathbf{A}=0$ *(i.e.* $\left\langle \underline{f}\right\rangle=\left\langle 1\right\rangle$*). In this case, the system* $(\underline{f})$ *does not admit any zero in any nontrivial* $\mathbf{K}$*-algebra.*
2. *Or* $r=0$*, and* $\mathbf{A}$ *is a nonzero strictly finite* $\mathbf{K}$*-algebra (in particular, the natural homomorphism* $\mathbf{K}\to\mathbf{A}$ *is injective).*
3. *Or* $r\geqslant 1$*, and there exists a* $\mathbf{K}$*-linear change of variables (the new variables are denoted* $Y_1,\dots,Y_n$*) satisfying the following properties.*
   - *We have* $\mathfrak{f}\cap\mathbf{K}[Y_1,\dots,Y_r]=0$*. In other words, the polynomial ring* $\mathbf{K}[Y_1,\dots,Y_r]$ *can be identified with a subring of* $\mathbf{A}$*.*
   - *Each* Y_j *for* $j\in[\![r+1..n]\!]$ *is integral over* $\mathbf{K}[Y_1,\dots,Y_r]$ *modulo* $\mathfrak{f}$ *and the ring* $\mathbf{A}$ *is a* $\mathbf{K}[Y_1,\dots,Y_r]$*-finitely presented module.*

- *There exists an integer N such that for each $(\alpha_1, \ldots, \alpha_r) \in \mathbf{K}^r$, the quotient algebra $\mathbf{A}/\langle Y_1 - \alpha_1, \ldots, Y_r - \alpha_r\rangle$ is a nonzero $\mathbf{K}$-vector space of finite dimension $\leqslant N$.*
- *We have finitely generated ideals $\mathfrak{f}_j \subseteq \mathbf{K}[Y_1, \ldots, Y_j]$ $(j \in [\![r..n]\!])$ with the following inclusions and equalities.*

$$\begin{array}{ll}\langle 0\rangle = \mathfrak{f}_r \subseteq \mathfrak{f}_{r+1} \subseteq \cdots \subseteq \mathfrak{f}_{n-1} \subseteq \mathfrak{f}_n = \mathfrak{f} & \\ \mathfrak{f}_j \subseteq \mathfrak{f}_\ell \cap \mathbf{K}[Y_1, \ldots, Y_j] & (j < \ell,\ j, \ell \in [\![r..n]\!]) \\ \mathrm{D}(\mathfrak{f}_j) = \mathrm{D}\left(\mathfrak{f}_\ell \cap \mathbf{K}[Y_1, \ldots, Y_j]\right) & (j < \ell,\ j, \ell \in [\![r..n]\!])\end{array}$$

D We essentially reason as in the proof of Theorem III-9.5. To simplify we keep the same variable names at each step of the construction. Let $\mathfrak{f}_n = \mathfrak{f}$.

- Either $\mathfrak{f} = 0$, and $r = n$ in item *3*.
- Or there is a nonzero polynomial among the f_i's, we make a linear change of variables that renders it monic in the last variable, and we compute the resultant ideal $\mathfrak{Res}_{X_n}(\mathfrak{f}_n) = \mathfrak{f}_{n-1} \subseteq \mathbf{K}[X_1, \ldots, X_{n-1}] \cap \mathfrak{f}_n$. Since $\mathfrak{f}_n \cap \mathbf{K}[X_1, \ldots, X_{n-1}]$ and $\mathfrak{f}_{n-1}$ have the same nilradical, they are simultaneously null.
- If $\mathfrak{f}_{n-1} = 0$, item *3* or *2* is satisfied with $r = n - 1$.
- Otherwise, we iterate the process.
- If the process halts with $\mathfrak{f}_r = 0$, $r \geqslant 0$, item *3* or *2* is satisfied with this value of r.
- Otherwise, $\mathfrak{f}_0 = \langle 1\rangle$ and the computation has allowed us to construct 1 as an element of $\mathfrak{f}$.

There are two things left for us to verify.
First of all, that $\mathbf{A}$ is a $\mathbf{K}[Y_1, \ldots, Y_r]$-finitely presented module. It is clear that it is a finitely generated module, the fact that it is finitely presented is therefore given by Theorem VI-3.17.
Then, that when we specialize the Y_i's $(i \in [\![1..r]\!])$ in some $\alpha_i \in \mathbf{K}$, the $\mathbf{K}$-vector space obtained is finitely presented (so finite dimensional) and nonzero. Theorem VI-3.9 on changing the base ring gives us the fact that, after specialization, the algebra remains a finitely presented module, so that the obtained $\mathbf{K}$-vector space is indeed finite dimensional. We must show that it is nonzero. However, we notice that, by assuming the changes of variables already made at the start, all the computations done in $\mathbf{K}[Y_1, \ldots, Y_n]$ specialize, i.e. remain unchanged, if we replace the indeterminates $Y_1, \ldots, Y_r$ by the scalars $\alpha_1, \ldots, \alpha_r$. The conclusion $\mathfrak{f} \cap \mathbf{K}[Y_1, \ldots, Y_r] = 0$ is replaced by the same result specialized in the α_i's, i.e. precisely what we wanted.
We can obtain the same conclusion in the more scholarly form below. This

specialization is a change of the base ring $\mathbf{K}[Y_1,\dots,Y_r] \to \mathbf{K}$. Apply item *1c* of the general elimination lemma IV-10.1 with

$$\mathbf{k} = \mathbf{K}[Y_1,\dots,Y_r],\ \mathbf{C} = \mathbf{A} \text{ and } \mathbf{k}' = \mathbf{K}.$$

The elimination ideal and the resultant ideal in $\mathbf{k}$ are null, therefore after scalar extension the resultant ideal remains null in $\mathbf{K}$.
Therefore, the same thing holds for the elimination ideal, and the natural homomorphism $\mathbf{K} \to \mathbf{A}/\langle Y_1 - \alpha_1, \dots, Y_r - \alpha_r\rangle$ is injective.

Let us end by explaining why the integer r is well-defined. First of all the case $r = -1$ is the only case where $\mathbf{A} = 0$, then for $r \geqslant 0$, it is possible to show that r is the maximum number of elements algebraically independent over $\mathbf{K}$ in $\mathbf{A}$ (see the proofs Theorems XIII-5.1 and XIII-5.4). □

Remarks. 1) We have used resultant ideals $\mathfrak{Res}(\mathfrak{b})$ (Theorem IV-10.2) instead of ideals $\mathfrak{R}(g_1,\dots,g_s)$ (with g_1 monic and $\langle g_1,\dots,g_s\rangle = \mathfrak{b}$), introduced in Lemma III-9.2. However, Lemma III-9.2 shows that the latter ideals would do just as well.
2) For any arbitrary homomorphism $\mathbf{K}[Y_1,\dots,Y_r] \to \mathbf{B}$, when $\mathbf{B}$ is a reduced $\mathbf{K}$-algebra, the last argument in the proof of the theorem works, which tells us that $\mathbf{B} \subseteq \mathbf{B} \otimes_{\mathbf{K}[Y_1,\dots,Y_r]} \mathbf{A}$.
3) The last item of *3* recalls the workings of the proof by induction which constructs the finitely generated ideals $\mathfrak{f}_j$ to reach the Noether position. This also gives a certain description of the "zeros" of the polynomial system (more delicate than in the case where we have an algebraically closed field $\mathbf{L}$ that contains $\mathbf{K}$, and where we describe the zeros with coordinates in $\mathbf{L}$, as in Theorem III-9.5). ■

It remains for us to lift the restriction introduced by the consideration of an infinite discrete field $\mathbf{K}$. For this we need a change of variables lemma that is a bit more general, using Nagata's trick.

Changing variables

1.2. Definition. We call a *change of variables* in the polynomial ring $\mathbf{k}[\underline{X}] = \mathbf{k}[X_1,\dots,X_n]$ an automorphism θ of this $\mathbf{k}$-algebra. If each $\theta(X_i)$ is denoted by Y_i, the Y_i's are called *the new variables.* Each Y_i is a polynomial in the X_j's, and each X_i is a polynomial in the Y_j's.

The most frequently used are the "linear changes of variables," in which we include, despite their name, the translations and all the affine transformations.

Comment. A nonlinear change of variables, like for instance

$$(X,Y) \mapsto (X + Y^2, Y),$$

does not respect the geometry in the intuitive sense. For example a line is transformed into a parabola; the algebraic geometry of the affine plane is not an extension of the affine geometry, it directly contradicts it! It is only in the context of projective spaces that we find what we expect: the automorphisms of the projective plane, from the algebraic geometry point of view, are necessarily linear, and the notion of a "(straight) line" reclaims its rights. ■

Pseudomonic polynomials

Let $\mathbf{k}$ be a connected ring. A polynomial in $\mathbf{k}[T]$ is said to be *pseudomonic* (in the variable T) if it is of the form $\sum_{i=0}^{p} a_k T^k$ with a_p invertible.

In general, without assuming that $\mathbf{k}$ is connected, a polynomial in $\mathbf{k}[T]$ is said to be *pseudomonic* (in the variable T) if there exists a fundamental system of orthogonal idempotents $(e_0, \ldots, e_r)$ such that, for each j, when taking $\mathbf{k}[1/e_j] = \mathbf{k}_j$, the polynomial is expressible in the form $\sum_{k=0}^{j} a_{k,j} T^k$ with $a_{j,j}$ invertible in $\mathbf{k}_j$.

A polynomial in $\mathbf{k}[X_1, \ldots, X_n] = \mathbf{k}[\underline{X}]$ is said to be *pseudomonic in the variable* X_n if it is pseudomonic as an element of $\mathbf{k}[X_1, \ldots, X_{n-1}][X_n]$.

NB: See also the notion of a locally monic polynomial in Exercise X-14.

Recall that a polynomial of $\mathbf{k}[X_1, \ldots, X_n]$ is said to be *primitive* when its coefficients generate the ideal $\langle 1 \rangle$. Also recall that if $\mathbf{k}$ is reduced, we have the equality $\mathbf{k}[X_1, \ldots, X_n]^\times = \mathbf{k}^\times$ (Lemma II-2.6).

1.3. Fact. *Let* $\mathbf{K}$ *be a reduced zero-dimensional ring and* $P \in \mathbf{K}[T]$. *The following properties are equivalent.*

- *The polynomial* P *is regular.*
- *The polynomial* P *is primitive.*
- *The polynomial* P *is pseudomonic.*
- *The quotient algebra* $\mathbf{K}[T]/\langle P \rangle$ *is finite over* $\mathbf{K}$.

D The equivalences are clear in the discrete fields case. To obtain the general result we can apply the elementary local-global machinery of reduced zero-dimensional rings (page 213). □

A simple and efficient lemma

1.4. Lemma. (Changes of variables lemma à la Nagata)
Let $\mathbf{K}$ *be a reduced zero-dimensional ring and* $g \in \mathbf{K}[\underline{X}] = \mathbf{K}[X_1, \ldots, X_n]$ *be a regular element.*

1. *There exists a change of variables such that, by calling the new variables* Y_1, …, Y_n, *the polynomial* g *becomes pseudomonic in* Y_n. *Consequently the* $\mathbf{K}$*-algebra* $\mathbf{K}[\underline{X}]/\langle g \rangle$ *is finite over* $\mathbf{K}[Y_1, \ldots, Y_{n-1}]$.
2. *When* $\mathbf{K}$ *is an infinite discrete field, we can take a linear changes of variables.*

3. *The result also applies to a finite family of regular polynomials of* $\mathbf{K}[\underline{X}]$ *(they can be made simultaneously pseudomonic by the same change of variables).*

D For the case of an infinite discrete field see Lemma III-9.4.
In the general case we can assume that $\mathbf{K}$ is a discrete field and we make a change of variables "à la Nagata." For example with three variables, if the polynomial g is of degree $< d$ in each of the variables X, Y, Z, we make the change of variables $X \mapsto X$, $Y \mapsto Y + X^d$, $Z \mapsto Z + X^{d^2}$. Then, seen as an element of $\mathbf{K}[Y, Z][X]$, g has become pseudomonic in X.
Item *3* is left to the reader. □

The general case

By reasoning as we did for Theorem 1.1 and by using the changes of variables of the previous lemma we obtain the general form of the weak Nullstellensatz and of the Noether position in constructive mathematics.

1.5. Theorem. (Weak Nullstellensatz and Noether position, 3)
With the same hypotheses as in Theorem 1.1 but by only supposing that the discrete field $\mathbf{K}$ *is nontrivial, we get the same conclusions, except that the change of variables is not necessarily linear.*

1.6. Definition. Consider the case $1 \notin \langle f_1, \ldots, f_s \rangle$ of the previous theorem.

1. We say that the change of variables (which eventually changes nothing at all) has put the ideal $\mathfrak{f}$ in *Noether position.*
2. The integer r that intervenes in the Noether positioning is called the *dimension of the polynomial system*, or of the variety defined by the polynomial system, or of the quotient algebra $\mathbf{A}$. By convention the null algebra is said to be of dimension -1.

Remarks. 1) It is clear by the theorem that $r = 0$ if and only if the quotient algebra is finite nonzero, which implies (Lemma VI-3.14) that it is a nontrivial zero-dimensional ring.
Conversely, if $\mathbf{A}$ is zero-dimensional and $\mathbf{K}$ nontrivial, Lemma IV-8.15 shows that the ring $\mathbf{K}[Y_1, \ldots, Y_r]$ is zero-dimensional, which implies that $r \leqslant 0$ (if $r > 0$, then an equality $Y_r^m\big(1 + Y_r Q(Y_1, \ldots, Y_r)\big) = 0$ implies that $\mathbf{K}$ is trivial). Therefore there is no conflict with the notion of a zero-dimensional ring. Let us however note that the null algebra is still a zero-dimensional ring.

2) The link with the Krull dimension will be made in Theorem XIII-5.4.

3) A "non-Noetherian" version of the previous theorem for a reduced zero-dimensional ring $\mathbf{K}$ is given in Exercise 3. ■

1.7. Theorem. (Simultaneous Noether position)
Let $\mathfrak{f}_1, \ldots, \mathfrak{f}_k$ be finitely generated ideals of $\mathbf{K}[\underline{X}] = \mathbf{K}[X_1, \ldots, X_n]$.

1. *There exist integers $r_1, \ldots, r_k \in [\![-1..n]\!]$ and a change of variables such that, by calling $Y_1, \ldots, Y_n$ the new variables, we have for each $j \in [\![1..k]\!]$ the following situation.*
   If $r_j = -1$, then $\mathfrak{f}_j = \langle 1 \rangle$, otherwise
   a. $\mathbf{K}[Y_1, \ldots, Y_{r_j}] \cap \mathfrak{f}_j = \{0\}$,
   b. for $\ell > r_j$, Y_ℓ is integral modulo $\mathfrak{f}_j$ over $\mathbf{K}[Y_1, \ldots, Y_{r_j}]$.
   When $\mathbf{K}$ is infinite, we can take a linear changes of variables.
2. *If $\langle 1 \rangle \neq \mathrm{D}(\mathfrak{f}_1) \supset \mathrm{D}(\mathfrak{f}_2) \supset \cdots \supset \mathrm{D}(\mathfrak{f}_k)$ with the strictly increasing dimensions r_j, we can insert radicals of finitely generated ideals such that the obtained sequence of dimensions is $0, 1, \ldots, n$.*

NB: In item *1*, we say that the change of variables (which eventually changes nothing at all) has simultaneously put the ideals $\mathfrak{f}_1, \ldots, \mathfrak{f}_k$ in Noether position.

D *1.* The same proof as for the previous theorem works considering the fact that a change of variables can simultaneously render a finite number of nonzero polynomials monic in the last variable.
2. Let $\mathbf{A}_i = \mathbf{K}[X_1, \ldots, X_i]$. Suppose for example that $\mathfrak{f}_1$ is of dimension 2 and $\mathfrak{f}_2$ of dimension 5. We have to insert ideals of dimensions 3 and 4. Suppose without loss of generality that the $\mathfrak{f}_i$'s are in Noether position with respect to $X_1, \ldots, X_n$.
We have by hypothesis $\mathbf{A}_2 \cap \mathfrak{f}_1 = 0$, with monic polynomials

$$h_3 \in \mathbf{A}_2[X_3] \cap \mathfrak{f}_1,\ h_4 \in \mathbf{A}_2[X_4] \cap \mathfrak{f}_1,\ \ldots,\ h_n \in \mathbf{A}_2[X_n] \cap \mathfrak{f}_1.$$

We then have the following inclusions,

$$\mathfrak{h}_1 = \mathfrak{f}_2 + \langle h_5, h_4 \rangle \supseteq \mathfrak{h}_2 = \mathfrak{f}_2 + \langle h_5 \rangle \supseteq \mathfrak{f}_2 \quad \text{and} \quad \mathrm{D}(\mathfrak{f}_1) \supseteq \mathrm{D}(\mathfrak{h}_1) \supseteq \mathrm{D}(\mathfrak{h}_2) \supseteq \mathrm{D}(\mathfrak{f}_2),$$

with $\mathfrak{h}_1$ of dimension 3 and $\mathfrak{h}_2$ of dimension 4, both in Noether position with respect to $(X_1, \ldots, X_n)$. □

The actual Nullstellensatz

In Theorems 1.1 (infinite discrete field) and 1.5 (arbitrary discrete field) the Nullstellensatz is in the weak form; i.e. the proven equivalence is between, on the one hand,
• the polynomial system does not have any zero in any finite nonzero **K**-algebra,
and on the other,
• the corresponding quotient algebra is null.

The general Nullstellensatz states under what condition a polynomial is annihilated at the zeros of a polynomial system. Here, since we do not have an algebraically closed field at our disposal, we will consider the zeros in the finite **K**-algebras and we obtain two Nullstellensätze depending on whether we only consider the reduced **K**-algebras or not.

These two theorems generalize from a constructive point of view (with explicit "either-or's") the classical Nullstellensatz stated in the form of Theorem III-9.7.

1.8. Theorem. (Classical Nullstellensatz, general constructive version)
Let $\mathbf{K}$ *be a discrete field and* $f_1, \dots, f_s$*,* g *be in* $\mathbf{K}[X_1, \dots, X_n]$*. Consider the quotient algebra* $\mathbf{A} = \mathbf{K}[\underline{X}]/\langle f_1, \dots, f_s\rangle$*.*

1. *Either there exists a nonzero quotient* $\mathbf{B}$ *of* $\mathbf{A}$ *which is a reduced finite* $\mathbf{K}$*-algebra with* $g \in \mathbf{B}^{\times}$ *(a fortiori* $g \neq 0$ *in* $\mathbf{B}$*).*
2. *Or* g *is nilpotent in* $\mathbf{A}$ *(in other words, there exists an integer* N *such that* $g^N \in \langle f_1, \dots, f_s\rangle_{\mathbf{K}[\underline{X}]}$*).*

D We use Rabinovitch's trick. We introduce an additional indeterminate T and we notice that g is nilpotent in $\mathbf{A}$ if and only if the quotient algebra $\mathbf{A}'$ for the polynomial system $(f_1, \dots, f_s, 1 - gT)$ is null. We end with the weak Nullstellensatz: if $\mathbf{A}' \neq 0$, we find a nonzero quotient $\mathbf{B}'$ of $\mathbf{A}'$ which is a finite dimensional $\mathbf{K}$-vector space. As g is invertible in $\mathbf{A}'$, it is also invertible in $\mathbf{B}'$ and in $\mathbf{B} = \mathbf{B}'_{\mathrm{red}}$, and as $\mathbf{B} \neq 0$, $g \neq 0$ in $\mathbf{B}$. □

1.9. Theorem. (Nullstellensatz with multiplicities)
Let $\mathbf{K}$ *be a discrete field and* $f_1, \dots, f_s$*,* g *be in* $\mathbf{K}[X_1, \dots, X_n]$*. Consider the quotient algebra* $\mathbf{A} = \mathbf{K}[\underline{X}]/\langle f_1, \dots, f_s\rangle$*.*

1. *Either there exists a quotient* $\mathbf{B}$ *of* $\mathbf{A}$ *which is a finite dimensional* $\mathbf{K}$*-vector space with* $g \neq 0$ *in* $\mathbf{B}$*.*
2. *Or* $g = 0$ *in* $\mathbf{A}$ *(in other words,* $g \in \langle f_1, \dots, f_s\rangle_{\mathbf{K}[\underline{X}]}$*).*

Proof using Gröbner bases. If when placing in the Noether position we have $r = 0$, the result is clear. The delicate point is when $r \geqslant 1$. Suppose the ideal is in Noether position. We consider an elimination order for the variables $(Y_1, \dots, Y_r)$ and the normal form of g with respect to the corresponding Gröbner basis of $\mathfrak{f}$. For "everything to remain as is" after a specialization $Y_i \mapsto \alpha_i = \overline{Y_i}$ in a quotient ring $\mathbf{L}$ of $\mathbf{K}[Y_1, \dots, Y_r]$, it suffices that the leading coefficients in the Gröbner basis of $\mathfrak{f}$ and in the normal form of g (those coefficients are elements of $\mathbf{K}[Y_1, \dots, Y_r]$) specialize in invertible elements of $\mathbf{L}$. If we have at our disposal enough distinct elements in $\mathbf{K}$ to find suitable α_i's in $\mathbf{K}$ we can take $\mathbf{L} = \mathbf{K}$, otherwise we consider the product h of all the leading coefficients previously considered, and we replace $\mathbf{K}[Y_1, \dots, Y_r]$ with a nonzero quotient $\mathbf{L}$, strictly finite over $\mathbf{K}$, in which h is invertible (this is possible by Theorem 1.8, applied to h with no equation f_i). The solution to our problem is then given by the algebra

$$\mathbf{B} = \mathbf{L} \otimes_{\mathbf{K}[Y_1,\ldots,Y_r]} \mathbf{A},$$

which is a quotient of $\mathbf{A}$ strictly finite over $\mathbf{K}$. □

Syzygies

Another important consequence of the change of variables lemma (Lemma 1.4) is the following theorem.

1.10. Theorem. *Let* $\mathbf{K}$ *be a discrete reduced zero-dimensional ring.*

1. *Every finitely presented* $\mathbf{K}$*-algebra is a strongly discrete coherent ring.*
2. *Consequently every finitely presented module over such an algebra is coherent and strongly discrete.*

D We prove the first item for $\mathbf{K}[X_1,\ldots,X_n]$ in the case where $\mathbf{K}$ is a discrete field. The zero-dimensional ring case is deduced from it by the usual technique (elementary local-global machinery no. 2). Then item *2* is a consequence of Theorem IV-4.3.

We give a proof by induction over n, the $n = 0$ case being clear. Suppose $n \geqslant 1$ and let $\mathbf{B} = \mathbf{K}[X_1,\ldots,X_n]$. We must show that an arbitrary finitely generated ideal $\mathfrak{f} = \langle f_1,\ldots,f_s\rangle$ is finitely presented and detachable.

If $\mathfrak{f} = 0$ then it is clear, otherwise we can assume by applying Lemma 1.4 that f_s is monic in X_n of degree d. If $s = 1$, the annihilator of f_1 is null, and therefore also the module of syzygies for (f_1). The ideal $\mathfrak{f}$ is detachable thanks to Euclidean division with respect to X_n.

If $s \geqslant 2$, let $\mathbf{A} = \mathbf{K}[X_1,\ldots,X_{n-1}]$. The ring $\mathbf{A}$ is strongly discrete coherent by induction hypothesis. Let R_i be the syzygy that corresponds to the equality $f_i f_s - f_s f_i = 0$ ($i \in [\![1..s-1]\!]$). Modulo the syzygies R_i we can rewrite each $X_n^k f_i = g_{k,i}$, for $k \in [\![0..d-1]\!]$ and $i \in [\![1..s-1]\!]$ as vectors in the free $\mathbf{A}$-module $L \subseteq \mathbf{B}$ with basis $(1, X_n, \ldots, X_n^{d-1})$. Modulo the syzygies R_i every syzygy for $(f_1,\ldots,f_s)$ with coefficients in $\mathbf{B}$ can be rewritten as a syzygy for

$$V = (g_{0,1},\ldots,g_{d-1,1},\ldots,g_{0,s-1},\ldots,g_{d-1,s-1}) \in L^{d(s-1)}$$

with coefficients in $\mathbf{A}$. As L is a free $\mathbf{A}$-module, it is strongly discrete coherent. We have in particular a finite number of $\mathbf{A}$-syzygies for V that generate them all. Let us call them S_1, …, S_ℓ. Each $\mathbf{A}$-syzygy S_j for V can be read as a $\mathbf{B}$-syzygy S'_j for $(f_1,\ldots,f_s)$. Finally, the syzygies R_i and S'_j generate the $\mathbf{B}$-module of the syzygies for $(f_1,\ldots,f_s)$.

Concerning the strongly discrete character, we proceed in the same way. To test if an element of $\mathbf{B}$ is in $\mathfrak{f}$ we start by dividing it by f_s with respect to X_n. We then obtain a vector in the $\mathbf{A}$-module L for which we must test whether it belongs to the submodule generated by the $g_{i,j}$'s. □

2. The dynamic method

I do not believe in miracles.
A constructive mathematician.

In classical mathematics proofs of existence are rarely explicit. Two essential obstacles appear each time that we try to render such a proof explicit.

The first obstacle is the application of **LEM**. For instance, if you consider the proof that every univariate polynomial over a field $\mathbf{K}$ admits a decomposition into prime factors, you have a kind of algorithm whose key ingredient is: if P is irreducible all is well, if P can be decomposed into a product of two factors of degree $\geqslant 1$, all is still well, by induction hypothesis. Unfortunately the disjunction used to make the proof work "P is irreducible or P can be decomposed into a product of two factors of degree $\geqslant 1$" is not explicit in general. In other words, even if a field is defined constructively, we cannot be sure that this disjunction can be made explicit by an algorithm. Here we find ourselves in the presence of a typical case where **LEM** "is an issue," because the existence of an irreducible factor cannot be the object of a general algorithm.

The second obstacle is the application of Zorn's lemma, which allows us to generalize to the uncountable case the usual proofs by induction in the countable case.

For example in Modern Algebra by van der Waerden the second pitfall is avoided by limiting ourselves to the countable algebraic structures.

However, we have two facts that are now well established from experience:

- The *universal* concrete results proven by the dubious abstract methods above have never been contradicted. We have even very often successfully extracted unquestionable constructive proofs from them. This would suggest that even if the abstract methods are in some way incorrect or contradictory, they have until now only been used with a sufficient amount of discernment.
- The key concrete results proven by the dubious abstract methods have not been invalidated either. On the contrary, they have often been validated by algorithms proven constructively.[1]

Faced with this slightly paradoxical situation: the abstract methods are a priori dubious, but they do not fundamentally deceive us when they give us a result of a concrete nature. There are two possible reactions.

[1] On this second point, our assertion is less clear. If we return to the example of the decomposition of a polynomial into prime factors, it is impossible to achieve the result algorithmically over certain fields.

Either we believe that the abstract methods are fundamentally correct because they reflect a "truth," some sort of "ideal Cantor universe" in which exists the true semantic of mathematics. This is the stance taken by Platonic realism, defended for instance by Gödel.

Or we think that the abstract methods truly are questionable. But then, unless we believe that mathematics falls within the domain of magic or of miracles, it must be explained why classical mathematics makes such few mistakes. If we believe in neither Cantor, nor miracles, we are led to believe that the abstract proofs of concrete results necessarily contain sufficient "hidden ingredients" to construct the corresponding concrete proofs.

This possibility of constructively certifying concrete results obtained by dubious methods, if we manage to execute it systematically enough, is in line with Hilbert's program.

The dynamic method in constructive algebra is a general method for decrypting abstract proofs from classical mathematics when they use "ideal" objects whose existence relies on non-constructive principles: **LEM** and the axiom of choice. The ambition of this new method is to "give a constructive semantic for the usually practiced classical mathematics."

We replace the abstract objects from classical mathematics with incomplete but concrete specifications of these objects. This is the constructive counterpart of the abstract objects. For example a *finite potential prime ideal* (a notion that will be introduced in Section XV-1) is given by a finite number of elements in the ideal and a finite number of elements in its complement. This constitutes an incomplete but concrete specification of a prime ideal.

More precisely, the dynamic method aims at giving a systematic interpretation of classical proofs that use abstract objects by rereading them as constructive proofs with respect to constructive counterparts of these abstract objects.

This is in keeping with the thought-process behind certain techniques developed in Computer Algebra. Here we are thinking about "lazy evaluation," or "dynamic evaluation," i.e. lazy evaluation managed as a tree structure, as in the D5 system [58] which performs this tour de force very innocently: compute with certainty in the algebraic closure of an arbitrary field, even though we know that this object (the algebraic closure) cannot be constructed in all generality.

In the current chapter an incomplete specification of the splitting field of a separable polynomial over a field $\mathbf{K}$ will be given by a $\mathbf{K}$-algebra $\mathbf{A}$ and a finite group of automorphisms G of this algebra. In $\mathbf{A}$ the polynomial can be decomposed into linear factors such that a splitting field is a quotient of $\mathbf{A}$, and G is an approximation of the Galois group in a suitable sense (in particular, it contains a copy of the Galois group). We will explain how to compute with such an approximation without ever making a mistake: when an oddity occurs, we know how to better the approximation during computation and to make the oddity disappear.

Splitting fields and Galois theory in classical mathematics

In this subsection we will offer a possible presentation of the splitting field of an arbitrary polynomial and of the Galois theory of a separable polynomial in classical mathematics. This allows us to understand the "detours" that we will be obligated to take to have an entirely constructive theory.

If f is a monic polynomial, we work with the universal splitting algebra of f, $\mathbf{A} = \mathrm{Adu}_{\mathbf{K},f}$ in which $f(T) = \prod_i (T - x_i)$, with S_n as a group of automorphisms (see Section III-4).
This algebra being a finite dimensional $\mathbf{K}$-vector space, all the ideals are themselves finite dimensional $\mathbf{K}$-vector spaces and we have the right to consider a strict ideal $\mathfrak{m}$ of maximum dimension as a $\mathbf{K}$-vector space (all of this by applying **LEM**). This ideal is automatically a maximal ideal. The quotient algebra $\mathbf{L} = \mathbf{A}/\mathfrak{m}$ is then a splitting field for f. The group $G = \mathrm{St}(\mathfrak{m})$ operates on $\mathbf{L}$ and the fixed field of G, $\mathbf{L}^G = \mathbf{K}_1$, possesses the two following properties:

- $\mathbf{L}/\mathbf{K}_1$ is a Galois extension with $\mathrm{Gal}(\mathbf{L}/\mathbf{K}_1) \simeq G$.
- $\mathbf{K}_1/\mathbf{K}$ is an extension obtained by successive additions of p^{th} roots, where $p = \mathrm{char}(\mathbf{K})$.

Moreover, if $\mathbf{L}'$ is another splitting field for f with $f = \prod_i (T - \xi_i)$ in $\mathbf{L}'[T]$, we have a unique homomorphism of $\mathbf{K}$-algebras $\varphi : \mathbf{A} \to \mathbf{L}'$ satisfying the equalities $\varphi(x_i) = \xi_i$ for $i \in [\![1..n]\!]$. We can then show that $\mathrm{Ker}\,\varphi$, which is a maximal ideal of $\mathbf{A}$, is necessarily a conjugate of $\mathfrak{m}$ under the action of S_n. Thus the splitting field is unique, up to isomorphism (this isomorphism is not unique if $G \neq \{\mathrm{Id}\}$).
Finally, when f is separable, the situation is simplified because the universal splitting algebra is étale, and $\mathbf{K}_1 = \mathbf{K}$.

The previous approach is possible from a constructive point of view if the field $\mathbf{K}$ is separably factorial and if the polynomial f is separable, because then, since the universal splitting algebra $\mathbf{A}$ is étale, it can be decomposed into a finite product of étale fields over $\mathbf{K}$ (Corollary VI-1.13).
But when the field is not separably factorial, we face an a priori insurmountable obstacle, and we cannot hope to systematically and algorithmically obtain a splitting field that is strictly finite over $\mathbf{K}$.
If the characteristic is finite and if the polynomial is not separable, we need stronger factorization properties to construct a splitting field (the question is delicate, and very well presented in [MRR]).

Lazily bypassing the obstacle

What is generally proposed in Computer Algebra is, for instance in the case of a separable polynomial, at the very least to avoid computing a universal resolvent R (as in Theorem III-6.15) whose degree, $n!$, promptly renders computations impractical.

Here, we find ourselves in the most general framework possible, and we avoid all recourse to the factorization of the polynomials which can turn out to be impossible, or which, when possible, has the risk of being too costly.

The idea is to use the universal splitting algebra $\mathbf{A}$, or a Galois quotient $\mathbf{A}/\langle 1-e\rangle$, with a Galoisian idempotent e (see page 364) as a substitute for $\mathbf{L}$. This "dynamic splitting field" can be managed without too many problems because each time something strange happens, which indicates that the substitute of $\mathbf{L}$ is not entirely satisfying, we are able to "immediately repair the oddity" by computing a Galoisian idempotent that refines the previous one, and in the new approximation of the splitting field, the strange thing has disappeared.

To develop this point of view we will need to better know the universal splitting algebra, and Section 4 is dedicated to this objective.

Moreover, we will study in Section 5 a dynamic and constructive version of the splitting field of a (not necessarily separable) polynomial.

3. Introduction to Boolean algebras

A *lattice* is a set $\mathbf{T}$ equipped with an order relation $\leqslant$ for which there exist a minimum element, denoted by $0_{\mathbf{T}}$, a maximum element, denoted by $1_{\mathbf{T}}$, and every pair of elements (a, b) admits a least upper bound, denoted by $a \vee b$, and a greatest lower bound, denoted by $a \wedge b$. A mapping from one lattice to another is called a *lattice homomorphism* if it respects the operations $\vee$ and $\wedge$ as well as the constants 0 and 1. The lattice is called a *distributive lattice* when each of the two operations $\vee$ and $\wedge$ is distributive with respect to the other.

We will give a succinct study of the structure of distributive lattices and of structures that relate back to them in Chapter XI.

3.1. Proposition and definition. (Boolean algebras)

1. *By definition a ring* $\mathbf{B}$ *is a* Boolean algebra *if and only if every element is idempotent. Consequently* $2 =_{\mathbf{B}} 0$ *(because* $2 =_{\mathbf{B}} 4$*).*
2. *We can define over* $\mathbf{B}$ *an order relation* $x \preccurlyeq y$ *by:* x *is a multiple of* y*, i.e.* $\langle x\rangle \subseteq \langle y\rangle$*. Then, two arbitrary elements admit a lower bound, their lcm* $x \wedge y = xy$*, and an upper bound, their gcd* $x \vee y = x + y + xy$*. We thus obtain a distributive lattice with* 0 *as its minimum element and* 1 *as its maximum element.*

3. *For every $x \in \mathbf{B}$, the element $x' = 1 + x$ is the unique element that satisfies the equalities $x \wedge x' = 0$ and $x \vee x' = 1$, we call it* the complement *of x.*

Notation conflict. Here we find ourselves with a conflict of notation. Indeed, divisibility in a ring leads to a notion of the gcd, which is commonly denoted by $a \wedge b$, because it is taken as a lower bound (a divides b being understood as "a smaller than b" in the sense of the divisibility). This conflicts with the gcd of the elements in a Boolean algebra, which is an upper bound. This is due to the fact that the order relation has been reversed, so that the elements 0 and 1 of the Boolean algebra are indeed the minimum and the maximum in the lattice. This inevitable conflict will appear in an even stronger sense when we will consider the Boolean algebra of the idempotents of a ring $\mathbf{A}$. ■

Even though all the elements of a Boolean algebra are idempotents we will keep the terminology "fundamental system of orthogonal idempotents[2]" for a finite family (x_i) of pairwise orthogonal elements (i.e. $x_i x_j = 0$ for $i \neq j$) with sum 1. This convention is all the more justified in that we will mainly preoccupy ourselves with the Boolean algebra that naturally appears in commutative algebra: that of the idempotents of a ring $\mathbf{A}$.

Discrete Boolean algebras

3.2. Proposition. (Every discrete Boolean algebra behaves in computations as the algebra of the detachable subsets of a finite set)
Let $(r_1, \ldots, r_m)$ be a finite family in a Boolean algebra $\mathbf{B}$.
Let $s_i = 1 - r_i$ and, for a finite subset I of $\{1, \ldots, m\}$, let $r_I = \prod_{i \in I} r_i \prod_{j \notin I} s_j$.

1. *The r_I's form a fundamental system of orthogonal idempotents and they generate the same Boolean algebra as the r_i's.*
2. *Suppose that $\mathbf{B}$ is discrete. Then, if there are exactly N nonzero elements r_I, the Boolean subalgebra generated by the r_i's is isomorphic to the algebra of finite subsets of a set with N elements.*

As a corollary we obtain the following fact and the fundamental structure theorem that summarizes it. Recall that we denote by $\mathrm{P_f}(S)$ the set of finite subsets of a set S.

In a discrete Boolean algebra an element e is called an *atom* if it satisfies one of the following equivalent properties.

- e is minimal among the nonzero elements.
- $e \neq 0$ and for every f, f is orthogonal or greater than e.

[2] It would be more natural to say: fundamental system of orthogonal elements.

- $e \neq 0$ and for every f, $ef = 0$ or e, or $ef = 0$ or $e(1-f) = 0$.
- $e \neq 0$ and the equality $e = e_1 + e_2$ with $e_1 e_2 = 0$ implies $e_1 = 0$ or $e_2 = 0$.

We also say that e is *indecomposable*. It is clear that an automorphism of a discrete Boolean algebra preserves the set of atoms and that for two atoms e and f, we have $e = f$ or $ef = 0$.

3.3. Theorem. (Structure theorem)

1. *Every finite Boolean algebra is isomorphic to the algebra of the detachable subsets of a finite set.*
2. *More precisely, for a Boolean algebra C the following properties are equivalent.*
   a. *C is finite.*
   b. *C is discrete and finitely generated.*
   c. *The set S of atoms is finite, and 1_C is the sum of this set.*

   In such a case C is isomorphic to the Boolean algebra $\mathrm{P_f}(S)$.

Boolean algebra of the idempotents of a commutative ring

3.4. Fact. *The idempotents of a ring $\mathbf{A}$ form a Boolean algebra, denoted by $\mathbb{B}(\mathbf{A})$, with the operations $\wedge$, $\vee$, $\neg$ and $\oplus$ given by*

$$r \wedge s = rs, \;\; r \vee s = r + s - rs \;\;, \;\; \neg\, r = 1 - r \;\; \textit{and} \;\; r \oplus s = (r-s)^2.$$

If $\mathbf{A}$ is a Boolean algebra, $\mathbb{B}(\mathbf{A}) = \mathbf{A}$. If $\varphi : \mathbf{A} \to \mathbf{B}$ is a morphism of rings, its restriction to $\mathbb{B}(\mathbf{A})$ gives a morphism $\mathbb{B}(\varphi) : \mathbb{B}(\mathbf{A}) \to \mathbb{B}(\mathbf{B})$.

D It suffices to show that if we equip the set $\mathbb{B}(\mathbf{A})$ with the laws $\oplus$ and $\wedge$ we obtain a Boolean algebra with $0_\mathbf{A}$ and $1_\mathbf{A}$ as neutral elements. The computations are left to the reader. □

Theorem 3.3 has the following immediate consequence.

3.5. Fact. *The following properties are equivalent.*

1. *The Boolean algebra of the idempotents $\mathbb{B}(\mathbf{A})$ is finite.*
2. *The ring $\mathbf{A}$ is a finite product of nontrivial connected rings.*

D It suffices to show that *1* implies *2*. If e is an atom of $\mathbb{B}(\mathbf{A})$, the ring $\mathbf{A}[1/e]$ is nontrivial and connected. If $\mathbb{B}(\mathbf{A})$ is finite, the finite set A of its atoms forms a fundamental system of orthogonal idempotents of $\mathbf{A}$, and we have a canonical isomorphism $\mathbf{A} \to \prod_{e \in A} \mathbf{A}[1/e]$. □

Remark. If $\mathbb{B}(\mathbf{A})$ has a single element, $\mathbf{A}$ is trivial and the finite product is an empty product. This also applies to the following corollary. ■

3.6. Corollary. *The following properties are equivalent.*

1. $\mathbb{B}(\mathbf{A})$ *is finite and* $\mathbf{A}$ *is zero-dimensional.*
2. $\mathbf{A}$ *is a finite product of nontrivial zero-dimensional local rings.*

Galoisian elements in a Boolean algebra

3.7. Definition.

1. If G is a group that operates over a Boolean algebra C, we say that the pair (C, G) is a G-Boolean algebra.
2. An element e of a G-Boolean algebra C is said to be *Galoisian* if its orbit under G is a fundamental system of orthogonal idempotents.
3. A G-Boolean algebra is said to be *transitive* if 0 and 1 are the only elements fixed by G.

Definition VI-7.21 of Galoisian idempotents agrees with the previous definition when a finite group G acts on a $\mathbf{k}$-algebra $\mathbf{C}$ and when we consider the action of G over the Boolean algebra $\mathbb{B}\mathrm{o}(\mathbf{C})$.

Now we study the case where the group is finite and the algebra discrete.

3.8. Fact. *Let G be a finite group and C be a transitive, discrete and nontrivial G-Boolean algebra. Let $e \neq 0$ in C, and $\{e_1, \dots, e_k\}$ be the orbit of e under G. The following properties are equivalent.*

1. *The element e is Galoisian.*
2. *For all $i > 1$, $e_1 e_i = 0$.*
3. *For all $\sigma \in G$, $e\sigma(e) = e$ or 0.*
4. *For all $i \neq j \in \{1, \dots, k\}$, $e_i e_j = 0$.*

D Item *1* clearly implies the others. Items *2* and *4* are easily equivalent and imply item *3*. Item *3* means that for every σ, $\sigma(e) \geqslant e$ or $\sigma(e)e = 0$. If we have $\sigma(e) \geqslant e$ for some σ, then we obtain

$$e \leqslant \sigma(e) \leqslant \sigma^2(e) \leqslant \sigma^3(e) \leqslant \dots ,$$

which gives us $e = \sigma(e)$ when considering an ℓ such that $\sigma^\ell = 1_G$. Therefore, item *3* implies item *2*. Finally, if item *4* is satisfied, the sum of the orbit is an element > 0 fixed by G therefore equal to 1. □

3.9. Lemma. (Meeting of two Galoisian elements)
Let G be a finite group and C be a nontrivial discrete G-Boolean algebra. Given two Galoisian elements e, f in (C, G), let

$$G.e = \{e_1, \dots, e_m\},\ E = \mathrm{St}_G(e),\ \textit{and}\ F = \mathrm{St}_G(f).$$

1. *There exists a $\tau \in G$ such that $f\tau(e) \neq 0$.*
2. *If $e \leqslant f$, then $E \subseteq F$ and $f = \sum_{i:e_i \leqslant f} e_i = \sum_{\sigma \in F/E} \sigma(e)$.*

Suppose C is transitive and $ef \neq 0$. We obtain the following results.

3. *The element ef is Galoisian, with stabilizer $E \cap F$, and the orbit $G.ef$ consists of nonzero elements of $(G.e)(G.f)$. In particular, $G.ef$ generates the same Boolean subalgebra of C as $G.e \cup G.f$.*

4. *If $E \subseteq F$, then $e \leqslant f$.*

$\triangleright$ *1.* Indeed, $f = \sum_i fe_i$.

2. Generally, for $x' = \sigma(x)$ where $x \neq 0$ satisfies $x \leqslant f$, let us show

$$(\star) \qquad x' \leqslant f \overset{[a]}{\Longrightarrow} fx' \neq 0 \overset{[b]}{\Longrightarrow} \sigma(f) = f \overset{[c]}{\Longrightarrow} x' \leqslant f.$$

We obtain $[a]$ by multiplying $x' \leqslant f$ by x', $[b]$ by multiplying $x' \leqslant \sigma(f)$ (deduced from $x \leqslant f$) by f and by using the fact that f is Galoisian and finally $[c]$ by applying σ to $x \leqslant f$. The assertions of $(\star)$ are therefore equivalences. We deduce $\mathrm{St}_G(x) \subseteq \mathrm{St}_G(f)$. If in addition, $1 = \sum_{x' \in G.x} x'$, then

$$f = \textstyle\sum_{x' \in G.x} fx' = \sum_{x' \in G.x \mid x' \leqslant f} x' = \sum_{\sigma \in F/\mathrm{St}_G(x)} \sigma(x).$$

This applies to $x = e$.

3. Let $G.f = \{f_1, \ldots, f_p\}$. For $\sigma \in G$ there exist i, j such that

$$e\,f\,\sigma(ef) = e\,f\,e_i\,f_j,$$

which is equal to ef if $\sigma \in E \cap F$ and to 0 otherwise. By Fact 3.8, ef is therefore a Galoisian element with stabilizer $E \cap F$. Now assume $e_i f_j \neq 0$. Then, by item *1*, there exists a $\tau \in G$ such that $\tau(ef)e_i f_j \neq 0$. Since e and f are Galoisian, this implies $\tau(e) = e_i$ and $\tau(f) = f_j$, so $e_i f_j \in G.ef$.

4. Immediately results from *3.* □

The paradigmatic application of the next theorem is the following. We have a nontrivial connected ring $\mathbf{k}$, $(\mathbf{k}, \mathbf{C}, G)$ is a pre-Galois (cf. Definition 4.2) or Galois algebra and we take $C = \mathbb{B}(\mathbf{C})$.

3.10. Theorem. (Galois structure theorem, 1) *Let G be a finite group and C be a transitive, discrete and nontrivial G-Boolean algebra.*

1. (Structure of the transitive finite G-Boolean algebras)
The algebra C is finite if and only if there exists an atom e. In this case the structure of (C, G) is entirely characterized by $E = \mathrm{St}_G(e)$.
More precisely, the idempotent e is Galoisian, $G.e$ is the set of atoms, $C \simeq \mathrm{P_f}(G.e)$, G operates over $G.e$ as it does over G/E, and over C as it does over $\mathrm{P_f}(G/E)$. In particular, $|C| = 2^{|\,G:E\,|}$.
We will say that e is a Galoisian generator *of C.*

2. *Every finite family of elements of C generates a finite G-subalgebra.*

3. *The Boolean algebra C cannot have more than $2^{|G|}$ elements.*

4. *Let e and f be Galoisian elements, $E = \mathrm{St}_G(e)$ and $F = \mathrm{St}_G(f)$.*

a. *There exists a $\sigma \in G$ such that $f\sigma(e) \neq 0$.*

b. If $ef \neq 0$, ef is a Galoisian generator of the G-subBoolean algebra of G generated by e and f, and $\mathrm{St}_G(ef) = E \cap F$.

c. If $e \leqslant f$ (i.e. $fe = e$), then $E \subseteq F$ and $f = \sum_{\sigma \in F/E} \sigma(e)$.

5. (Characterization of the Galoisian elements in a finite G-subalgebra) *Let e be a Galoisian element and f be a sum of r elements of $G.e$, including e. Let $E = \mathrm{St}_G(e)$ and $F = \mathrm{St}_G(f)$. Then the following properties are equivalent.*

a. f is Galoisian.

b. $E \subseteq F$ and $f = \sum_{\sigma \in F/E} \sigma(e)$.

c. $|F| = r \times |E|$.

d. $|F| \geqslant r \times |E|$.

D *1.* If C is finite there exists an atom. If e is an atom, for every $\sigma \in G$, we have $e\,\sigma(e) = 0$ or e, so e is Galoisian (Fact 3.8). The rest follows by taking into account Theorem 3.3.

2. Consider the Boolean subalgebra $C' \subseteq C$ generated by the orbits of the elements of the given finite family. C' is finitely generated and discrete therefore finite. Consequently its atoms form a finite set $S = \{e_1, \dots, e_k\}$ and C' is isomorphic to the Boolean algebra of the finite subsets of S

$$C' = \left\{ \textstyle\sum_{i \in F} e_i \,|\, F \in \mathcal{P}_k \right\}.$$

Clearly, G operates on C'. For $\sigma \in G$, $\sigma(e_1)$ is an atom, so e_1 is Galoisian (Fact 3.8 *3*) and $(e_1, \dots, e_k)$ is its orbit.

3. Results from *1* and *2*.

4. Already seen in Lemma 3.9.

5. We write $\sigma_1 = 1_G$, $G.e = \{\sigma_1.e, \dots, \sigma_k.e\}$ with $k = |\,G : E\,|$, as well as $f = \sigma_1.e + \cdots + \sigma_r.e$.

a ⇒ *b.* We apply item *4*.

b ⇒ *a.* For $\tau \in F$, $\tau.f = f$.

For $\tau \notin F$, $F.e \cap (\tau F).e = \emptyset$, and so $f\,\tau(f) = 0$.

b ⇒ *c.* We have $F.e = \{1_G.e, \sigma_2.e, \dots, \sigma_r.e\}$, and since E is the stabilizer of e, we obtain $|F| = r \times |E|$.

d ⇒ *b.* We have $F = \{\,\tau \,|\, \tau\,\{\sigma_1.e, \dots, \sigma_r.e\} = \{\sigma_1.e, \dots, \sigma_r.e\}\,\}$. Hence the inclusion $F.e \subseteq \{\sigma_1.e, \dots, \sigma_r.e\}$, and $F.e = \{\sigma_1.e, \dots, \sigma_s.e\}$ with $s \leqslant r \leqslant k$. The stabilizer of e for the action of F on $F.e$ is equal to $E \cap F$. Therefore

$$|F| = |F.e|\ |E \cap F| = s\ |E \cap F| \leqslant r\ |E \cap F| \leqslant r\ |E|\,.$$

Therefore if $|F| \geqslant r\ |E|$, we have $|F.e| = r$ and $|E| = |E \cap F|$, i.e. $E \subseteq F$ and $F.e = \{\sigma_1, \dots, \sigma_r\}$. □

Under the hypotheses of Theorem 3.10 we can compute a Galoisian element e_1 such that $G.e_1$ and $G.e$ generate the same Boolean algebra, by means of Algorithm 3.11.

3.11. Algorithm. Computation of a Galoisian element and of its stabilizer.

```
Input: $e$: nonzero element of a Boolean algebra $C$; $G$: finite group of automorphisms of $C$; $S = \mathrm{St}_G(e)$.
# Suppose that $0$ and $1$ are the only fixed points for the action of $G$ on $C$.
Output: $e_1$: a Galoisian element of $C$ such that $G.e_1$ generates the same Boolean algebra as $G.e$; $H$: the stabilizer subgroup of $e_1$.
Local variables: $h$: in $C$; $\sigma$: in $G$; $L$: list of elements of $\overline{G/S}$;
$E$: corresponding set of elements of $G/S$;
#  $G/S$ is the set of left cosets of $S$.
#  $\overline{G/S}$ is a system of representatives of the left cosets of $S$
Begin
  $E \leftarrow \emptyset$; $L \leftarrow [\,]$; $e_1 \leftarrow e$;
  for $\sigma$ in $\overline{G/S}$ do
    $h \leftarrow e_1\sigma(e)$;
    if $h \neq 0$ then $e_1 \leftarrow h$; $L \leftarrow L \bullet [\sigma]$; $E \leftarrow E \cup \{\sigma S\}$
    end if;
  end for;
  $H \leftarrow \mathrm{St}_G(E)$   #  $H = \big\{\, \alpha \in G \,|\, \forall \sigma \in L, \alpha\sigma \in \bigcup_{\tau \in L} \tau S \,\big\}$.
End.
```

Correctness proof of the algorithm. We denote by G/S a system of representatives of the left cosets of S. Let us write $e_1 = e\sigma_2(e)\cdots\sigma_r(e)$ where the σ_i's are all the σ's which have successfully passed the test $h \neq 0$ in the algorithm (and $\sigma_1 = \mathrm{Id}$). We want to show that e_1 is an atom of C' (the Boolean algebra generated by $G.e$), which is the same as saying that for all $\sigma \in G/S$ we have $e_1\sigma(e) = e_1$ or 0 (since C' is generated by the $\tau(e)$'s). However, σ has been tested by the algorithm, therefore either σ is one of the σ_i's, in which case $e_1\sigma(e) = e_1$, or $g\sigma(e) = 0$ for some idempotent g which divides e_1, and a fortiori $e_1\sigma(e) = 0$.

Let us show that the stabilizer H of e_1 indeed satisfies the required condition. We have $e_1 = \prod_{\tau \in L} \tau(e)$, and for $\sigma \in G$ we have the equivalences

$$\sigma \in \textstyle\bigcup_{\tau \in L} \tau S \iff e_1\sigma(e) = e_1 \iff e_1 \leqslant \sigma(e), \qquad \text{and}$$
$$\sigma \notin \textstyle\bigcup_{\tau \in L} \tau S \iff e_1\sigma(e) = 0.$$

For $\alpha \in G$ we have $\alpha(e_1) = \prod_{\tau \in L} \alpha\big(\tau(e)\big)$. This is an element of the orbit of e_1, it is equal to e_1 if and only if $e_1 \leqslant \alpha(e_1)$, if and only if $e_1 \leqslant \alpha\big(\sigma(e)\big)$ for each σ in L. Finally, for some arbitrary σ in G, $e_1 \leqslant \alpha\big(\sigma(e)\big)$ if and only if $\alpha\sigma$ is in $\bigcup_{\tau \in L} \tau S$. □

Note that the element e_1 obtained as a result of this computation depends on the order in which the finite set G/S is enumerated and that there is no (intrinsic) natural order on this set.

Example. We can ask ourselves if there exists a relation between the stabilizer S of e and the stabilizer H of a Galoisian element e_1 associated with e. Here is an example that shows that there is no close relation, with $G = \mathrm{S}_6$ operating on $\mathrm{Adu}_{\mathbb{Q},f}$ with the polynomial $f(T) = T^6 - 4T^3 + 7$. We consider the idempotent $e = 1/6(x_5^3 x_6^3 - 2x_5^3 - 2x_6^3 + 7)$ that we compute from a factorization of the minimal polynomial of the element $x_5 + x_6$ (cf. Proposition 6.6).
We find $\mathrm{St}(e) = S = \langle (1432), (12), (56) \rangle \simeq \mathrm{S}_4 \times \mathrm{S}_2$ with $|S| = 48$, and

$$\mathrm{St}(e_1) = H = \langle (24), (123456) \rangle = (\langle (13), (135) \rangle \times \langle (24), (246) \rangle) \rtimes \langle (14)(25)(36) \rangle$$

with $H \simeq (\mathrm{S}_3 \times \mathrm{S}_3) \rtimes \mathrm{S}_2$, $|H| = 72$, and $S \cap H = \langle (24), (1234)(56) \rangle$ dihedral of order 8.
In short, H (not even the conjugacy class of H in G) cannot be computed solely from S. Indeed, the list L of left cosets selected by the algorithm does not only depend on subgroup S of G but also on the way in which G operates on C. ■

4. The universal splitting algebra (2)

Here is a small reading guide for the end of this chapter.

In Section III-6, we have seen that if $\mathbf{k}$ is an infinite discrete field, if f is separable and if we are able to decompose a Galois resolvent into a product of irreducible factors, then the universal splitting algebra $\mathbf{A}$ is isomorphic to $\mathbf{L}^r$, where $\mathbf{L}$ is a splitting field for f and $r = |\,\mathrm{S}_n : G\,|$, where G is a subgroup of S_n which is identified with $\mathrm{Gal}(\mathbf{L}/\mathbf{k})$. Moreover, $[\,\mathbf{L} : \mathbf{k}\,] = |G|$.

We will see that this ideal situation can serve as a guideline for a lazy approach to the construction of a splitting field. What replaces the complete factorization of a Galois resolvent is the discovery or the construction of a Galoisian idempotent. Then, we have a situation analogous to the ideal situation previously described: $\mathbf{A} \simeq \mathbf{B}^r$, where $\mathbf{B}$ is a Galois quotient of $\mathbf{A}$, equipped with a group of automorphisms that can be identified with a subgroup G of S_n, with $[\,\mathbf{B} : \mathbf{k}\,] = |G|$ and $r = |\,\mathrm{S}_n : G\,|$.

Throughout Section 4, $\mathbf{k}$ is a commutative ring,
$f = T^n + \sum_{k=1}^{n} (-1)^k s_k T^{n-k} \in \mathbf{k}[T]$ is monic of degree n,
and $\mathbf{A} = \mathrm{Adu}_{\mathbf{k},f}$ is the universal splitting algebra of f over $\mathbf{k}$.

Recall that the universal splitting algebra

$$\mathbf{A} = \mathrm{Adu}_{\mathbf{k},f} = \mathbf{k}[\underline{X}]/\langle S_1 - s_1, \ldots, S_n - s_n\rangle = \mathbf{k}[\underline{X}]/\mathcal{J}(f)$$

(where the S_i's are the elementary symmetric polynomials in the X_i's) is the algebra which solves the universal problem linked to the decomposition of the polynomial f into a product of factors $T - \xi_j$ (cf. Fact III-4.2). The $\mathbf{k}$-module $\mathbf{A} = \mathrm{Adu}_{\mathbf{k},f}$ is free, and a basis is formed by the "monomials" $x_1^{d_1} \cdots x_{n-1}^{d_{n-1}}$ such that for $k \in [\![0..n-1]\!]$, we have $d_k \leqslant n-k$ (see Fact III-4.4). We will denote this basis by $\mathcal{B}(f)$.

By a change of the base ring, we obtain the following important fact (to be distinguished from Fact III-4.3).

4.1. Fact. (Changing the base ring for a universal splitting algebra) *Let $\rho : \mathbf{k} \to \mathbf{k}_1$ be a $\mathbf{k}$-algebra. Let f^ρ be the image of f in $\mathbf{k}_1[T]$. Then, the algebra $\rho_\star(\mathrm{Adu}_{\mathbf{k},f}) = \mathbf{k}_1 \otimes_{\mathbf{k}} \mathrm{Adu}_{\mathbf{k},f}$ is naturally isomorphic to $\mathrm{Adu}_{\mathbf{k}_1,f^\rho}$.*

Galois quotients of pre-Galois algebras

If $\mathbf{C}$ is a $\mathbf{k}$-algebra, we denote by $\mathrm{Aut}_{\mathbf{k}}(\mathbf{C})$ its group of automorphisms.

We now give a definition that allows us to place the universal splitting algebra in a framework that is a little more general and useful.

4.2. Definition. *(pre-Galois algebras)*
A *pre-Galois algebra* is given by a triple $(\mathbf{k}, \mathbf{C}, G)$ where

1. $\mathbf{C}$ is a $\mathbf{k}$-algebra with $\mathbf{k} \subseteq \mathbf{C}$, $\mathbf{k}$ a direct summand in $\mathbf{C}$,
2. G is a finite group of $\mathbf{k}$-automorphisms of $\mathbf{C}$,
3. $\mathbf{C}$ is a projective $\mathbf{k}$-module of constant rank $|G|$,
4. for every $z \in \mathbf{C}$, we have $\mathrm{C}_{\mathbf{C}/\mathbf{k}}(z)(T) = \mathrm{C}_G(z)(T)$.

Remark. Recall that by Lemma VI-4.3, if $\mathbf{B}$ is a faithful strictly finite $\mathbf{k}$-algebra , then $\mathbf{k}$ (identified with its image in $\mathbf{B}$) is a direct summand in $\mathbf{B}$. Consequently item *1* above results from item *3*. ■

Examples. 1) From what we already know on the universal splitting algebra (Section III-4) and by Lemma III-5.12, for every monic polynomial f, the triple $(\mathbf{k}, \mathrm{Adu}_{\mathbf{k},f}, \mathrm{S}_n)$ is a pre-Galois algebra.

2) Artin's theorem (Theorem VI-7.11) shows that every Galois algebra is a pre-Galois algebra. ■

The reader should refer to page 364 for the definitions of a Galoisian idempotent, of a Galoisian ideal and of a Galois quotient.

4.3. Theorem. (Galoisian structure theorem, 2)
Consider a pre-Galois algebra $(\mathbf{k},\mathbf{C},G)$*. Let* e *be a Galoisian idempotent of* $\mathbf{C}$*, and* $\{e_1,\dots,e_m\}$ *its orbits under* G*. Let* H *be the stabilizer of* $e=e_1$ *and* $r=|H|$*, so that* $rm=|G|$*. Let* $\mathbf{C}_i=\mathbf{C}[1/e_i]$ *for* $(i\in[\![1..m]\!])$*. Finally, let* $\pi:\mathbf{C}\to\mathbf{C}_1$ *be the canonical projection.*

1. $(\mathbf{k},\mathbf{C}_1,H)$ *is a pre-Galois algebra (in other words a Galois quotient of a pre-Galois algebra is a pre-Galois algebra).*
2. *The* $\mathbf{C}_i$*'s are pairwise isomorphic* $\mathbf{k}$*-algebras, and* $\mathbf{C}\simeq\mathbf{C}_1^m$*.*
3. *The algebra* $\mathbf{C}_1$ *is a projective* $\mathbf{k}$*-module of constant rank* $r=|H|$*. The restriction of* π *to* $\mathbf{k}$*, and even to* $\mathbf{C}^G$*, is injective, and* $\mathbf{k}$ *(identified with its image in* $\mathbf{C}_1$*) is a direct summand in* $\mathbf{C}_1$*.*
4. *The group* H *operates on* $\mathbf{C}_1$ *and* $\mathbf{C}_1^H$ *is canonically isomorphic to* $\mathbf{C}^G$*; more precisely,* $\mathbf{C}_1^H=\pi(\mathbf{C}^H)=\pi(\mathbf{C}^G)$*.*
5. *For all* $z\in\mathbf{C}_1$*,* $\mathrm{C}_{\mathbf{C}_1/\mathbf{k}}(z)(T)=\mathrm{C}_H(z)(T)$*.*
6. *Let* g_1 *be a Galoisian idempotent of* $(\mathbf{k},\mathbf{C}_1,H)$*,* K *its stabilizer in* H*, and* $g'\in e_1\mathbf{C}$ *be such that* $\pi(g')=g_1$*. Then,* g' *is a Galoisian idempotent of* $(\mathbf{k},\mathbf{C},G)$*, its stabilizer is* K*, and we have a canonical isomorphism* $\mathbf{C}_1/\langle 1-g_1\rangle\simeq\mathbf{C}/\langle 1-g'\rangle$*.*
7. *If* $(\mathbf{k},\mathbf{C},G)$ *is a Galois algebra, then so is* $(\mathbf{k},\mathbf{C}_1,H)$*.*

D Item *1* is a partial synthesis of items *2*, *3*, *4*, *5*.

Item *2* is obvious. An immediate consequence is the first assertion of item *3*. Let $(\tau_1,\tau_2,\dots,\tau_m)$ be a system of representatives for G/H, with $\tau_1=\mathrm{Id}$ and $\tau_i(e_1)=e_i$. Let us show that the restriction of π to $\mathbf{C}^G$ is injective. If $a\in\mathbf{C}^G$ and $e_1a=0$, then, by transforming by the τ_j's, all the e_ja's are null, and hence so is their sum, a. Finally, $\pi(\mathbf{k})$ is a direct summand in $\mathbf{C}_1$ by Lemma VI-4.3.

4. Let us first show $\mathbf{C}_1^H=\pi(\mathbf{C}^H)$. Let $z\in\mathbf{C}_1^H$ and $u\in\mathbf{C}$ such that $\pi(u)=z$. Since $z\in\mathbf{C}_1^H$, for $\sigma\in H$, $\sigma(u)\equiv u \bmod \langle 1-e_1\rangle$, i.e. $e_1\sigma(u)=e_1u$ or, since $\sigma(e_1)=e_1$, $\sigma(e_1u)=e_1u$. By letting $y=e_1u$, we see that y is H-invariant and $\pi(y)=z$.
Let us now show that $z\in\pi(\mathbf{C}^G)$. Let

$$v=\textstyle\sum_i\tau_i(y)=\sum_i\tau_i(e_1y)=\sum_i e_i\tau_i(y).$$

As $\pi(e_i)=\delta_{1i}$, we have $\pi(v)=\pi(y)$. The element v constructed thus is independent of the system of representatives for G/H. Indeed, if (τ'_i) is another system of representatives, even if it means reordering the indices, we can assume that $\tau'_iH=\tau_iH$, and so, y being H-invariant, $\tau'_i(y)=\tau_i(y)$. For $\sigma\in G$, the $(\sigma\circ\tau_i)$'s form a system of representatives for G/H, so $\sigma(v)=v$: the element v is G-invariant.

5. We have a decomposition $\mathbf{C}=\mathbf{C}'_1\oplus\cdots\oplus\mathbf{C}'_m$, where $\mathbf{C}'_j=e_j\mathbf{C}$ is a finitely generated projective $\mathbf{k}$-module of rank r and the restriction $\pi:\mathbf{C}'_1\to\mathbf{C}_1$ is an isomorphism of $\mathbf{k}$-modules. For all $y \in \mathbf{C}$, we have

$$\mathrm{C}_{\mathbf{C}/\mathbf{k}}(y)(T) = \prod_{j=1}^{m} \mathrm{C}_{\mathbf{C}'_j/\mathbf{k}}(e_j y)(T) \text{ and } \mathrm{C}_G(y)(T) = \prod_{j=1}^{m} \prod_{\tau \in H} \big(T - (\tau_j \circ \tau)(y)\big).$$

Let y be the unique element of $\mathbf{C}'_1$ such that $\pi(y) = z$. The equality on the left-hand side gives

$$\mathrm{C}_{\mathbf{C}/\mathbf{k}}(y)(T) = T^{(m-1)r}\, \mathrm{C}_{\mathbf{C}_1/\mathbf{k}}(z)(T).$$

Next, apply π to the equality on the right-hand side by letting $(\tau_j \circ \tau)(y) \in \mathbf{C}'_j$ (use $y = e_1 y$ and apply $\tau_j \circ \tau$). We then obtain

$$\mathrm{C}_G(y)(T) = T^{(m-1)r}\, \mathrm{C}_H(z)(T).$$

Hence $\mathrm{C}_{\mathbf{C}_1/\mathbf{k}}(z)(T) = \mathrm{C}_H(z)(T)$.

6. Taking into account the fact that the restriction of π to $e_1\mathbf{C}$ is an isomorphism we have $g'^2 = g' = g'e_1$. Similarly for $\sigma \in H$ we have $\sigma(g') = g'$ if $\sigma \in K$, or $g'\sigma(g') = 0$ if $\sigma \notin K$. Finally, for $\sigma \in G \setminus H$, $e_1\sigma(e_1) = 0$, and so $g'\sigma(g') = 0$. This shows that g' is a Galoisian idempotent of $\mathbf{C}$ with stabilizer K. The canonical isomorphism is immediate.

7. Item *4* implies that $\mathbf{k}$ is the set of fixed points. It remains to see that H is separating. If $\sigma \in H = \mathrm{St}(e)$ is distinct of the identity, we have some elements a_i and $x_i \in \mathbf{C}$ such that $\sum_i a_i(\sigma(x_i) - x_i) = 1$. This equality remains true if we localize at e. □

Case where the Boolean algebra of a universal decomposition algebra is discrete

It is desirable that one can test the equality of two idempotents e_1, e_2 in the universal splitting algebra $\mathbf{A}$, which is the same as knowing how to test $e = 0$ for an arbitrary idempotent of $\mathbf{A}$ (as in every additive group). However, $e\mathbf{A}$ is a finitely generated projective $\mathbf{k}$-module and $e = 0$ if and only if $\mathrm{R}_{e\mathbf{A}}(X) = 1$ (Theorem V-8.4 item *6*). Since the rank polynomial $\mathrm{R}_{e\mathbf{A}}$ can be explicitly computed, we can test the equality of two idempotents in $\mathbf{A}$ if and only if we can test the equality of two idempotents in $\mathbf{k}$. The above argument works in a slightly more general framework and we obtain the following result.

4.4. Fact. *If $\mathbb{B}(\mathbf{k})$ is a discrete Boolean algebra, so is $\mathbb{B}(\mathbf{A})$. More generally , if $\mathbf{C}$ is a strictly finite $\mathbf{k}$-algebra, and if $\mathbb{B}(\mathbf{k})$ is discrete, then $\mathbb{B}(\mathbf{C})$ is discrete.*

4.5. Fact. *If $(\mathbf{k}, \mathbf{C}, G)$ is a pre-Galois algebra, every idempotent e of $\mathbf{C}$ fixed by G is an element of $\mathbf{k}$.*

D The characteristic polynomial $\mathrm{C}_G(e) = (T - e)^{|G|}$ belongs to $\mathbf{k}[T]$, so its constant coefficient, which is equal to $\pm e$, is in $\mathbf{k}$. □

4.6. Fact. *Let $(\mathbf{k}, \mathbf{C}, G)$ be a pre-Galois algebra with $\mathbf{k}$ connected and nontrivial, then*

1. *0 and 1 are the only idempotents of $\mathbf{C}$ fixed by G,*
2. *$\mathbb{B}(\mathbf{C})$ is discrete,*
3. *every atom of $\mathbb{B}(\mathbf{C})$ is a Galoisian idempotent,*
4. *two atoms are conjugated under G,*
5. *an idempotent $e \neq 0$ is Galoisian if and only if its orbit under G is formed of pairwise orthogonal elements,*
6. *if f is an idempotent $\neq 0$, the ideal $\langle 1 - f\rangle$ is Galoisian if and only if its orbit under G is formed of pairwise comaximal ideals.*

D Items *1* and *2* clearly result from Facts *4.5* and *4.4*.

3. If e is an atom, so is $\sigma(e)$, therefore $\sigma(e) = e$ or $e\sigma(e) = 0$. Thus two elements of the orbit of e are orthogonal, so the sum of the orbit of e is a nonzero idempotent fixed by G; it is equal to 1.

4. If e' is another atom, it is equal to the sum of the $e'e_i$'s, where e_i ranges over the orbit of e, and since the e_i's are atoms, each e_ie' is zero or equal to e_i.

5. See Fact 3.8.

6. Stems from *5* since $\langle 1 - f, 1 - f'\rangle = \langle 1 - ff'\rangle$ for idempotents f and f'.□

Theorem 3.3 implies that the Boolean algebra $\mathbb{B}(\mathbf{C})$ is finite if and only if the indecomposable idempotents form a finite set (they are necessarily pairwise orthogonal) and if they generate $\mathbb{B}(\mathbf{C})$.

Comment. A set X is said to be *bounded* if we know an integer k which is an upper bound of the number of elements in X, i.e. more precisely, if for every finite family $(b_i)_{i\in[\![0..k]\!]}$ in X, we have $b_i = b_j$ for two distinct indices. In classical mathematics this implies that the set is finite, but from a constructive point of view many distinct situations can occur.
A common situation is that of a bounded and discrete Boolean algebra C for which we do not know of an atom with certainty. The finitely generated ideals of C, all principal, are identified with elements of C, so C is identified with its own Zariski lattice $\mathsf{Zar}\, C$.[3] Moreover, in classical mathematics the atoms are in bijection with the prime ideals (all maximal) of C via $e \mapsto \langle 1 - e\rangle$. Thus the set of atoms of C (supposed bounded) is identified with $\mathsf{Spec}\, C$. We therefore once again find in this special case the following general fact: the Zariski lattice is the constructive, practical and "point-free" version of the Zariski spectrum, a topological space whose points can turn

[3] For a commutative ring $\mathbf{k}$, $\mathsf{Zar}\,\mathbf{k}$ is the set of radicals of finitely generated ideals of $\mathbf{k}$ (Section XI-4). It is a distributive lattice. In classical mathematics, $\mathsf{Zar}\,\mathbf{k}$ is identified with the lattice of quasi-compact open sets of the spectral space $\mathsf{Spec}\,\mathbf{k}$ (Section XIII-1).

out to be inaccessible from a constructive point of view. But this situation, although familiar, is perhaps more troubling in the case of a discrete and bounded topological space. This is typically a compact space for which we do not have a good description via a dense countable subset, therefore which is not included in the context of compact metric spaces à la Bishop (cf. [Bishop, Bishop & Bridges]). ■

Here is a corollary of the Galois structure theorem (Theorem 3.10) in the context of pre-Galois algebras.

4.7. Proposition. *Let* $(\mathbf{k}, \mathbf{C}, G)$ *be a pre-Galois algebra with* $\mathbf{k}$ *connected. For an idempotent* h *of* $\mathbf{C}$ *the following properties are equivalent.*

1. *h is a Galoisian idempotent.*
2. *$\mathbf{C}[1/h]$ is a projective $\mathbf{k}$-module of rank equal to $\mathrm{St}_G(h)$.*
3. *$\mathbf{C}[1/h]$ is a projective $\mathbf{k}$-module of rank less than or equal to $\mathrm{St}_G(h)$.*

D We use Theorem 3.10. By item *2* of this theorem we can assume that there exists a Galoisian idempotent e such that h is equal to a sum $e_1 + \cdots + e_r$ of elements of the orbit $G.e$. We have isomorphisms of $\mathbf{k}$-modules $e\mathbf{C} \simeq \mathbf{C}[1/e]$ and $\mathbf{C} \simeq (e\mathbf{C})^{|G.e|}$, so $e\mathbf{C}$ is projective of constant rank $|\, G : G.e \,| = |\mathrm{St}_G(e)|$. We deduce that the $\mathbf{k}$-module

$$\mathbf{C}[1/h] \simeq h\mathbf{C} = e_1\mathbf{C} \oplus \cdots \oplus e_r\mathbf{C} \simeq (e\mathbf{C})^r$$

is projective of rank $r \times |\mathrm{St}_G(e)|$. We then apply item *5* of Theorem 3.10 with $f = h$.
Therefore, here item *2* (resp. item *3*) means the same thing as item *5c* (resp. item *5d*) in Theorem 3.10. □

Discriminant

Recall that in $\mathbf{A} = \mathrm{Adu}_{\mathbf{k},f}$ we have $\mathrm{disc}(f) = \prod_{1 \leqslant i < j \leqslant n}(x_i - x_j)^2$ and $\mathrm{Disc}_{\mathbf{A}/\mathbf{k}} = \mathrm{disc}(f)^{n!/2}$.

In the following theorem, we speak of the $\mathbf{A}$-module of differentials $\Omega_{\mathbf{A}/\mathbf{k}}$ of the $\mathbf{k}$-algebra $\mathbf{A}$. It actually suffices to know that the module of differentials of a finitely presented algebra is isomorphic to the cokernel of the transpose of the Jacobian matrix of the polynomial system that defined the algebra. For more details on this subject see Theorems VI-6.6 and VI-6.7.

4.8. Theorem. *Let J be the Jacobian of the system of n equations with n unknowns defining the universal splitting algebra $\mathbf{A} = \mathrm{Adu}_{\mathbf{k},f}$.*

1. a. *We have $J = \prod_{1 \leqslant i < j \leqslant n}(x_i - x_j)$ in $\mathbf{A}$.*
   b. *We have $J^2 = \mathrm{disc}(f) \in \mathbf{k}$.*
2. *In particular, the following properties are equivalent.*

a. $\mathrm{Disc}_{\mathbf{A}/\mathbf{k}}$ *is invertible (resp. regular) in* $\mathbf{k}$*.*

b. $\mathrm{disc}(f)$ *is invertible (resp. regular) in* $\mathbf{k}$*.*

c. J *is invertible (resp. regular) in* $\mathbf{A}$*.*

d. The $x_i - x_j$*'s are invertible (resp. regular) in* $\mathbf{A}$*.*

e. $x_1 - x_2$ *is invertible (resp. regular) in* $\mathbf{A}$*.*

f. $\Omega_{\mathbf{A}/\mathbf{k}} = 0$ *(resp.* $\Omega_{\mathbf{A}/\mathbf{k}}$ *is a "torsion"* $\mathbf{A}$*-module, i.e. annihilated by a regular element).*

g. S_n *is a separating group for* $\mathbf{A}$ *(resp. for* $\mathrm{Adu}_{\mathrm{Frac}(\mathbf{k}),f}$*).*

3. The analogous equivalences are valid for every Galois quotient of the universal splitting algebra.

D Item *1a* is easy by induction on n, with the exact sign if we consider the system which we used in the definition of the universal splitting algebra. For example, here is the computation for $n = 4$

$$\begin{aligned}
J &= \begin{vmatrix} 1 & 1 & 1 & 1 \\ \sum_{i\neq 1} x_i & \sum_{i\neq 2} x_i & \sum_{i\neq 3} x_i & \sum_{i\neq 4} x_i \\ \sum_{i,j\neq 1} x_i x_j & \sum_{i,j\neq 2} x_i x_j & \sum_{i,j\neq 3} x_i x_j & \sum_{i,j\neq 4} x_i x_j \\ x_2x_3x_4 & x_1x_3x_4 & x_1x_2x_4 & x_1x_2x_3 \end{vmatrix} \\
&= \begin{vmatrix} 1 & 0 & 0 & 0 \\ \sum_{i\neq 1} x_i & x_1 - x_2 & x_1 - x_3 & x_1 - x_4 \\ \displaystyle\sum_{i,j\neq 1} x_i x_j & (x_1 - x_2)\displaystyle\sum_{i\neq 1,2} x_i & (x_1 - x_3)\displaystyle\sum_{i\neq 1,3} x_i & (x_1 - x_4)\displaystyle\sum_{i\neq 1,4} x_i \\ x_2x_3x_4 & (x_1 - x_2)x_3x_4 & (x_1 - x_3)x_2x_4 & (x_1 - x_4)x_2x_3 \end{vmatrix} \\
&= (x_1 - x_2)(x_1 - x_3)(x_1 - x_4) \begin{vmatrix} 1 & 1 & 1 \\ x_3 + x_4 & x_2 + x_4 & x_2 + x_3 \\ x_3x_4 & x_2x_4 & x_2x_3 \end{vmatrix}
\end{aligned}$$

etc...

We deduce from it item *1b*, then the equivalence of items *2a* through *2e*.

2f. Since $\Omega_{\mathbf{A}/\mathbf{k}}$ is an $\mathbf{A}$-module isomorphic to the cokernel of the transpose of the Jacobian matrix, we obtain that $\mathrm{Ann}(\Omega_{\mathbf{A}/\mathbf{k}})$ and $J\mathbf{A}$ have the same nilradical (Lemma IV-9.6). Finally, the element J is regular (resp. invertible) if and only if the ideal $\sqrt{J\mathbf{A}}$ contains a regular element (resp. contains 1).

2g. Suppose that f is separable (resp. regular), if $\sigma \in \mathrm{S}_n$ is distinct from $\mathrm{Id}_{\mathbf{A}}$, there is some $i \in [\![1..n]\!]$ such that $x_{\sigma i} \neq x_i$. Since $x_{\sigma i} - x_i$ is invertible (resp. regular), σ is separating (resp. separating once we invert the discriminant). For the converse, consider for example the transposition σ that swaps 1 and 2. We clearly have $\langle g - \sigma(g) | g \in \mathbf{A} \rangle = \langle x_1 - x_2 \rangle$. The result follows.

3. Clear since the universal splitting algebra is always isomorphic to a power of any of its Galois quotients. □

Fixed points

Let $\mathrm{di}(f) = \prod_{i<j\in[\![1..n]\!]}(x_i + x_j) \in \mathbf{k}$.

It is clear that $\mathrm{di}(f)$ is congruent to $\prod_{i<j\in[\![1..n]\!]}(x_i - x_j)$ modulo 2, which gives $\left\langle 2, \mathrm{di}(f)^2\right\rangle = \langle 2, \mathrm{disc}(f)\rangle$.

4.9. Theorem. (Universal splitting algebra and fixed points)
Let $\mathfrak{a} := \mathrm{Ann}_{\mathbf{k}}\big(\langle 2, \mathrm{di}(f)\rangle\big)$. *Then* $\mathrm{Fix}(\mathrm{S}_n) \subseteq \mathbf{k} + \mathfrak{a}\mathbf{A}$. *In particular, if* $\mathfrak{a} = 0$ *and a fortiori if* $\mathrm{Ann}_{\mathbf{k}}\big(\langle 2, \mathrm{disc}(f)\rangle\big) = 0$*, we obtain* $\mathrm{Fix}(\mathrm{S}_n) = \mathbf{k}$.

D It suffices to prove the first assertion.
Let us consider the case where $n = 2$ with $f(T) = T^2 - s_1T + s_2$.
An element $z = c + dx_1 \in \mathbf{A}$ (with c, $d \in \mathbf{k}$) is invariant under S_2 if and only if $d(x_1 - x_2) = d(s_1 - 2x_1) = 0$, or yet again if $ds_1 = 2d = 0$, but we have $\mathrm{di}(f) = s_1$.
We then proceed by induction on n. For the Cauchy modules we use the notations of Section III-4. For $n > 2$ consider the ring $\mathbf{k}_1 = \mathbf{k}[x_1] \simeq \mathbf{k}[X_1]/\langle f(X_1)\rangle$ and the polynomial $g_2(T) = f_2(x_1, T)$ which is in $\mathbf{k}_1[T]$. We identify $\mathrm{Adu}_{\mathbf{k}_1,g_2}$ with $\mathrm{Adu}_{\mathbf{k},f}$ (Fact III-4.3). To switch from the expression of an element $y \in \mathbf{A}$ over the basis $\mathcal{B}(g_2)$ ($\mathbf{A}$ seen as a $\mathbf{k}_1$-module) to its expression over the basis $\mathcal{B}(f)$ ($\mathbf{A}$ seen as a $\mathbf{k}$-module), it suffices to express each coordinate, which is an element of $\mathbf{k}_1$, over the $\mathbf{k}$-basis $(1, x_1, \ldots, x_1^{n-1})$ of $\mathbf{k}_1$. Let us also take note that $\mathrm{di}(f) = (-1)^{n-1}g_2(-x_1)\,\mathrm{di}(g_2)$ by a direct computation. Therefore, if we let $\mathfrak{a}_1 = \mathrm{Ann}_{\mathbf{k}_1}(\langle 2, \mathrm{di}(g_2)\rangle)$, we obtain $\mathfrak{a}_1\mathbf{A} \subseteq \mathfrak{a}\mathbf{A}$ and $\mathfrak{a}_1 \subseteq \mathfrak{a}\mathbf{k}_1$.
Let us move on to the actual induction.
Let $y \in \mathbf{A}$ be a fixed point of S_n, and consider it as being an element of the universal splitting algebra $\mathrm{Adu}_{\mathbf{k}_1,g_2}$. Since y is invariant under S_{n-1}, we have $y \in \mathbf{k}_1 + \mathfrak{a}_1\mathbf{A}$, and so $y \equiv h(x_1) \bmod \mathfrak{a}_1\mathbf{A}$ for some $h \in \mathbf{k}[X]$. A fortiori $y \equiv h(x_1) \bmod \mathfrak{a}\mathbf{A}$. It remains to see that $h(x_1) \in \mathbf{k} + \mathfrak{a}\mathbf{A}$. Since y is invariant under S_n, by permuting x_1 and x_2 we obtain the congruence

$$h(x_1) \equiv y \equiv h(x_2) \mod \mathfrak{a}\mathbf{A} \qquad (*)$$

Let $h = \sum_{i=0}^{n-1} + c_iX^i \in \mathbf{k}[X]$. Note that $h(x_1)$ is a reduced expression over the canonical basis $\mathcal{B}(f)$. Regarding $h(x_2)$, to obtain the reduced expression, we must, in the term $c_{n-1}x_2^{n-1}$, replace x_2^{n-1} with its expression over the canonical basis, which results from $f_2(x_1, x_2) = 0$.
This rewriting sparks the apparition of the term $-c_{n-1}x_1^{n-2}x_2$, and this implies by $(*)$ that $c_{n-1} \in \mathfrak{a}$. But then, $h(x_2) - c_{n-1}x_2^{n-1}$ and $h(x_1) - c_{n-1}x_1^{n-1}$ are reduced expressions of two elements equal modulo $\mathfrak{a}\mathbf{A}$. Therefore, the c_i's for $i \in [\![1..n-2]\!]$ are in $\mathfrak{a}$, and we saw that $c_{n-1} \in \mathfrak{a}$. □

Remark. In the $n = 2$ case, the above study shows that as soon as $\mathfrak{a} \neq 0$ the ring $\mathrm{Fix}(\mathrm{S}_2) = \mathbf{k} \oplus \mathfrak{a}\,x_1 = \mathbf{k} + \mathfrak{a}\mathbf{A}$ strictly contains $\mathbf{k}$.

A computation in the $n = 3$ case gives the same converse: if $\mathfrak{a} \neq 0$, the ring $\mathrm{Fix}(\mathrm{S}_3)$ strictly contains $\mathbf{k}$. We indeed find an element

$$v = x_1^2 x_2 + s_1 x_1^2 + (s_1^2 + s_2)x_1 + s_2 x_2 \neq 0$$

(one of its coordinates over $\mathcal{B}(f)$ is equal to 1) such that $\mathrm{Fix}(\mathrm{S}_3) = \mathbf{k} \oplus \mathfrak{a}\, v$. However, for $n \geqslant 4$, the situation becomes complicated. ■

We obtain as a corollary the following theorem.

4.10. Theorem. *If f is a separable polynomial of $\mathbf{k}[T]$, the universal splitting algebra $\mathrm{Adu}_{\mathbf{k},f}$, as well as every Galois quotient, is a Galois algebra.*

D By the structure theorem 4.3 (item *7*) it suffices to show that $\mathrm{Adu}_{\mathbf{k},f}$ is Galoisian. However, we have just proven the fixed point condition, and the separating automorphisms condition is given in Theorem 4.8. □

By Artin's theorem VI-7.11, and in light of the previous theorem, we know that every universal splitting algebra for a separable polynomial, or every Galois quotient of such a $\mathbf{k}$-algebra, diagonalizes itself. We examine this question in further detail in the following subsection. Even with regard to the precise result that we have just mentioned, it is interesting to see things work "concretely" for a universal splitting algebra.

Separability

When the polynomial $f \in \mathbf{k}[T]$ is separable, its universal splitting algebra $\mathbf{A} = \mathrm{Adu}_{\mathbf{k},f} = \mathbf{k}[x_1, \dots, x_n]$ is strictly étale, by Fact III-5.11. The following theorem then simply recalls Theorem VI-5.8 regarding strictly étale algebras in the current context.

4.11. Theorem. *Suppose f is separable.*

1. *The nilradical $\mathrm{D}_{\mathbf{A}}(0)$ is the ideal generated by $\mathrm{D}_{\mathbf{k}}(0)$. In particular, if $\mathbf{k}$ is reduced, so is $\mathbf{A}$.*
2. *For every reduced algebra $\mathbf{k} \xrightarrow{\rho} \mathbf{k}'$, the algebra $\rho_\star(\mathbf{A}) \simeq \mathrm{Adu}_{\mathbf{k}',\rho(f)}$ is reduced.*

Diagonalization of a universal splitting algebra

4.12. Theorem. (Diagonalization of a universal splitting algebra)
Let $\varphi : \mathbf{k} \to \mathbf{C}$ be an algebra in which f can be completely factorized, *i.e. $\varphi(f) = \prod_{i=1}^n (T - u_i)$. Also suppose that f is separable over $\mathbf{C}$, i.e. the $u_i - u_j$'s are invertible for $i \neq j$.*
Let $\mathbf{C} \otimes_{\mathbf{k}} \mathbf{A} \simeq \mathrm{Adu}_{\mathbf{C},\varphi(f)}$, and, for $\sigma \in \mathrm{S}_n$, let $\phi_\sigma : \mathbf{C} \otimes_{\mathbf{k}} \mathbf{A} \to \mathbf{C}$ be the unique homomorphism of $\mathbf{C}$-algebras which sends each $1_{\mathbf{C}} \otimes x_i$ to $u_{\sigma i}$.
Let $\Phi : \mathbf{C} \otimes_{\mathbf{k}} \mathbf{A} \to \mathbf{C}^{n!}$ be the $\mathbf{C}$-homomorphism defined by $y \mapsto \big(\phi_\sigma(y)\big)_{\sigma \in \mathrm{S}_n}$.

1. *Φ is an isomorphism: $\mathbf{C}$ diagonalizes $\mathbf{A}$.*

2. *More precisely, in* $\mathbf{C} \otimes_{\mathbf{k}} \mathbf{A}$*, write* x_i *instead of* $1_{\mathbf{C}} \otimes x_i$*,* u_i *instead of* $u_i \otimes 1_{\mathbf{A}}$ *(in accordance with the* $\mathbf{C}$*-algebra structure of* $\mathbf{C} \otimes_{\mathbf{k}} \mathbf{A}$*) and let* $g_\sigma = \prod_{j \neq \sigma i}(x_i - u_j)$*. Then,*
$$\phi_\sigma(g_\sigma) = \pm\varphi\big(\operatorname{disc}(f)\big) = \pm \operatorname{disc}\big(\varphi(f)\big),$$
and $\phi_\sigma(g_\tau) = 0$ *for* $\tau \neq \sigma$*, so that if we let* $e_\sigma = g_\sigma/\phi_\sigma(g_\sigma)$*, the* e_σ*'s form the fundamental system of orthogonal idempotents corresponding to the isomorphism* Φ*.*
3. *Moreover,* $x_i e_\sigma = u_{\sigma i} e_\sigma$*, so that the basis* (e_σ) *of the* $\mathbf{C}$*-module* $\mathbf{C} \otimes_{\mathbf{k}} \mathbf{A}$ *is a common diagonal basis for the multiplications by the* x_i*'s.*

In particular, when f *is separable, the enveloping algebra*
$$\mathbf{A}^{\mathrm{e}}_{\mathbf{k}} = \mathbf{A} \otimes_{\mathbf{k}} \mathbf{A} \simeq \operatorname{Adu}_{\mathbf{A},f}$$
is canonically isomorphic to $\mathbf{A}^{n!}$*;* $\mathbf{A}$ *diagonalizes itself.*

NB: We will however be careful when letting $\operatorname{Adu}_{\mathbf{A},f} = \mathbf{A}[u_1, \dots, u_n]$ since the x_i's are already taken as elements of $\mathbf{A}$.

D *1.* The two algebras are, as $\mathbf{C}$-modules, isomorphic to $\mathbf{C}^{n!}$ and Φ is a $\mathbf{C}$-linear map whose surjectivity is all that we need to prove. The surjectivity results by the Chinese remainder theorem from the $\operatorname{Ker}\phi_\sigma$'s being pairwise comaximal: $\operatorname{Ker}\phi_\sigma$ contains $x_i - u_{\sigma i}$, $\operatorname{Ker}\phi_\tau$ contains $x_i - u_{\tau i}$, therefore $\operatorname{Ker}\phi_\sigma + \operatorname{Ker}\phi_\tau$ contains the $u_{\sigma i} - u_{\tau i}$'s, and there is at least one index i for which $\sigma i \neq \tau i$, which shows that $u_{\sigma i} - u_{\tau i}$ is invertible.

2. The fundamental system of orthogonal idempotents corresponding to the isomorphism Φ is the unique solution of the system of linear equations $\phi_\sigma(e_\tau) = \delta_{\sigma,\tau}$ (where δ is the Kronecker symbol).
However, the equalities $\phi_\sigma(g_\sigma) = \pm\varphi\big(\operatorname{disc}(f)\big)$ and $\phi_\sigma(g_\tau) = 0$ are easy.

3. Fix i. The equality $x_i g_\sigma = u_{\sigma i} g_\sigma$ results from the fact that in g_σ there is already a product of the $x_i - u_j$'s for $j \neq \sigma i$, so $(x_i - u_{\sigma i})g_\sigma$ is a multiple of $\varphi(f)(x_i)$, which is null. □

Remark. Actually, generally speaking, Φ is a linear map whose determinant can be computed with respect to the natural bases: the square of this determinant is a power of $\varphi\big(\operatorname{disc}(f)\big)$ and we therefore find that Φ is an isomorphism if and only if $\varphi\big(\operatorname{disc}(f)\big)$ is invertible in $\mathbf{C}$. For this, and for a "complete converse," see Exercise 6. ■

The previous theorem implies the following result: if $\mathbf{A}$ is a universal splitting algebra for a separable polynomial, then every $\mathbf{A}$-algebra diagonalizes $\mathbf{A}$. We now give a generalization of this result for a Galois quotient of $\mathbf{A}$.

4.13. Theorem. (Diagonalization of a Galois quotient of a universal splitting algebra) *Let e be a Galoisian idempotent of* $\mathbf{A}$*,*

$$\mathbf{B} = \mathbf{A}/\langle 1-e\rangle = \mathbf{k}[y_1, \ldots, y_n] \ \ \textit{and} \ \ G = \mathrm{St}_{\mathrm{S}_n}(e),$$

(we have denoted by $y_i = \pi(x_i)$ the class of x_i in $\mathbf{B}$*). Let $\phi : \mathbf{B} \to \mathbf{C}$ be a ring homomorphism. Let $u_i = \phi(y_i)$. Consider the* $\mathbf{C}$*-algebra*

$$\phi_\star(\mathbf{B}) \simeq \mathbf{C} \otimes_{\mathbf{k}} \mathbf{B} \simeq \mathrm{Adu}_{\mathbf{C},f}/\langle 1-\phi(e)\rangle$$

obtained from the $\mathbf{k}$*-algebra* $\mathbf{B}$ *by scalar extension. For $\sigma \in G$ let ϕ_σ : $\mathbf{C} \otimes_{\mathbf{k}} \mathbf{B} \to \mathbf{C}$ be the unique homomorphism of* $\mathbf{C}$*-algebras which sends each $1_{\mathbf{C}} \otimes y_i$ to $u_{\sigma i}$. Let $\Phi : \mathbf{C} \otimes_{\mathbf{k}} \mathbf{B} \to \mathbf{C}^{|G|}$ be the homomorphism of* $\mathbf{C}$*-algebras defined by $z \mapsto \big(\phi_\sigma(z)\big)_{\sigma \in G}$.*

1. *If $\phi\big(\mathrm{disc}(f)\big) \in \mathbf{C}^\times$, Φ is an isomorphism, so* $\mathbf{C}$ *diagonalizes* $\mathbf{B}$*.*
2. *In particular, if f is separable, $\mathbf{B} \otimes_{\mathbf{k}} \mathbf{B}$ is canonically isomorphic to $\mathbf{B}^{|G|}$, i.e.* $\mathbf{B}$ *diagonalizes itself.*

D The two $\mathbf{C}$-algebras are projective $\mathbf{C}$-modules of constant rank $|G|$ and Φ is a $\mathbf{C}$-linear map whose surjectivity is all that we need to prove. In $\mathbf{C} \otimes_{\mathbf{k}} \mathbf{B}$ we write y_i instead of $1_{\mathbf{C}} \otimes y_i$ and u_i instead of $u_i \otimes 1_{\mathbf{B}}$. The surjectivity results by the Chinese remainder theorem from the fact that the $\mathrm{Ker}\,\phi_\sigma$'s are pairwise comaximal: $\mathrm{Ker}\,\phi_\sigma$ contains $y_i - u_{\sigma i}$, $\mathrm{Ker}\,\phi_\tau$ contains $y_i - u_{\tau i}$, so $\mathrm{Ker}\,\phi_\sigma + \mathrm{Ker}\,\phi_\tau$ contains the $u_{\sigma i} - u_{\tau i}$. However, there is at least one index i for which $\sigma i \neq \tau i$ and $u_{\sigma i} - u_{\tau i}$ is invertible because $\phi\big(\mathrm{disc}(f)\big)$ is the product of the $(u_j - u_k)^2$'s for $1 \leqslant j < k \leqslant n$. □

Triangular structure of Galoisian ideals

In this subsection we prove Theorem 4.15 which implies that the structure of the ideal $\mathcal{J}(f)$, which is a "triangular" structure (in the Lazard sense) when we consider the Cauchy modules as generators, remains a triangular structure for all the Galoisian ideals of the universal splitting algebra in the case of a separable polynomial over a discrete field.

4.14. Lemma. *Let* $\mathbf{k}'$ *be a* $\mathbf{k}$*-algebra which is a finitely generated projective module of constant rank m, $x \in \mathbf{k}'$ and $r(T) \in \mathbf{k}[T]$ be the characteristic polynomial of x over* $\mathbf{k}$*. If $\mathrm{disc}(r) \in \mathbf{k}^\times$, then $\mathbf{k}' = \mathbf{k}[x]$ and $(1, x, \ldots, x^{m-1})$ is a* $\mathbf{k}$*-basis of* $\mathbf{k}'$*.*

D The case where $\mathbf{k}'$ is free of rank m has been proven in III-5.10. In the general case, consider a system of comaximal elements of $\mathbf{k}$ such that each localization makes of $\mathbf{k}'$ a free $\mathbf{k}$-module of rank m. □

4.15. Theorem. *Let* $(\mathbf{k}, \mathbf{C}, G)$ *be a Galois algebra with*

- $\mathbf{C} = \mathbf{k}[x_1, \ldots, x_n] \simeq \mathbf{k}[X_1, \ldots, X_n]/\mathfrak{a}$,
- G *operates on* $\{x_1, \ldots, x_n\}$ *and*
- *the* $x_i - x_j$*'s are invertible for* $i \neq j$.

A typical example of this situation: $\mathbf{C}$ *is a Galois quotient of the universal splitting algebra of a separable polynomial.*
Let

$$G_i = \left\{ \sigma \in G \mid \sigma(x_k) = x_k,\ k \in [\![1..i]\!] \right\} \text{ for } i \in [\![0..n]\!] \text{ (so } G_0 = G\text{)},$$
$$r_i(T) = \textstyle\prod_{\sigma \in G_{i-1}/G_i} \big(T - \sigma(x_i)\big) \quad \text{for } i \in [\![1..n]\!],$$

where G_{i-1}/G_i *designates a system of representatives of the left cosets. Let* $d_i = |\, G_{i-1} : G_i \,|$.
We then have the following results.

1. $\mathbf{k}[x_1, \ldots, x_i] = \mathrm{Fix}(G_i)$ *and* $G_i = \mathrm{Stp}(\mathbf{k}[x_1, \ldots, x_i])$.
2. *The polynomial* $r_i(T)$ *is monic with coefficients in* $\mathbf{k}[x_1, \ldots, x_{i-1}]$*, of degree* d_i*. Let* $R_i(X_1, \ldots, X_i) \in \mathbf{k}[X_1, \ldots, X_i]$ *be a monic polynomial in* X_i *of degree* d_i *such that* $R_i(x_1, \ldots, x_{i-1}, X_i) = r_i(X_i)$.
3. $\mathfrak{a}_i = \mathfrak{a} \cap \mathbf{k}[X_1, \ldots, X_i]$ *is generated by* $R_1(X_1)$, …, $R_i(X_1, \ldots, X_i)$.

Consequently each algebra $\mathbf{k}[x_1, \ldots, x_i]$ *is both a free* $\mathbf{k}[x_1, \ldots, x_{i-1}]$*-module of rank* d_i *and a free* $\mathbf{k}$*-module of rank* $|\, G : G_i \,|$ *at the same time, and each of the ideals* $\mathfrak{a}_i$ *is a triangular ideal (in the Lazard sense) of* $\mathbf{k}[X_1, \ldots, X_i]$.

D The group G_1 is a separating group of automorphisms of ring $\mathbf{C}$. Let $\mathbf{k}_1 = \mathbf{C}^{G_1}$. We know that $\mathbf{C}$ is a projective $\mathbf{k}_1$-module of constant rank $|G_1|$ and that $\mathbf{k}[x_1] \subseteq \mathbf{k}_1$. Moreover, $\mathbf{k}_1$ is a direct summand in $\mathbf{C}$, therefore it is a projective $\mathbf{k}$-module of constant rank $d_1 = \deg_T(r_1)$.
The ideal $\mathfrak{a}_1$ is formed by all the $R \in \mathbf{k}[X_1]$'s such that $R(x_1) = 0$.
Therefore, $R\big(\sigma(x_1)\big) = 0$ for every $\sigma \in G/G_1$. In other words R is a multiple of each $T - \sigma(x_1)$, and since the $x_i - x_j$'s are invertible, R is a multiple of r_1. Thus $\mathfrak{a}_1 = \langle r_1(X_1) \rangle$ and $\mathbf{k}[x_1] \simeq \mathbf{k}[X_1]/\langle r_1(X_1) \rangle$.
Proposition VI-7.17 gives us the equality

$$\mathrm{C}_{\mathbf{k}_1/\mathbf{k}}(x_1)(T) = \textstyle\prod_{\sigma \in G/G_1} \big(T - \sigma(x_1)\big) = r_1(T).$$

This implies that the characteristic polynomial $\mathrm{C}_{\mathbf{k}_1/\mathbf{k}}(x_1)(T)$ is separable, and Lemma 4.14 says that $(1, x_1, \ldots, x_1^{d_1-1})$ is a basis of $\mathbf{k}_1$.
Thus $\mathbf{k}[x_1] = \mathbf{k}_1 = \mathrm{Fix}(G_1)$ and $(\mathbf{k}[x_1], \mathbf{C}, G_1)$ is a Galois algebra.

Then, $\mathbf{C} = \mathbf{k}_1[x_2, \ldots, x_n]$ with G_1 operating on $\{x_2, \ldots, x_n\}$ and the $x_i - x_j$'s being invertible. The whole previous process works identically when replacing $\mathbf{k}$ by $\mathbf{k}_1$, G by G_1, x_1 by x_2 and G_1 by G_2. The result then follows by induction. □

5. Splitting field of a polynomial over a discrete field

In this section we give a constructive and dynamic approach to the splitting field of a monic polynomial over a discrete field, in the absence of a factorization algorithm of the polynomials.

In Section 5, $\mathbf{K}$ is a nontrivial discrete field,
f is a monic polynomial of degree n and
$\mathbf{A} = \mathrm{Adu}_{\mathbf{K},f} = \mathbf{K}[X_1, \ldots, X_n]/\mathcal{J}(f) = \mathbf{K}[x_1, \ldots, x_n]$.

The quotients of the universal splitting algebra $\mathbf{A}$ are finite $\mathbf{K}$-algebras, therefore they are zero-dimensional rings.

"Reduced" Galois quotients of the universal splitting algebra

We have placed quotation marks around "reduced" because, a priori, one does not speak of a Galois quotient *that is* reduced, but of a Galois quotient *that one* reduces (by killing the nilpotents).

Given Fact III-5.11, if the polynomial f is separable the universal splitting algebra is étale, therefore reduced, and every ideal generated by an idempotent is equal to its nilradical (since the quotient ring is reduced). We can then replace in the statements that follow each ideal $\mathrm{D}_{\mathbf{A}}(1-e) = \sqrt{\langle 1-e \rangle}$ with the ideal $\langle 1-e \rangle$.

In the following lemma we know by hypothesis that $\mathbf{B}$ is strictly finite over $\mathbf{K}$, but we do not necessarily know a basis of $\mathbf{B}_{\mathrm{red}}$ as a $\mathbf{K}$-vector space. The goal is then to give a "satisfying enough" description of $\mathbf{B}_{\mathrm{red}}$ as a quotient of the universal splitting algebra.

5.1. Lemma. *Let* $\mathbf{B}$ *be a strictly finite* $\mathbf{K}$*-algebra. Suppose that* f *can be entirely decomposed in* $\mathbf{B}_{\mathrm{red}}$ *and that* $\mathbf{B}_{\mathrm{red}}$ *is generated by the corresponding zeros of* f*. Then, there exists an idempotent* e *of* $\mathbf{A} = \mathrm{Adu}_{\mathbf{K},f}$ *such that* $\mathbf{B}_{\mathrm{red}} \simeq \mathbf{A}/\mathrm{D}_{\mathbf{A}}(1-e)$*.*

D Let $y_1, \ldots, y_n \in \mathbf{B}$ such that $f(T) = \prod_i (T - \overline{y_i})$ in $\mathbf{B}_{\mathrm{red}}$. There exists a unique homomorphism $\lambda : \mathbf{K}[X_1, \ldots, X_n] \to \mathbf{B}$ which sends the X_i's to the y_i's. Let $\mathfrak{b}$ be the (finitely generated) ideal of $\mathbf{B}$ generated by $\lambda\big(\mathcal{J}(f)\big)$. We then have $\mathfrak{b} \subseteq \mathrm{D}_{\mathbf{B}}(0)$, and $\mathbf{B}' := \mathbf{B}/\mathfrak{b}$ is a strictly finite $\mathbf{K}$-algebra satisfying $\mathbf{B}_{\mathrm{red}} \simeq \mathbf{B}'_{\mathrm{red}}$. We thus obtain a diagram

$$\begin{tikzcd}
\mathbf{K}[\underline{X}] \arrow[r, two heads] \arrow[d, "\lambda"'] & \mathbf{A} \arrow[d, "\varphi"] \arrow[dr, two heads, "\psi"] & \\
\mathbf{B} \arrow[r] & \mathbf{B}' \arrow[r] & \mathbf{B}'_{\mathrm{red}} = \mathbf{B}_{\mathrm{red}}
\end{tikzcd}$$

in which φ is the unique homomorphism which sends x_i to the class of y_i. Since $\mathbf{B}'$ is strictly finite, $\operatorname{Ker}\varphi$ is a finitely generated ideal of $\mathbf{A}$, and there exists a $d \geqslant 0$ such that $(\operatorname{Ker}\varphi)^d = (\operatorname{Ker}\varphi)^{d+1}$ therefore $(\operatorname{Ker}\varphi)^d$ is generated by an idempotent $1-e$. The result follows because on the one hand, ψ is surjective, and on the other, $\operatorname{Ker}\psi = \mathrm{D}_{\mathbf{A}}(\operatorname{Ker}\varphi) = \mathrm{D}_{\mathbf{A}}\big((\operatorname{Ker}\varphi)^d\big) = \mathrm{D}_{\mathbf{A}}(1-e)$. □

Remark. Note that ψ is surjective, but a priori $\operatorname{Ker}\psi$ is not a finitely generated ideal of $\mathbf{A}$. Symmetrically, a priori φ is not surjective, but $\operatorname{Ker}\varphi$ is a finitely generated ideal of $\mathbf{A}$. ■

In classical mathematics a splitting field (Definition III-6.6) for a monic polynomial f over a discrete field $\mathbf{K}$ is obtained as a quotient of the universal splitting algebra $\mathbf{A}$ by a maximal ideal. Such an ideal exists: take a strict ideal that is a $\mathbf{K}$-vector space of maximal dimension, by **LEM**.

In constructive mathematics we obtain the following more precise theorem (to be compared with Theorem III-6.7).

5.2. Theorem.

1. *The following properties are equivalent.*
   a. *There exists in* $\mathbf{A} = \mathrm{Adu}_{\mathbf{K},f}$ *an indecomposable idempotent* e.
   b. *There exists an extension* $\mathbf{L}$ *of* $\mathbf{K}$ *that is a splitting field of* f *and denoted by* $\mathbf{B}_{\mathrm{red}}$ *where* $\mathbf{B}$ *is a strictly finite* $\mathbf{K}$*-algebra.*
   c. *The Boolean algebra* $\mathbb{B}(\mathbf{A})$ *is finite.*
2. *In this case every splitting field of* f *is isomorphic to* $\mathbf{A}/\mathrm{D}_{\mathbf{A}}(1-e)$, *and it is discrete.*

D The equivalence of *1a* and *1c* is valid in the general context of Boolean algebras (Theorem 3.10). It is clear that *1a* implies *1b*. Conversely if we have a splitting field $\mathbf{L} = \mathbf{B}/\mathrm{D}_{\mathbf{B}}(0)$, where $\mathbf{B}$ is a strictly finite $\mathbf{K}$-algebra, Lemma 5.1 provides an idempotent e, and it is indecomposable because $\mathbf{L}$ is connected.

Let us look at item *2*. Let $\mathbf{M}$ be a splitting field for f. Write

$$f(T) = \textstyle\prod_{i=1}^n (T - \xi_i) \text{ in } \mathbf{M}.$$

By the universal property of $\mathrm{Adu}_{\mathbf{K},f}$, there exists a unique homomorphism of $\mathbf{K}$-algebras $\varphi : \mathbf{A} \to \mathbf{M}$ such that $\varphi(x_i) = \xi_i$ for $i \in [\![1..n]\!]$. Let $(e_\ell)_{\ell=1,\dots,k}$ be the orbit of e. It is a fundamental system of orthogonal idempotents, so $\big(\varphi(e_\ell)\big)_{\ell=1,\dots,k}$ also, and since $\mathbf{M}$ is a discrete field this implies that there is some j for which $\varphi(e_\ell) = \delta_{j,\ell}$ (Kronecker symbol).

Then, $\langle 1 - e_j\rangle \subseteq \operatorname{Ker}\varphi$, so $\mathbf{M}$ is a quotient of $\mathbf{A}/\mathrm{D}_{\mathbf{A}}(1-e_j)$, which is a discrete field. As $\mathbf{M}$ is nontrivial, this implies $\mathbf{M} \simeq \mathbf{A}/\mathrm{D}_{\mathbf{A}}(1-e_j)$. Finally, all the $\mathbf{A}/\mathrm{D}_{\mathbf{A}}(1-e_\ell)$ are pairwise isomorphic. □

Comment. In [MRR], it is shown that every enumerable discrete field possesses an algebraic closure. However, a splitting field for f, which therefore exists, does not necessarily possess a finite basis as a $\mathbf{K}$-vector space, in the constructive mathematics sense, and we do not know of a constructive uniqueness theorem for such a splitting field. We can describe as follows an analogous procedure to that of [MRR] to obtain a splitting field for f. First of all we construct an enumeration $(z_m)_{m\in\mathbb{N}}$ of the universal splitting algebra. Next we construct a sequence of finitely generated ideals $(\mathfrak{a}_m)$ of $\mathbf{A}$ by letting $\mathfrak{a}_0 = 0$, and $\mathfrak{a}_{m+1} = \mathfrak{a}_m + \langle z_m\rangle$ if $\mathfrak{a}_m + \langle z_m\rangle \neq \langle 1\rangle$, and $\mathfrak{a}_{m+1} = \mathfrak{a}_m$ otherwise (the test works because we can compute a basis for the $\mathbf{K}$-vector space $\mathfrak{a}_m + \langle z_m\rangle$). Then, the ideal $\bigcup_m \mathfrak{a}_m$ is a maximal ideal of $\mathbf{A}$, and the quotient is a splitting field, which is discrete. Our point of view is slightly different. We do not a priori start from an enumerable field, and even in the case of an enumerable field, we do not favor one enumeration over another. We would rather answer questions about the splitting field as they arise, as we shall see in the following theorem. ■

The following theorem explains how to bypass the difficulty of the nonexistence of the splitting field in constructive mathematics. The splitting field of f is replaced by an "approximation" given in the form of a reduced quotient $(\mathbf{A}/\langle 1-e\rangle)_{\mathrm{red}}$ of the universal splitting algebra, where e is a Galoisian idempotent.

We rely on the following fact which is already established in the general context of zero-dimensional rings (Lemma IV-8.2). We recall a direct proof.

For all $y \in \mathbf{A} = \mathrm{Adu}_{\mathbf{K},f}$, there exists an idempotent $e_y \in \mathbf{K}[y] \subseteq \mathbf{A}$ such that y is invertible modulo $1-e_y$ and nilpotent modulo e_y.

D Let $P(T)$ be the minimal polynomial of y. There exists an invertible element v of $\mathbf{K}$ such that $vP(T) = T^k\big(1-TR(T)\big)$ with $k \geqslant 0$. The idempotent e_y is $\big(yR(y)\big)^k$. □

5.3. Theorem. (Dynamic management of a splitting field)
Let $(z_i)_{i\in I}$ be a finite family of elements of $\mathrm{Adu}_{\mathbf{K},f} = \mathbf{A}$. There exists a Galoisian idempotent e of $\mathbf{A}$ such that by letting $\mathbf{B} = \mathbf{A}/\langle 1-e\rangle$ each $\pi(z_i)$ is null or invertible in the quotient algebra $\mathbf{B}_{\mathrm{red}}$ (here, $\pi : \mathbf{A} \to \mathbf{B}_{\mathrm{red}}$ is the canonical projection).

D For each $i \in I$ there is an idempotent $g_i \in \mathbf{A}$ such that z_i is invertible modulo $1-g_i$ and nilpotent modulo g_i. Applied to the family of the g_i's Theorem 3.10 gives a Galoisian idempotent e, such that for each i, $1-e$ divides g_i or $1-g_i$. Therefore, in the quotient algebra $\mathbf{B} = \mathbf{A}/\langle 1-e\rangle$ each $\pi(z_i)$ is nilpotent or invertible. □

Remarks. 1) The reader may worry that we do not a priori have a finite generator set of the ideal $\mathrm{D}_{\mathbf{A}}(1-e)$ available. Consequently the finite algebra $\mathbf{B}_{\mathrm{red}}$ is not necessarily a finite dimensional $\mathbf{K}$-vector space in the constructive sense. Actually the nilpotents can also be managed dynamically. We have in $\mathbf{B} = \mathbf{A}/\langle 1-e\rangle$ a test of nilpotence and if a nilpotent element x is revealed, we can replace $\mathbf{B}$ with its quotient by the ideal $\mathfrak{a}$ generated by the orbit of x under the action of $G = \mathrm{St}_{\mathrm{S}_n}(e)$. Then, $\mathbf{B}/\mathfrak{a}$ is finite dimensional and G operates on $\mathbf{B}/\mathfrak{a}$.

2) In Theorem 5.3 it can be in our best interest to saturate the family $(z_i)_{i\in I}$ by the action of S_n in order to make manifest in $\mathbf{B}$ all the possible "scenarios." ■

Uniqueness of the splitting field

The uniqueness theorem of the splitting field admits an "operative" constructive version (which always works, even if we do not dispose of an indecomposable idempotent in the universal splitting algebra) in the following form.

5.4. Theorem. (Uniqueness of the splitting field, dynamic version)
Let $\mathbf{B}_1$, $\mathbf{B}_2$ be two nonzero strictly finite $\mathbf{K}$-algebras for which the polynomial f can be decomposed into a product of linear factors in $(\mathbf{B}_1)_{\mathrm{red}}$ and $(\mathbf{B}_2)_{\mathrm{red}}$. Moreover suppose that $(\mathbf{B}_i)_{\mathrm{red}}$ is generated by the corresponding zeros of f. Then, there exists a Galoisian idempotent e of $\mathbf{A}$ such that, with the algebra $\mathbf{B} = \mathbf{A}/\langle 1-e\rangle$, we have two integers r_i such that $(\mathbf{B}_i)_{\mathrm{red}} \simeq \mathbf{B}_{\mathrm{red}}^{r_i}$.

D Lemma 5.1 gives idempotents e_1, $e_2 \in \mathbf{A}$ such that

$$(\mathbf{B}_i)_{\mathrm{red}} \simeq \mathbf{A}/\mathrm{D}_{\mathbf{A}}(1-e_i) \quad (i = 1, 2)$$

Theorem 3.10 item *2* gives a Galoisian idempotent e and r_1, $r_2 \in \mathbb{N}$ such that $\mathbf{A}/\langle 1-e_i\rangle \simeq \mathbf{B}^{r_i}$. Therefore $(\mathbf{B}_i)_{\mathrm{red}} \simeq \mathbf{B}_{\mathrm{red}}^{r_i}$. □

6. Galois theory of a separable polynomial over a discrete field

In Section 6, $\mathbf{K}$ is a nontrivial discrete field,
f is a separable monic polynomial of degree n and $\mathbf{A} = \mathrm{Adu}_{\mathbf{K},f}$.
We highlight the fact that f *is not assumed to be irreducible.*

Recall that for a separably factorial field, every separable polynomial has a splitting field (Corollary VI-1.13), unique up to automorphism (Theorem III-6.7). We are now interested in the case where the field *is not* separably factorial (or even in the case where the factorization of the separable polynomials is too costly).

Here, as promised, we give the constructive and dynamic version of the Galois theory of a separable polynomial over a discrete field.

Existence and uniqueness of the dynamic and static splitting fields

Fact III-5.11 (or Corollary VI-1.8) assures us that $\mathbf{A}$ is an étale $\mathbf{K}$-algebra. The same goes for its Galois quotients. Theorem 5.2 can be re-expressed as follows.

Theorem 5.2 bis (Separable polynomial: when a splitting field exists and is a strictly finite extension)

1. *The following properties are equivalent.*
   - a. *There exists in* $\mathbf{A} = \mathrm{Adu}_{\mathbf{K},f}$ *an indecomposable idempotent* e.
   - b. *There exists a strictly finite extension* $\mathbf{L}$ *of* $\mathbf{K}$ *that is a splitting field of* f.
   - c. *The Boolean algebra* $\mathbb{B}(\mathbf{A})$ *is finite.*
2. *In this case every splitting field of* f *is a Galois extension of* $\mathbf{K}$, *isomorphic to* $\mathbf{A}[1/e]$.

Item *2* also results from the fact that if a splitting field exists and is strictly finite over $\mathbf{K}$, two splitting fields are isomorphic (Theorem III-6.7).

The uniqueness theorem 5.4 can be re-expressed as follows.

Theorem 5.4 bis (Uniqueness of the splitting field of a separable polynomial, dynamic version) *Given two nonzero strictly finite* $\mathbf{K}$*-algebras* $\mathbf{B}_1$ *and* $\mathbf{B}_2$ *in which* f *can be decomposed into a product of linear factors and which are generated by the corresponding zeros of* f, *there exists a Galois quotient* $\mathbf{B} = \mathbf{A}[1/e]$ *of the universal splitting algebra and two integers* r_i *such that* $\mathbf{B}_1 \simeq \mathbf{B}^{r_1}$ *and* $\mathbf{B}_2 \simeq \mathbf{B}^{r_2}$.

Structure of the Galois quotients of the universal splitting algebra

For the remainder of Section 6 we fix the following notations.

6.1. Notations. *(Context of a Galois quotient)*
Let e be a Galoisian idempotent of $\mathbf{A} = \mathrm{Adu}_{\mathbf{K},f}$, $\mathfrak{b} = \langle 1-e \rangle_{\mathbf{A}}$. Let

$$\mathbf{B} = \mathbf{A}/\mathfrak{b} = \mathbf{A}[1/e],\ \pi = \pi_{\mathbf{A},\mathfrak{b}} : \mathbf{A} \to \mathbf{B},\ \text{ and }\ G = \mathrm{St}_{\mathrm{S}_n}(e).$$

Let $(e_1, \ldots, e_m)$ be the orbit of e under S_n. Each $\mathbf{K}$-algebra $\mathbf{A}[1/e_i]$ is isomorphic to $\mathbf{B}$. The group G operates on $\mathbf{B}$.

Note that for $y \in \mathbf{B}$, the polynomial $\mathrm{Min}_y(T)$ is separable (because $\mathbf{B}$ is étale over $\mathbf{K}$). In addition y is invertible if and only if $\mathrm{Min}_y(0) \neq 0$. Also note that a finitely generated ideal of $\mathbf{B}$ (different from $\langle 1 \rangle$) is a Galoisian ideal if and only if its orbit under G is formed of pairwise comaximal ideals (every finitely generated ideal is generated by an idempotent, and Fact 4.6).

The structure theorem 4.3 reads as follows, taking into account Theorems 5.3 and 4.10.

6.2. Theorem. (Galois structure theorem, 3)
In the context of 6.1 we obtain the following results.

1. $(\mathbf{K}, \mathbf{B}, G)$ *is a Galois quotient of* $(\mathbf{K}, \mathbf{A}, \mathrm{S}_n)$.
In particular, $\mathbf{B}$ *is a finite dimensional* $\mathbf{K}$*-vector space* $|G|$ *and for every* $y \in \mathbf{B}$*,* $\mathrm{C}_{\mathbf{B}/\mathbf{K}}(y)(T) = \mathrm{C}_G(y)(T)$*. In addition,* $\mathrm{Fix}(G) = \mathbf{K}$*.*
2. *We have an isomorphism of* $\mathbf{K}$*-algebras* $\mathbf{A} \simeq \mathbf{B}^m$*.*
3. *If* $\mathbf{B}$ *is connected, it is a splitting field for* f *and a Galois extension of* $\mathbf{K}$ *with* G *as its Galois group.*
4. *Let* (y_i) *be a finite family of elements of* $\mathbf{B}$*. There exists a Galoisian idempotent* $e_{\mathbf{B}}$ *of* $(\mathbf{K}, \mathbf{B}, G)$ *such that in* $\mathbf{B}[1/e_{\mathbf{B}}]$*, each* y_i *is null or invertible.*
5. *The restriction* $\pi : e\mathbf{A} \to \mathbf{B}$ *is a* $\mathbf{K}$*-linear isomorphism and establishes a biunivocal correspondence between the Galoisian idempotents of* $(\mathbf{K}, \mathbf{A}, \mathrm{S}_n)$ *contained in* $e\mathbf{A}$ *and those of* $(\mathbf{K}, \mathbf{B}, G)$*. The stabilizers and residual quotients are preserved; i.e. if* $e_{\mathbf{A}} \in e\mathbf{A}$ *and* $e_{\mathbf{B}} \in \mathbf{B}$ *are two Galoisian idempotents that correspondent to each other, then* $\mathrm{St}_{\mathrm{S}_n}(e_{\mathbf{A}}) = \mathrm{St}_G(e_{\mathbf{B}})$ *and* $\mathbf{A}[1/e_{\mathbf{A}}] \simeq \mathbf{B}[1/e_{\mathbf{B}}]$*.*

NB: In what follows, we only give the statements for the relative situation, the absolute situation is indeed the special case where $e = 1$.

6.3. Lemma. (Resolvent and minimal polynomial) *Context 6.1,* $y \in \mathbf{B}$*.*

1. $\mathrm{Rv}_{G,y}(T)$ *has coefficients in* $\mathbf{K}$*.*
2. Min_y *divides* $\mathrm{Rv}_{G,y}$ *which divides a power of* Min_y*.*
3. $\mathrm{C}_{\mathbf{B}/\mathbf{K}}(y)(T) = \mathrm{C}_G(y)(T) = \mathrm{Rv}_{G,y}(T)^{|\mathrm{St}_G(y)|}$*.*

D *1.* Consequence of item *1* in the structure theorem.
2. We deduce that Min_y divides $\mathrm{Rv}_{G,y}$, because $\mathrm{Rv}_{G,y}(y) = 0$, and since each y_i annihilates Min_y, the product of the $T - y_i$'s divides a power of Min_y.
3. The second equality is obvious, and the first is in item *1* of the structure theorem. □

Where the computations take place

Recall that f is a separable monic polynomial of $\mathbf{K}[T]$ with $\mathbf{K}$ a nontrivial discrete field.

We denote by $\mathbf{Z}_0$ the subring of $\mathbf{K}$ generated by the coefficients of f and by $1/\mathrm{disc}(f)$. We denote by $\mathbf{Z}$ the integral closure of $\mathbf{Z}_0$ in $\mathbf{K}$.

Here we highlight the fact that "all the computations take place, and all the results are written, in the ring $\mathbf{Z}$," since this follows from Theorems VI-5.12 and 4.15.[4]

These theorems give us in the current framework items *1*, *2* and *4* of the following theorem. As for item *3*, it is an immediate consequence of item *2*.

6.4. Theorem. (The subring $\mathbf{Z}$ of $\mathbf{K}$ is sufficient)

1. *Let $\mathbf{Z}_1$ be an intermediate ring between $\mathbf{Z}$ and $\mathbf{K}$ (for example $\mathbf{Z}_1 = \mathbf{Z}$). Then the universal splitting algebras*
$$\mathrm{Adu}_{\mathbf{Z}_0,f} \subseteq \mathrm{Adu}_{\mathbf{Z},f} \subseteq \mathrm{Adu}_{\mathbf{Z}_1,f} \subseteq \mathrm{Adu}_{\mathbf{K},f}$$
are Galois algebras (with respect to their base rings, and with the group S_n).
2. *Every idempotent of $\mathbf{A} = \mathrm{Adu}_{\mathbf{K},f}$ is in $\mathrm{Adu}_{\mathbf{Z},f}$: its coordinates over the basis $\mathcal{B}(f)$ are in $\mathbf{Z}$.*
3. *The* Galois theories of f *over* $\mathbf{Z}$*, over* $\mathbf{Z}_1$*, over* $\mathrm{Frac}(\mathbf{Z})$ *and over* $\mathbf{K}$ *are* identical*, in the following sense.*
   a. *Every Galois quotient of $\mathrm{Adu}_{\mathbf{Z}_1,f}$ is obtained by scalar extension to $\mathbf{Z}_1$ from a Galois quotient of $\mathrm{Adu}_{\mathbf{Z},f}$.*
   b. *Every Galois quotient of $\mathrm{Adu}_{\mathrm{Frac}(\mathbf{Z}),f}$ is obtained by scalar extension to $\mathrm{Frac}(\mathbf{Z})$ from a Galois quotient of $\mathrm{Adu}_{\mathbf{Z},f}$. This scalar extension is in fact the same thing as passing to the total ring of fractions of the Galois quotient.*
   c. *Every Galois quotient of $\mathrm{Adu}_{\mathbf{K},f}$ is obtained by scalar extension to $\mathbf{K}$ from a Galois quotient of $\mathrm{Adu}_{\mathrm{Frac}(\mathbf{Z}),f}$.*
4. *Let e be a Galoisian idempotent of $\mathbf{A}$ and $\mathbf{Z}_1$ be the subring of $\mathbf{Z}$ generated by $\mathbf{Z}_0$ and the coordinates of e over $\mathcal{B}(f)$. Then, the triangular structure of the ideal of $\mathbf{Z}_1[X_1,\ldots,X_n]$ generated by $1-e$ and the Cauchy modules is made explicit by means of polynomials with coefficients in $\mathbf{Z}_1$.*

   For those that know Gröbner bases: the Gröbner basis (for a lexicographical monomial order) of the ideal that defines the corresponding approximation of the splitting field of f is formed of monic polynomials with coefficients in $\mathbf{Z}_1$.

[4] It follows that if $\mathbf{K}$ is a general field (see Section IX-1), the questions of computability are actually discussed entirely in $\mathrm{Frac}(\mathbf{Z}) = \mathrm{Frac}(\mathbf{Z}_0) \otimes_{\mathbf{Z}_0} \mathbf{Z} = (\mathbf{Z}_0^{\star})^{-1}\mathbf{Z}$, and $\mathrm{Frac}(\mathbf{Z})$ is discrete if $\mathbf{Z}_0$ is itself a discrete ring. As $\mathbf{Z}_0$ is a finitely generated ring, it certainly is, in classical mathematics, an effective (also called computable) ring with an explicit equality test, in the sense of recursion theory via Turing machines.

But this last result is not a truly satisfying approach to the reality of the computation. It is indeed akin to results in classical mathematics of the form "every recursive real number admits a recursive development into a continued fraction", a theorem that is evidently false from a practical point of view, since to implement it, one must first know whether the number is rational or not.

Note the simplifications in the following special cases. If $\mathbf{K} = \mathbb{Q}$ and $f \in \mathbb{Z}[T]$ monic, then $\mathbf{Z} = \mathbf{Z}_0 = \mathbb{Z}[1/\mathrm{disc}(f)]$. Similarly, for q a prime power and $\mathbf{K}$ the field of rational fractions $\mathbf{K} = \mathbb{F}_q(u)$ we have, if $f \in \mathbb{F}_q[u][T]$ is monic, $\mathbf{Z} = \mathbf{Z}_0 = \mathbb{F}_q[u][1/\mathrm{disc}(f)]$.

Remarks. 1) Experiments suggest not only that "$\mathbf{Z}$ is sufficient," but that in fact all the results of computations (coefficients of an idempotent over $\mathcal{B}(f)$, a Gröbner basis of a Galoisian ideal) only use as denominators elements whose square divides the discriminant of f.

2) *Absolute Galois theory of a polynomial.* Given a separable polynomial $f \in \mathbf{K}[T]$, rather than considering $\mathbf{K}$ and the integral closure $\mathbf{Z}$ of $\mathbf{Z}_0$ in $\mathbf{K}$, we can consider $\mathbf{K}' = \mathrm{Frac}(\mathbf{Z}_0)$ and the integral closure $\mathbf{Z}'$ of $\mathbf{Z}_0$ in $\mathbf{K}'$. ■

Changing the base ring, modular method

Since everything takes place in $\mathbf{Z}$, one can look at what happens after an arbitrary scalar extension $\varphi : \mathbf{Z} \to \mathbf{k}$.

It is possible for example that $\mathbf{k}$ is a "simple" discrete field and that we know how to compute $\mathrm{Gal}_{\mathbf{k}}\big(\varphi(f)\big)$; i.e. identifying an indecomposable idempotent e' in $\mathrm{Adu}_{\mathbf{k},\varphi(f)}$. This group will necessarily be (isomorphic to) a subgroup of the unknown Galois group $\mathrm{Gal}_{\mathbf{Z}}(f) = \mathrm{Gal}_{\mathbf{K}}(f)$.

Suppose that we have computed a Galois quotient $\mathbf{B}$ of $\mathrm{Adu}_{\mathbf{Z},f}$ with a group $G \subseteq \mathrm{S}_n$.

If e is the Galoisian idempotent of $\mathrm{Adu}_{\mathbf{Z},f}$ corresponding to $\mathbf{B}$, we can reduce back to the case where $\varphi(e)$ is a sum of conjugates of e' and where

$$\mathrm{Gal}_{\mathbf{k}}\big(\varphi(f)\big) = H = \mathrm{St}_G(e') \subseteq G.$$

As this is true for every Galois quotient of $\mathrm{Adu}_{\mathbf{Z},f}$, we obtain a double inclusion

$$H \subseteq \mathrm{Gal}_{\mathbf{Z},f} \subseteq G \tag{1}$$

except that the group $\mathrm{Gal}_{\mathbf{Z},f}$ is only defined up to conjugation, and that it can a priori remain forever unknown.

This type of information, "the Galois group of f over $\mathbf{K}$, up to conjugation, contains H" is outside of the dynamic method that we have presented, because this one takes a step in the other direction: giving information of the type "the Galois group of f over $\mathbf{K}$, up to conjugation, is contained in G."

It is therefore a priori interesting to use the two methods in parallel, in the hope of completely determining $\mathrm{Gal}_{\mathbf{K}}(f)$.

Replacing the field $\mathbf{K}$ by a subring is important from this point of view as we dispose of a lot more morphisms of scalar extension from the domain $\mathbf{Z}$ than from the domain $\mathbf{K}$.

In particular, it is often useful to work modulo $\mathfrak{p}$, a maximal ideal of $\mathbf{Z}$. This method is called a *modular method.*

This method seems to have been invented by Dedekind for the determination of the Galois group of f over $\mathbb{Q}$ when $f \in \mathbb{Z}[T]$. Note that in this case a maximal ideal of $\mathbf{Z} = \mathbf{Z}_0 = \mathbb{Z}[1/\operatorname{disc}(f)]$ is given by a prime number p which does not divide $\operatorname{disc}(f)$.

Lazy Galois theory

The structure theorem 6.2 and Lemma 6.3 (which gives a few details) are the theoretical constructive results that allow a lazy evaluation of the splitting field and of the Galois group of a separable polynomial.

Please note that the term "lazy" is absolutely not pejorative. It simply indicates that we can work with complete confidence in the splitting field of a separable polynomial over $\mathbf{K}$, even in the absence of any factorization algorithm of the polynomials over $\mathbf{K}$. Indeed, any anomalies with the algebra $\mathbf{B}$, the "ongoing" approximation of the splitting field of f, for instance the presence of a nonzero zerodivisor, can be exploited to significantly improve our knowledge of the Galois group and of the splitting field. A Galoisian idempotent that is strictly a multiple of the "ongoing" idempotent e can indeed be computed. In the new Galois algebra, which is a quotient of the previous one, all the previously made computations remain valid, by passage to the quotient. Moreover, the number of significant improvements that may occur this way does not exceed the maximum length of a chain of subgroups of S_n.

We therefore develop a "Galoisian" variant of the D5 system, which was the first computer algebra system to compute, both systematically and without risk of errors, in the algebraic closure of a field in the absence of a factorization algorithm for polynomials (see [58, Duval&al.]).

Here, in contrast to what happens with the D5 system, the dynamic aspect of things does not consist in "opening separate branches of computation" each time an anomaly occurs, but in improving the approximation of the splitting field (and of its Galois group) that constitutes the ongoing Galois quotient of the universal splitting algebra each time.

The basic algorithm

We can rewrite Algorithm 3.11 in the current setting as follows, when we have an element y neither null nor invertible in the Galois quotient $\mathbf{B} = \mathbf{A}/\mathfrak{b}$ at our disposal.

6.5. Algorithm. Computation of a Galoisian ideal and of its stabilizer

```
Input: $\mathfrak{b}$: Galoisian ideal of a universal splitting algebra $\mathbf{A}$ for a separable
polynomial, $\mathfrak{b}$ is given by a finite generator set; $y$: nonzero zerodivisor in
$\mathbf{B} = \mathbf{A}/\mathfrak{b}$; $G = \mathrm{St}_{\mathrm{S}_n}(\mathfrak{b})$; $S_y = \mathrm{St}_G(y)$.
Output: $\mathfrak{b}'$: a Galoisian ideal of $\mathbf{B}$ containing $y$; $H$: $\mathrm{St}_G(\mathfrak{b}')$.
Local variables: $\mathfrak{a}$: finitely generated ideal of $\mathbf{B}$; $\sigma$: element of $G$;
$L$: list of elements of $\overline{G/S_y}$;
   # $\overline{G/S_y}$ is a system of representatives of the left cosets of $S_y$
$E$: corresponding set of elements of $G/S_y$;
   # $G/S_y$ is the set of left cosets of $S_y$.
Begin
   $E \leftarrow \emptyset$; $L \leftarrow [\,]$; $\mathfrak{b}' \leftarrow \langle y \rangle$;
   for $\sigma$ in $\overline{G/S_y}$ do
      $\mathfrak{a} \leftarrow \mathfrak{b}' + \langle \sigma(y) \rangle$;
      if $1 \notin \mathfrak{a}$ then $\mathfrak{b}' \leftarrow \mathfrak{a}$; $L \leftarrow L \bullet [\sigma]$; $E \leftarrow E \cup \{\sigma S_y\}$
      end if;
   end for;
   $H \leftarrow \mathrm{St}_G(E)$    # $H = \big\{\, \alpha \in G \,|\, \forall \sigma \in L, \alpha\sigma \in \bigcup_{\tau \in L} \tau S_y \,\big\}$.
End.
```

The ideal $\mathfrak{b}$ is given by a finite generator set, and $G = \mathrm{St}_{\mathrm{S}_n}(\mathfrak{b})$. Let e be the idempotent of $\mathbf{B}$ such that $\langle 1 - e \rangle_{\mathbf{B}} = \langle y \rangle_{\mathbf{B}}$, and e' be a Galoisian idempotent such that $G.e$ and $G.e'$ generate the same Boolean algebra.

We are looking to compute the Galoisian ideal $\mathfrak{c}$ of $\mathbf{A}$ which gives the new Galois quotient $\mathbf{A}/\mathfrak{c} \simeq \mathbf{B}/\mathfrak{b}'$, where $\mathfrak{b}' = \langle 1 - e' \rangle_{\mathbf{B}}$, i.e. $\mathfrak{c} = \pi_{\mathbf{A},\mathfrak{b}}^{-1}(\mathfrak{b}')$.

In Algorithm 3.11 we find the product of e and a maximum number of conjugates, avoiding obtaining a null product.

Here we do not compute e, nor $\sigma(e)$, nor e', because experimentation often shows that the computation of e is very long (this idempotent often occupies a lot of memory space, significantly more than e'). We then reason with the corresponding ideals $\langle 1 - e \rangle = \langle y \rangle$ and $\langle 1 - \sigma(e) \rangle = \langle \sigma(y) \rangle$. It follows that in the algorithm the product of the idempotents is replaced by the sum of the ideals.

Moreover, as we do not compute e, we replace $\mathrm{St}_G(e)$ by $\mathrm{St}_G(y)$, which is contained in $\mathrm{St}_G(e)$, generally strictly so. Nevertheless, experience shows that, even though $\overline{G/S_y}$ is larger, the whole computation is faster. We leave it to the reader to show that the last assignment in the algorithm indeed provides the desired group $\mathrm{St}_G(\mathfrak{b}')$; i.e. that the subgroup H of G, the stabilizer of E in G/S_y, is indeed equal to $\mathrm{St}_G(\mathfrak{b}')$.

When a relative resolvent factorizes

Often an anomaly in a Galois quotient of the universal splitting algebra corresponds to the observation that a relative resolvent can be factorized. We therefore treat this case in all generality to reduce it to a case where a nonzero zerodivisor is present.

6.6. Proposition. (When a relative resolvent factorizes)
In the context of 6.1 let $y \in \mathbf{B}$ and $G.y = \{y_1, \dots, y_r\}$.

1. *If $\mathrm{Min}_y = R_1R_2$ with R_1 and R_2 of degrees $\geqslant 1$, $R_1(y)$ and $R_2(y)$ are nonzero zerodivisors, and there exists an idempotent e such that $\langle e \rangle = \langle R_1(y) \rangle$ and $\langle 1 - e \rangle = \langle R_2(y) \rangle$.*
2. *If $\deg(\mathrm{Min}_y) < \deg(\mathrm{Rv}_{G,y})$, then one of the $y_1 - y_i$'s divides zero (we can therefore construct an idempotent $\neq 0, 1$ of $\mathbf{B}$).*
3. *If P is a strict divisor of $\mathrm{Rv}_{G,y}$ in $\mathbf{K}[T]$, then at least one of the two following case occurs:*
   - *$P(y)$ is a nonzero zerodivisor, we are in item 1.*
   - *an element $y_1 - y_i$ is a nonzero zerodivisor, we are in item 2.*

D *1.* Since Min_y is separable, R_1 and R_2 are comaximal. With a Bézout relation $U_1R_1 + U_2R_2 = 1$, let $e = (U_1R_1)(y)$ and $e' = 1 - e$. We have $ee' = 0$, so e and e' are idempotents. We also immediately have

$$eR_2(y) = e'R_1(y) = 0,\ eR_1(y) = R_1(y) \text{ and } e'R_2(y) = R_2(y).$$

Therefore $\langle e \rangle = \langle R_1(y) \rangle$ and $\langle 1 - e \rangle = \langle R_2(y) \rangle$.

2. The proof that shows that over an integral ring a monic polynomial of degree d cannot have more than d distinct roots is reread as follows.
Over an arbitrary ring, if a monic polynomial P of degree d admits some $(a_1, \dots, a_d)$ as zeros with each $a_i - a_j$ regular for $i \neq j$, then we have $P(T) = \prod (T - a_i)$. Therefore if $P(t) = 0$ and t is distinct from the a_i's, at least two of the $t - a_i$'s are nonzero zerodivisors. We apply this to the minimal polynomial Min_y which has more zeros in $\mathbf{B}$ than its degree (those are the y_i's). This gives a nonzero zerodivisor $y_j - y_k$, and via some $\sigma \in G$ we transform $y_j - y_k$ into a $y_1 - y_i$.

3. If P is a multiple of Min_y, we are in item *2*.
Otherwise, $\gcd(\mathrm{Min}_y, P) = R_1$ is a strict divisor of Min_y, and $R_1 \neq 1$ because we have $\gcd\big((\mathrm{Min}_y)^k, P\big) = P$ for large enough k. Therefore $\mathrm{Min}_y = R_1R_2$, with $\deg(R_1)$ and $\deg(R_2) \geqslant 1$. We are in item *1*. □

From this we deduce the following corollary which generalizes item *4* of the structure theorem 6.2.

6.7. Theorem. *In the context of 6.1 let $(u_j)_{j\in J}$ be a finite family in $\mathbf{B}$. There exists a Galoisian ideal $\mathfrak{c}$ of $\mathbf{B}$ such that, by letting $H = \mathrm{St}_G(\mathfrak{c})$, $\mathbf{C} = \mathbf{B}/\mathfrak{c}$, and $\beta : \mathbf{B} \to \mathbf{C}$ be the canonical projection, we have*

1. *Each $\beta(u_j)$ is null or invertible.*
2. *In $\mathbf{C}$, $\mathrm{Min}_{\beta(u_j)}(T) = \mathrm{Rv}_{H,\beta(u_j)}(T)$.*
3. *The $\mathrm{Min}_{\beta(u_j)}$'s are pairwise equal or comaximal.*

Remark. In the previous theorem it is sometimes in our best interest to saturate the family $(u_j)_{j\in J}$ by the action of G (or of S_n by lifting the u_j to $\mathbf{A}$) in order to make manifest in $\mathbf{C}$ all the possible "scenarios." ■

Example. We reuse the example of page 115. We ask `Magma` what it thinks about the element `x5 + x6`. Finding that the resolvent is of degree 15 (without having to compute it) whilst the minimal polynomial is of degree 13, it struggles to reduce the oddity and obtains a Galois quotient of the universal splitting algebra of degree 48 (the splitting field of degree 24 is not yet reached) with the corresponding group. The computation is almost instantaneous. Here is the result.

```
y:=x5+x6;
MinimalPolynomial(y);
  T^13 - 13*T^12 + 87*T^11 - 385*T^10 +
     1245*T^9 - 3087*T^8 + 6017*T^7 - 9311*T^6 + 11342*T^5
     - 10560*T^4 + 7156*T^3 - 3284*T^2 + 1052*T - 260
//new Galois algebra, computed from deg(Min)<deg(Rv) :
Affine Algebra of rank 6 over Rational Field
Variables: x1, x2, x3, x4, x5, x6
Quotient relations:
  x1 + x2 - 1,
  x2^2 - x2 + x4^2 - x4 + x6^2 - x6 + 3,
  x3 + x4 - 1,
  x4^4 - 2*x4^3 + x4^2*x6^2 - x4^2*x6 + 4*x4^2 - x4*x6^2 + x4*x6 -
        3*x4 + x6^4 - 2*x6^3 + 4*x6^2 - 3*x6 - 1,
  x5 + x6 - 1,
  x6^6 - 3*x6^5 + 6*x6^4 - 7*x6^3 + 2*x6^2 + x6 - 1
Permutation group acting we have set of cardinality 6
Order = 48 = 2^4 * 3
    (1, 2)
    (3, 5)(4, 6)
    (1, 3, 5)(2, 4, 6)
```

Certain special cases of the situation examined in Proposition 6.6 are used as exercises. Each time the goal is to obtain more precise information on what happens when we reduce the observed oddity. See Exercises 11, 12 and 13.

When the triangular structure is missing

Consider some elements $\alpha_1, \dots, \alpha_\ell$ of $\mathbf{B}$ and the nested $\mathbf{K}$-algebras

$$\mathbf{K} \subseteq \mathbf{K}_1 = \mathbf{K}[\alpha_1] \subseteq \mathbf{K}_2 = \mathbf{K}[\alpha_1, \alpha_2] \subseteq \cdots \subseteq \mathbf{K}_\ell = \mathbf{K}[\alpha_1, \dots, \alpha_\ell] \subseteq \mathbf{B}.$$

For $i = 2, \dots, \ell$ the structure of $\mathbf{K}_i$ as a $\mathbf{K}_{i-1}$-module can be made explicit by different techniques. If $\mathbf{B}$ is a splitting field for f, all the $\mathbf{K}_i$'s are fields and each of the modules is free.

If one of these modules is not free, then we can construct an idempotent $\neq 0, 1$ in $\mathbf{B}$ by using the same technique as for the proof of the structure theorem VI-1.4, item *2b*.

Using the Gröbner basis technique can turn out to be efficient, with the ideal that defines $\mathbf{B}$ as a quotient of $\mathbf{K}[X_1, \dots, X_n]$. We introduce some variable names a_i for the α_i's and we choose a lexicographical order with $a_1 < \cdots < a_\ell < X_1 < \cdots < X_n$.

If $\mathbf{B}$ is a field the Gröbner basis must have a triangular structure. To each α_i must correspond one and only one polynomial in the Gröbner basis, $P_i(a_1, \dots, a_i)$ monic in a_i.

If this triangular structure is not respected for the variable a_i, we are certain that $\mathbf{K}_{i-1}$ is not a field, and we can explicitly construct a nonzero zerodivisor in this $\mathbf{K}$-algebra.

Actually, let $P(a_1, \dots, a_i)$ be a polynomial that appears in the Gröbner basis and that is not monic in a_i. Its leading coefficient as a polynomial in a_i is a polynomial $Q(a_1, \dots, a_{i-1})$ which necessarily gives a nonzero zerodivisor $Q(\alpha_1, \dots, \alpha_{i-1})$ in the zero-dimensional algebra $\mathbf{K}_{i-1} \simeq \mathbf{K}[a_1, \dots, a_{i-1}]/\mathfrak{a}$, where $\mathfrak{a}$ is the ideal generated by the first polynomials, in the variables a_1, …, a_{i-1}, that appear in the Gröbner basis. Otherwise, we could multiply P by the inverse of Q modulo $\mathfrak{a}$, and reduce the result modulo $\mathfrak{a}$, and we would obtain a monic polynomial in a_i that precedes P in the lexicographical ordering, and that would render the presence of P pointless.

Exercises and problems

Exercise 1. We recommend that the proofs which are not given, or are sketched, or left to the reader, etc, be done. But in particular, we will cover the following cases.

- Prove Propositions 3.1, 3.2 and Theorem 3.3.
- Explain Fact 4.1.

Exercise 2. *(Structure of finite algebras over a field, classical version, dynamic constructive version)*
1. Prove in classical mathematics the following result.
Every finite algebra over a field is a finite product of finite local algebras.
2. Explain why we cannot hope to obtain a constructive proof of this result, even if we assume that the field is discrete.
3. Propose a constructive version of the previous result.

Exercise 3. Show that the elementary local-global machinery no. 2 (page 213) applied to the proof of Theorem 1.5 gives the following result, equivalent to Theorem 1.5 in the case of a nontrivial discrete field.

Theorem 1.5 bis (Weak Nullstellensatz and Noether position, reduced zero-dimensional rings case) *Let $\mathbf{K}$ be a reduced zero-dimensional ring, $\mathfrak{f}$ be a finitely generated ideal of $\mathbf{K}[\underline{X}] = \mathbf{K}[X_1, \ldots, X_n]$ and $\mathbf{A} = \mathbf{K}[\underline{X}]/\mathfrak{f}$ be the quotient algebra. Then, there exists a fundamental system of orthogonal idempotents $(e_{-1}, e_0, \ldots, e_n)$ of $\mathbf{K}$ and a change of variables such that, naming the new variables $Y_1, \ldots, Y_n$, and letting*

$$\mathbf{K}_r = \mathbf{K}[1/e_r] \quad \textit{and} \quad \mathbf{A}_r = \mathbf{A}[1/e_r] = \mathbf{K}_r \otimes_{\mathbf{K}} \mathbf{A} \simeq \mathbf{K}_r[\underline{X}]/\mathfrak{f}\ \mathbf{K}_r[\underline{X}],$$

we have the following results.

1. $\mathbf{A}_{-1} = 0$ *and* $\mathbf{K} \cap \mathfrak{f} = e_{-1}\mathbf{K}$.
2. $\mathbf{A}_0$ *is a free* $\mathbf{K}_0$*-module of finite rank* $\geqslant 1$.
3. *For* $r = 1, \ldots, n$ *we have*
   - $\mathbf{K}_r[Y_1, \ldots, Y_r] \cap \mathfrak{f} = 0$. *In other words the algebra* $\mathbf{K}_r[Y_1, \ldots, Y_r]$ *can be considered as a* $\mathbf{K}_r$*-subalgebra of* $\mathbf{A}_r$.
   - $\mathbf{A}_r$ *is a finitely presented module over* $\mathbf{K}_r[Y_1, \ldots, Y_r]$.
   - *There exists an integer N such that for each* $(\alpha_1, \ldots, \alpha_r) \in \mathbf{K}_r^r$, *the* $\mathbf{K}_r$*-algebra*
     $$\mathbf{B}_r = \mathbf{A}_r/\langle Y_1 - \alpha_1, \ldots, Y_r - \alpha_r\rangle$$
     is a quasi-free $\mathbf{K}_r$*-module of finite rank* $\leqslant N$, *and the natural homomorphism* $\mathbf{K}_r \to \mathbf{B}_r$ *is injective.*

In particular, the $\mathbf{K}$*-algebra* $\mathbf{A}$ *is a finitely presented module over the "polynomial" subalgebra* $\mathbf{A} = \bigoplus_{r=0}^{n} \mathbf{K}_r[Y_1, \ldots, Y_r]$. *We say that the change of variables (which eventually changes nothing at all) has put the ideal in* Noether position.
Finally, the fundamental system of orthogonal idempotents that intervenes here does not depend on the change of variables that puts the ideal in Noether position.

Exercise 4. *(Magic squares and commutative algebra)*
In this exercise we provide an application of commutative algebra to a combinatorial problem; the free character that intervenes in the Noether positioning of question *2* is an example of the Cohen-Macaulay property in a graded environment.
A *magic square* of size n is a matrix of $\mathbb{M}_n(\mathbb{N})$ for which the sum of each row and each column is the same. The set of these magic squares is an additive submonoid of $\mathbb{M}_n(\mathbb{N})$; we will admit here that it is the monoid generated by the $n!$

permutation matrices. We are interested in counting the magic squares of size 3 of fixed sum d. Here are the 6 permutation matrices of $\mathbb{M}_3(\mathbb{N})$

$$P_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},\ P_2 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix},\ P_3 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

$$P_4 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix},\ P_5 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix},\ P_6 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

They are linked by the relation $P_1 + P_2 + P_3 = P_4 + P_5 + P_6$. Let $\mathbf{k}[(x_{ij})_{i,j\in[\![1..3]\!]}]$ be the polynomial ring with nine indeterminates where $\mathbf{k}$ is an arbitrary ring. We identify the matrix $M = (m_{ij}) \in \mathbb{M}_3(\mathbb{N})$ with the monomial $\prod_{i,j} x_{ij}^{m_{ij}}$, denoted $\underline{x}^M$; for example $\underline{x}^{P_1} = x_{11}x_{22}x_{33}$.

1. Let $U_1, \ldots, U_6$ be six indeterminates over $\mathbf{k}$ and $\varphi : \mathbf{k}[\underline{U}] \twoheadrightarrow \mathbf{k}[\underline{x}^{P_1}, \ldots, \underline{x}^{P_6}]$ defined by $U_i \mapsto \underline{x}^{P_i}$.
We want to show that $\operatorname{Ker}\varphi$ is the ideal $\mathfrak{a} = \langle U_1U_2U_3 - U_4U_5U_6\rangle$.

- *a.* Show, for a, b, c, d, e, $f \in \mathbb{N}$ and $m = \min(a, b, c)$, that
$$U_1^aU_2^bU_3^cU_4^dU_5^eU_6^f \equiv U_1^{a-m}U_2^{b-m}U_3^{c-m}U_4^{d+m}U_5^{e+m}U_6^{f+m} \bmod \mathfrak{a}$$
- *b.* Let $\mathfrak{a}^\bullet$ be the $\mathbf{k}$-submodule of $\mathbf{k}[\underline{U}]$ with the monomials not divisible by $U_1U_2U_3$ as its basis. Show that $\mathbf{k}[\underline{U}] = \mathfrak{a} \oplus \mathfrak{a}^\bullet$ and that $\operatorname{Ker}\varphi = \mathfrak{a}$.
- *c.* Deduce that the number M_d of magic squares of size 3 and of sum d is equal to $\binom{d+5}{5} - \binom{d+2}{5}$ since the convention is that $\binom{i}{j} = 0$ for $i < j$.

2. Let $\mathbf{B} = \mathbf{k}[\underline{U}]/\mathfrak{a} = \mathbf{k}[\underline{u}]$.

- *a.* Define a Noether position $\mathbf{A} = \mathbf{k}[v_2, v_3, u_4, u_5, u_6]$ of $\mathbf{B}$ where v_2, v_3 are linear forms in $\underline{u}$, such that $(1, u_1, u_1^2)$ is an $\mathbf{A}$-basis of $\mathbf{B} = \mathbf{A} \oplus \mathbf{A}u_1 \oplus \mathbf{A}u_1^2$.
- *b.* Deduce that the number M_d is also equal to $\binom{d+4}{4}+\binom{d+3}{4}+\binom{d+2}{4}$ (MacMahon's formula, which in passing gives an identity between binomial coefficients).

3. Suppose that $\mathbf{k}$ is a discrete field. We want to show that the ring $\mathbf{B}$, regarded as the ring $\mathbf{k}[\underline{x}^{P_1}, \ldots, \underline{x}^{P_6}]$, is integrally closed (see also Problem XII-2). Let $E \subset \mathbb{M}_3(\mathbb{Z})$ be the $\mathbb{Z}$-submodule of magic squares (analogous definition) and the subring $\mathbf{B}_{11} \subset \mathbf{k}[x_{ij}^{\pm 1}, i, j \in [\![1..3]\!]]$

$$\mathbf{B}_{11} = \mathbf{k}[\underline{x}^{P_1}, \underline{x}^{P_6}][\underline{x}^{\pm P_2}, \underline{x}^{\pm P_3}, \underline{x}^{\pm P_4}, \underline{x}^{\pm P_5}]$$

such that $\mathbf{B}_{11} \subset \mathbf{k}[\,\underline{x}^M \,|\, M \in E,\ m_{11} \geqslant 0\,]$.

- *a.* Verify that $\mathbf{B}$ and $\mathbf{B}_{11}$ have the same quotient field, which is the quotient field $\mathbf{k}(E)$, the field of rational fractions over $\mathbf{k}$ with 5 indeterminates.
- *b.* Show that $\mathbf{B}_{11}$ is integrally closed.
- *c.* For i, $j \in [\![1..3]\!]$, define a ring $\mathbf{B}_{ij}$ analogous to $\mathbf{B}_{11}$ and deduce that $\mathbf{B}$ is integrally closed.

Exercise 5. Give a direct proof (not using a reductio ad absurdum) that if a discrete field has two automorphisms that generate a noncyclic finite group, the field contains some $x \neq 0$, all the powers of which are pairwise distinct, i.e. it is not a root of unity.

Exercise 6. *(A "discriminantal" identity)*
Let $n \geqslant 1$. Let E be the set of $\alpha \in \mathbb{N}^n$ such that $0 \leqslant \alpha_i < i$ for $i \in [\![1..n]\!]$; it is a set of cardinality $n!$ which we order by "factorial numeration," i.e. $\alpha \preccurlyeq \beta$ if $\sum_i \alpha_i i! \leqslant \sum_i \beta_i i!$. We order the symmetric group S_n by the lexicographic ordering, I_n being the smallest permutation. Consider n indeterminates over $\mathbb{Z}$ and define a matrix $M \in \mathbb{M}_{n!}(\mathbb{Z}[\underline{x}])$, indexed by $\mathrm{S}_n \times E$,

$$M_{\sigma,\alpha} = \sigma(\underline{x}^{\alpha}), \qquad \sigma \in \mathrm{S}_n, \quad \alpha \in E.$$

Thus for $n = 3$:

$$M = \begin{bmatrix} 1 & x_2 & x_3 & x_2x_3 & x_3^2 & x_2x_3^2 \\ 1 & x_3 & x_2 & x_2x_3 & x_2^2 & x_2^2x_3 \\ 1 & x_1 & x_3 & x_1x_3 & x_3^2 & x_1x_3^2 \\ 1 & x_3 & x_1 & x_1x_3 & x_1^2 & x_1^2x_3 \\ 1 & x_1 & x_2 & x_1x_2 & x_2^2 & x_1x_2^2 \\ 1 & x_2 & x_1 & x_1x_2 & x_1^2 & x_1^2x_2 \end{bmatrix}$$

1. Show that $\det(M) = \delta^{n!/2}$ with $\delta = \prod_{i<j}(x_i - x_j)$.

2. Let $s_1, \ldots, s_n \in \mathbb{Z}[\underline{x}]$ be the n elementary symmetric functions, $F(T)$ be the universal polynomial $F(T) = T^n - s_1T^{n-1} + \cdots + (-1)^n s_n$, and $U \in \mathbb{M}_{n!}(\mathbb{Z}[\underline{x}])$ be the trace-valued matrix, indexed by $E \times E$, with term $\mathrm{Tr}_{\mathrm{S}_n}(\underline{x}^{\alpha+\beta})$, $\alpha, \beta \in E$. Let $f \in \mathbf{k}[T]$ be a monic polynomial of degree n, $\mathbf{A} = \mathrm{Adu}_{\mathbf{k},f}$.
Prove the equality $\mathrm{Disc}_{\mathbf{k}}\,\mathbf{A} = \mathrm{disc}(f)^{n!/2}$ (also found in Fact III-5.11).
And conversely?

3. Revisit Theorem 4.12.

Exercise 7. *(The universal splitting algebra of the polynomial $f(T) = T^n$)*
Let $f(T) = T^n$ and $\mathbf{A} = \mathrm{Adu}_{\mathbf{k},f} = \mathbf{k}[x_1, \ldots, x_n]$. Describe the structure of $\mathbf{A}$.

Exercise 8. *(Invertible polynomials and nilpotency indices)*
Here we propose a quantitative version of item *4* of Lemma II-2.6. Let $\mathbf{k}$ be a commutative ring, f, $g \in \mathbf{k}[X]$ satisfying $fg = 1$ and $f(0) = g(0) = 1$. We write $f = \sum_{i=0}^{n} a_i X^i$, $g = \sum_{j=0}^{m} b_j X^j$. Show that

$$a_1^{\alpha_1} a_2^{\alpha_2} \cdots a_n^{\alpha_n} b_1^{\beta_1} b_2^{\beta_2} \cdots b_m^{\beta_m} = 0 \quad \text{if} \quad \textstyle\sum_i i\alpha_i + \sum_j j\beta_j > nm.$$

In particular, for $i \geqslant 1$, we have $a_i^{\lceil (nm+1)/i \rceil} = 0$ and therefore $a_1^{nm+1} = 0$.

Exercise 9. *(The universal splitting algebra of the polynomial $f(T) = T^p - a$ in characteristic p)*
Let p be a prime number, $\mathbf{k}$ be a ring in which $p \cdot 1_{\mathbf{k}} = 0$ and $a \in \mathbf{k}$.
Let $f(T) = T^p - a \in \mathbf{k}[T]$, $\mathbf{A} = \mathrm{Adu}_{\mathbf{k},f} = \mathbf{k}[x_1, \ldots, x_p]$, $\mathbf{k}[\alpha] = \mathbf{k}[T]/\langle f \rangle$, such that $T - a = (T - \alpha)^p$. Let $\varphi : \mathbf{A} \twoheadrightarrow \mathbf{k}[\alpha]$ be the $\mathbf{k}$-morphism $x_i \mapsto \alpha$. Make the ideal $\mathrm{Ker}\,\varphi$ explicit and describe the structure of the $\mathbf{k}$-algebra $\mathbf{A}$.
NB: if $\mathbf{k}$ is a discrete field and a is not a p^{th} power in $\mathbf{k}$, by Exercise III-10, the polynomial $f(T)$ is irreducible and $\mathbf{k}[\alpha]$ is a field of decomposition of f over $\mathbf{k}$.

Exercise 10.
(The trinomial $T^5 + 5bT \pm 4b$ where $b = 5a^2 - 1$, with Galois group A_5*)*
Consider a trinomial $T^5 + bT + c$. We will determine b, c such that its discriminant is a square and obtain an irreducible polynomial with Galois group A_5 as an illustration of the modular method.
We use the equality $\mathrm{disc}_T(T^5 + bT + c) = 4^4b^5 + 5^5c^4$ (see Problem III-1).

1. To force the discriminant into being a square in $\mathbb{Z}$, explain why what follows is reasonable: $b \leftarrow 5b$, $c \leftarrow 4c$, then $f_a(T) = T^5 + 5(5a^2 - 1)T \pm 4(5a^2 - 1)$. The discriminant is then the square $2^8 5^6 a^2 (5a^2 - 1)^4$.

2. Taking $a = 1$, we obtain $f_1(T) = T^5 + 20T \pm 16$ in $\mathbb{Z}[T]$. By examining the factorizations of f_1 modulo 3 and 7, show that f_1 is irreducible with Galois group A_5. Deduce that for $a \equiv 1 \bmod 21$, f_a is irreducible with Galois group A_5. Show that the same thing holds for f_a given as a polynomial with coefficients in the field of rational fractions $\mathbb{Q}(a)$.

Exercise 11. *(When a resolvent admits a zero in the base field)*
In the context of 6.1 let $y \in \mathbf{B}$, $G.y = \{y_1, \ldots, y_r\}$ and $g(T) = \mathrm{Rv}_{G,y}(T)$.

1. Suppose that $a \in \mathbf{K}$ is a simple zero of g.
   a. $\mathfrak{c} = \langle y - a \rangle_{\mathbf{B}}$ is a Galoisian ideal of $(\mathbf{K}, \mathbf{B}, G)$.
   b. If $\beta : \mathbf{B} \to \mathbf{C} = \mathbf{B}/\mathfrak{c}$ is the canonical projection, and if $H = \mathrm{St}_G(\mathfrak{c})$ is the new approximation of the Galois group, then $\beta(y_1) = a$ and for $j \neq 1$, Rv_{H,y_j} divides $g(T)/(T - a)$ (as usual we identify $\mathbf{K}$ with a subfield of $\mathbf{B}$ and $\beta(\mathbf{K})$ with a subfield of $\mathbf{C}$).
2. Suppose that $a \in \mathbf{K}$ is a zero of g with multiplicity k.
   a. There exist $j_2, \ldots, j_k \in [\![2..r]\!]$ such that $\mathfrak{c} = \langle y_1 - a, y_{j_2} - a, \ldots, y_{j_k} - a \rangle$ is a minimal Galoisian ideal among those that contain $y - a$.
   Let $j_1 = 1$. Show that, for $j \neq j_1, \ldots, j_k$, $y_j - a$ is invertible modulo $\mathfrak{c}$.
   b. Let $\beta : \mathbf{B} \to \mathbf{C} = \mathbf{B}/\mathfrak{c}$ be the canonical projection, and $H = \mathrm{St}_G(\mathfrak{c})$.
   Then $\beta(y_{j_1}) = \cdots = \beta(y_{j_k}) = a$, and for $j \neq j_1, \ldots, j_k$, the resolvent Rv_{H,y_j} divides $g(T)/(T - a)^k$.
3. Suppose that $\mathfrak{c}$ is a Galoisian ideal of $\mathbf{B}$ and that $\mathrm{St}_G(y)$ contains $\mathrm{St}_G(\mathfrak{c})$, then $g(T)$ admits a zero in $\mathbf{K}$.

Remark. Item *1* justifies the "Jordan method" for the computation of the Galois group. See page 443. ■

Exercise 12. *(When we know the decomposition into prime factors of a separable resolvent)* In the context of 6.1 let $y \in \mathbf{B}$ and $G.y = \{y_1, \ldots, y_r\}$.
Suppose that $\mathrm{Rv}_{G,y} = \mathrm{Min}_y = R_1 \cdots R_\ell$, with the R_i being irreducible and $\ell > 1$. Compute a Galoisian idempotent e of $\mathbf{B}$ with the following properties, where we let $(\mathbf{K}, \mathbf{C}, H)$ be the corresponding Galois quotient and $\beta : \mathbf{B} \to \mathbf{C}$ be the canonical projection.

1. For each $i \in [\![1..r]\!]$, the polynomial $\mathrm{Min}_{\beta(y_i)}$ is equal to one of the R_j's.
2. The group H operates over $\{\beta(y_1), \ldots, \beta(y_r)\}$.

3. The orbits are of length $d_1 = \deg(R_1), \ldots, d_\ell = \deg(R_\ell)$.
4. This situation recurs in every Galois quotient of $(\mathbf{K}, \mathbf{C}, H)$.

Remark. Exercise 12 is the basis of the "McKay-Soicher method" for the computation of the Galois group. See page 443. ■

Exercise 13. *(When a minimal polynomial strictly divides a resolvent)*
In the context of 6.1 let $y \in \mathbf{B}$ and $G.y = \{y_1, \ldots, y_r\}$.
Suppose that $g(T) = \mathrm{Rv}_{G,y}(T) \neq \mathrm{Min}_y(T)$. Let $(\mathbf{K}, \mathbf{C}, H)$ be a Galois quotient (with the canonical projection $\beta : \mathbf{B} \to \mathbf{C}$) in which each $\beta(y_i)$ admits a minimal polynomial equal to its resolvent.
Show that for the different zeros $\beta(y_j)$ of $g_1(T) = \mathrm{Min}_{\beta(y_1)}(T)$ in $\mathbf{C}$, the fibers $\beta^{-1}\big(\beta(y_j)\big)$ all have the same number of elements, say n_1.
In addition, $g_1^{n_1}$ divides g and $g/g_1^{n_1}$ is comaximal with g_1.

Some solutions, or sketches of solutions

Exercise 2. *1.* This results from the fact that a connected zero-dimensional ring is local and from the fact that, by **LEM**, we know the indecomposable idempotents of the algebra, which form a fundamental system of orthogonal idempotents.

2. In the case of an algebra $\mathbf{K}[X]/\langle f \rangle$ with separable f, finding the idempotents is the same as factoring the polynomial. But there does not exist any general factorization algorithm for separable polynomials.

3. A constructive version consists in asserting that, concerning a computation, we can always "act as though" the result (proven by means of **LEM**) were true. This *dynamic version* is expressed as follows.
Let $\mathbf{K}$ *be a zero-dimensional ring (special case: a discrete field).*
Let $(x_i)_{i \in I}$ *be a finite family of elements in an integral* $\mathbf{K}$*-algebra* $\mathbf{B}$ *(special case: a finite* $\mathbf{K}$*-algebra).*
There exists a fundamental system of orthogonal idempotents $(e_1, \ldots, e_n)$ *such that in each component* $\mathbf{B}/\langle 1 - e_j \rangle$*, each* x_i *is nilpotent or invertible.*
We prove this result as follows: Lemma VI-3.14 tells us that $\mathbf{B}$ is zero-dimensional; we conclude by the zero-dimensional splitting lemma (Lemma IV-8.10).

Exercise 4. We easily check that the $\mathbb{Z}$-syzygy module between the matrices P_1, …, P_6 is generated by $(1, 1, 1, -1, -1, -1)$. We will also use the fact that the number of monomials of degree d in n variables is $\binom{d+n-1}{n-1}$.

1a. Let $S(Y, Z) = \sum_{i+j=m-1} Y^i Z^j$, so $Y^m - Z^m = (Y - Z)S(Y, Z)$. In this equality, we make $Y = U_1U_2U_3$, $Z = U_4U_5U_6$. We obtain the desired result by multiplying by $U_1^{a-m}U_2^{b-m}U_3^{c-m}U_4^dU_5^eU_6^f$.

1b. We clearly have $\mathfrak{a} \subseteq \operatorname{Ker} \varphi$. The equality $\mathbf{k}[\underline{U}] = \mathfrak{a} + \mathfrak{a}^\bullet$ results from item *1a.* It therefore suffices to see that $\operatorname{Ker} \varphi \cap \mathfrak{a}^\bullet = \{0\}$, i.e. that the restriction of φ to $\mathfrak{a}^\bullet$ is injective. As φ transforms a monomial into a monomial, it suffices to see that if two monomials $U_1^a \cdots U_6^f$ and $U_1^{a'} \cdots U_6^{f'} \in \mathfrak{a}^\bullet$ have the same image under φ, then they are equal.

We have $(a,b,c,\dots,f) = (a',b',c',\dots,f') + k(1,1,1,-1,-1,-1)$ with $k \in \mathbb{Z}$, and as $\min(a,b,c) = \min(a',b',c') = 0$, we have $k = 0$, which gives the equality of the two monomials.

1c. The number M_d that we are searching for is the dimension over $\mathbf{k}$ of the homogeneous component of degree d of $\mathbf{k}[\underline{x}^{P_1},\dots,\underline{x}^{P_6}]$ or (via φ) that of $\mathfrak{a}_d^\bullet$.
But we also have $\mathbf{k}[\underline{U}] = \mathfrak{b} \oplus \mathfrak{a}^\bullet$ where $\mathfrak{b}$ is the (monomial) ideal generated by the monomials divisible by $U_1U_2U_3$ (in some way, $\mathfrak{b}$ is an initial ideal of $\mathfrak{a}$).
We therefore have $\mathbf{k}[\underline{U}]_d = \mathfrak{b}_d \oplus \mathfrak{a}_d^\bullet$ and

$$\dim_{\mathbf{k}} \mathbf{k}[\underline{U}]_d = \tbinom{d+5}{5}, \quad \dim_{\mathbf{k}} \mathfrak{b}_d = \tbinom{d+5-3}{5}, \quad M_d = \dim_{\mathbf{k}} \mathfrak{a}_d^\bullet = \tbinom{d+5}{5} - \tbinom{d+2}{5}.$$

2a. We define V_2, V_3 by $U_2 = U_1 + V_2$, $U_3 = U_1 + V_3$.
The polynomial $U_1U_2U_3 - U_4U_5U_6$ given in $\mathbf{k}[U_1,V_2,V_3,U_4,U_5,U_6]$ becomes monic in U_1 of degree 3. We leave it up to the reader to check the other details.

2b. The number we are looking for is also $M_d = \dim_{\mathbf{k}} \mathbf{B}_d$. But we have

$$\mathbf{B}_d = \mathbf{A}_d \oplus \mathbf{A}_{d-1}u_1 \oplus \mathbf{A}_{d-2}u_1^2 \simeq \mathbf{A}_d \oplus \mathbf{A}_{d-1} \oplus \mathbf{A}_{d-2}.$$

It suffices to use the fact that $\mathbf{A}$ is a polynomial ring over $\mathbf{k}$ with 5 indeterminates. As an indication, for $d = 0$, 1, 2, 3, 4, 5, $M_d = 1$, 6, 21, 55, 120, 231.

3a. The $\mathbb{Z}$-module E is free of rank 5: 5 arbitrary matrices among $\{P_1,\dots,P_6\}$ form a $\mathbb{Z}$-basis of it.

3b. Since $P_1 + P_2 + P_3 = P_4 + P_5 + P_6$, we have

$$\mathbf{B}_{11} = \mathbf{k}[\underline{x}^{P_1}][\underline{x}^{\pm P_2},\underline{x}^{\pm P_3},\underline{x}^{\pm P_4},\underline{x}^{\pm P_5}] = \mathbf{k}[\underline{x}^{P_6}][\underline{x}^{\pm P_2},\underline{x}^{\pm P_3},\underline{x}^{\pm P_4},\underline{x}^{\pm P_5}].$$

We then see that $\mathbf{B}_{11}$ is a localized ring of $\mathbf{k}[\underline{x}^{P_1},\underline{x}^{P_2},\underline{x}^{P_3},\underline{x}^{P_4},\underline{x}^{P_5}]$, which is a polynomial ring with 5 indeterminates over $\mathbf{k}$, so integrally closed.

3c. We define $\mathbf{B}_{ij}$ such that it is contained in $\mathbf{k}[\,\underline{x}^M \mid M \in E,\ m_{ij} \geqslant 0\,]$. For example, for $(i,j) = (3,1)$, the matrices P_k with a null coefficient in position $(3,1)$ are those other than P_3, P_5, which leads to the definition of $\mathbf{B}_{31}$:

$$\mathbf{B}_{31} = \mathbf{k}[\underline{x}^{P_3},\underline{x}^{P_5}][\underline{x}^{\pm P_1},\underline{x}^{\pm P_2},\underline{x}^{\pm P_4},\underline{x}^{\pm P_6}].$$

We then have the equality $\mathbf{B} = \bigcap_{i,j} \mathbf{B}_{ij}$, and as the $\mathbf{B}_{ij}$'s are all integrally closed with the same quotient field $\mathrm{Frac}\,\mathbf{B}$, the ring $\mathbf{B}$ is integrally closed.

Exercise 6. *2.* We write $U = {}^{\mathrm{t}}MM$ and take the determinant.
This gives $\mathrm{Disc}_{\mathbf{k}}\,\mathbf{A} = \mathrm{disc}(f)^{n!/2}$ from $\det(M) = \delta^{n!/2}$. Conversely, since this is a matter of algebraic identities in $\mathbb{Z}[\underline{x}]$, the equality $(\det M)^2 = (\delta^{n!/2})^2$ implies $\det M = \pm\delta^{n!/2}$.

3. In Theorem 4.12, let us not assume that f is separable over $\mathbf{C}$. By hypothesis, we have $\varphi(f)(T) = \prod_{i=1}^n (T - u_i)$.
With $\mathbf{A} = \mathbf{k}[x_1,\dots,x_n] = \mathrm{Adu}_{\mathbf{k}}(f)$, we then have a morphism of $\mathbf{C}$-algebras $\Phi : \mathbf{C} \otimes_{\mathbf{k}} \mathbf{A} \to \mathbf{C}^{n!}$ which performs $1 \otimes x_i \mapsto (u_{\sigma(i)})_{\sigma \in \mathrm{S}_n}$.
The canonical $\mathbf{k}$-basis $\mathcal{B}(f)$ of $\mathbf{A}$ is a $\mathbf{C}$-basis of $\mathbf{C} \otimes_{\mathbf{k}} \mathbf{A}$ and the matrix of Φ for this basis (at the start) and for the canonical basis of $\mathbf{C}^{n!}$ (at the end) is the above matrix M where x_i is replaced by u_i. We deduce that Φ is an isomorphism if and only if $\varphi\big(\mathrm{disc}(f)\big) \in \mathbf{C}^\times$, i.e. if f is separable over $\mathbf{C}$.

Finally, let us only suppose that an algebra $\varphi : \mathbf{k} \to \mathbf{C}$ diagonalizes $\mathbf{A}$. This means that we give $n!$ characters $\mathrm{Adu}_{\mathbf{C},\varphi(f)} \to \mathbf{C}$ which, when put together, give an isomorphism of $\mathbf{C}$-algebras of $\mathrm{Adu}_{\mathbf{C},\varphi(f)}$ over $\mathbf{C}^{n!}$.

Since there exists a character $\mathrm{Adu}_{\mathbf{C},\varphi(f)} \to \mathbf{C}$, the polynomial $\varphi(f)(T)$ completely factorizes in $\mathbf{C}$.
Finally, the discriminant of the canonical basis of $\mathrm{Adu}_{\mathbf{C},\varphi(f)}$ is $\varphi\big(\operatorname{disc}(f)\big)^{n!/2}$ and the discriminant of the canonical basis of $\mathbf{C}^{n!}$ is 1. Therefore, f is separable over $\mathbf{C}$.

Exercise 7. We have $\mathbf{A} = \mathbf{k}[X_1,\dots,X_n]/\langle S_1,\dots,S_n\rangle$ where S_1, …, S_n are the n elementary symmetric functions of $(X_1,\dots,X_n)$; the ideal $\langle S_1,\dots,S_n\rangle$ being homogeneous, the $\mathbf{k}$-algebra $\mathbf{A}$ is graded (by the degree). Let $\mathbf{A}_d$ be its homogeneous component of degree d and $\mathfrak{m} = \langle x_1,\dots,x_n\rangle$; we therefore have $\mathbf{A} = \mathbf{A}_0 \oplus \mathbf{A}_1 \oplus \mathbf{A}_2 \oplus \dots$ with $\mathbf{A}_0 = \mathbf{k}$ and

$$\mathfrak{m}^d = \mathbf{A}_d \oplus \mathbf{A}_{d+1} \oplus \dots, \qquad \mathfrak{m}^d = \mathbf{A}_d \oplus \mathfrak{m}^{d+1}.$$

Since $x_i^n = 0$, we have $\mathfrak{m}^{n(n-1)+1} = 0$, so $\mathbf{A}_d = 0$ for $d \geqslant n(n-1)+1$. Recall the basis $\mathcal{B}(f)$ of $\mathbf{A}$, formed from the elements $x_1^{\alpha_1}\dots x_n^{\alpha_n}$ with $0 \leqslant \alpha_i < n-i$. For all d, the homogeneous component $\mathbf{A}_d$ of degree d is a free $\mathbf{k}$-module whose basis is the set of the $x_1^{\alpha_1}\dots x_n^{\alpha_n}$ with $0 \leqslant \alpha_i < n-i$ and $|\alpha| = d$. The cardinality of this basis is the coefficient of degree d in the polynomial $S(t) \in \mathbb{Z}[t]$

$$S(t) = 1(1+t)(1+t+t^2)\cdots(1+t+\cdots+t^{n-1}) = \textstyle\prod_{i=1}^{n} \dfrac{t^i-1}{t-1}.$$

Indeed, a multi-index $(\alpha_1,\dots,\alpha_n)$ such that $0 \leqslant \alpha_i < n-i$ and $|\alpha| = d$ is obtained by choosing a monomial t^{α_n} of the polynomial $1+t+\cdots+t^{n-1}$, a monomial $t^{\alpha_{n-1}}$ of the polynomial $1+t+\cdots+t^{n-2}$ and so on, the product of these monomials being t^d. We thus obtain the Hilbert-Poincaré series $S_{\mathbf{A}}(t)$ of $\mathbf{A}$,

$$S_{\mathbf{A}}(t) \overset{\text{def}}{=} \textstyle\sum_{i=0}^{\infty} \dim_{\mathbf{k}} \mathbf{A}_d\ t^d \overset{\text{here}}{=} \sum_{0 \leqslant \alpha_i < n-i} t^{|\alpha|} = S(t).$$

The polynomial S is a monic polynomial of degree $e = 1+\cdots+n-1 = n(n-1)/2$. We have $S(1) = n!$, in accordance with $S(1) = \dim_{\mathbf{k}} \mathbf{A}$.

Variant. Let $\mathbf{B} = \mathbf{k}[S_1,\dots,S_n] \subset \mathbf{C} = \mathbf{k}[X_1,\dots,X_n]$.
Then $\mathbf{C}$ is a free $\mathbf{B}$-module with the $\underline{X}^\alpha = X_1^{\alpha_1}\cdots X_n^{\alpha_n}$ as its basis, with $0 \leqslant \alpha_i < n-i$. This basis is above the basis $\mathcal{B}(f)$ of $\mathbf{A}$ over $\mathbf{k}$ if we consider that we have a commutative diagram where each vertical arrow is a reduction modulo $\langle S_1,\dots,S_n\rangle$.

$$\begin{tikzcd}
\mathbf{B} \arrow[r] \arrow[d, two heads] & \mathbf{C} \arrow[d, two heads] \\
\mathbf{k} \arrow[r] & \mathbf{A}
\end{tikzcd}$$

Writing $\mathbf{C} = \bigoplus_{\alpha} \mathbf{B}\underline{X}^\alpha$, with the shift $S_{\mathbf{B}\underline{X}^\alpha}(t) = t^{|\alpha|}S_{\mathbf{B}}(t)$, we have the following equality between the Hilbert-Poincaré series

$$S_{\mathbf{C}} = S_{\mathbf{A}}\ S_{\mathbf{B}} \qquad \text{with} \qquad S_{\mathbf{A}} = \textstyle\sum_{0 \leqslant \alpha_i < n-i} t^{|\alpha|}.$$

However, it is easy to see that

$$S_{\mathbf{C}}(t) = \tfrac{1}{(1-t)^n},\ S_{\mathbf{B}}(t) = \textstyle\prod_{d=1}^{n} \tfrac{1}{1-t^d}, \ \text{ and so } \ S_{\mathbf{A}}(t) = \dfrac{S_{\mathbf{C}}}{S_{\mathbf{B}}} = \textstyle\prod_{d=1}^{n} \dfrac{1-t^d}{1-t},$$

once again giving us the result for $S_{\mathbf{A}}$.

Let us now move onto the powers of the ideal $\mathfrak{m}$.
Let $\varphi : \mathbf{A} \twoheadrightarrow \mathbf{k}$ be the character $x_i \mapsto 0$ with kernel $\mathfrak{m} = \langle x_1,\dots,x_n\rangle$.
We have $\mathbf{A} = \mathbf{k}[x_1,\dots,x_n] = \mathbf{k} \oplus \mathfrak{m}$, $\mathfrak{m} \subseteq \mathrm{D}_{\mathbf{A}}(0) \subseteq \mathrm{Rad}(\mathbf{A})$ and for $z \in \mathbf{A}$,

$$z \in \mathbf{A}^\times \iff \varphi(z) \in \mathbf{k}^\times \iff z \in \mathbf{k}^\times \oplus \mathfrak{m}.$$

We have $\mathrm{D}_{\mathbf{A}}(0) = \mathrm{D}_{\mathbf{k}}(0) \oplus \mathfrak{m}$, $\mathrm{Rad}(\mathbf{A}) = \mathrm{Rad}(\mathbf{k}) \oplus \mathfrak{m}$.
Since $\mathfrak{m} \subseteq \mathrm{Rad}(\mathbf{A})$ is finitely generated, we have

$$\mathfrak{m}^d = \mathfrak{m}^{d+1} \iff \mathfrak{m}^d = 0$$

(Lemma IX-3.2), which, since $\mathfrak{m}^d = \mathbf{A}_d \oplus \mathfrak{m}^{d+1}$, is equivalent to $\mathbf{A}_d = 0$. We deduce that $\mathfrak{m}^{e+1} = 0$.

Remark. if $\mathbf{k}$ is local, then so is $\mathbf{A}$, and $\mathrm{Rad}\,\mathbf{A} = \varphi^{-1}(\mathrm{Rad}\,\mathbf{k})$. ■

Exercise 8. Consider the polynomial ring $\mathbf{C} = \mathbf{k}[a_1, \ldots, a_n, b_1, \ldots, b_m]$, let $f(X) = 1 + \sum_{i=1}^n a_i X^i$, $g(X) = 1 + \sum_{j=1}^m b_j X^j$, and $\mathfrak{c} = \mathrm{c}_{\mathbf{C}}(fg - 1)$. We assign to a_i the weight i and to b_j the weight j. The coefficient of degree k of $fg-1$ is homogeneous of degree k, so the ideal $\mathfrak{c}$ is homogeneous.
Let $\mathbf{C}' = \mathbf{C}/\mathfrak{c}$. This $\mathbf{k}$-algebra $\mathbf{C}'$ is graded via the above weight and we must show that $\mathbf{C}'_d = 0$ for $d > nm$. It is clear that $\mathbf{C}'_d = 0$ for large enough d. We will determine the Hilbert-Poincaré series $S_{\mathbf{C}'}$ of $\mathbf{C}'$ (which here is a polynomial)

$$S_{\mathbf{C}'}(t) \overset{\mathrm{def}}{=} \sum\nolimits_{d \geqslant 0} \dim_{\mathbf{k}} \mathbf{C}'_d\, t^d = \frac{\prod_{d=1}^{n+m}(1-t^d)}{\prod_{i=1}^{n}(1-t^i)\prod_{j=1}^{m}(1-t^j)} .$$

To prove this equality, we construct $\mathbf{C}$ and $\mathbf{C}'$ in a different way.
We consider $n+m$ indeterminates $(X_1, \ldots, X_n, Y_1, \ldots, Y_m)$, and let $(a_1, \ldots, a_n)$ be the elementary symmetric functions of $(X_1, \ldots, X_n)$, and $(b_1, \ldots, b_m)$ be the elementary symmetric functions of $(Y_1, \ldots, Y_m)$. Since
$\prod_{i=1}^n (T + X_i) \prod_{j=1}^m (T + Y_j) = (T^n + a_1 T^{n-1} + \cdots + a_n)(T^m + b_1 T^{m-1} + \cdots + b_m)$,
we see, by letting $a_0 = b_0 = 1$, that $\sum_{i+j=d} a_i b_j$ is the d^{th} elementary symmetric function of $(X_1, \ldots, X_n, Y_1, \ldots, Y_m)$. As $(a_1, \ldots, a_n, b_1, \ldots, b_m)$ are algebraically independent over $\mathbf{k}$, we can consider that $\mathbf{C}$ is the following graded subalgebra

$$\mathbf{C} = \mathbf{k}[a_1, \ldots, a_n, b_1, \ldots, b_m] \subset \mathbf{D} = \mathbf{k}[X_1, \ldots, X_n, Y_1, \ldots, Y_m],$$

and that the ideal $\mathfrak{c}$ of $\mathbf{C}$ is generated by the $n+m$ sums $\sum_{i+j=d} a_i b_j$, which are the elementary symmetric functions of $(X_1, \ldots, X_n, Y_1, \ldots, Y_m)$.
The algebra $\mathbf{D}$ is free over $\mathbf{C}$ of rank $n!m!$, as for a double universal splitting algebra. More precisely, here are some bases.
The $\underline{X}^\alpha = X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ for $0 \leqslant \alpha_i < n - i$ form a basis of $\mathbf{k}[\underline{X}]$ over $\mathbf{k}[\underline{a}]$.
The $\underline{Y}^\beta = Y_1^{\beta_1} \cdots Y_m^{\beta_m}$ with $0 \leqslant \beta_j < m - j$ form a basis of $\mathbf{k}[\underline{Y}]$ over $\mathbf{k}[\underline{b}]$.
Thus, the $\underline{X}^\alpha \underline{Y}^\beta$ form a basis of $\mathbf{D} = \mathbf{k}[\underline{X}, \underline{Y}]$ over $\mathbf{C} = \mathbf{k}[\underline{a}, \underline{b}]$.
Finally, by the scalar extension $\mathbf{C} \to \mathbf{C}' = \mathbf{C}/\mathfrak{c}$, the $\underline{x}^\alpha \underline{y}^\beta$ form a basis of $\mathbf{D}' = \mathbf{D}/\mathfrak{c}\mathbf{D} = \mathbf{k}[\underline{x}, \underline{y}]$ over $\mathbf{C}'$.

$$\begin{tikzcd} \mathbf{C} \arrow[r] \arrow[d, two heads] & \mathbf{D} \arrow[d, two heads] \\ \mathbf{C}' \arrow[r] & \mathbf{D}' \end{tikzcd}$$

We have a commutative diagram at our disposal where each vertical arrow is a reduction modulo $\mathfrak{c}$. Our aim is to determine the Hilbert-Poincaré series $S_{\mathbf{C}'}$ of $\mathbf{C}'$ given that we know those of $\mathbf{D}'$, $\mathbf{C}$ and $\mathbf{D}$ (because $\mathbf{C}$ and $\mathbf{D}$ are polynomial rings, and $\mathbf{D}'$ is the universal splitting algebra of T^{n+m} over $\mathbf{k}$).
We conclude the computations in the following simple manner.
We write $\mathbf{D} = \bigoplus_{\alpha,\beta} \mathbf{C}\, \underline{X}^\alpha \underline{Y}^\beta$, so

$$S_{\mathbf{D}}(t) = F(t) S_{\mathbf{C}}(t) \quad \text{with} \quad F(t) = \sum\nolimits_{\alpha,\beta} t^{|\alpha|+|\beta|} = \sum\nolimits_\alpha t^{|\alpha|} \sum\nolimits_\beta t^{|\beta|},$$

and we also have $S_{\mathbf{D}'}(t) = F(t)S_{\mathbf{C}'}(t)$. We have seen in Exercise 7 that

$$F(t) = \prod\nolimits_{i=1}^{n} \tfrac{1-t^i}{1-t} \prod\nolimits_{j=1}^{m} \tfrac{1-t^j}{1-t}, \qquad S_{\mathbf{D}'}(t) = \prod\nolimits_{d=1}^{n+m} \tfrac{1-t^d}{1-t}.$$

Then let $S_d(t) = (1-t^d)/(1-t)$. It is a polynomial of degree $d-1$ and $S_d(1) = d$. We have therefore obtained

$$S_{\mathbf{C}'}(t) = \frac{S_1 S_2 \cdots S_{n+m}}{S_1 S_2 \cdots S_n \, S_1 S_2 \cdots S_m},$$

with

$$\deg S_{\mathbf{C}'} = \frac{(n+m-1)(n+m) - (n-1)n - m(m-1)}{2} = nm.$$

Thus, as desired, $\mathbf{C}'_k = 0$ for $k > nm$.
Please note that $\dim_{\mathbf{k}} \mathbf{C}' = S_{\mathbf{C}'}(1) = \binom{n+m}{n}$.

Exercise 9. For each $i \in [\![1..p]\!]$ the restriction $\varphi : \mathbf{k}[x_i] \to \mathbf{k}[\alpha]$ is an isomorphism. Consider the ideal

$$\mathfrak{m} = \langle x_i - x_j, i, j \in [\![1..p]\!] \rangle = \langle x_1 - x_i, i \in [\![2..p]\!] \rangle .$$

Then $\mathbf{A} = \mathbf{k}[x_1] \oplus \mathfrak{m}$, hence $\mathfrak{m} = \operatorname{Ker} \varphi$.
Actually we can regard $\mathbf{A}$ as the universal splitting algebra $\operatorname{Adu}_{\mathbf{k}[x_1],g}$ for the polynomial $g(T) = f(T)/(T - x_1) = (T - x_1)^{p-1}$ over the ring $\mathbf{k}[x_1]$ which brings us back to Exercise 7. In particular

$$\mathfrak{m}^{1+(p-1)(p-2)/2} = 0, \ \mathrm{D}_{\mathbf{A}}(0) = \mathrm{D}_{\mathbf{k}[x_1]}(0) \oplus \mathfrak{m} \text{ and } \operatorname{Rad}(\mathbf{A}) = \operatorname{Rad}(\mathbf{k}[x_1]) \oplus \mathfrak{m}.$$

Exercise 10. *1.* The goal of the operation $b \leftarrow 5b$, $c \leftarrow 4c$ is to replace $4^4 b^5 + 5^5 c^4$ by $4^4 5^5 (b^5 + c^4)$; by imposing $c = \pm b$, we obtain $4^4 5^5 b^4 (b+1)$ which is easy to turn into a square by imposing $5(b+1) = a^2$. To avoid the denominator 5, we impose $5(b+1) = (5a)^2$ instead, i.e. $b = 5a^2 - 1$.

2. For $a \in \mathbb{Q}^\star$, the polynomial $f_a(T) \in \mathbb{Q}[T]$ is separable. Modulo the small prime numbers we find the following decompositions of $f_1(T) = T^5 + 20T + 16\varepsilon$, with $\varepsilon \in \{\pm 1\}$, into irreducible factors

$$\begin{array}{lll}
\text{mod} \ 2 & : & T^5 \\
\text{mod} \ 3 & : & f_1(T) \\
\text{mod} \ 5 & : & (T+\varepsilon)^5 \\
\text{mod} \ 7 & : & (T+2\varepsilon)(T+3\varepsilon)(T^3 + 2\varepsilon T^2 + 5T + 5\varepsilon)
\end{array}$$

The result modulo 3 proves that $f_1(T)$ is irreducible over $\mathbb{Z}$. Its Galois group G is a transitive subgroup of A_5 that contains a 3-cycle (given the reduction modulo 7). This implies $G = \mathrm{A}_5$. Indeed, a transitive subgroup of S_5 containing a 3-cycle is equal to S_5 or A_5. As for $\mathbb{Q}(a)$ as a base field, the polynomial $f_a(T)$ is irreducible in $\mathbb{Q}[a][T]$ since its reduction modulo $a = 1$ is irreducible in $\mathbb{Q}[T]$. Therefore it is irreducible in $\mathbb{Q}(a)[T]$. Using the fact that its discriminant is a square and the reduction modulo $a = 1$, we obtain that its Galois group is A_5.
The readers might ask themselves the following question: For every $a \in \mathbb{Z} \setminus \{0\}$, is the polynomial $f_a(T)$ irreducible with Galois group A_5?

Possible experiment.
Here is the distribution of the types of permutation of the transitive subgroups

of S_5.

For the 7 types that appear in S_5, we use the following notation

$$t_1 = (1^5),\ t_2 = (2, 1^3),\ t_{22} = (2^2, 1),\ t_3 = (3, 1^2),\ t_{3,2} = (3, 2),\ t_4 = (4, 1),\ t_5 = (5).$$

Thus t_{22} is the type of the double-transpositions, t_3 that of the 3-cycles, etc… The announced table:

G	C_5	$\mathbb{ASL}_1(\mathbb{F}_5)$	$\mathbb{AGL}_1(\mathbb{F}_5)$	A_5	S_5
$\#G$	5	10	20	60	120
	$t_1^1\ t_5^4$	$t_1^1\ t_{22}^5\ t_5^4$	$t_1^1\ t_{22}^5\ t_4^{10}\ t_5^4$	$t_1^1\ t_{22}^{15}\ t_3^{20}\ t_5^{24}$	$t_1^1\ t_2^{10}\ t_{22}^{15}\ t_3^{20}\ t_{32}^{20}\ t_4^{30}\ t_5^{24}$

For example in the last row, under A_5, $t_1^1\ t_{22}^{15}\ t_3^{20}\ t_5^{24}$ means that A_5 contains the identity, 15 double-transpositions, 20 3-cycles and 24 5-cycles ($1{+}15{+}20{+}24 = 60$).

The reader will be able to experimentally test Cebotarev's density theorem with the help of a Computer Algebra system. We must examine the factorization of $f_1(T)$ modulo "a lot" of primes p and compare the distribution obtained from the types of factorization with that of the types of permutation of A_5.

The author of the exercise has considered the first 120 prime numbers — other than 2 and 5 which divide $\mathrm{disc}(f_1)$ — and his program has found the following distribution

$$t_{22}^{33}\ t_3^{38}\ t_5^{49}.$$

This means that we have found a factorization of type t_{22} (2 irreducible factors of degree 2, 1 irreducible factor of degree 1) 33 times, a factorization of type t_3 38 times and a factorization of type t_5 49 times (no factorization of type t_1). A distribution to be compared with that of A_5. As for the type t_1, the smallest prime p for which $f_1(T) \bmod p$ is entirely decomposed is $p = 887$. Finally, when treating 1200 primes instead of 120, we find the distribution

$$t_1^{16}\ t_{22}^{304}\ t_3^{428}\ t_5^{452}.$$

Exercise 11. *1a.* We need to show that $\langle y_1 - a\rangle + \langle y_j - a\rangle = \langle 1\rangle$ for $j \in [\![2..r]\!]$. For example in the quotient $\mathbf{B}/\langle y_1 - a, y_2 - a\rangle$ the polynomial $g(T) = \prod(T - y_j)$ has two factors equal to $T - a$ which implies that $g'(a) = 0$. As $g'(a)$ is invertible by hypothesis (which remains true in a quotient), we indeed have $0 = 1$ in the quotient.

1b. We easily see that $H = \mathrm{St}(y_1)$. Therefore H operates over $\{\beta(y_2), \dots, \beta(y_r)\}$. However, $g(T)/(T - y_1) = \prod_{j=2}^{r}(T - y_j)$ in $\mathbf{B}$, so $g(T)/(T - a) = \prod_{j=2}^{r}\big(T - \beta(y_j)\big)$ in $\mathbf{C}$.

2a. It is clear that $y_1 - a$ is a nonzero zerodivisor in $\mathbf{B}$. A minimal Galoisian ideal $\mathfrak{c}$ containing $\langle y_1 - a\rangle$ is obtained by adding as many conjugates of $\langle y_1 - a\rangle$ as possible under the condition of not reaching the ideal $\langle 1\rangle$. The ideal $\mathfrak{c}$ is therefore of the form $\langle y_j - a \,|\, j \in J\rangle$ for a subset J of $[\![1..r]\!]$. It remains to see if the number of j's such that $y_j - a \in \mathfrak{c}$ is k. However, for every index j, the element $y_j - a$ is null or invertible modulo $\mathfrak{c}$. Since $g(T) = \prod_j \big(T - \beta(y_j)\big)$, and since a is a zero with multiplicity k of g, the number of j's such that $\beta(y_j) = a$ is equal to k (let $g(a) = g'(a) = \cdots = g^{(k-1)}(a) = 0$ and $g^{(k)}(a)$ be invertible).

2b. Reason as in *1b.*

3. The Galois quotient $\mathbf{C} = \mathbf{B}/\mathfrak{c}$ is obtained with its group $H = \mathrm{St}_G(\mathfrak{c})$. By hypothesis $\overline{y_1} \in \mathrm{Fix}(H)$ so $\overline{y_1} \in \mathbf{K}$. Let a be the element of $\mathbf{K}$ in question. In $\mathbf{C}$ we have $g(T) = \prod_j (T - \overline{y_j})$, so $g(a) = 0$. Finally, $\mathbf{K}$ is identified with its image in $\mathbf{C}$.

Example. Here is an example with $\deg f = 6$. We ask `Magma` to compute the minimal polynomial of $y = x_4 + x_5 x_6$, and then to factorize it. If g is the first factor, $z = g(y)$ is a nonzero zerodivisor. We launch Algorithm 6.5 with z. We therefore obtain the new approximations of the splitting field and of the Galois group by treating the oddity "z is a nonzero zerodivisor," but we can observe a posteriori that z has multiplicity 6 in its resolvent and that $\langle z \rangle$ is Galoisian.

```
f:= T^6 - 3*T^5 + 4*T^4 - 2*T^3 + T^2 - T + 1;
y:=x4+x5*x6; pm:=MinimalPolynomial(y);
  T^60 - 46*T^59 + 1035*T^58 - 15178*T^57 + 163080*T^56 + ... + 264613
Factorization(pm);
    <T^6 - 4*T^5 + 8*T^4 - 6*T^3 + T + 1, 1>,
    ...
z:=Evaluate(T^6 - 4*T^5 + 8*T^4 - 6*T^3 + T + 1,y);
20*x4^3*x5^3*x6^3 - 15*x4^3*x5^3*x6^2 - 15*x4^3*x5^2*x6^3 +
  11*x4^3*x5^2*x6^2 + 2*x4^3*x5^2*x6 + 2*x4^3*x5*x6^2 + x4^3*x5*x6 - ...
// z divides 0, we compute the new Galois quotient
Affine Algebra of rank 6 over Rational Field
Variables: x1, x2, x3, x4, x5, x6
Quotient relations:
  x1 + x2 + x3 - x6^5 + 2*x6^4 - x6^3 - x6^2 - 1,
  x2^2 + x2*x3 - x2*x6^5 + 2*x2*x6^4 - x2*x6^3 - x2*x6^2 - x2 + x3^2 -
      x3*x6^5 + 2*x3*x6^4 - x3*x6^3 - x3*x6^2 - x3 + x6^5 - 2*x6^4 +
      x6^3 + x6^2,
  x3^3 - x3^2*x6^5 + 2*x3^2*x6^4 - x3^2*x6^3 - x3^2*x6^2 - x3^2 +
      x3*x6^5 -  2*x3*x6^4 + x3*x6^3 + x3*x6^2 - x6^5 + 2*x6^4 - x6^3 -
      x6^2 + 1,
  x4 + x5 + x6^5 - 2*x6^4 + x6^3 + x6^2 + x6 - 2,
  x5^2 + x5*x6^5 - 2*x5*x6^4 + x5*x6^3 + x5*x6^2 + x5*x6 - 2*x5 -
      x6^4 + 2*x6^3 - x6^2 - x6,
  x6^6 - 3*x6^5 + 4*x6^4 - 2*x6^3 + x6^2 - x6 + 1
Permutation group G2 acting we have set of cardinality 6
Order = 72 = 2^3 * 3^2
    (1, 4)(2, 5)(3, 6)
    (1, 2)
    (2, 3)
Degree(MinimalPolynomial(z)); 55
#Orbit(z,G); 60
```

Exercise 12. Notice that the $y_i - y_j$'s for $i \neq j$ are invertible, and that this remains true in every Galois quotient.

Bibliographic comments

The dynamic method is clearly presented, for the first time it seems, in the article by Paul Lorenzen [136] published in 1953, which uses the equivalent of the closed covering principle XI-2.10. See on this subject articles [46] and [47].

Theorem 1.10 says that a polynomial ring over a zerodimensional reduced ring is stronbly discrete and coherent. It admits a remarkable generalization to strongly discrete coherent Prüfer rings: see [Yengui] and [72].

The versions that we have given of the Nullstellensatz "without algebraic closure" can be found in a related form in [MRR, VIII.2.4, VIII.3.3].

The intrinsic difficulty of the problem of the isomorphism of two algebraic closures of a field is illustrated in [170, Sander, Theorem 26], which shows that, in the presence of **LEM** but in the absence of the axiom of dependent choice, it is impossible to prove in ZF that two algebraic closures of $\mathbb{Q}$ are isomorphic.

The treatment of Galois theory based on Galois quotients of the universal splitting algebra dates back to Jules Drach [65, 1898] and to Ernest Vessiot [196, 1904]. Here is an extract of the introduction of the latter article, which speaks in the language of the time about Galois quotients of the universal splitting algebra:

"Étant donnée une equation algébrique, que l'on considère comme remplacée par le système (S) des relations entre les racines $x_1, \ldots, x_n$ et les coefficients, on étudie d'abord le problème fondamental suivant: *Quel parti peut-on tirer de la connaissance de certaines relations* (A) *entre* $x_1, \ldots, x_n$*, en n'employant que des opérations rationnelles?* Nous montrons que l'on peut déduire du système (S, A) un système analogue, dont le système (S, A) admet toutes les solutions, et qui est, comme nous le disons, *automorphe*: ce qui veut dire que ses diverses solutions se déduisent de l'une quelconque d'entre elles par les substitutions d'un groupe G, qui est dit *le groupe associé au système*, ou simplement le *groupe du système*. On remarquera que S est déjà un système automorphe, ayant le groupe général pour groupe associé. Dès lors, si l'on se place du point de vue de Galois, … on voit que l'on peut se limiter à ne considérer que des systèmes (S, A) rationnels and automorphes."[5]

[5] This quote translates as: "Given an algebraic equation, that we consider as replaced by the system (S) of relations between the roots $x_1, \ldots, x_n$ and the coefficients, we first study the following fundamental problem: *What subset can we extract from the knowledge of certain relations* (A) *between* $x_1, \ldots, x_n$*, by only employing rational operations?* We show that we can deduce from the system (S, A) an analogous system, for which the system (S, A) admits all the solutions, and which is, as we say, *automorphic*: which means that its diverse solutions are deduced from any one of them by the substitutions of a group G, which is said to be *the group associated with the system*, or simply the *group*

The universal splitting algebra is dealt with in considerable detail in Chapter 2 of the book [Pohst & Zassenhaus, 1989].

Among the good modern works that present all of classical Galois theory, we cite [Tignol] and [Cox].

The "dynamic Galois theory" presented in detail in this chapter is presented in [59, Díaz-Toca] and [63, 64, Díaz-Toca&al.].

Regarding Theorem 4.9 on the fixed points of S_n in the universal splitting algebra, the "f is separable" case belongs to folklore. We find it, with a proof related to the one given here, in Lionel Ducos' thesis [66]. We have given another proof of it in Theorem III-6.15 for the discrete fields case. The refinement that we give is found in [63], it is inspired by [Pohst & Zassenhaus] (see Theorem 2.18 page 46, Corollary 3.6 page 49 and the following remark, page 50).

Theorem 4.15, published in [63] under a restrictive hypothesis, generalizes a result given separately in the universal splitting algebra over a field case by L. Ducos [67] and by P. Aubry and A. Valibouze [2]. Our method of proof is closer to that of L. Ducos, but it is different because the framework is more general: we start off with an arbitrary commutative ring.

A related version of Theorem 4.12 is found in [66, lemme II.4.1].

Regarding the explicit methods of computing Galois groups over $\mathbb{Q}$ recently developed in Computer Algebra we refer to [91, Geissler&Klüners].

The modular method, made popular by van der Waerden, is due to Dedekind (letter addressed to Frobenius on June 18, 1882, see [20, Brandl]).

The Stauduhar [178] and Soicher-McKay [177] methods are based on computations of resolvents and on the knowledge of the transitive subgroups of the groups S_n. These have been tabulated up to $n = 31$ [109, Hulpke]. In most of the existing algorithms the computation determines the Galois group of an irreducible polynomial, without computing the splitting field. See however [120, Klüners&Malle] and [2, 149, 192, Valibouze&al.].

Moreover, let us cite the remarkable polynomial time computability result [124, Landau&Miller] regarding the solvability by radicals.

Alan Steel [179, 180] was inspired by D5 to implement a very efficient "dynamic" algebraic closure of $\mathbb{Q}$ in `Magma`. The efficiency depends on him not using a factorization algorithm for the polynomials of $\mathbb{Z}[X]$, nor an algorithm of representation of the finite extensions by means of primitive elements. Nevertheless he uses factorization algorithms modulo p to control the process.

of the system. We will notice that S is already an automorphic system, with the general group being its associated group. From then on, if we take Galois' point of view, ... we see that we can limit ourselves to only considering rational and automorphic systems (S, A)."

The process is dynamic in the sense that the progressively constructed closure depends on the user's questions. The author however does not give (and could not do so in his chosen framework) an implementation of the splitting field of a polynomial (let us say separable for the sake of simplification) over a "general" field.

For the Computer Algebra system `Magma`, see [19, 28, Bosma&al.].

Chapter VIII

Flat modules

Contents

Introduction

Dear elements,
if you aren't free,
it isn't my fault.
A flat module.

Flatness is a fundamental notion of commutative algebra, introduced by Serre in [173].

In this chapter we introduce the notion of a flat module, of a flat algebra and of a faithfully flat algebra, and prove some of the essential properties of these objects.

An integral ring whose finitely generated ideals are flat is called a Prüfer domain. This is another fundamental notion of commutative algebra which will only be introduced here. It will be further developed in Chapter XII.

1. First properties

Definition and basic properties

We give an elementary definition and later develop the relationship with the exactness of the functor $M \otimes \bullet$.

1.1. Definition. Consider an $\mathbf{A}$-module M.

1. A *syzygy in M* is given by $L \in \mathbf{A}^{1\times n}$ and $X \in M^{n\times 1}$ which satisfy $LX = 0$.
2. We say that *the syzygy* $LX = 0$ *is explained in* M if we find $Y \in M^{m\times 1}$ and a matrix $G \in \mathbf{A}^{n\times m}$ that satisfy
$$LG = 0 \quad \text{and} \quad GY = X\,. \tag{1}$$
3. The $\mathbf{A}$-module M is called a *flat module* if every syzygy in M is explained in M. (Intuitively speaking: if there is a syzygy between elements of M, the module is not to blame.)

Remarks. 1) In items *1* and *2* the symbol 0 is specified implicitly by the context. In *1* it is 0_M, whereas in *2* it is $0_{\mathbf{A}^{m\times 1}}$.

2) In item *2*, when we say that the syzygy $LX = 0$ is explained in M, we mean that the explanation "does not touch L." However, the equalities given by the matrix equation $LG = 0$ take place in $\mathbf{A}$ and not in M. ■

Examples. 1) If M is free and finitely generated,[1] it is flat: if $LX = 0$, we write $X = GY$ with a column vector Y which forms a basis, and $LX = 0$ implies $LG = 0$.

[1] Or more generally if M is freely generated by a discrete set, i.e. $M \simeq \mathbf{A}^{(I)} = \bigoplus_{i\in I} \mathbf{A}$ with I discrete. For another generalization see Exercise 16.

2) If $M = \bigcup_{i \in I} M_i$ with $\forall i, j \in I,\ \exists k \in I,\ M_k \supseteq M_i \cup M_j$ (we then say that M is a *filtering union* of the M_i's), and if each M_i is flat, then M is flat.

3) Let a be a regular element in $\mathbf{A}$, M be an $\mathbf{A}$-module and $u \in M$ such that $au = 0$. If this syzygy is explained in M, we write $u = \sum_i a_i u_i$ ($a_i \in \mathbf{A}$, $u_i \in M$) with each $aa_i = 0$, so $u = 0$. Thus in a flat module, every element annihilated by a regular element is null.

4) (Continued) The *torsion submodule* of a module M is the module

$$N = \{\, x \in M \mid \exists a \in \mathrm{Reg}(\mathbf{A}),\ ax = 0 \,\},$$

where $\mathrm{Reg}(\mathbf{A})$ designates the filter of the regular elements of $\mathbf{A}$. This torsion submodule is the kernel of the morphism of scalar extension to $\operatorname{Frac} \mathbf{A}$ for the module M. The torsion submodule of a flat module is reduced to 0.

When the ring $\mathbf{A}$ *is integral*, we say that a module is *torsion-free* if its torsion submodule is reduced to 0. Over a Bézout domain, or more generally over a Prüfer domain, a module is flat if and only if it is torsion-free (Exercise 1 and Theorem XII-3.2 item *2b*).

Later we give a generalization of the notion of a torsion-free module for an arbitrary commutative ring (Definition 3.3).

5) We will see (Proposition 4.2) that a finitely generated flat ideal $\mathfrak{a}$ is locally principal, which implies $\bigwedge^2 \mathfrak{a} = 0$ (Theorem V-7.3). Thus, when $\mathbf{A}$ is a nontrivial integral ring and $\mathbf{B} = \mathbf{A}[x, y]$, the ideal $\mathfrak{a} = \langle x, y \rangle$ is an example of a $\mathbf{B}$-module that is torsion-free, but not flat (since $\bigwedge^2_{\mathbf{B}} \mathfrak{a} = \mathbf{A}$ by Example on page 195). In fact, the relation $[\, y \ \ -x \,] \begin{bmatrix} x \\ y \end{bmatrix} = 0$ is not explained in $\mathfrak{a}$, but in $\mathbf{B}$. ■

The following proposition says that the "explanation" which is given for the syzygy $LX = 0$ in the definition of a flat module extends to a finite number of syzygies.

1.2. Proposition. *Let M be a flat* $\mathbf{A}$*-module. Consider a family of k syzygies, written in the form $LX = 0$, where $L \in \mathbf{A}^{k \times n}$ and $X \in M^{n \times 1}$. Then, we can find an integer m, a vector $Y \in M^{m \times 1}$ and a matrix $G \in \mathbf{A}^{n \times m}$ satisfying the equalities*

$$GY = X \quad \text{and} \quad LG = 0.$$

D Let $L_1, \ldots, L_k$ be rows of L. The syzygy $L_1 X = 0$ is explained by two matrices G_1 and Y_1 and by two equalities $X = G_1 Y_1$ and $L_1 G_1 = 0$. The syzygy $L_2 X = 0$ is rewritten as $L_2 G_1 Y_1 = 0$ i.e. $L_2' Y_1 = 0$. This syzygy is explained in the form $Y_1 = G_2 Y_2$ and $L_2' G_2 = 0$.

Therefore $X = G_1 Y_1 = G_1 G_2 Y_2$. With $L_1 G_1 G_2 = 0$ and $L_2 G_1 G_2 = L_2' G_2 = 0$. The column vector Y_2 and the matrix $H_2 = G_1 G_2$ therefore explain the two syzygies $L_1 X = 0$ and $L_2 X = 0$.

All that remains is to iterate the process. □

The following theorem reformulates Proposition 1.2 in the language of categories. The proof is a translation exercise left to the reader.

1.3. Theorem. (Characterization of flat modules, 1)
For some $\mathbf{A}$-module M the following properties are equivalent.

1. *The module M is flat.*
2. *Every linear map from a finitely presented module P to M is factorized by a free module of finite rank.*

1.4. Theorem. *An $\mathbf{A}$-module M is finitely presented and flat if and only if it is finitely generated projective.*

D The condition is necessary by the following remark. It is sufficient, because the identity of M is factorized by a free $\mathbf{A}$-module L of finite rank. Then, the composition $L \to M \to L$ is a projection whose image is isomorphic to M. □

It is immediate that the $\mathbf{A}$-module $M \oplus N$ is flat if and only if the modules M and N are flat.

The following proposition gives a slightly better result (see also Theorem 1.16 and Exercise 16).

1.5. Proposition. *Let $N \subseteq M$ be two $\mathbf{A}$-modules. If N and M/N are flat, then M is flat.*

D Write $\overline{x}$ the object x (defined over M) considered modulo N. Consider a syzygy $LX = 0$ in M. Since M/N is flat, we obtain G over $\mathbf{A}$ and Y over M such that $LG = 0$ and $G\overline{Y} = \overline{X}$. Consider the vector $X' = X - GY$ over N. We have $LX' = 0$, and since N is flat, we obtain H over $\mathbf{A}$ and Z over N such that $LH = 0$ and $HZ = X - GY$.

Thus the matrix $\begin{array}{|c|c|}\hline G & H \\ \hline\end{array}$ and the vector $\begin{array}{|c|}\hline Y \\ \hline Z \\ \hline\end{array}$ explain the relation $LX = 0$.□

1.6. Fact. *Let S be a monoid of the ring $\mathbf{A}$.*

1. *The localized ring $\mathbf{A}_S$ is flat as an $\mathbf{A}$-module.*
2. *If M is an $\mathbf{A}$-flat module, then M_S is flat as an $\mathbf{A}$-module and as an $\mathbf{A}_S$-module.*

D It suffices to prove item *2.* If we have a syzygy $LX = 0$ in the $\mathbf{A}$-module M_S, we write $X = X'/s$ and we have a syzygy $uLX' = 0$ in M (with $u, s \in S$). We therefore find Y' over M and G over $\mathbf{A}$ such that $GY' = X'$ in M and $uLG = 0$ in $\mathbf{A}$. This implies, for $Y = Y'/(su)$, the equality $uGY = X$ in M_S, such that uG and Y explain the relation $LX = 0$ in M_S. We can construct an analogous proof by starting with the syzygy in M_S considered as an $\mathbf{A}_S$-module. □

Local-global principle

Flatness is a local notion in the following sense.

1.7. Concrete local-global principle. (For flat modules)
Let $S_1, \ldots, S_r$ be comaximal monoids of a ring $\mathbf{A}$, and let M be an $\mathbf{A}$-module.

1. *A syzygy $LX = 0$ in M is explained in M if and only if it is explained in each of the M_{S_i}'s.*
2. *The module M is flat over $\mathbf{A}$ if and only if each of the M_{S_i}'s is flat over $\mathbf{A}_{S_i}$.*

D It suffices to prove the first item. The “only if” is given by Fact 1.6.
Let us prove the other implication. Let $LX = 0$ be a syzygy between elements of M (where $L \in \mathbf{A}^{1\times n}$ and $X \in M^{n\times 1}$). We want to find $m \in \mathbb{N}$, $Y \in M^{m\times 1}$ and a matrix $G \in \mathbf{A}^{n\times m}$ which satisfy Equation (1). We have a solution (m_i, Y_i, G_i) for (1) in each localized ring $\mathbf{A}_{S_i}$.
We can write $Y_i = Z_i/s_i$, $G_i = H_i/s_i$ with $Z_i \in M^{m_i\times 1}$, $H_i \in \mathbf{A}^{n\times m_i}$ and some $s_i \in S_i$ that are suitable. We then have $u_i H_i Z_i = v_i X$ in M and $u_i L H_i = 0$ in $\mathbf{A}$ for some u_i and $v_i \in S_i$. We write $\sum_{i=1}^{r} b_i v_i = 1$ in $\mathbf{A}$. For G we take the matrix obtained by juxtaposing the matrices $b_i u_i H_i$ in a row, and for Y we take the vector obtained by superposing the vectors Z_i in a column. We obtain $GY = \sum_{i=1}^{r} b_i v_i X = X$ in M, and $LG = 0$ in $\mathbf{A}$.□

The corresponding principle in classical mathematics is the following.

1.8. Abstract local-global principle*. (For flat modules)

1. *A syzygy $LX = 0$ in M is explained in M if and only if it is explained in $M_{\mathfrak{m}}$ for every maximal ideal $\mathfrak{m}$.*
2. *An $\mathbf{A}$-module M is flat if and only if for every maximal ideal $\mathfrak{m}$, the module $M_{\mathfrak{m}}$ is flat over $\mathbf{A}_{\mathfrak{m}}$.*

D It suffices to show the first item. However, the fact that a syzygy $LX = 0$ can be explained is a finite character property (Definition II-2.9). We therefore apply Fact II-2.12 which allows us to pass from the concrete local-global principle to the corresponding abstract local-global principle.□

Other characterizations of flatness

We will now consider *syzygies over M with coefficients in another module N* and we will show that when M is flat, every syzygy with coefficients in any module N is explained in M.

1.9. Definition. Let M and N be two $\mathbf{A}$-modules.
For $L = [\,a_1 \;\cdots\; a_n\,] \in N^{1\times n}$ and $X = {}^{\mathrm{t}}[\,x_1 \;\cdots\; x_n\,] \in M^{n\times 1}$, let

$$L \odot X \overset{\mathrm{def}}{=} \textstyle\sum_{i=1}^{n} a_i \otimes x_i \;\in N \otimes M.$$

1. If $L \odot X = 0$ we say that we have a syzygy between the x_i's with coefficients in N.
2. We say that *the syzygy* $L{\odot}X = 0$ *is explained in* M if we have $Y \in M^{m\times 1}$ and a matrix $G \in \mathbf{A}^{n\times m}$ which satisfy

$$LG =_{N^{1\times m}} 0 \quad \text{and} \quad X =_{M^{n\times 1}} GY\,. \tag{2}$$

Remark. 1) When we say that the syzygy $LX = 0$ is explained in M, we mean that the explanation "does not touch L."

2) We note that in general the equality $L \odot GY = LG \odot Y$ is assured for every matrix G with coefficients in $\mathbf{A}$ because $a \otimes \alpha y = a\alpha \otimes y$ when $a \in N$, $y \in M$ and $\alpha \in \mathbf{A}$. ■

1.10. Proposition. *Let M and N be two $\mathbf{A}$-modules.*
If M is a flat $\mathbf{A}$-module every syzygy with coefficients in N is explained in M.

D We assume that we are given a syzygy $L \odot X = 0$ with $L = [\,a_1 \;\cdots\; a_n\,] \in N^{1\times n}$ and $X = {}^{\mathrm{t}}[\,x_1 \;\cdots\; x_n\,] \in M^{n\times 1}$.

Case where N is free of finite rank. Proposition 1.2 gives the result.

Case where N is finitely presented.
Write $N = P/R = \mathbf{A}^k/(\mathbf{A}c_1 + \cdots \mathbf{A}c_r)$. The a_i's are given by the b_i's of P. The relation $L \odot X = 0$ means that $\sum_i b_i \otimes x_i \in R \otimes M \subseteq P \otimes M$, i.e. we have an equality

$$\textstyle\sum_i b_i \otimes x_i + \sum_\ell c_\ell \otimes z_\ell = 0$$

in $P{\otimes}M$. We then observe that when we explain in M this syzygy (regarding the x_i's and the z_ℓ's) with coefficients in the free module P, we explain at the same time the syzygy $L \odot X = 0$ with coefficients in N.

Case of an arbitrary $\mathbf{A}$-module N.
A relation $L \odot X = \sum_i a_i \otimes x_i = 0$ comes from a finite computation, in which only a finite number of elements of N and of relations between these elements intervene. There exist therefore a finitely presented module N', a linear map $\varphi : N' \to N$ and some $b_i \in N'$ such that on the one hand $\varphi(b_i) = a_i$ ($i \in [\![1..n]\!]$), and on the other hand $\sum_i b_i \otimes x_i = 0$ in $N' \otimes M$. We then observe that when, in M, we explain this syzygy with coefficients in N' (which is a finitely presented module), we explain at the same time the syzygy $L \odot X = 0$ with coefficients in N. □

1.11. Theorem. (Characterization of flat modules, 2)
For an $\mathbf{A}$*-module* M *the following properties are equivalent.*

1. *The module* M *is flat.*
2. *For all* $\mathbf{A}$*-modules* N*, every syzygy between elements of* M *with coefficients in* N *is explained in* M*.*
3. *For every finitely generated ideal* $\mathfrak{b}$ *of* $\mathbf{A}$ *the canonical map* $\mathfrak{b}\otimes_{\mathbf{A}} M \to M$ *is injective (this therefore establishes an isomorphism from* $\mathfrak{b} \otimes_{\mathbf{A}} M$ *to* $\mathfrak{b}M$*).*
4. *For all* $\mathbf{A}$*-modules* $N \subseteq N'$*, the canonical linear map*
$$N \otimes_{\mathbf{A}} M \to N' \otimes_{\mathbf{A}} M$$
is injective.
5. *The functor* $\bullet \otimes M$ *preserves exact sequences.*

D The implication *5* ⇒ *3* is trivial.

4 ⇒ *5.* Short exact sequences are preserved by the functor $\bullet \otimes M$. However every exact sequence decomposes into short exact sequences (see page 61).

1 ⇔ *3.* By the null tensor lemma IV-4.14.

1 ⇒ *2.* This is Proposition 1.10.

2 ⇔ *4.* By the null tensor lemma IV-4.14. □

The previous theorem admits some important corollaries.

1.12. Corollary. (Tensor product)
The tensor product of two flat modules is a flat module.

D Use item *4* of Theorem 1.11. □

1.13. Corollary. (Other basic constructions)
The tensor, exterior and symmetric powers of a flat module are flat modules.

D The proof is left to the reader. □

1.14. Corollary. (Intersection)
Let $N_1, \dots, N_r$ *be submodules of a module* N *and* M *be a flat module. Since* M *is flat, for* $N' \subseteq N$*, we identify* $N' \otimes M$ *with its image in* $N \otimes M$*. Then we have the equality*
$$\left(\bigcap_{i=1}^{r} N_i\right) \otimes M = \bigcap_{i=1}^{r} (N_i \otimes M).$$

D The exact sequence
$$0 \to \bigcap_{i=1}^{r} N_i \to N \to \bigoplus_{i=1}^{r} (N/N_i)$$
is preserved by the tensor product with M and the module $(N/N_i) \otimes M$ is identified with $(N \otimes M)/(N_i \otimes M)$. □

1.15. Corollary. (Scalar extension) *Let $\rho : \mathbf{A} \to \mathbf{B}$ be an algebra. If M is a flat $\mathbf{A}$-module, then $\rho_\star(M)$ is a flat $\mathbf{B}$-module.*

D Note that for a $\mathbf{B}$-module N, we have

$$N \otimes_{\mathbf{B}} \rho_\star(M) \simeq N \otimes_{\mathbf{B}} \mathbf{B} \otimes_{\mathbf{A}} M \simeq N \otimes_{\mathbf{A}} M.$$

We then apply item *4* of Theorem 1.11. Note that the last tensor product is equipped with a $\mathbf{B}$-module structure via N. □

Remark. Without mentioning it, we have just used a generalized form of associativity of the tensor product whose proof we leave to the reader. The form in question is the following.

First we say that an abelian group P is an $(\mathbf{A}, \mathbf{B})$-bimodule if it is equipped with two external laws which respectively make an $\mathbf{A}$-module and a $\mathbf{B}$-module, and if these two structures are compatible in the following sense: for all $a \in \mathbf{A}$, $b \in \mathbf{B}$ and $x \in P$, we have $a(bx) = b(ax)$.

In such a case, if M is a $\mathbf{B}$-module, then the tensor product $M \otimes_{\mathbf{B}} P$ can itself be equipped with a structure of an $(\mathbf{A}, \mathbf{B})$-bimodule by letting, for $a \in \mathbf{A}$, $a(x \otimes y) =_{M \otimes_{\mathbf{B}} P} x \otimes ay$.

Similarly, when N is an $\mathbf{A}$-module, the tensor product $P \otimes_{\mathbf{A}} N$ can itself be equipped with a structure of an $(\mathbf{A}, \mathbf{B})$-bimodule by letting, for $b \in \mathbf{B}$, $b(y \otimes z) =_{P \otimes_{\mathbf{A}} N} by \otimes z$.

Finally, under these hypotheses, there exists a unique linear map (for the structure of an $(\mathbf{A}, \mathbf{B})$-bimodule) $\varphi : (M \otimes_{\mathbf{B}} P) \otimes_{\mathbf{A}} N \to M \otimes_{\mathbf{B}} (P \otimes_{\mathbf{A}} N)$ which satisfies

$$\varphi\big((x \otimes y) \otimes z\big) = x \otimes (y \otimes z)$$

for all $x \in M$, $y \in P$, $z \in N$, and φ is an isomorphism. ■

Flat quotients

1.16. Theorem. (Flat quotients)
Let M be an $\mathbf{A}$-module, K be a submodule and $N = M/K$, with the exact sequence

$$0 \to K \xrightarrow{\imath} M \xrightarrow{\pi} N \to 0.$$

1. *If N is flat, for every module P, the sequence*
$$0 \to K \otimes P \xrightarrow{\imath_P} M \otimes P \xrightarrow{\pi_P} N \otimes P \to 0$$
is exact ($\imath_P = \imath \otimes \mathrm{I}_P$, $\pi_P = \pi \otimes \mathrm{I}_P$).
2. *If N and M are flat, K is flat.*
3. *If N and K are flat, M is flat.*
4. *If M is flat, the following properties are equivalent.*
   a. *N is flat.*
   b. *For every finitely generated ideal $\mathfrak{a}$, we have $\mathfrak{a}M \cap K = \mathfrak{a}K$.*

c. Every finitely generated ideal $\mathfrak{a}$ *gives an exact sequence*

$$0 \to K/\mathfrak{a}K \xrightarrow{\imath_{\mathfrak{a}}} M/\mathfrak{a}M \xrightarrow{\pi_{\mathfrak{a}}} N/\mathfrak{a}N \to 0.$$

NB: Item *3* has already been the object of Proposition 1.5. Here we give it another proof, leaving it up to the reader to compare them.

D *1. Case where P is finitely generated.* We write P as a quotient of a finite free module Q with a short exact sequence

$$0 \to R \xrightarrow{a} Q \xrightarrow{p} P \to 0.$$

We then consider the following commutative diagram in which all the horizontal and vertical sequences are exact because N and Q are flat

$$\begin{tikzcd}
 & & & 0 \arrow[d] & \\
 & K \otimes R \arrow[r, "\imath_R"] \arrow[d, "a_K"'] & M \otimes R \arrow[r, "\pi_R"] \arrow[d, "a_M"'] & N \otimes R \arrow[r] \arrow[d, "a_N"'] & 0 \\
0 \arrow[r] & K \otimes Q \arrow[r, "\imath_Q"] \arrow[d, "p_K"'] & M \otimes Q \arrow[r, "\pi_Q"] \arrow[d, "p_M"'] & N \otimes Q \arrow[r] & 0 \\
 & K \otimes P \arrow[r, "\imath_P"] \arrow[d] & M \otimes P \arrow[d] & & \\
 & 0 & 0 & &
\end{tikzcd}$$

We must show that $\imath_P$ is injective. This is a special case of the snake lemma, which we can prove by "diagram chasing."

Suppose $\imath_P(x) = 0$. We write $x = p_K(y)$ and $v = \imath_Q(y)$. We have $p_M(v) = 0$, so we write $v = a_M(z)$.

As $\pi_Q(v) = 0$, we have $a_N(\pi_R(z)) = 0$, so $\pi_R(z) = 0$.

Therefore we write $z = \imath_R(u)$ and we have

$$\imath_Q(a_K(u)) = a_M(\imath_R(u)) = a_M(z) = v = \imath_Q(y),$$

and since $\imath_Q$ is injective, $y = a_K(u)$, hence $x = p_K(y) = p_K(a_K(u)) = 0$.

General case. One possibility is to describe P as a quotient of a flat module Q (see Exercise 16 on the subject) in which case the previous proof remains unchanged. We can also do without this slightly cumbersome construction as follows. Let us show that $\imath_P$ is injective. Let $x = \sum_i x_i \otimes y_i \in K \otimes P$ such that $\imath_P(x) =_{M \otimes P} 0$, i.e. $\sum_i x_i \otimes y_i =_{M \otimes P} 0$.

By definition of the tensor product, there exists a finitely generated submodule $P_1 \subseteq P$ such that we also have $\sum_i x_i \otimes y_i =_{M \otimes P_1} 0$. By the already examined case, we have $\sum_i x_i \otimes y_i =_{K \otimes P_1} 0$, and this implies $\sum_i x_i \otimes y_i =_{K \otimes P} 0$.

2 and *3.* Let $\mathfrak{a}$ be an arbitrary finitely generated ideal. Since N is flat, we have by item *1* a commutative diagram with exact sequences

$$\begin{tikzcd}
 & & & 0 \arrow[d] & \\
0 \arrow[r] & \mathfrak{a}\otimes K \arrow[r, "\imath_{\mathfrak{a}}"] \arrow[d, "\varphi_K"] & \mathfrak{a}\otimes M \arrow[r, "\pi_{\mathfrak{a}}"] \arrow[d, "\varphi_M"] & \mathfrak{a}\otimes N \arrow[r] \arrow[d, "\varphi_N"] & 0 \\
0 \arrow[r] & K \arrow[r, "\imath"] & M \arrow[r, "\pi"] & N \arrow[r] & 0.
\end{tikzcd}$$

If M is flat, φ_M is injective, hence so is $\varphi_M \circ \imath_{\mathfrak{a}}$, then φ_K. By item *3* of Theorem 1.11 we conclude that K is flat.

If K is flat, φ_K is injective and a short diagram chase shows that φ_M is injective. Let $x \in \mathfrak{a}\otimes M$ with $\varphi_M(x) = 0$. As $\varphi_N(\pi_{\mathfrak{a}}(x)) = 0$, we have $\pi_{\mathfrak{a}}(x) = 0$ and we can write $x = \imath_{\mathfrak{a}}(y)$. Then $\imath(\varphi_K(y)) = \varphi_M(x) = 0$, so $y = 0$, thus $x = 0$.

4a ⇒ *4b.* Since M and N are flat, so is K and the top row of the previous diagram gives the exact sequence

$$0 \to \mathfrak{a}K \xrightarrow{\imath|_{\mathfrak{a}K}} \mathfrak{a}M \xrightarrow{\pi|_{\mathfrak{a}M}} \mathfrak{a}N \to 0. \tag{+}$$

However, the kernel of $\pi|_{\mathfrak{a}M}$ is by definition $\mathfrak{a}M \cap K$.

4b ⇔ *4c.* The sequence

$$0 \to K/\mathfrak{a}K \xrightarrow{\imath_{\mathfrak{a}}} M/\mathfrak{a}M \xrightarrow{\pi_{\mathfrak{a}}} N/\mathfrak{a}N \to 0$$

is obtained from the exact sequence $0 \to K \to M \to N$ by scalar extension to $\mathbf{A}/\mathfrak{a}$. Saying that it is exact is the same as saying that $\imath_{\mathfrak{a}}$ is injective. However, an element $\overline{x} \in K/\mathfrak{a}K$ is sent to 0 if and only if we have $x \in \mathfrak{a}M \cap K$.

4b ⇒ *4a.* Since $\mathfrak{a}K = \mathfrak{a}M \cap K$ the sequence (+) is exact. Consider the following commutative diagram with exact sequences, for which we must show that φ_N is injective.

$$\begin{tikzcd}
 & & 0 \arrow[d] & & \\
 & \mathfrak{a}\otimes K \arrow[r, "\imath_{\mathfrak{a}}"] \arrow[d, "\varphi_K"] & \mathfrak{a}\otimes M \arrow[r, "\pi_{\mathfrak{a}}"] \arrow[d, "\varphi_M"] & \mathfrak{a}\otimes N \arrow[r] \arrow[d, "\varphi_N"] & 0 \\
0 \arrow[r] & \mathfrak{a}K \arrow[r, "\imath|_{\mathfrak{a}K}"] \arrow[d] & \mathfrak{a}M \arrow[r, "\pi|_{\mathfrak{a}M}"] \arrow[d] & \mathfrak{a}N \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

This is obtained by a short diagram chase. If $\varphi_N(x) = 0$, we write $x = \pi_{\mathfrak{a}}(y)$. As $\pi\,|_{\mathfrak{a}M}\,(\varphi_M(y)) = 0$, we have $z \in \mathfrak{a}K$ such that $\varphi_M(y) = \imath\,|_{\mathfrak{a}K}\,(z)$, we write $z = \varphi_K(u)$, with $\varphi_M(\imath_{\mathfrak{a}}(u)) = \varphi_M(y)$, and since φ_M is injective, $y = \imath_{\mathfrak{a}}(u)$ and $x = \pi_{\mathfrak{a}}(y) = 0$. □

1.17. Corollary. (A flat algebra) *Let $f \in \mathbf{A}[\underline{X}] = \mathbf{A}[X_1, \dots, X_n]$ and $\mathbf{A}[\underline{x}] = \mathbf{A}[\underline{X}]/\langle f \rangle$. The $\mathbf{A}$-module $\mathbf{A}[\underline{x}]$ is flat if and only if $\mathrm{c}(f)^2 = \mathrm{c}(f)$, i.e. if and only if the ideal $\mathrm{c}(f)$ is generated by an idempotent.*

D The $\mathbf{A}$-module $\mathbf{A}[\underline{x}]$ is flat if and only if for every finitely generated ideal $\mathfrak{a}$ of $\mathbf{A}$ we have $\boxed{\langle f \rangle \cap \mathfrak{a}[\underline{X}] = f\mathfrak{a}[\underline{X}]\ (*)}$.

If $\mathbf{A}[\underline{x}]$ is flat, we obtain, for $\mathfrak{a} = \mathrm{c}(f)$, that $\mathrm{c}(f)^2 = \mathrm{c}(f)$, because $f \in \langle f \rangle \cap \mathfrak{a}[\underline{X}]$.

Conversely, let us suppose that $\mathrm{c}(f)^2 = \mathrm{c}(f)$ and show that $\mathbf{A}[\underline{x}]$ is flat. The idempotent e such that $\langle e \rangle = \langle \mathrm{c}(f) \rangle$ splits the ring into two components. In the first we have $f = 0$ and the result is clear. In the second, f is primitive. Now suppose that f is primitive.

By the Dedekind-Mertens lemma,[2] for every $\mathbf{A}$-module M the $\mathbf{A}$-linear map $M[\underline{X}] \xrightarrow{\times f} M[\underline{X}]$ is injective. Applied to $M = \mathbf{A}/\mathfrak{a}$, this gives $(*)$. Indeed, let $M[\underline{X}] = \mathbf{A}[\underline{X}]/\mathfrak{a}[\underline{X}]$ and suppose that $g \in \langle f \rangle \cap \mathfrak{a}[\underline{X}]$. Then $g = fh$ for some $h \in \mathbf{A}[\underline{X}]$, and $\overline{h}$ is in the kernel of $\mathbf{A}[\underline{X}]/\mathfrak{a}[\underline{X}] \xrightarrow{\times f} \mathbf{A}[\underline{X}]/\mathfrak{a}[\underline{X}]$, therefore $\overline{h} = 0$, i.e. $h \in \mathfrak{a}[\underline{X}]$, and $g \in f\mathfrak{a}[\underline{X}]$. □

2. Finitely generated flat modules

In the finitely generated module case, flatness is a more elementary property.

2.1. Lemma. *Consider a finitely generated $\mathbf{A}$-module M, and let $X \in M^{n \times 1}$ be a column vector whose coordinates x_i generate M. The module M is flat if and only if for every syzygy $LX = 0$ (where $L \in \mathbf{A}^{1 \times n}$), we can find two matrices G, $H \in \mathbb{M}_n(\mathbf{A})$ which satisfy the equalities*

$$H + G = \mathrm{I}_n, \quad LG = 0 \text{ and } HX = 0.$$

In particular, a cyclic module $M = \mathbf{A}y$ is flat if and only if

$$\forall a \in \mathbf{A}, (\, ay = 0 \implies \exists s \in \mathbf{A},\ \ as = 0 \text{ and } sy = y\,).$$

Remark. The symmetry between L and X in the statement is only apparent; the module M is generated by the coordinates of X, while the ring $\mathbf{A}$ is not generated (as a submodule) by the coordinates of L. ■

D We reduce an arbitrary syzygy $L'X' = 0$ to a syzygy $LX = 0$ by expressing X' in terms of X. A priori we should write X in the form G_1Y with $LG_1 = 0$.

As $Y = G_2X$, we take $G = G_1G_2$ and $H = \mathrm{I}_n - G$. □

[2] Actually, this refers to a variant, with essentially the same proof, which we leave to the reader.

Remark. For cyclic modules, by letting $t = 1 - s$, we obtain conditions on t rather than on s

$$a = at \qquad \text{and} \qquad ty = 0,$$

which implies that the annihilator $\mathfrak{a}$ of y satisfies $\mathfrak{a}^2 = \mathfrak{a}$. In fact, by Theorem 1.16, $\mathbf{A}/\mathfrak{a}$ is flat over $\mathbf{A}$ if and only if for every finitely generated ideal $\mathfrak{b}$ we have the equality $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}$. ■

Here is a generalization of Lemma 2.1 in the same style of Proposition 1.2.

2.2. Proposition. *Let M be a finitely generated flat $\mathbf{A}$-module, and $X \in M^{n\times 1}$ be a column vector that generates M. Let there be a family of k syzygies expressed in the form $LX = 0$ where $L \in \mathbf{A}^{k\times n}$ and $X \in M^{n\times 1}$. Then, we can find a matrix $G \in \mathbb{M}_n(\mathbf{A})$ which satisfies the equalities*

$$LG = 0 \quad \textit{and} \quad GX = X.$$

D Identical to the proof of Proposition 1.2. □

A constructive substitute for the property according to which every vector space over a field admits a basis (only true in classical mathematics) is the fact that every vector space over a discrete field is flat. More precisely, we have the following result.

2.3. Theorem. *The following properties are equivalent.*

1. *Every $\mathbf{A}$-module $\mathbf{A}/\langle a\rangle$ is flat.*
2. *Every $\mathbf{A}$-module is flat.*
3. *The ring $\mathbf{A}$ is reduced zero-dimensional.*

D *1 ⇒ 3.* If $\mathbf{A}/\langle a\rangle$ is flat, then $\langle a\rangle = \langle a\rangle^2$ and if it is true for every a, then $\mathbf{A}$ is reduced zero-dimensional.

3 ⇒ 2. Let us first treat the case of a discrete field.

Consider a syzygy $LX = a_1x_1 + \cdots + a_nx_n = 0$ for some elements $x_1, \ldots, x_n$ of an $\mathbf{A}$-module M. If all the a_i's are null the relation is explained with $Y = X$ and $G = \mathrm{I}_n$: $LG = 0$ and $GY = X$. If one of the a_i's is invertible, for instance a_1, let $b_j = -a_1^{-1}a_j$ for $j \neq 1$. We have $x_1 = b_2x_2 + \cdots + b_nx_n$ and $a_1b_j + a_j = 0$ for $j > 1$. The syzygy is explained by $Y = {}^{\mathrm{t}}[\,x_2 \ \cdots \ x_n\,]$ and by the following matrix G because $LG = 0$ and $GY = X$,

$$G = \begin{bmatrix} b_2 & b_3 & \cdots & b_n \\ 1 & 0 & \cdots & 0 \\ 0 & \ddots & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{bmatrix}.$$

For a reduced zero-dimensional ring, we apply the elementary local-global machinery no. 2 (page 213) which brings us back to the case of a discrete field. □

NB: This justifies the term “absolutely flat” for reduced zero-dimensional.

2.4. Lemma. *Same context as in Lemma 2.1. If* $\mathbf{A}$ *is a local ring and* M *is flat, we obtain under the hypothesis* $LX = 0$ *the following alternative. The vector* L *is null, or one of the* x_i*'s linearly depends on the others (it can therefore be deleted from the list of generators of* M*).*

D This is a “determinant trick.” We note that $\det(G) = \det(\mathrm{I}_n - H)$ can be written as $1+\sum_{i,j} b_{i,j}h_{i,j}$. Therefore $\det(G)$ or one of the $h_{i,j}$'s is invertible. In the first case $L = 0$. In the second, since $HX = 0$, one of the vectors x_i is a linear combination of the others. □

The same proof in the case of an arbitrary ring gives the following result.

2.5. Lemma. *Same context as in Lemma 2.1. If* M *is flat and* $LX = 0$*, there exist comaximal elements* s_1*, …,* s_ℓ *such that over each of the rings* $\mathbf{A}[1/s_j]$ *we have* $L = 0$*, or one of the* x_i*'s is a linear combination of the others.*

In classical mathematics, Lemma 2.4 implies the following fact.

2.6. Fact*. *A finitely generated flat module over a local ring is free and a basis can be extracted from any generator set.*

From Lemma 2.5, we obtain the following.

2.7. Fact*. *A finitely generated flat module over an integral ring is finitely generated projective.*

Here is a constructive version of Fact* 2.6.

2.8. Proposition. *Let* $\mathbf{A}$ *be a local ring and* M *be a flat* $\mathbf{A}$*-module generated by* $(x_1, \dots, x_n)$*. Suppose that* M *is strongly discrete or that the existence of nontrivial syzygies is explicit in* M*. Then,* M *is freely generated by a finite sequence* $(x_{i_1}, \dots, x_{i_k})$ *(with* $k \geqslant 0$*).*

D First suppose that M is strongly discrete, we can then find a finite sequence of integers $1 \leqslant i_1 < \cdots < i_k \leqslant n$ (where $k \geqslant 0$) such that none of the x_{i_ℓ}'s is a linear combination of the others, and $(x_{i_1}, \dots, x_{i_k})$ generates M. To simplify the notation, suppose from now on that $k = n$, i.e. none of the x_i's is a linear combination of the others. Lemma 2.4 then tells us that every syzygy between the x_i's is trivial.
Now suppose that the existence of nontrivial syzygies is explicit in M, i.e. for every family of elements of M, we know how to tell whether there is a nontrivial syzygy between these elements and how to provide one if necessary. Then, by using Lemma 2.4 we can delete the superfluous elements one after the other in the (x_i) family without changing the module M, until

all that remains is a subfamily without a nontrivial syzygy (a limiting case is provided by the empty subset when the module is null). □

Comment. Note that the proof uniquely uses the hypothesis "M is strongly discrete," or "the existence of nontrivial syzygies is explicit in M" with families extracted from the generator set (x_i). Moreover, each of these hypotheses is trivially true in classical mathematics. ■

Now here is a constructive version of Fact* 2.7.

2.9. Proposition. *Let $\mathbf{A}$ be an integral ring and M be a flat $\mathbf{A}$-module generated by $(x_1, \ldots, x_n)$. Suppose that for every finite subset J of $[\![1..n]\!]$ the existence of nontrivial syzygies between $(x_j)_{j \in J}$ is explicit in M (in other words, by passing to the quotient field we obtain a finite dimensional vector space). Then, M is finitely generated projective.*

D Suppose without loss of generality that $\mathbf{A}$ is nontrivial. By using Lemma 2.5 we obtain the following alternative. Either $(x_1, \ldots, x_n)$ is a basis, or after localization at comaximal elements the module is generated by $n-1$ of the x_j's. We conclude by induction on n: indeed, the syzygies after localization at s with $s \neq 0$ are the same as those over $\mathbf{A}$.
Note that for $n = 1$, either (x_1) is a basis, or $x_1 = 0$. □

3. Flat principal ideals

A ring $\mathbf{A}$ is said to be *without zerodivisors* if we have:

$$\forall a, b \in \mathbf{A} \quad \big(ab = 0 \ \Rightarrow\ (a = 0 \text{ or } b = 0)\big) \tag{3}$$

An integral ring (in particular a discrete field) is without zerodivisors. A discrete ring without zerodivisors is integral. A nontrivial ring is integral if and only if it is discrete and without zerodivisors.

3.1. Lemma. (When a principal ideal is flat)

1. *A principal ideal, or more generally a cyclic $\mathbf{A}$-module $\mathbf{A}a$, is a flat module if and only if*
$$\forall x \in \mathbf{A} \quad \big(xa = 0 \ \Rightarrow\ \exists z \in \mathbf{A}\ (za = 0 \ \textit{and}\ xz = x)\big).$$
2. *If $\mathbf{A}$ is local, an $\mathbf{A}$-module $\mathbf{A}a$ is flat if and only if*
$$\forall x \in \mathbf{A} \quad \big(xa = 0 \ \Rightarrow\ (x = 0 \ \textit{or}\ a = 0)\big).$$
3. *Let $\mathbf{A}$ be a local ring, if $\mathbf{A}$ is discrete, or if we have a test to answer the question "is x regular?," then, an ideal $\langle a \rangle$ is flat if and only if a is null or regular.*
4. *For a local ring $\mathbf{A}$ the following properties are equivalent.*
   a. *Every principal ideal is flat.*
   b. *The ring is without zerodivisors.*

D Lemma 2.1 gives item *1.* The computation for item *2* results from it, because z or $1 - z$ is invertible. The rest is clear. □

We similarly have the following equivalences.

3.2. Lemma. *For a ring* $\mathbf{A}$*, the following properties are equivalent.*

1. *Every principal ideal of* $\mathbf{A}$ *is flat.*
2. *If* $xy = 0$*, we have* $\operatorname{Ann} x + \operatorname{Ann} y = \mathbf{A}$.
3. *If* $xy = 0$*, there exist comaximal monoids* S_i *such that in each of the localized rings* $\mathbf{A}_{S_i}$*,* x *or* y *becomes null.*
4. *If* $xy = 0$*, there exists a* $z \in \mathbf{A}$ *with* $zy = 0$ *and* $xz = x$*.*
5. *For all* x, $y \in \mathbf{A}$, $\quad \operatorname{Ann} xy = \operatorname{Ann} x + \operatorname{Ann} y$*.*

The property for a ring to be without zerodivisors behaves badly under patching and that for a module to be flat is well-behaved under localization and patching. This justifies the following definition.

3.3. Definition.

1. A ring $\mathbf{A}$ is said to be *a pf-ring* (principal ideals are flat) when it satisfies the equivalent properties of Lemma 3.2.
2. An $\mathbf{A}$-module M is said to be *torsion-free* when all of its cyclic submodules are flat (see Lemma 3.1).

Remarks.

1) The torsion submodule of a torsion-free module is reduced to 0. Our definition is therefore a little more constraining than the more usual definition, which says that a module is torsion-free when its torsion module is reduced to 0. We will note that the two definitions coincide when the ring $\mathbf{A}$ is a pp-ring.

2) Every submodule of a torsion-free module is torsion-free, which is not the case in general when we replace “torsion-free” by “flat.”

3) In the French literature, the term “locally without zerodivisors” is often used for a pf-ring.

4) A pf-ring is reduced.

5) A local ring is a pf-ring if and only if it is without zerodivisors.

6) The field of reals *is not* without zerodivisors (*nor* a pf-ring): it is a local ring for which we do not know how to explicitly perform the implication (3) on page 458.

7) In classical mathematics a ring is a pf-ring if and only if it becomes integral after localization at every prime ideal (Exercise 4). ■

3.4. Lemma. *Let $\mathbf{A}$ be a pf-ring and M be a flat $\mathbf{A}$-module.*

1. *The module M is torsion-free.*
2. *The annihilator $(0 : y)$ of any $y \in M$ is idempotent.*

D *1.* Suppose $ay = 0$, $a \in \mathbf{A}$, $y \in M$. Since M is flat we have elements x_i of M, elements b_i of $\mathbf{A}$, and an equality $y = \sum_{i=1}^{n} b_i x_i$ in M, with $ab_i = 0$ ($i \in [\![1..n]\!]$) in $\mathbf{A}$.
For each i, since $ab_i = 0$, there exists a c_i such that $ac_i = a$ and $c_i b_i = 0$. Let $c = c_1 \cdots c_n$. Then, $a = ca$ and $cy = 0$.

2. Indeed, when $ay = 0$, then $a = ca$ with $c \in (0 : y)$. □

Using item *2* of Lemma 3.4 and the fact that an idempotent finitely generated ideal is generated by an idempotent (Lemma II-4.6) we obtain the following result.

3.5. Fact. *Let $\mathbf{A}$ be a ring in which the annihilator of every element is finitely generated.*

1. *$\mathbf{A}$ is a pf-ring if and only if it is a pp-ring.*
2. *$\mathbf{A}$ is without zerodivisors if and only if it is integral.*

In particular, a coherent pf-ring is a pp-ring.

Note that item *2* is obvious in classical mathematics, where the hypothesis "the annihilator of every element is finitely generated" is superfluous.

4. Finitely generated flat ideals

We now study the flatness of finitely generated ideals. In classical mathematics, the following proposition is an immediate corollary of Proposition 2.8. In constructive mathematics, it is necessary to provide a new proof, which gives algorithmic information of a different nature from that given in the proof of Proposition 2.8. Indeed, we no longer make the same hypotheses regarding the discrete character of things.

4.1. Proposition. (Finitely generated flat ideals over a local ring)
Let $\mathbf{A}$ be a local ring, $x_1, \ldots, x_n \in \mathbf{A}$ and $\mathfrak{a} = \langle x_1, \ldots, x_n \rangle$.

1. *If $\mathfrak{a}$ is principal, it is generated by one of the x_j's.* (Bézout is always trivial over a local ring.)
2. *If $\mathfrak{a}$ is flat, it is principal, generated by one of the x_j's.*
3. *Suppose that $\mathbf{A}$ is discrete, or that we have a test to answer the question "is x regular?" Then, a finitely generated ideal is flat if and only if it is free of rank 0 or 1.*

D *1.* We have $\mathfrak{a} = \langle x_1, \dots, x_n \rangle = \langle z \rangle$, $z = a_1x_1 + \cdots + a_nx_n$, $zb_j = x_j$, so $z(1 - \sum_j a_jb_j) = 0$. If $1 - \sum_j a_jb_j$ is invertible, $\mathfrak{a} = 0 = \langle x_1 \rangle$. If a_jb_j is invertible $\mathfrak{a} = \langle x_j \rangle$.

2. Consider the syzygy $x_2x_1 + (-x_1)x_2 = 0$. Let $G = \begin{bmatrix} a_1 & \dots & a_n \\ b_1 & \dots & b_n \end{bmatrix}$ be a matrix such that $G \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$ and $[\, x_2 \;\; -x_1 \,]\, G = [\, 0 \;\; 0 \,]$.

If a_1 is invertible, the equality $a_1x_2 = b_1x_1$ shows that $\mathfrak{a} = \langle x_1, x_3, \dots, x_n \rangle$. If $1 - a_1$ is invertible, the equality $a_1x_1 + \cdots + a_nx_n = x_1$ shows that we have $\mathfrak{a} = \langle x_2, x_3, \dots, x_n \rangle$.

We finish by induction on n.

3. Results from *2* and from Lemma 3.1, item *3*. □

Recall that a finitely generated ideal $\mathfrak{a}$ of a ring $\mathbf{A}$ is said to be *locally principal* if there exist comaximal monoids S_1, …, S_n of $\mathbf{A}$ such that each $\mathfrak{a}_{S_j}$ is principal in $\mathbf{A}_{S_j}$. The proposition that follows shows that *every finitely generated flat ideal is locally principal.* Its proof follows directly from that for the local case.

4.2. Proposition. (Finitely generated flat ideals over an arbitrary ring) *Every finitely generated flat ideal is locally principal. More precisely, if* $\mathfrak{a} = \langle x_1, \dots, x_n \rangle \subseteq \mathbf{A}$*, the following properties are equivalent.*

1. *The ideal* $\mathfrak{a}$ *is a flat module.*
2. *After localization at suitable comaximal monoids, the ideal* $\mathfrak{a}$ *is flat and principal.*
3. *After localization at suitable comaximal elements, the ideal* $\mathfrak{a}$ *is flat and principal, generated by one of the* x_i*'s.*

D We obviously have *3* ⇒ *2*. We have *2* ⇒ *1* by the local-global principle 1.7. To show *1* ⇒ *3* we reuse the proof of item *2* of Proposition 4.1. Consider the syzygy $x_2x_1 + (-x_1)x_2 = 0$. Let $G = \begin{bmatrix} a_1 & \dots & a_n \\ b_1 & \dots & b_n \end{bmatrix}$ be a matrix such that $G \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$ and $[\, x_2 \;\; -x_1 \,]\, G = [\, 0 \;\; 0 \,]$. With the localized ring $\mathbf{A}[1/a_1]$ the equality $a_1x_2 = b_1x_1$ shows that $\mathfrak{a} =_{\mathbf{A}[1/a_1]} \langle x_1, x_3, \dots, x_n \rangle$. With the localized ring $\mathbf{A}[1/(1-a_1)]$ the equality $a_1x_1 + \cdots + a_nx_n = x_1$ shows that $\mathfrak{a} =_{\mathbf{A}[1/(1-a_1)]} \langle x_2, x_3, \dots, x_n \rangle$. We finish by induction on n. □

Arithmetic rings and Prüfer rings

The following definition of Prüfer rings, based on flatness, is due to Hermida and Sánchez-Giralda [103].

4.3. Definition. *(Arithmetic rings)* A ring $\mathbf{A}$ is said to be *arithmetic* if every finitely generated ideal is locally principal.

4.4. Proposition and definition. (Prüfer rings)
The following properties are equivalent.

1a. Every finitely generated ideal of $\mathbf{A}$ *is flat.*

1b. Every ideal of $\mathbf{A}$ *is flat.*

1c. For all finitely generated ideals $\mathfrak{a}$ *and* $\mathfrak{b}$ *of* $\mathbf{A}$*, the canonical linear map* $\mathfrak{a} \otimes \mathfrak{b} \to \mathfrak{a}\mathfrak{b}$ *is an isomorphism.*

2a. The ring $\mathbf{A}$ *is locally without zerodivisors and arithmetic.*

2b. The ring $\mathbf{A}$ *is reduced and arithmetic.*

A ring satisfying these properties is called a Prüfer ring*.*

D The equivalence between *1a* and *1c* is given by Theorem 1.11 (item *3*). The equivalence of *1a* and *1b* is immediate. We already know that *1a* $\Rightarrow$ *2a*, and the implication *2a* $\Rightarrow$ *2b* is clear.

2b $\Rightarrow$ *2a.* Let x, y be such that $xy = 0$. There exist s, t with $s + t = 1$, $sx \in \langle y \rangle$ and $ty \in \langle x \rangle$. Therefore $sx^2 = 0$ and $ty^2 = 0$ then ($\mathbf{A}$ is reduced) $sx = ty = 0$.

2a $\Rightarrow$ *1a.* After suitable localizations, the ideal becomes principal, and therefore flat, since the ring is a pf-ring. We finish by the local-global principle 1.7 for flat modules. □

Local-global principle

The different notions previously introduced are local in the sense of the following concrete local-global principle. The proofs are based on the basic local-global principle and are left to the reader.

4.5. Concrete local-global principle. (Arithmetic rings)
Let $S_1, \ldots, S_n$ *be comaximal monoids of a ring* $\mathbf{A}$ *and* $\mathfrak{a}$ *be an ideal of* $\mathbf{A}$*. We have the following equivalences.*

1. *The ideal* $\mathfrak{a}$ *is locally principal if and only if each of the* $\mathfrak{a}_{S_i}$*'s is locally principal.*
2. *The ring* $\mathbf{A}$ *is a pf-ring if and only if each of the* $\mathbf{A}_{S_i}$*'s is a pf-ring.*
3. *The ring* $\mathbf{A}$ *is arithmetic if and only if each of the* $\mathbf{A}_{S_i}$*'s is arithmetic.*
4. *The ring* $\mathbf{A}$ *is a Prüfer ring if and only if each of the* $\mathbf{A}_{S_i}$*'s is a Prüfer ring.*

Local-global machinery

An ordered set $(E, \leqslant)$ is said to be *totally ordered* if for all x, y we have $x \leqslant y$ or $y \leqslant x$. A priori we do not assume it to be discrete and we therefore do not have a test for strict inequality.

For local rings, Proposition 4.1 gives the following result.

4.6. Lemma. (Local arithmetic rings)

1. *A ring $\mathbf{A}$ is local and arithmetic if and only if for all a, $b \in \mathbf{A}$, we have $a \in b\mathbf{A}$ or $b \in a\mathbf{A}$. Equivalently, every finitely generated ideal is principal and the set of finitely generated ideals is totally ordered with respect to the inclusion.*
2. *Let $\mathbf{A}$ be a local arithmetic ring. For two arbitrary ideals $\mathfrak{a}$ and $\mathfrak{b}$, if $\mathfrak{a}$ is not contained in $\mathfrak{b}$, then $\mathfrak{b}$ is contained in $\mathfrak{a}$. Therefore in classical mathematics, the "set" of all the ideals is totally ordered with respect to the inclusion.*

Thus, arithmetic local rings are the same thing as local Bézout rings. They have already been studied in Section IV-7 (page 206).

The ease with which we prove properties for arithmetic rings is mostly due to the following local-global machinery.

Local-global machinery of arithmetic rings
When we have to prove a property regarding an arithmetic ring and that a finite family of elements (a_i) of the ring intervenes in the computation, we start by proving the result in the local case. We can therefore suppose that the ideals $\langle a_i \rangle$ are totally ordered by inclusion. In this case the proof is in general very simple. Moreover, since the ring is arithmetic, we know that we can return to the previous situation after localization at a finite number of comaximal elements. We can therefore conclude if the property to be proven obeys a concrete local-global principle.

Here is an application of this machinery.

4.7. Proposition. (Determinantal ideals over an arithmetic ring)
Let $\mathbf{A}$ be a coherent arithmetic ring, M be a matrix $\in \mathbf{A}^{n \times m}$ and $\mathfrak{d}_k = \mathcal{D}_{\mathbf{A},k}(M)$ its determinantal ideals ($k \in \llbracket 1..p \rrbracket$ with $p = \inf(m, n)$). There exist finitely generated ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_p$ such that

$$\mathfrak{d}_1 = \mathfrak{a}_1,\ \mathfrak{d}_2 = \mathfrak{d}_1\mathfrak{a}_1\mathfrak{a}_2,\ \mathfrak{d}_3 = \mathfrak{d}_2\mathfrak{a}_1\mathfrak{a}_2\mathfrak{a}_3,\ \ldots$$

D Let $\mathfrak{b}_k = (\mathfrak{d}_k : \mathfrak{d}_{k-1})$ for all k, so $\mathfrak{b}_1 = \mathfrak{d}_1$. We have $\mathfrak{b}_k\mathfrak{d}_{k-1} = \mathfrak{d}_k$ because the ring is arithmetic and coherent. Let $\mathfrak{c}_k = \mathfrak{b}_1 \cap \cdots \cap \mathfrak{b}_k$ for $k \geqslant 1$. This is a nonincreasing sequence of finitely generated ideals. Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_p$ be finitely generated ideals satisfying $\mathfrak{a}_1 = \mathfrak{d}_1$ and $\mathfrak{a}_k\mathfrak{c}_{k-1} = \mathfrak{c}_k$ for $k \geqslant 2$. It is sufficient to prove the equalities $\boxed{\mathfrak{c}_k\mathfrak{d}_{k-1} = \mathfrak{d}_k}$. This is clear for $k = 1$.

If $\mathbf{A}$ is a local arithmetic ring, the matrix admits a reduced Smith form (Proposition IV-7.2). Let $p = \inf(m, n)$
The algorithm that produces the reduced Smith form in the local case and the previous local-global machinery of arithmetic rings provide us with a system of comaximal elements $(s_1, \dots, s_r)$ such that, over each ring $\mathbf{A}[1/s_i]$, the matrix M admits a reduced Smith form with the diagonal sub-matrix $\mathrm{Diag}(c_1, c_2, \dots, c_p)$ and $c_1 \mid c_2 \mid \dots \mid c_p$. Moreover, for $k \geqslant 1$, $\mathfrak{d}_k = \langle c_1 \cdots c_k \rangle$.
It is sufficient to prove $\mathfrak{c}_k \mathfrak{d}_{k-1} = \mathfrak{d}_k$ after localization at these comaximal elements. Since $\mathfrak{b}_k \mathfrak{d}_{k-1} = \mathfrak{d}_k$, we get $\mathfrak{c}_k \mathfrak{d}_{k-1} \subseteq \mathfrak{d}_k$.
In order to prove the other inclusion let us show that for all $k \geqslant 1$ we have $c_k \in \mathfrak{c}_k$ (this implies $\mathfrak{c}_k \mathfrak{d}_{k-1} \supseteq \mathfrak{d}_k$). We have $c_k \mathfrak{d}_{k-1} = \mathfrak{d}_k$, thus $c_k \in \mathfrak{b}_k$. Moreover c_k is multiple of $c_i \in \mathfrak{b}_i$ for $i \leqslant k-1$, so $c_k \in \mathfrak{b}_1 \cap \cdots \cap \mathfrak{b}_{k-1}$. This finishes the proof. □

We will return to arithmetic rings and Prüfer rings in greater length in Chapter XII.

5. Flat algebras

Intuitively speaking, an $\mathbf{A}$-algebra $\mathbf{B}$ is flat when the homogeneous systems of linear equations over $\mathbf{A}$ have "no more" solutions in $\mathbf{B}$ than in $\mathbf{A}$, and it is faithfully flat if this assertion is also true for nonhomogeneous systems of linear equations. More precisely, we adopt the following definitions.

5.1. Definition. Let $\rho : \mathbf{A} \to \mathbf{B}$ be an $\mathbf{A}$-algebra.

1. $\mathbf{B}$ is said to be *flat (over* $\mathbf{A}$*)* when every $\mathbf{B}$-linear dependence relation between elements of $\mathbf{A}$ is a $\mathbf{B}$-linear combination of $\mathbf{A}$-linear dependence relations between these same elements. In other words, for every linear form $\psi : \mathbf{A}^n \to \mathbf{A}$, we require that $\mathrm{Ker}\, \rho_\star(\psi) = \langle \rho(\mathrm{Ker}\, \psi) \rangle_{\mathbf{B}}$.
   We will also say that *the ring homomorphism ρ is flat.*
2. A *flat* $\mathbf{A}$-algebra $\mathbf{B}$ is said to be *faithfully flat* if for every linear form $\psi : \mathbf{A}^n \to \mathbf{A}$ and all $a \in \mathbf{A}$, when the equation $\psi(X) = a$ admits a solution in $\mathbf{B}$ (i.e. $\exists X \in \mathbf{B}^n$, $\big(\rho_\star(\psi)\big)(X) = \rho(a)$), then it admits a solution in $\mathbf{A}$.
   We will also say that *the ring homomorphism ρ is faithfully flat.*

For a faithfully flat $\mathbf{A}$-algebra, when considering the case where $n = 1$ and $\psi = 0$, we see that $\rho(a) = 0$ implies $a = 0$. Thus, ρ is an injective homomorphism. We therefore say that $\mathbf{B}$ is a *faithfully flat extension* of $\mathbf{A}$. We can then identify $\mathbf{A}$ with a subring of $\mathbf{B}$ and the condition on the nonhomogeneous linear equation is easier to formulate: it is exactly the same equation that we seek to solve in $\mathbf{A}$ or $\mathbf{B}$.

5.2. Fact.

An **A**-*algebra* **B** *is flat if and only if* **B** *is a flat* **A**-*module.*

D Translation exercise left to the reader. □

Fundamental examples. The following lemma provides some examples.

5.3. Lemma.

1. *A localization morphism* $\mathbf{A} \to S^{-1}\mathbf{A}$ *gives a flat* $\mathbf{A}$*-algebra.*
2. *If* $S_1, \ldots, S_n$ *are comaximal monoids of* $\mathbf{A}$ *and if* $\mathbf{B} = \prod_i \mathbf{A}_{S_i}$*, the canonical "diagonal" homomorphism* $\rho : \mathbf{A} \to \mathbf{B}$ *gives a faithfully flat algebra.*
3. *If* $\mathbf{k}$ *is reduced zero-dimensional, every* $\mathbf{k}$*-algebra* $\mathbf{L}$ *is flat.*

D *1.* See Fact II-6.6 or Facts 5.2 and 1.6.

2. This results from the basic local-global principle (we could even say that it is the basic local-global principle).

3. Results from 5.2 and from the fact that every $\mathbf{K}$-module is flat (Theorem 2.3). □

Remarks. Regarding item *3* of the previous lemma.

1) It seems difficult to replace $\mathbf{k}$ in the hypothesis with a (Heyting) field that we do not assume to be zero-dimensional.

2) See Theorem 6.2 for the faithfully flat question. ■

In the following proposition, an analog of Propositions II-3.1 (for coherent rings) and 1.2 (for flat modules), we pass from an equation to a system of equations. To lighten the text, we act as though we have an inclusion $\mathbf{A} \subseteq \mathbf{B}$ (even if $\mathbf{B}$ is only assumed to be flat), in other words we do not specify that when we pass into $\mathbf{B}$, everything must be transformed by means of the homomorphism $\rho : \mathbf{A} \to \mathbf{B}$.

5.4. Proposition. *Let* $M \in \mathbf{A}^{n \times m}$*,* $C \in \mathbf{A}^{n \times 1}$ *and* $\mathbf{B}$ *be a flat* $\mathbf{A}$*-algebra.*

1. *Every solution in* $\mathbf{B}$ *of the homogeneous system of linear equations* $MX = 0$ *is a* $\mathbf{B}$*-linear combination of solutions in* $\mathbf{A}$*.*
2. *If in addition* $\mathbf{B}$ *is faithfully flat, and if the system* $MX = C$ *admits a solution in* $\mathbf{B}$*, it admits a solution in* $\mathbf{A}$*.*

D The definitions of flat and faithfully flat $\mathbf{A}$-algebras concern the systems of linear equations with a single equation. To solve a general system of linear equations we apply the usual technique: we start by solving the first equation, then substitute the general solution of the first equation into the second, and so forth. □

5.5. Proposition.
Let $\mathbf{A} \xrightarrow{\rho} \mathbf{B}$ *be a flat* $\mathbf{A}$*-algebra and* $\mathfrak{a}$*,* $\mathfrak{b}$ *be two ideals of* $\mathbf{A}$*.*

1. *The natural* $\mathbf{B}$*-linear map* $\rho_\star(\mathfrak{a}) \to \rho(\mathfrak{a})\mathbf{B}$ *is an isomorphism.*

In the remainder we identify $\rho_\star(\mathfrak{c})$ *with the ideal* $\rho(\mathfrak{c})\mathbf{B}$ *for every ideal* $\mathfrak{c}$ *of* $\mathbf{A}$*.*

2. *We have* $\rho_\star(\mathfrak{a} \cap \mathfrak{b}) = \rho_\star(\mathfrak{a}) \cap \rho_\star(\mathfrak{b})$*.*
3. *If in addition* $\mathfrak{a}$ *is finitely generated, we have* $\rho_\star(\mathfrak{b} : \mathfrak{a}) = \big(\rho_\star(\mathfrak{b}) : \rho_\star(\mathfrak{a})\big)$*.*

D The first two items result from analogous facts regarding flat modules (Theorem 1.11 item *4* and Corollary 1.14).
3. If $\mathfrak{a} = \langle a_1, \ldots, a_n \rangle$, then $\mathfrak{b} : \mathfrak{a} = \bigcap_i (\mathfrak{b} : a_i)$, therefore given item *2* we are reduced to the case of a principal ideal $\langle a \rangle$. We then consider the exact sequence

$$0 \to \mathfrak{b} : a \longrightarrow \mathbf{A} \xrightarrow{\;a\;} \mathbf{A}/\mathfrak{b}\ ,$$

we tensor with $\mathbf{B}$ and we obtain the exact sequence (use the flatness and Fact IV-4.8)

$$0 \to \rho_\star(\mathfrak{b} : a) \longrightarrow \mathbf{B} \xrightarrow{\rho(a)} \mathbf{B}/\rho_\star(\mathfrak{b})\ ,$$

which gives the desired result. □

5.6. Theorem. *Let $\rho : \mathbf{A} \to \mathbf{B}$ be an algebra. The following properties are equivalent.*

1. *$\mathbf{B}$ is a flat $\mathbf{A}$-algebra.*
2. *$\mathbf{B}$ is a flat $\mathbf{A}$-module.*
3. *For every flat $\mathbf{A}$-module M, the $\mathbf{A}$-module $\rho_\star(M)$ is flat.*
4. *For every finitely generated ideal $\mathfrak{a}$ of $\mathbf{A}$, the canonical $\mathbf{A}$-linear map*
$$\mathbf{B} \otimes_{\mathbf{A}} \mathfrak{a} \simeq \rho_\star(\mathfrak{a}) \to \mathfrak{a}\mathbf{B}$$
is an isomorphism.
5. *For all $\mathbf{A}$-modules $N \subseteq M$, the $\mathbf{B}$-linear map $\rho_\star(N) \to \rho_\star(M)$ is injective.*
6. *For every $\mathbf{A}$-linear map $\psi : M \to P$, the natural $\mathbf{B}$-linear map*
$$\rho_\star\big(\operatorname{Ker}(\psi)\big) \longrightarrow \operatorname{Ker}\big(\rho_\star(\psi)\big)$$
is an isomorphism.
7. *For every exact sequence of $\mathbf{A}$-modules $M \xrightarrow{f} N \xrightarrow{g} P$ the sequence*
$$\rho_\star(M) \xrightarrow{\rho_\star(f)} \rho_\star(N) \xrightarrow{\rho_\star(g)} \rho_\star(P)$$
is an exact sequence of $\mathbf{B}$-modules.

Item *5* allows us to identify $\rho_\star(P)$ with a $\mathbf{B}$-submodule of $\rho_\star(Q)$ each time that we have two $\mathbf{A}$-modules $P \subseteq Q$ and that $\mathbf{B}$ is flat over $\mathbf{A}$.

D The reader will verify that the equivalences are clear by what we already know (Fact 5.2, Theorem 1.11, Corollary 1.12). We note that Proposition 5.4 gives item *6* in the case of a linear map between free modules of finite rank. □

The following proposition generalizes Propositions V-9.2 and V-9.3.

5.7. Proposition. *Let $\rho : \mathbf{A} \to \mathbf{B}$ be a flat $\mathbf{A}$-algebra and M, N be $\mathbf{A}$-modules. If M is finitely generated (resp. finitely presented), the natural $\mathbf{B}$-linear map*

$$\rho_\star\big(\mathrm{L}_{\mathbf{A}}(M, N)\big) \to \mathrm{L}_{\mathbf{B}}\big(\rho_\star(M), \rho_\star(N)\big)$$

is injective (resp. is an isomorphism).

▷ Consider an exact sequence

$$K \longrightarrow \mathbf{A}^k \longrightarrow M \to 0, \qquad (*)$$

corresponding to the fact that M is finitely generated (if M is finitely presented the module K is also free of finite rank).

Let $M_1 = \rho_\star(M)$, $N_1 = \rho_\star(N)$ and $K_1 = \rho_\star(K)$. First we have the exact sequence

$$K_1 \longrightarrow \mathbf{B}^k \longrightarrow M_1 \to 0. \qquad (**)$$

Next we obtain the exact sequences below. The first comes from $(*)$, the last one comes from $(**)$ and the second results from the first by scalar extension since $\mathbf{B}$ is flat over $\mathbf{A}$.

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{L}_{\mathbf{A}}(M,N) \arrow[r] & \mathrm{L}_{\mathbf{A}}(\mathbf{A}^k,N) \simeq N^k \arrow[r] & \mathrm{L}_{\mathbf{A}}(K,N) \\
0 \arrow[r] & \rho_\star\big(\mathrm{L}_{\mathbf{A}}(M,N)\big) \arrow[r] \arrow[d] & \rho_\star(\mathrm{L}_{\mathbf{A}}(\mathbf{A}^k,N) \simeq N_1^k \arrow[r] \arrow[d] & \rho_\star\big(\mathrm{L}_{\mathbf{A}}(K,N)\big) \arrow[d] \\
0 \arrow[r] & \mathrm{L}_{\mathbf{B}}(M_1,N_1) \arrow[r] & \mathrm{L}_{\mathbf{B}}(\mathbf{B}^k,N_1) \simeq N_1^k \arrow[r] & \mathrm{L}_{\mathbf{B}}(K_1,N_1)
\end{tikzcd}$$

In addition, we have natural "vertical" $\mathbf{B}$-linear maps from the second to the third exact sequence, and the diagrams commute. The second vertical arrow is an isomorphism (the identity of N_1^k after the canonical identifications). This implies that the first vertical arrow (the $\mathbf{B}$-linear map that we are interested in) is injective.

If M is finitely presented and if $K \simeq \mathbf{A}^\ell$, the two $\mathbf{B}$-modules on the right are isomorphic to N_1^ℓ and the corresponding vertical arrow is an isomorphism. This implies that the first vertical arrow is an isomorphism. □

Retrospectively the given proof for Proposition V-9.3 seems quite complicated. The new proof given here in a more general framework is conceptually simpler.

6. Faithfully flat algebras

We have already said that if $\mathbf{A} \xrightarrow{\rho} \mathbf{B}$ is a faithfully flat algebra, ρ is injective. It is also clear that ρ *reflects the units*, i.e.

$$\rho(a) \in \mathbf{B}^\times \implies a \in \mathbf{A}^\times.$$

We now present a few characteristic properties. In what follows we will take note of the equivalence of items *1*, *2a*, *3a* and *4*.

6.1. Theorem. (Characterizations of faithfully flat algebras)
Let $\rho : \mathbf{A} \to \mathbf{B}$ be a flat algebra. The following properties are equivalent.

1. *The algebra $\mathbf{B}$ is faithfully flat.*

2a. The homomorphism ρ is injective, and when identifying $\mathbf{A}$ *with a subring of* $\mathbf{B}$*, for every finitely generated ideal* $\mathfrak{a}$ *of* $\mathbf{A}$ *we have*

$$\mathfrak{a}\mathbf{B} \cap \mathbf{A} = \mathfrak{a}.$$

2b. Similarly with an arbitrary ideal of $\mathbf{A}$*.*

3a. For every finitely generated ideal $\mathfrak{a}$ *of* $\mathbf{A}$ *we have the implication*

$$1_{\mathbf{B}} \in \rho_\star(\mathfrak{a}) \implies 1_{\mathbf{A}} \in \mathfrak{a}.$$

3b. For every finitely generated ideal $\mathfrak{a}$ *of* $\mathbf{A}$*, if* $\rho_\star(\mathbf{A}/\mathfrak{a}) = 0$*, then* $\mathbf{A}/\mathfrak{a} = 0$*.*

3c. For all $\mathbf{A}$*-modules* $N \subseteq M$*, if* $\rho_\star(N) = \rho_\star(M)$*, then* $N = M$*.*

3d. For every $\mathbf{A}$*-module* M*, if* $\rho_\star(M) = 0$*, then* $M = 0$*.*

3e. For every $\mathbf{A}$*-module* M *the natural* $\mathbf{A}$*-linear map* $M \to \rho_\star(M)$ *is injective.*

4. The scalar extension from $\mathbf{A}$ *to* $\mathbf{B}$ reflects the exact sequences*.*
In other words, given an arbitrary sequence of $\mathbf{A}$*-modules*

$$N \xrightarrow{f} M \xrightarrow{g} P,$$

it is exact if the sequence of $\mathbf{B}$*-modules*

$$\rho_\star(N) \xrightarrow{\rho_\star(f)} \rho_\star(M) \xrightarrow{\rho_\star(g)} \rho_\star(P)$$

is exact.

D Item *1* implies that ρ is injective. Once this has been shown, *2a* is a simple reformulation of *1*, and it is easy to show that *2a* is equivalent to *2b*.

3a ⇒ *1.* We start by noticing that the implication is still valid if we replace the finitely generated ideal $\mathfrak{a}$ by an arbitrary ideal $\mathfrak{c}$. Indeed, if $1 \in \rho_\star(\mathfrak{c})$ we will also have $1 \in \rho_\star(\mathfrak{c}')$ for a finitely generated ideal $\mathfrak{c}'$ contained in $\mathfrak{c}$.
Now let $\mathfrak{a} = \langle a_1, \ldots, a_n \rangle$ and $c \in \mathbf{A}$. The equation $\sum_i a_i x_i = c$ admits a solution if and only if $c \in \mathfrak{a}$, i.e. $1 \in (\mathfrak{a} : c)_{\mathbf{A}}$. Since $\mathbf{B}$ is flat, we have $\big(\rho_\star(\mathfrak{a}) : \rho(c)\big)_{\mathbf{B}} = \rho_\star(\mathfrak{a} : c)$ (Proposition 5.5). If $\sum_i \rho(a_i) y_i = \rho(c)$ admits a solution in $\mathbf{B}$, then $1 \in \big(\rho_\star(\mathfrak{a}) : \rho(c)\big)_{\mathbf{B}}$, so the hypothesis *3a* implies that $1 \in (\mathfrak{a} : c)$, i.e. $\sum_i a_i x_i = c$ admits a solution in $\mathbf{A}$.

The implications *3e* ⇒ *3d* ⇒ *3b* are trivial.

3d ⇒ *3c.* Consider the module M/N. The module $\rho_\star(N)$ is identified with a submodule of $\rho_\star(M)$ and $\rho_\star(M/N)$ is identified with $\rho_\star(M)/\rho_\star(N)$. The result follows.

3c ⇒ *3d.* We take $N = 0$.

3a ⇔ *3b.* Same reasoning.

1 ⇒ *3e.* We identify $\mathbf{A}$ with a subring of $\mathbf{B}$.
Let $x \in M$ such that $1 \otimes x = 0$ in $\rho_\star(M)$. Since $\mathbf{B}$ is a flat $\mathbf{A}$-module, this syzygy is explained in the $\mathbf{A}$-module $\mathbf{B}$: there exist $u_1, \ldots, u_n \in \mathbf{B}$ and $a_1, \ldots, a_n \in \mathbf{A}$ such that $\sum_i a_i u_i = 1$ and $a_i x = 0$ for $i \in [\![1..n]\!]$. The equation in the y_i's, $\sum_i a_i y_i = 1$, admits a solution in $\mathbf{B}$, so it admits one in $\mathbf{A}$. Hence $x = 0$.

4 ⇒ *3d.* We make $N = P = 0$ in the sequence $N \to M \to P$. It is exact after scalar extension to $\mathbf{B}$, so it is exact.

1 ⇒ *4.* Suppose that the sequence of $\mathbf{B}$-modules is exact. We must show that the sequence of $\mathbf{A}$-modules is exact. First of all $g \circ f = 0$, because the $\mathbf{B}$-linear map $P \to \rho_\star(P)$ is injective, and the diagrams commute. Next, since $\mathbf{B}$ is flat, we can identify $\rho_\star(\operatorname{Ker} g)$ with $\operatorname{Ker} \rho_\star(g)$ and $\rho_\star(\operatorname{Im} f)$ with $\operatorname{Im} \rho_\star(f)$. We are back in item *3c.* □

Given Theorem 2.3, we obtain as a consequence of the characterization *2a* the following theorem.

6.2. Theorem. *Every extension of a discrete field or of a reduced zero-dimensional ring is faithfully flat.*

D We have $\mathbf{k} \subseteq \mathbf{A}$ with $\mathbf{k}$ reduced zero-dimensional. We know that the extension is flat by Theorem 2.3. We must show that if $\mathfrak{a}$ is a finitely generated ideal of $\mathbf{k}$, then $\mathfrak{a}\mathbf{A} \cap \mathbf{k} = \mathfrak{a}$. However, $\mathfrak{a} = \langle e \rangle$ for an idempotent e; the membership of an element x in an ideal $\langle e \rangle$ (e idempotent) being characterized by the equality $x = xe$, it is independent of the ring. In other words, for an idempotent e of a ring $\mathbf{B} \subseteq \mathbf{B}'$, we always have $e\mathbf{B}' \cap \mathbf{B} = e\mathbf{B}$. □

As a special case of the characterization *3a* we obtain the following corollary.

6.3. Corollary. *Let ρ be a flat homomorphism between local rings. It is faithfully flat if and only if it* reflects the units, *i.e.* $\rho^{-1}(\mathbf{B}^\times) = \mathbf{A}^\times$.

A homomorphism between local rings that reflects the units is called a *local homomorphism.*

The proofs of the two following facts result from simple considerations about the preservation and about the "reflection" of the exact sequences. The details are left to the reader.

6.4. Fact. (Transitivity) *Let* $\mathbf{B}$ *be an* $\mathbf{A}$*-algebra and* $\mathbf{C}$ *be a* $\mathbf{B}$*-algebra.*

1. *If* $\mathbf{B}$ *is flat over* $\mathbf{A}$ *and* $\mathbf{C}$ *flat over* $\mathbf{B}$*, then* $\mathbf{C}$ *is flat over* $\mathbf{A}$.
2. *If* $\mathbf{B}$ *is faithfully flat over* $\mathbf{A}$ *and* $\mathbf{C}$ *faithfully flat over* $\mathbf{B}$*, then* $\mathbf{C}$ *is faithfully flat over* $\mathbf{A}$.
3. *If* $\mathbf{C}$ *is faithfully flat over* $\mathbf{B}$ *and flat over* $\mathbf{A}$*, then* $\mathbf{B}$ *is flat over* $\mathbf{A}$.
4. *If* $\mathbf{C}$ *is faithfully flat over* $\mathbf{B}$ *and over* $\mathbf{A}$*, then* $\mathbf{B}$ *is faithfully flat over* $\mathbf{A}$.

6.5. Fact. (Changing the base ring)
Let $\mathbf{B}$ *and* $\mathbf{C}$ *be two* $\mathbf{A}$*-algebras, and* $\mathbf{D} = \mathbf{B} \otimes_{\mathbf{A}} \mathbf{C}$.

1. *If* $\mathbf{C}$ *is flat over* $\mathbf{A}$*,* $\mathbf{D}$ *is flat over* $\mathbf{B}$.
2. *If* $\mathbf{C}$ *is faithfully flat over* $\mathbf{A}$*,* $\mathbf{D}$ *is faithfully flat over* $\mathbf{B}$.

6.6. Concrete local-global principle. (Localization at the source, flat algebras)
Let $\rho : \mathbf{A} \to \mathbf{B}$ be an algebra and $S_1, \ldots, S_r$ be comaximal monoids of $\mathbf{A}$.

1. *The algebra $\mathbf{B}$ is flat over $\mathbf{A}$ if and only if for each i, $\mathbf{B}_{S_i}$ is flat over $\mathbf{A}_{S_i}$.*
2. *The algebra $\mathbf{B}$ is faithfully flat over $\mathbf{A}$ if and only if for each i, the algebra $\mathbf{B}_{S_i}$ is faithfully flat over $\mathbf{A}_{S_i}$.*

D We introduce the faithfully flat $\mathbf{A}$-algebra $\mathbf{C} = \prod_i \mathbf{A}_{S_i}$ that gives by scalar extension the faithfully flat $\mathbf{B}$-algebra $\mathbf{D} = \prod_i \mathbf{B}_{S_i}$. It remains to apply Facts 6.4 and 6.5. □

The following theorem generalizes the concrete local-global principles that assert the local character (in the constructive sense) of certain properties of finiteness for modules.

6.7. Theorem. *Let $\mathbf{A} \xrightarrow{\rho} \mathbf{B}$ be a faithfully flat $\mathbf{A}$-algebra.*
Let M be an $\mathbf{A}$-module and $M_1 = \rho_\star(M) \simeq \mathbf{B} \otimes_{\mathbf{A}} M$.

1. *The $\mathbf{A}$-module M is flat if and only if the $\mathbf{B}$-module M_1 is flat.*
2. *The $\mathbf{A}$-module M is finitely generated if and only if the $\mathbf{B}$-module M_1 is finitely generated.*
3. *If the $\mathbf{B}$-module M_1 is coherent, the $\mathbf{A}$-module M is coherent.*
4. *The $\mathbf{A}$-module M is finitely presented if and only if the $\mathbf{B}$-module M_1 is finitely presented.*
5. *The $\mathbf{A}$-module M is finitely generated projective if and only if the $\mathbf{B}$-module M_1 is finitely generated projective.*
6. *If the $\mathbf{B}$-module M_1 is Noetherian, the $\mathbf{A}$-module M is Noetherian.*

D In items *1*, *2*, *4*, *5*, we already know that any scalar extension preserves the concerned property. Therefore all that remains to be proven are the converses.

1. Consider an exact sequence $N \xrightarrow{f} Q \xrightarrow{g} P$ of $\mathbf{A}$-modules. We want to show that it is exact after tensorization by M. We know that it is exact after tensorization by $\mathbf{B} \otimes M$. However, $\mathbf{B} \otimes \bullet$ reflects the exact sequences.

2. Consider some elements $y_i \in \rho_\star(M)$ $(i \in [\![1..n]\!])$ that generate this module. These elements are constructed as $\mathbf{B}$-linear combinations of a finite family of elements $1 \otimes x_j$ $(x_j \in M,\ j \in [\![1..m]\!])$. This implies that the $\mathbf{A}$-linear map $\varphi : \mathbf{A}^m \to M$ which sends the canonical basis to $(x_j)_{j \in [\![1..m]\!]}$ is surjective after tensorization by $\mathbf{B}$. However, $\mathbf{B}$ is faithfully flat, therefore φ is surjective.

3. Let $N = \mathbf{A}x_1 + \cdots + \mathbf{A}x_n$ be a finitely generated submodule of M. Consider the corresponding surjective $\mathbf{A}$-linear map $\mathbf{A}^n \to N$, let K be its kernel. The exact sequence $0 \to K \to \mathbf{A}^n \to N \to 0$ gives by scalar extension an exact sequence (because $\mathbf{B}$ is flat). Since $\rho_\star(M)$ is coherent, $\rho_\star(K)$ is finitely generated. It remains to apply item *2.*

4. Same reasoning as for item *3.*

5. A module is finitely generated projective if and only if it is flat and finitely presented.

6. Consider an ascending sequence $(N_k)_{k\in\mathbb{N}}$ of finitely generated submodules of M and extend the scalars to $\mathbf{B}$. Two consecutive terms $\rho_\star(N_\ell)$ and $\rho_\star(N_{\ell+1})$ are equal. Since $\mathbf{B}$ is faithfully flat, we also have the equalities $N_\ell = N_{\ell+1}$. □

The following theorem generalizes the concrete local-global principles that asserts the local character (in the constructive sense) of certain properties of finiteness for algebras.

6.8. Theorem.
Let $\rho : \mathbf{A} \to \mathbf{B}$ be a faithfully flat $\mathbf{A}$-algebra and $\varphi : \mathbf{A} \to \mathbf{C}$ be an $\mathbf{A}$-algebra.
Let $\mathbf{D} = \rho_\star(\mathbf{C})$ be the faithfully flat $\mathbf{C}$-algebra obtained by scalar extension.

$$\begin{tikzcd}
\mathbf{A} \arrow[r, "\varphi", ""{name=U, below}] \arrow[d, "\rho"'] & \mathbf{C} \arrow[d] \\
\mathbf{B} \arrow[r, "\rho_\star(\varphi)"', ""{name=L, above}] & \mathbf{D}
\arrow[from=U, to=L, squiggly, "\rho_\star"]
\end{tikzcd}$$

In order for $\mathbf{C}$ to have one of the properties below as an $\mathbf{A}$-algebra it is necessary and sufficient that $\mathbf{D}$ possesses the same property as a $\mathbf{B}$-algebra:

- *finite (as a module),*
- *finitely presented as a module,*
- *strictly finite,*
- *flat,*
- *faithfully flat,*
- *strictly étale,*
- *separable,*
- *finitely generated (as an algebra),*
- *finitely presented (as an algebra).*

D The first three properties are properties of modules and thus falls within Theorem 6.7.

Flat, faithfully flat algebras. We apply Facts 6.4 and 6.5.

Strictly étale algebras. We already have the equivalence for the strictly finite character. If $\mathbf{B}$ is free over $\mathbf{A}$ we use the fact that the discriminant is well-behaved under scalar extension, and we conclude by using the fact that a faithfully flat extension reflects the units.
In the general case we return to the free case by localization at comaximal elements, or we invoke Theorem VI-6.13: a strictly finite algebra is separable if and only if it is strictly étale.

Separable algebras. Consider at the commutative diagram in Fact VI-6.11 (beware, the names change). The vertical arrow on the right is obtained by faithfully flat scalar extension from the one on the left. They are therefore simultaneously surjective.

Finitely generated algebras. The fact of being finitely generated or finitely presented is preserved by any scalar extension. Let us take a look at the converse.

We identify $\mathbf{A}$ with a subring of $\mathbf{B}$ and $\mathbf{C}$ with a subring of $\mathbf{D}$.

Let $\mathbf{A}_1 = \varphi(\mathbf{A})$ and $\mathbf{B}_1 = \rho_\star(\varphi)(\mathbf{B})$. Since $\mathbf{D} = \mathbf{B} \otimes_{\mathbf{A}} \mathbf{C}$ is finitely generated over $\mathbf{B}$, and since every element of $\mathbf{D}$ is expressible as a $\mathbf{B}$-linear combination of elements of $\mathbf{C}$, we can write $\mathbf{D} = \mathbf{B}_1[x_1, \ldots, x_m]$ with some $x_i \in \mathbf{C} \subseteq \mathbf{D}$. This gives an exact sequence

$$\mathbf{B}[X_1, \ldots, X_m] \xrightarrow{\rho_\star(\varphi),\, X_i \mapsto x_i} \mathbf{D} \longrightarrow 0.$$

We will show that $\mathbf{C} = \mathbf{A}_1[x_1, \ldots, x_m]$. Indeed, the exact sequence above is obtained by faithfully flat scalar extension from the sequence

$$\mathbf{A}[X_1, \ldots, X_m] \xrightarrow{\varphi,\, X_i \mapsto x_i} \mathbf{C} \longrightarrow 0.$$

Finitely presented algebras.

Let us begin with an elementary general but useful remark about quotient algebras $\mathbf{k}[\underline{X}]/\mathfrak{a}$. We can regard $\mathbf{k}[\underline{X}]$ as the free $\mathbf{k}$-module having as its basis the family of monomials $(X^{\underline{\alpha}})_{\underline{\alpha} \in \mathbb{N}^m}$. If $f \in \mathfrak{a}$, we then obtain the equality

$$f \cdot \mathbf{k}[\underline{X}] = \textstyle\sum_{\underline{\alpha}} (X^{\underline{\alpha}} f) \cdot \mathbf{k}.$$

Therefore the ideal $\mathfrak{a}$ is the $\mathbf{k}$-submodule of $\mathbf{k}[\underline{X}]$ generated by all the $X^{\underline{\alpha}} f$, where $\underline{\alpha}$ ranges over $\mathbb{N}^m$ and f ranges over a generator set of $\mathfrak{a}$.

Let us then return to the proof by continuing with the same notations as in the previous item.

Suppose that $\mathbf{D} = \mathbf{B}_1[x_1, \ldots, x_m] \simeq \mathbf{B}[\underline{X}]/\langle f_1, \ldots, f_s \rangle$. In the remainder we consider an equation $f_j = 0$ as a syzygy between the monomials present in f_j. Since the $\mathbf{B}$-module $\mathbf{D}$ is obtained by flat scalar extension of the $\mathbf{A}$-module $\mathbf{C}$, the $\mathbf{B}$-linear dependence relation f_j is a $\mathbf{B}$-linear combination of $\mathbf{A}$-linear dependence relations $f_{j,k}$ (between the same monomials viewed in $\mathbf{C}$). Each equality $f_{j,k}(\underline{x}) = 0$ can also be read as an $\mathbf{A}$-algebraic dependence relation (a relator) between x_i's $\in \mathbf{C}$. Consider then the $\mathbf{A}$-submodule of $\mathbf{A}[\underline{X}]$ generated by all the $X^{\underline{\alpha}} f_{j,k}$'s. By scalar extension from $\mathbf{A}$ to $\mathbf{B}$ the sequence of $\mathbf{A}$-modules

$$0 \to \textstyle\sum_{j,k,\underline{\alpha}} (X^{\underline{\alpha}} f_{j,k}) \cdot \mathbf{A} \to \mathbf{A}[\underline{X}] \to \mathbf{C} \to 0 \quad (*)$$

gives the exact sequence of $\mathbf{B}$-modules

$$0 \to \textstyle\sum_{j,k,\underline{\alpha}} (X^{\underline{\alpha}} f_{j,k}) \cdot \mathbf{B} \to \mathbf{B}[\underline{X}] \to \mathbf{D} \to 0.$$

Indeed, $\sum_{j,k,\underline{\alpha}} (X^{\underline{\alpha}} f_{j,k}) \cdot \mathbf{B} = \sum_{j,k} f_{j,k} \cdot \mathbf{B}[\underline{X}] = \sum_j f_j \cdot \mathbf{B}[\underline{X}] = \mathfrak{a}$. Therefore, since the extension is faithfully flat, the sequence $(*)$ is itself exact. Finally, since $\sum_{j,k,\underline{\alpha}} (X^{\underline{\alpha}} f_{j,k}) \cdot \mathbf{A} = \sum_{j,k} f_{j,k} \cdot \mathbf{A}[\underline{X}]$, $\mathbf{C}$ is a finitely presented $\mathbf{A}$-algebra. □

Exercises and problems

Exercise 1. We recommend that the proofs which are not given, or are sketched, or left to the reader, etc, be done. But in particular, we will cover the following cases.

- Over a Bézout domain, a module is flat if and only if it is torsion-free.
- Prove Theorem 1.3.
- Prove Lemma 3.2.
- Prove Fact 5.2 and Theorem 5.6.
- Prove Facts 6.4 and 6.5.

Exercise 2. Let $\pi : N \to M$ be a surjective linear map.
1. If M is flat, for every finitely presented module P, the natural linear map

$$\mathrm{L}_{\mathbf{A}}(P, \pi) : \mathrm{L}_{\mathbf{A}}(P, N) \to \mathrm{L}_{\mathbf{A}}(P, M)$$

is surjective. *(Particular case of Theorem 1.16.)*
2. Suppose that $N = \mathbf{A}^{(I)}$, a free module over a discrete set I. If the previous property is satisfied, M is flat.

Comment. In constructive mathematics, an arbitrary module M is not necessarily a quotient of a module $N = \mathbf{A}^{(I)}$ as above, but this is true in the case where M is discrete, by taking $I = M$. If we don't need I discrete, we look at Exercise 16. ■

Exercise 3. Let M be a finitely generated $\mathbf{A}$-module. Prove that if M is flat its Fitting ideals are idempotents.

Exercise 4. Show using classical mathematics that a ring is a pf-ring if and only if it becomes integral after localization at any prime ideal.

Exercise 5. Show using classical mathematics that a ring is arithmetic if and only if it becomes a Bézout ring after localization at any prime ideal.

Exercise 6. The image of a locally principal ideal under a ring homomorphism is a locally principal ideal. Prove that the analogous result for invertible ideals is not always true.

Exercise 7. If $\mathfrak{a} = \langle x_1, \dots, x_k \rangle$ is locally principal, then $\mathfrak{a}^n = \langle x_1^n, \dots, x_k^n \rangle$.
Compute a principal localization matrix for $(x_1^n, \dots, x_k^n)$ from a principal localization matrix for $(x_1, \dots, x_k)$.
Explicate the membership of $x_1^{n_1} \cdots x_k^{n_k} \in \langle x_1^n, \dots, x_k^n \rangle$ when $n = n_1 + \cdots + n_k$.

Exercise 8. Given n elements in an arithmetic ring give an algorithm that constructs a principal localization matrix for those elements from principal localization matrices for pairs of elements only.

Exercise 9. Consider two finitely generated ideals $\mathfrak{a}$ and $\mathfrak{b}$ of a ring $\mathbf{A}$, generated respectively by m and n elements. Let f, $g \in \mathbf{A}[X]$ of degrees $m-1$ and $n-1$ with $\mathrm{c}(f) = \mathfrak{a}$ and $\mathrm{c}(g) = \mathfrak{b}$.

1. Show that if $\mathfrak{a}$ is locally principal, we have $\mathfrak{a}\mathfrak{b} = \mathrm{c}(fg)$ such that $\mathfrak{a}\mathfrak{b}$ is generated by $n + m - 1$ elements (localize and use Corollary III-2.3 *4*).

2. Show that if $\mathfrak{a}$ and $\mathfrak{b}$ are locally principal, $\mathfrak{a}\mathfrak{b}$ is locally principal. Explain how to construct a principal localization matrix for the coefficients of fg from two principal localization matrices, respectively for the generators of $\mathfrak{a}$ and for those of $\mathfrak{b}$.

Exercise 10. We are interested in the eventual equality

$$\mathfrak{a}\,\mathfrak{b} = (\mathfrak{a} \cap \mathfrak{b})(\mathfrak{a} + \mathfrak{b}) \tag{4}$$

for two finitely generated ideals $\mathfrak{a}$ and $\mathfrak{b}$ of a ring $\mathbf{A}$.

1. Show that the equality is satisfied if $\mathfrak{a} + \mathfrak{b}$ is locally principal. If in addition $\mathfrak{a}$ and $\mathfrak{b}$ are locally principal, then $\mathfrak{a} \cap \mathfrak{b}$ is locally principal.

2. Suppose $\mathbf{A}$ is integral. Show that if the equality is satisfied when $\mathfrak{a}$ and $\mathfrak{b}$ are principal ideals then the ring is arithmetic.

3. Show that the following properties are equivalent.

- $\mathbf{A}$ is a Prüfer ring.
- $\mathbf{A}$ is a pf-ring and Equation (4) is satisfied for principal ideals.
- $\mathbf{A}$ is a pf-ring and Equation (4) is satisfied for finitely generated ideals.

Exercise 11. (See also Exercise V-16) Let $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ be finitely generated ideals. Prove the following statements.

1. If $\mathfrak{a} + \mathfrak{b}$ is locally principal, then $(\mathfrak{a} : \mathfrak{b}) + (\mathfrak{b} : \mathfrak{a}) = \langle 1 \rangle$.

2. If $(\mathfrak{a} : \mathfrak{b}) + (\mathfrak{b} : \mathfrak{a}) = \langle 1 \rangle$, then

a. $(\mathfrak{a} + \mathfrak{b}) : \mathfrak{c} = (\mathfrak{a} : \mathfrak{c}) + (\mathfrak{b} : \mathfrak{c})$.

b. $\mathfrak{c} : (\mathfrak{a} \cap \mathfrak{b}) = (\mathfrak{c} : \mathfrak{a}) + (\mathfrak{c} : \mathfrak{b})$.

c. $(\mathfrak{a} + \mathfrak{b})(\mathfrak{a} \cap \mathfrak{b}) = \mathfrak{a}\,\mathfrak{b}$.

d. $\mathfrak{c}\,(\mathfrak{a} \cap \mathfrak{b}) = \mathfrak{c}\,\mathfrak{a} \cap \mathfrak{c}\,\mathfrak{b}$.

e. $\mathfrak{c} + (\mathfrak{a} \cap \mathfrak{b}) = (\mathfrak{c} + \mathfrak{a}) \cap (\mathfrak{c} + \mathfrak{b})$.

f. $\mathfrak{c} \cap (\mathfrak{a} + \mathfrak{b}) = (\mathfrak{c} \cap \mathfrak{a}) + (\mathfrak{c} \cap \mathfrak{b})$.

g. The following short exact sequence (where $\delta(x) = (x, -x)$ and $\sigma(y, z) = y + z$) is split:

$$0 \longrightarrow \mathfrak{a} \cap \mathfrak{b} \xrightarrow{\delta} \mathfrak{a} \times \mathfrak{b} \xrightarrow{\sigma} \mathfrak{a} + \mathfrak{b} \longrightarrow 0.$$

Exercise 12. *(Gaussian rings)* A ring $\mathbf{A}$ is said to be *Gaussian* when for all polynomials f, $g \in \mathbf{A}[X]$, we have the equality $\mathrm{c}(fg) = \mathrm{c}(f)\mathrm{c}(g)$. Prove the following statements.

1. Every arithmetic ring is Gaussian (see Exercise 9).

2. A Gaussian integral ring is a Prüfer ring.

3. A Gaussian reduced ring is a Prüfer ring. A Gaussian pp-ring is a coherent Prüfer ring (see Theorem XII-4.1).

Exercise 13. *(A useful ring for counterexamples)*
Let $\mathbf{K}$ be a nontrivial discrete field and V be a $\mathbf{K}$-vector space of dimension 2. Consider the $\mathbf{K}$-algebra $\mathbf{A} = \mathbf{K} \oplus V$ defined by x, $y \in V \Rightarrow xy = 0$. Show that every element of $\mathbf{A}$ is invertible or nilpotent (i.e. $\mathbf{A}$ is local zero-dimensional), and that the ring is coherent but not arithmetic. However, every finitely generated ideal that contains a regular element is equal to $\langle 1 \rangle$, a fortiori it is invertible.

Exercise 14. Let $\mathbf{A}$ be a residually discrete coherent local ring.
Let $\mathfrak{m} = \operatorname{Rad} \mathbf{A}$ and suppose that $\mathfrak{m}$ is flat over $\mathbf{A}$.

1. Show that $\mathbf{A}$ is integral.

2. Show that $\mathbf{A}$ is a valuation ring.

NB: We do not assume that $\mathbf{A}$ is nontrivial.

Exercise 15. *(Flat quotient of a flat module: a direct proof)*
Provide a direct proof of the following implication of Theorem 1.16: Let M be a flat $\mathbf{A}$-module and K be a submodule of M satisfying $\mathfrak{a}M \cap K = \mathfrak{a}K$ for every finitely generated ideal $\mathfrak{a}$; then M/K is flat.

Exercise 16. This exercise starts with a long introductory text. A single question is posed, at the very end. We specify in the following definition the construction of the direct sum $\bigoplus_{i \in I} M = M^{(I)}$ for an arbitrary (not necessarily discrete) set I and a module M.[3] This allows us to show that every module is a quotient of a flat module (actually a free module, not necessarily projective from a constructive point of view!).

Definition. Let I be an arbitrary set and M be an $\mathbf{A}$-module. We define the *direct sum* $M^{(I)}$ as a quotient set of the set of finite formal sums $\oplus_{k \in [\![1..n]\!]}(i_k, x_k)$, where $i_k \in I$ and $x_k \in M$ for each $k \in [\![1..n]\!]$: such a formal sum is defined as being precisely the family $(i_k, x_k)_{k \in [\![1..n]\!]}$.
The equivalence relation that defines the equality over $M^{(I)}$ is the equivalence relation generated by the following “equalities”:

- associativity and commutativity of the formal sums: we can reorder the family as we wish,
- if $i_k =_I i_\ell$ then (i_k, x_k) and (i_ℓ, x_ℓ) can be replaced by $(i_k, x_k + x_\ell)$ (“contraction” of the list); we can write this rewriting in the following form: if $i =_I j$ then $(i, x_i) \oplus (j, x_j) = (i, x_i + x_j)$;
- every term $(i, 0_M)$ can be deleted.

The addition over $M^{(I)}$ is defined by concatenation, and the external law is defined by $a \cdot \oplus_{k \in [\![1..n]\!]}(i_k, x_k) = \oplus_{k \in [\![1..n]\!]}(i_k, a x_k)$.
Finally, the $\mathbf{A}$-*module freely generated by* I is the module $\mathbf{A}^{(I)}$.

[3] Concerning the general notion of a family of sets indexed by an arbitrary set, see [MRR, page 18]; the construction of the direct sum of an arbitrary family of $\mathbf{A}$-modules is explained on pages 54 et 55.

The direct sum solves the corresponding universal problem, which we can schematize by the following graph for a family $(\varphi_i)_{i\in I}$ of linear maps from M to an arbitrary module N.

$$\begin{tikzcd}
 & & M_i = M \arrow[dll, "\varphi_i"'] \arrow[dl, "\jmath_i"] & \jmath_i(x) = (i,x) \\
N & P \arrow[l, dashed, "\varphi!"'] & & P = M^{(I)} \\
 & & M_j = M \arrow[ull, "\varphi_j"] \arrow[ul, "\jmath_j"'] & \\
 & & M_\ell = M \arrow[uull, "\varphi_\ell"] \arrow[uul, "\jmath_\ell"'] &
\end{tikzcd}$$

Let I be an arbitrary set with at least one element. The $\mathbf{A}$-module $\mathbf{A}^{(I)}$, is called the *module freely generated by the set I.* It solves the corresponding universal problem, which we can schematize by the following graph for a family $x = (x_i)_{i\in I}$ in an arbitrary module N.

$$\begin{tikzcd}
 & & I \arrow[dll, "x"'] \arrow[dl, "\jmath"] & x(i) = x_i \\
N & \mathbf{A}^{(I)} \arrow[l, dashed, "\psi!"'] & & \jmath(i) = (i,1)
\end{tikzcd}$$

Note that as a consequence, *if $(x_i)_{i\in I}$ is an arbitrary generator set of the module N, the latter is isomorphic to a quotient of $\mathbf{A}^{(I)}$.*

Let I be an arbitrary set and M be an $\mathbf{A}$-module. Prove that the module $M^{(I)}$ is flat if and only if M is flat. In particular this shows that the free module $\mathbf{A}^{(I)}$ is flat.

Some solutions, or sketches of solutions

Exercise 1.

Over a Bézout domain $\mathbf{Z}$, a module M is flat if and only if it is torsion-free.

We know that the condition is necessary. Let us prove that it is sufficient.
Consider a syzygy LX in M with $L = [\,a_1\ \cdots\ a_n\,]$ and $X = {}^{\rm t}[\,x_1\ \cdots\ x_n\,]$. If the a_i's are all null, we have $L\,\mathrm{I}_n = 0$ and $\mathrm{I}_n X = X$, which explains $LX = 0$ in M.
Otherwise, we write $\sum_i a_i u_i = g$ and $g b_i = a_i$, where g is the gcd of the a_i's.
We have $g(\sum_i b_i x_i) = 0$, and since M is torsion-free $\sum_i b_i x_i = 0$.
The matrix $C = \big((u_i b_j)_{i,j\in[\![1..n]\!]}\big) = UB$ with $B = \frac{1}{g}L$, is a principal localization matrix for $(a_1, \ldots, a_n)$. Let $G = \mathrm{I}_n - C$, we have $CX = 0$ and $LC = L$, so $LG = 0$ and $GX = X$, which explains $LX = 0$ in M.

Exercise 2.

1. Let $\mu : P \to M$ be a linear map. We know (Theorem 1.3) that μ factorizes through a finitely generated free module L: $\mu = \lambda \circ \psi$.

$$\begin{tikzcd}
P \arrow[r, "\psi"] \arrow[d, "?"'] \arrow[dr, "\mu"] & L \arrow[d, "\lambda"] & \\
N \arrow[r, "\pi"] & M \arrow[r] & 0
\end{tikzcd}$$

Since L is free, we can write $\lambda = \pi \circ \nu$ with a linear map $\nu : L \to N$, and so $\mu = \pi \circ \varphi$ for $\varphi = \nu \circ \psi$.

2. If the property is satisfied with $N = \mathbf{A}^{(I)}$, where I is a discrete set, we consider an arbitrary linear map $\mu : P \to M$ with P finitely presented. We write $\mu = \pi \circ \varphi$ with a linear map $\varphi : P \to N$. There then exists a finite subset I_0 of I such that for each generator g_j of P, $\varphi(g_j)$ has null coordinates outside of I_0. This shows that we can factorize μ via the free module of finite rank $\mathbf{A}^{(I_0)}$. Therefore by Theorem 1.3, M is flat.

Exercise 3.

Consider a finitely generated module M with a generator set $(x_1, \dots, x_n)$. Let $X = {}^{\rm t}[\, x_1 \ \cdots \ x_n \,]$. For $k \in [\![0..n]\!]$ and $k + r = n$, a typical generator of $\mathcal{F}_k(M)$ is $\delta = \det(L)$ where $L \in \mathbb{M}_r(\mathbf{A})$ and $LY = 0$, for a column vector extracted from X: $Y = {}^{\rm t}[\, x_{i_1} \ \cdots \ x_{i_r} \,]$.

We must show that $\delta \in \mathcal{F}_k(M)^2$. Actually we will show that $\delta \in \delta\, \mathcal{F}_k(M)$.

Suppose without loss of generality that $(i_1, \dots, i_r) = (1, \dots, r)$. We apply Proposition 2.2. We therefore have a matrix $H \in \mathbb{M}_{r,n}$ with $HX = Y$ and $LH = 0$.

Let $H' = \mathrm{I}_{r,r,n} = \begin{array}{|c|c|}\hline \mathrm{I}_r & 0 \\ \hline \end{array}$, and $K = H' - H$. We have

$$KX = Y - Y = 0 \ \text{ and } \ LK = LH' = \begin{array}{|c|c|}\hline L & 0 \\ \hline \end{array}.$$

Let K' be the matrix formed by the first r columns of K. Then $L = LK'$ and $\det(L) = \det(L)\det(K')$, and since $KX = 0$, we have $\det(K') \in \mathcal{F}_k(M)$.

Exercise 4. Suppose the ring $\mathbf{A}$ is a pf-ring. Let $\mathfrak{p}$ be a prime ideal and $xy = 0$ in $\mathbf{A}_\mathfrak{p}$. There exists a $u \notin \mathfrak{p}$ such that $uxy = 0$ in $\mathbf{A}$. Let s and $t \in \mathbf{A}$ such that $s + t = 1$, $sux = 0$ and $ty = 0$ in $\mathbf{A}$. The elements s and t cannot both be in $\mathfrak{p}$ (otherwise $1 \in \mathfrak{p}$). If $s \notin \mathfrak{p}$, then since $sux = 0$, we obtain $x =_{\mathbf{A}_\mathfrak{p}} 0$. If $t \notin \mathfrak{p}$, then since $ty = 0$, we obtain $y =_{\mathbf{A}_\mathfrak{p}} 0$. Thus $\mathbf{A}_\mathfrak{p}$ is an integral ring.

Now suppose that every localized ring $\mathbf{A}_\mathfrak{p}$ at every maximal ideal $\mathfrak{p}$ is integral and suppose that $xy =_{\mathbf{A}} 0$. For some arbitrary maximal ideal $\mathfrak{p}$ we have $x =_{\mathbf{A}_\mathfrak{p}} 0$ or $y =_{\mathbf{A}_\mathfrak{p}} 0$. In the first case let $s_\mathfrak{p} \notin \mathfrak{p}$ such that $s_\mathfrak{p} x =_{\mathbf{A}} 0$. Otherwise let $t_\mathfrak{p} \notin \mathfrak{p}$ such that $t_\mathfrak{p} y =_{\mathbf{A}} 0$. The family of the $s_\mathfrak{p}$'s or $t_\mathfrak{p}$'s generates the ideal $\langle 1 \rangle$ (because otherwise all $s_\mathfrak{p}$'s or $t_\mathfrak{p}$'s would be in some maximal ideal).

There is therefore a finite number of s_i's satisfying $s_i x = 0$ (in $\mathbf{A}$) and a finite number of t_j's satisfying $t_j y = 0$, with an equation $\sum_i c_i s_i + \sum_j d_j t_j = 1$.

We take $s = \sum_i c_i s_i$, $t = \sum_j d_j t_j$ and we obtain $sx = ty = 0$ and $s + t = 1$.

Exercise 5. We begin by recalling the following: by item *3* of Theorem V-7.3, an ideal $\langle a, b\rangle$ of a ring $\mathbf{A}$ is locally principal if and only if we can find s, t, u, $v \in \mathbf{A}$ such that $s + t = 1$, $sa = ub$ and $tb = va$.

Suppose the ring $\mathbf{A}$ is arithmetic. Let $\mathfrak{p}$ be a prime ideal. For a, $b \in \mathbf{A}_\mathfrak{p}$ we want to show that a divides b or b divides a (see Lemma IV-7.1). Without loss of generality we can take a and b in $\mathbf{A}$. Then let s, t, u, v be as above. The elements s and t cannot both be in $\mathfrak{p}$ (otherwise $1 \in \mathfrak{p}$). If $s \notin \mathfrak{p}$, then $a =_{\mathbf{A}_\mathfrak{p}} s^{-1}ub$ so b divides a in $\mathbf{A}_\mathfrak{p}$. If $t \notin \mathfrak{p}$, then a divides b in $\mathbf{A}_\mathfrak{p}$.

Now suppose that every localized ring $\mathbf{A}_\mathfrak{p}$ at every maximal ideal $\mathfrak{p}$ is a local Bézout ring and let a, $b \in \mathbf{A}$.

For an arbitrary maximal ideal $\mathfrak{p}$, we have that b divides a or a divides b in $\mathbf{A}_\mathfrak{p}$. In the first case let $s_\mathfrak{p} \notin \mathfrak{p}$ and $u_\mathfrak{p} \in \mathbf{A}$ such that $s_\mathfrak{p} a =_\mathbf{A} u_\mathfrak{p} b$. Otherwise let $t_\mathfrak{p} \notin \mathfrak{p}$ and $v_\mathfrak{p}$ such that $t_\mathfrak{p} b =_\mathbf{A} v_\mathfrak{p} a$. The family of the $s_\mathfrak{p}$'s or $t_\mathfrak{p}$'s generates the ideal $\langle 1\rangle$ (because otherwise all $s_\mathfrak{p}$'s or $t_\mathfrak{p}$'s would be in some maximal ideal).

Therefore there is a finite number of s_i's, u_i's satisfying $s_i a = u_i b$ (in $\mathbf{A}$) and a finite number of t_j's, v_j's satisfying $t_j b = v_j a$, with an equation $\sum_i c_i s_i + \sum_j d_j t_j = 1$. We take $s = \sum_i c_i s_i$, $u = \sum_i c_i u_i$, $t = \sum_j d_j t_j$, $v = \sum_j d_j v_j$ and we obtain the equalities $s + t = 1$, $sa = ub$ and $tb = va$.

For an ideal with a finite number of generators, we can reason analogously, or use the result of Exercise 8.

Exercise 6.

The image of the principal ideal $\langle 60\rangle$ of $\mathbb{Z}$ under the homomorphism $\mathbb{Z} \to \mathbb{Z}/27\mathbb{Z}$ is the ideal $\langle 3\rangle$ which does not contain any regular element, and which is not invertible. Actually, as a $\mathbb{Z}/27\mathbb{Z}$-module, the ideal $\langle 3\rangle$ is not even projective (its annihilator $\langle 9\rangle$ is not idempotent).

When $\rho : \mathbf{A} \to \mathbf{B}$ is a flat algebra, the image of an ideal $\mathfrak{a} \subseteq \mathbf{A}$ is isomorphic to $\rho_\star(\mathfrak{a}) \simeq \mathbf{B} \otimes_\mathbf{A} \mathfrak{a}$. Therefore if $\mathfrak{a}$ is invertible, as it is projective of rank 1, its image is also a projective module of rank 1.

Exercise 7.

We first note that a product of locally principal ideals is always locally principal, because after suitable comaximal localizations, each ideal becomes principal, and so does their product.

We are then content with the $\mathfrak{a} = \langle a, b\rangle$ case and with the $\left\langle a^4, b^4\right\rangle$ example. It will be clear that the computation technique is easily generalized.

We start with $sa = ub$, $tb = va$ and $s + t = 1$. Therefore $s^4a^4 = u^4b^4$ and $t^4b^4 = v^4a^4$. Since $\left\langle s^4, t^4\right\rangle = \langle 1\rangle$ (which is obtained by writing $1 = (s + t)^7$), we indeed obtain that the ideal $\left\langle a^4, b^4\right\rangle$ is locally principal.

Let us show, for example, that $a^2b^2 \in \left\langle a^4, b^4\right\rangle$.

We write $s^2a^2 = u^2b^2$ and $t^2b^2 = v^2a^2$. Therefore $s^2a^2b^2 = u^2b^4$ and $t^2a^2b^2 = v^2a^4$.

Finally, $1 = (s + t)^3 = s^2(s + 3t) + t^2(t + 3s)$. Therefore

$$a^2b^2 = (t + 3s)v^2a^4 + (s + 3t)u^2b^4.$$

Exercise 8. We do not need to assume that the ring is arithmetic.
We will show that if in a ring $\mathbf{A}$ each pair (a_i, a_j) admits a principal localization matrix, the same goes for the n-tuple $(a_1, \ldots, a_n)$.
This can be compared to Dedekind's proof of Theorem III-8.21, which concerns only invertible ideals, because over an integral ring the invertible ideals are precisely the nonzero locally principal ideals.
Also note that the result is a priori clear: by successive comaximal localizations, every leaf of each branch of an a priori very large computation tree will be a principal ideal. This will show that the ideal $\langle a_1, \ldots, a_n \rangle$ is always generated by one of the a_i's after localizations at comaximal elements. What we are aiming for here is rather a practical computation of the principal localization matrix.
We proceed by induction on n.

Let us show the induction step for the passage of $n = 3$ to $n + 1 = 4$.
Consider a_1, a_2, a_3, $a_4 \in \mathbf{Z}$.

By induction hypothesis we have a matrix $C = \begin{bmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \\ z_1 & z_2 & z_3 \end{bmatrix}$ suitable for (a_1, a_2, a_3), and matrices $\begin{bmatrix} c_{11} & c_{14} \\ d_{11} & d_{14} \end{bmatrix}$, $\begin{bmatrix} c_{22} & c_{24} \\ d_{22} & d_{24} \end{bmatrix}$, $\begin{bmatrix} c_{33} & c_{34} \\ d_{33} & d_{34} \end{bmatrix}$ respectively suitable for (a_1, a_4), (a_2, a_4) and (a_3, a_4). Then we will check that the <u>transpose</u> of the following matrix is suitable for (a_1, a_2, a_3, a_4)

$$\begin{bmatrix} c_{11}x_1 & c_{22}y_1 & c_{33}z_1 & d_{11}x_1 + d_{22}y_1 + d_{33}z_1 \\ c_{11}x_2 & c_{22}y_2 & c_{33}z_2 & d_{11}x_2 + d_{22}y_2 + d_{33}z_2 \\ c_{11}x_3 & c_{22}y_3 & c_{33}z_3 & d_{11}x_3 + d_{22}y_3 + d_{33}z_3 \\ c_{14}x_1 & c_{24}y_2 & c_{34}z_3 & d_{14}x_1 + d_{24}y_2 + d_{34}z_3 \end{bmatrix}$$

First of all, we must check that the trace of the matrix is equal to 1, i.e.

$$t = c_{11}x_1 + c_{22}y_2 + c_{33}z_3 + d_{14}x_1 + d_{24}y_2 + d_{34}z_3 = 1,$$

but $c_{11} + d_{14} = 1 = c_{22} + d_{24} = c_{33} + d_{34}$ so $t = x_1 + y_2 + z_3 = 1$.
We must check that each row of the transposed matrix is proportional to $[\, a_1 \; a_2 \; a_3 \; a_4 \,]$. Two cases arise. First of all, we consider one of the first three rows, for instance the row $[\, c_{11}x_1 \; c_{11}x_2 \; c_{11}x_3 \; c_{14}x_1 \,]$. Both of the following types of equalities must be satisfied

$$a_1c_{11}x_2 = a_2c_{11}x_1, \quad \text{and} \quad a_1c_{14}x_1 = a_4c_{11}x_1.$$

For the first equality we use $a_2x_1 = a_1x_2$ and for the second $a_1c_{14} = a_4c_{11}$.
Finally, we must verify that $[\, a_1 \; a_2 \; a_3 \; a_4 \,]$ is proportional to the transpose of

$$\begin{bmatrix} d_{11}x_1 + d_{22}y_1 + d_{33}z_1 \\ d_{11}x_2 + d_{22}y_2 + d_{33}z_2 \\ d_{11}x_3 + d_{22}y_3 + d_{33}z_3 \\ d_{14}x_1 + d_{24}y_2 + d_{34}z_3 \end{bmatrix}.$$

This results on the one hand from the proportionality of $[\, a_1 \; a_2 \; a_3 \,]$ to each of the rows $[\, x_i \; y_i \; z_i \,]$, and on the other hand from the proportionality of the rows $[\, a_i \; a_4 \,]$ to the rows $[\, d_{i1} \; d_{i4} \,]$.

To complete the proof, note that the passage of $n - 1$ to n (for any $n > 2$) is perfectly analogous.

Exercise 9. We write $\mathfrak{a} = \langle a_1, \ldots, a_m \rangle$, $\mathfrak{b} = \langle b_1, \ldots, b_n \rangle$. We can assume that $f = \sum_{k=1}^{m} a_k X^{k-1}$ and $g = \sum_{h=1}^{n} b_h X^{h-1}$.

1. Let F be a principal localization matrix for $(a_1, \ldots, a_m)$. If $\mathrm{c}(f) = \mathfrak{a}$, we have comaximal elements s_i (the diagonal of F) and polynomials $f_i \in \mathbf{A}[X]$ (given by the rows of F) that satisfy the equalities $s_i f = a_i f_i$ in $\mathbf{A}[X]$. In addition, the coefficient of X^{i-1} in f_i is equal to s_i, so $\mathrm{c}(f_i) \supseteq \langle s_i \rangle$.
By letting $\mathbf{A}_i = \mathbf{A}\left[\frac{1}{s_i}\right]$, we have $\mathrm{c}(f_i) =_{\mathbf{A}_i} \langle 1 \rangle$ and the equalities

$$s_i \mathrm{c}(fg) = \mathrm{c}(a_i f_i g) = a_i \mathrm{c}(f_i g) =_{\mathbf{A}_i} a_i \mathrm{c}(g) =_{\mathbf{A}_i} \mathrm{c}(a_i f_i)\mathrm{c}(g) = s_i \mathrm{c}(f)\mathrm{c}(g)$$

(the third equality comes from Corollary III-2.3 *4* because $\mathrm{c}(f_i) =_{\mathbf{A}_i} \langle 1 \rangle$).
Hence the equality $\mathrm{c}(fg) = \mathrm{c}(f)\mathrm{c}(g) = \mathfrak{a}\mathfrak{b}$ because it is true in each $\mathbf{A}_i$.

2. If g is also locally principal we obtain $t_j b = b_j g_j$ in $\mathbf{A}[X]$, with $\mathrm{c}(g_j) \supseteq \langle t_j \rangle$ and comaximal t_j in $\mathbf{A}$. We therefore have

$$s_i t_j \mathrm{c}(fg) =_{\mathbf{A}_{ij}} a_i b_j \mathrm{c}(f_i g_j) =_{\mathbf{A}_{ij}} \langle a_i b_j \rangle .$$

This tells us that the ideal $\mathrm{c}(fg) = \mathfrak{a}\,\mathfrak{b}$ becomes principal after mn comaximal localizations. As this ideal admits $m + n - 1$ generators (the coefficients of fg) there is a principal localization matrix for these generators.
To compute it, we can use the proof of the implication *1* ⇒ *3* in Theorem V-7.3. This proof is quite simple, as well as the computation it implies. But if we examine in detail what is going to happen, we realise that in the proof below we have used the Gauss-Joyal lemma: over the ring $\mathbf{A}_{ij}$, we have $1 \in \mathrm{c}(f_i)\mathrm{c}(g_j)$ because $1 \in \mathrm{c}(f_i)$ and $1 \in \mathrm{c}(g_j)$. This lemma admits several elementary proofs (see II-2.6 and III-2.3), but none of them gives a simple formula that allows us to provide the linear combination of the coefficients of fg equal to 1, from two linear combinations of the coefficients of f and of those of g.
We would be grateful to any reader who is able to indicate to us a short direct computation, for example in the case where the ring is integral with explicit divisibility.[4]

Exercise 10. We write $\mathfrak{a} = \langle a_1, \ldots, a_n \rangle$, $\mathfrak{b} = \langle b_1, \ldots, b_m \rangle$.
We will use the result of Exercise 8 which shows that if every ideal with two generators is locally principal, then every finitely generated ideal is locally principal.

1. In Exercise V-16 item *4* we have shown that $1 \in (\mathfrak{a} : \mathfrak{b}) + (\mathfrak{b} : \mathfrak{a})$, $\mathfrak{a} \cap \mathfrak{b}$ is finitely generated and $\mathfrak{a}\mathfrak{b} = (\mathfrak{a} \cap \mathfrak{b})(\mathfrak{a} + \mathfrak{b})$.
If $\mathfrak{a} + \mathfrak{b}$ is locally principal, there is a system of comaximal elements such that by inverting any one of them, the ideal is generated by some a_k or some b_ℓ. But if $\mathfrak{a} + \mathfrak{b} = \langle a_k \rangle \subseteq \mathfrak{a}$, we have $\mathfrak{b} \subseteq \mathfrak{a}$, so $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{b}$, locally principal by hypothesis. Thus $\mathfrak{a} \cap \mathfrak{b}$ is locally principal because it is locally principal after localization at comaximal elements.

2. If the ring is integral and if $(\mathfrak{a} + \mathfrak{b})(\mathfrak{a} \cap \mathfrak{b}) = \mathfrak{a}\mathfrak{b}$ for $\mathfrak{a} = \langle a \rangle$ and $\mathfrak{b} = \langle b \rangle$ (where $a, b \neq 0$), we get that $\langle a, b \rangle (\mathfrak{a} \cap \mathfrak{b}) = \langle ab \rangle$, so $\langle a, b \rangle$ is invertible (and

[4] Please note that in the case of an integral ring with explicit divisibility, a principal localization matrix is known from its only diagonal elements, which can simplify computations.

also $\langle a\rangle \cap \langle b\rangle$ at the same time). When it is satisfied for all $a, b \neq 0$, the ring is arithmetic.

3. The only delicate implication consists in showing that if $\mathbf{A}$ is a pf-ring and if $(\mathfrak{a}+\mathfrak{b})(\mathfrak{a}\cap\mathfrak{b}) = \mathfrak{a}\mathfrak{b}$ when $\mathfrak{a} = \langle a\rangle$ and $\mathfrak{b} = \langle b\rangle$ then the ring is arithmetic, in other words every ideal $\langle a, b\rangle$ is locally principal.

If $\langle a, b\rangle\,(\mathfrak{a}\cap\mathfrak{b}) = \langle ab\rangle$, we write $ab = au + bv$ with u and $v \in \mathfrak{a}\cap\mathfrak{b}$:

$$u = ax = by,\ v = az = bt,\ \text{ hence }\ au + bv = ab(y+z) = ab.$$

Since the ring is a pf-ring, from the equality $ab(y+z-1) = 0$, we deduce three comaximal localizations in which we obtain $a = 0$, $b = 0$ and $1 = y+z$ respectively. In the first two cases $\langle a, b\rangle$ is principal. In the last case $\langle a, b\rangle$ is locally principal (localize at y or at z).

Exercise 11. We write $\mathfrak{a} = \langle a_1, \ldots, a_n\rangle$, $\mathfrak{b} = \langle b_1, \ldots, b_m\rangle$.

1. Proven in item *4* of Exercise V-16.

2. Now suppose $(\mathfrak{a} : \mathfrak{b}) + (\mathfrak{b} : \mathfrak{a}) = \langle 1\rangle$, i.e. we have s, $t \in \mathbf{A}$ with

$$s + t = 1,\ s\mathfrak{a} \subseteq \mathfrak{b},\ t\mathfrak{b} \subseteq \mathfrak{a}.$$

2a. $(\mathfrak{a}+\mathfrak{b}) : \mathfrak{c} = (\mathfrak{a} : \mathfrak{c}) + (\mathfrak{b} : \mathfrak{c})$. In this equality as in the following (up to *2f*), an inclusion is not obvious (here it is $\subseteq$). Proving the non-obvious inclusion comes down to solving a system of linear equations (here, given some x such that $x\mathfrak{c} \subseteq \mathfrak{a}+\mathfrak{b}$, we look for y and z such that $x = y+z$, $y\mathfrak{c} \subseteq \mathfrak{a}$ and $z\mathfrak{c} \subseteq \mathfrak{b}$).

We can therefore use the basic local-global principle with the comaximal elements s and t.

When we invert s, we get $\mathfrak{a} \subseteq \mathfrak{b}$, and if we invert t, we get $\mathfrak{b} \subseteq \mathfrak{a}$. In both cases the desired inclusion becomes trivial.

For the record: *2b.* $\mathfrak{c} : (\mathfrak{a}\ \cap\ \mathfrak{b}) = (\mathfrak{c} : \mathfrak{a}) + (\mathfrak{c} : \mathfrak{b})$. *2c.* $(\mathfrak{a}+\mathfrak{b})(\mathfrak{a}\ \cap\ \mathfrak{b}) = \mathfrak{a}\ \mathfrak{b}$. *2d.* $\mathfrak{c}\,(\mathfrak{a}\ \cap\ \mathfrak{b}) = \mathfrak{c}\ \mathfrak{a}\ \cap\ \mathfrak{c}\ \mathfrak{b}$. *2e.* $\mathfrak{c} + (\mathfrak{a}\ \cap\ \mathfrak{b}) = (\mathfrak{c}+\mathfrak{a}) \cap (\mathfrak{c}+\mathfrak{b})$. *2f.* $\mathfrak{c}\ \cap\ (\mathfrak{a}+\mathfrak{b}) = (\mathfrak{c}\ \cap\ \mathfrak{a}) + (\mathfrak{c}\ \cap\ \mathfrak{b})$.

2g. The short exact sequence below (where $\delta(x) = (x, -x)$ and $\sigma(y, z) = y + z$) is split:

$$0 \longrightarrow \mathfrak{a}\ \cap\ \mathfrak{b} \xrightarrow{\delta} \mathfrak{a}\times\mathfrak{b} \xrightarrow{\sigma} \mathfrak{a}+\mathfrak{b} \longrightarrow 0.$$

We want to define $\tau : \mathfrak{a}+\mathfrak{b} \to \mathfrak{a}\times\mathfrak{b}$ such that $\sigma\circ\tau = \mathrm{Id}_{\mathfrak{a}+\mathfrak{b}}$.

If $\mathfrak{a} \subseteq \mathfrak{b}$, we can take $\tau(b) = (0, b)$ for all $b \in \mathfrak{b} = \mathfrak{a}+\mathfrak{b}$. If $\mathfrak{b} \subseteq \mathfrak{a}$, we can take $\tau(a) = (a, 0)$ for all $a \in \mathfrak{a} = \mathfrak{a}+\mathfrak{b}$.

In the first case this implies $s\tau(a_i) = \big(0, \sum_j x_{ij}b_j\big)$ and $s\tau(b_j) = (0, sb_j)$.

In the second case this implies $t\tau(b_j) = \big(\sum_i y_{ji}a_i, 0\big)$ and $t\tau(a_i) = (ta_i, 0)$.

We therefore try to define τ by the following formula which coincides with the two previous ones in the two special cases.

$$\tau(a_i) = \big(ta_i, \textstyle\sum_j x_{ij}b_j\big),\ \ \tau(b_j) = \big(\textstyle\sum_i y_{ji}a_i, sb_j\big).$$

For this attempt to succeed, it is necessary and sufficient that when $\sum_i \alpha_i a_i = \sum_j \beta_j b_j$, we have the equality

$$\textstyle\sum_i \alpha_i\big(ta_i, \sum_j x_{ij}b_j\big) = \sum_j \beta_j\big(\sum_i y_{ji}a_i, sb_j\big).$$

For the first coordinate, this results from the following computation (and similarly for the second coordinate).

$$\sum_i \alpha_i t a_i = t \sum_i \alpha_i a_i = t \sum_j \beta_j b_j = \sum_j \beta_j t b_j = \sum_j \beta_j \sum_i y_{ji} a_i.$$

Finally, the equality $\sigma \circ \tau = \mathrm{Id}_{\mathfrak{a}+\mathfrak{b}}$ is satisfied because it is satisfied when restricted to $\mathfrak{a}$ and $\mathfrak{b}$ (immediate computation).

Exercise 12.

1. Proven in Exercise 9.

2. Let a, b, c, $d \in \mathbf{A}$. Let $\mathfrak{a} = \langle a, b \rangle$

Consider $f = aX + b$ and $g = aX - b$. We get $\langle a, b\rangle^2 = \left\langle a^2, b^2 \right\rangle$, i.e.

$$ab = ua^2 + vb^2.$$

When considering $f = cX + d$ and $g = dX + c$, we obtain $\langle c, d\rangle^2 = \left\langle c^2 + d^2, cd \right\rangle$. In other words c^2 and $d^2 \in \left\langle c^2 + d^2, cd \right\rangle$.

Let $\mathfrak{b} = \langle ua, vb \rangle$. We have $ab \in \mathfrak{ab}$. It suffices to show that $\mathfrak{a}^2\mathfrak{b}^2 = \left\langle a^2 b^2 \right\rangle$ because this implies that $\mathfrak{a}$ is invertible (we treat the case a, $b \in \mathbf{A}^*$). However, we have

$$a^2b^2 \in \mathfrak{a}^2\mathfrak{b}^2 = \left\langle a^2, b^2 \right\rangle \left\langle u^2a^2, v^2b^2 \right\rangle.$$

We therefore need to show that u^2a^4 and $v^2b^4 \in \left\langle a^2b^2 \right\rangle$. Let $u_1 = ua^2$ and $v_1 = vb^2$. We have $u_1 + v_1 = ab$ and $u_1v_1 \in \left\langle a^2b^2 \right\rangle$. Therefore $u_1^2 + v_1^2 \in \left\langle a^2b^2 \right\rangle$ also.

Since $u_1^2 \in \left\langle u_1^2 + v_1^2, u_1v_1 \right\rangle$, we indeed get $u_1^2 \in \left\langle a^2b^2 \right\rangle$ (likewise for v_1^2).

3. The equalities of item *2* are all satisfied.

Let us first show that the ring is a pf-ring.

Assume $cd = 0$. Since $c^2 \in \left\langle c^2 + d^2, cd \right\rangle$, we have $c^2 = x(c^2 + d^2)$, i.e.

$$xd^2 = (1 - x)c^2.$$

We deduce that $xd^3 = 0$, and as $\mathbf{A}$ is reduced, $xd = 0$. Similarly $(1 - x)c = 0$.

Let us now see that the ring is arithmetic. We start from arbitrary a, b and we want to show that $\langle a, b \rangle$ is locally principal. By item *2* we have an ideal $\mathfrak{c}$ such that $\langle a, b \rangle\, \mathfrak{c} = \left\langle a^2b^2 \right\rangle$. We therefore have x and y with

$$\langle a, b \rangle \langle x, y \rangle = \left\langle a^2b^2 \right\rangle \text{ and } ax + by = a^2b^2.$$

We write $ax = a^2b^2v$ and $by = a^2b^2u$. From the equality $a(ab^2v - x) = 0$, we deduce two comaximal localizations, in the first $a = 0$, in the second $x = ab^2v$. We therefore suppose without loss of generality that $x = ab^2v$ and, symmetrically $y = ba^2u$. This gives

$$\langle a, b \rangle \langle x, y \rangle = ab \langle a, b \rangle \langle au, bv \rangle = \left\langle a^2b^2 \right\rangle.$$

We can also suppose without loss of generality that $\langle a, b \rangle \langle au, bv \rangle = \langle ab \rangle$.

We also have $ax + by = a^2b^2(u + v)$ and since $ax + by = a^2b^2$, we suppose without loss of generality that $u + v = 1$.

Since $a^2u = abu'$, we suppose without loss of generality that $au = bu'$.

Symmetrically $bv = av'$, and since $u + v = 1$, $\langle a, b \rangle$ is locally principal.

Exercise 14. *1.* Let $a \in \mathbf{A}$ and $a_1, \ldots, a_n \in \mathbf{A}$ generate $\mathfrak{a} = \mathrm{Ann}(a)$. If one of the a_i's is in $\mathbf{A}^\times$, we obtain $a = 0$ and $\mathfrak{a} = \langle 1 \rangle$. It remains to treat the case where all the a_i's are in $\mathfrak{m}$. Let b be one of the a_i's. Since $\mathfrak{m}$ is flat and $b \in \mathfrak{m}$, the equality $ab = 0$ gives us elements $c_1, \ldots, c_m \in \mathfrak{a}$ and $b_1, \ldots, b_m \in \mathfrak{m}$ with $b = \sum_{i \in [\![1..m]\!]} c_i b_i$. Therefore $b \in \mathfrak{am}$, which gives $b = \sum_{i \in [\![1..n]\!]} a_i z_i$ for some $z_i \in \mathfrak{m}$. Hence a matrix equality

$$[\, a_1 \ \cdots \ a_n \,] = M \, [\, a_1 \ \cdots \ a_n \,] \quad \text{ with } M \in \mathbb{M}_n(\mathfrak{m}).$$

Thus $[\, a_1 \ \cdots \ a_n \,](\mathrm{I}_n - M) = [\, 0 \ \cdots \ 0 \,]$ with $\mathrm{I}_n - M$ invertible, so $\mathfrak{a} = 0$.

2. Consider $a, b \in \mathbf{A}$. We must prove that one divides the other. If one of the two is invertible, the case is closed. It remains to examine the case where a and $b \in \mathfrak{m}$. We consider a matrix

$$P = \begin{bmatrix} a_1 & \cdots & a_n \\ b_1 & \cdots & b_n \end{bmatrix}$$

whose columns generate the module K, the kernel of $(x, y) \mapsto bx - ay$. In particular we have $a_i b = b_i a$ for each i. If one of the a_i's or b_i's is invertible, the case is closed. It remains to examine the case where the a_i's and b_i's are in $\mathfrak{m}$.

Let (c, d) be one of the (a_i, b_i)'s. Since $\mathfrak{m}$ is flat and $a, b \in \mathfrak{m}$, the equality $cb - da = 0$ gives

$$\begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} c_1 & \cdots & c_m \\ d_1 & \cdots & d_m \end{bmatrix} \begin{bmatrix} y_1 \\ \vdots \\ y_m \end{bmatrix} \quad \text{with the } y_i's \in \mathfrak{m} \text{ and the } \begin{bmatrix} c_j \\ d_j \end{bmatrix}' s \in K.$$

By expressing the $\begin{bmatrix} c_j \\ d_j \end{bmatrix}$ as linear combinations of the columns of P we obtain

$$\begin{bmatrix} c \\ d \end{bmatrix} = P \begin{bmatrix} z_1 \\ \vdots \\ z_n \end{bmatrix} \quad \text{with every } z_i \in \mathfrak{m}.$$

Hence $P = PN$ with a matrix $N \in \mathbb{M}_n(\mathfrak{m})$, so $P = 0$. This implies that $(a, b) = (0, 0)$, and a divides b (actually, in this case, $\mathbf{A}$ is trivial).

Exercise 15. Let $a_i \in \mathbf{A}$ and $x_i \in M$ satisfy $\sum_{i=1}^n a_i x_i \equiv 0 \bmod K$, a relation that we must explain. Let $\mathfrak{a} = \langle \underline{a} \rangle$ such that $\mathfrak{a}K = \sum_i a_i K$; since $\sum_i a_i x_i \in \mathfrak{a}M \cap K = \mathfrak{a}K$, we have an equality $\sum_i a_i x_i = \sum a_i y_i$ where each $y_i \in K$. We therefore have, with $z_i = x_i - y_i$, the relation $\sum_i a_i z_i = 0$ in M. Since M is flat, this relation produces a certain number of vectors of M, say 3 for simplicity, denoted by u, v, w and 3 sequences of scalars $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n)$, $\underline{\beta} = (\beta_1, \ldots, \beta_n)$ and $\underline{\gamma} = (\gamma_1, \ldots, \gamma_n)$, satisfying

$$(z_1, \ldots, z_n) = (\alpha_1, \ldots, \alpha_n)\, u + (\beta_1, \ldots, \beta_n)\, v + (\gamma_1, \ldots, \gamma_n)\, w$$

and $\langle \underline{a} \,|\, \underline{\alpha} \rangle = \langle \underline{a} \,|\, \underline{\beta} \rangle = \langle \underline{a} \,|\, \underline{\gamma} \rangle = 0$.

Since $z_i \equiv x_i \bmod K$, we obtain our sought explanation in M/K:

$$(x_1, \ldots, x_n) \equiv (\alpha_1, \ldots, \alpha_n)\, u + (\beta_1, \ldots, \beta_n)\, v + (\gamma_1, \ldots, \gamma_n)\, w \mod K.$$

Exercise 16. Without loss of generality suppose that I is finitely enumerated. In other words $I = \{i_1, \dots, i_n\}$. Let $P = M^{(I)}$. Any element of P can be written in the form $x = \oplus_{k \in [\![1..n]\!]}(i_k, x_k)$.

First suppose that the module M is flat, and consider a syzygy in P

$$0 = \sum\nolimits_{\ell \in [\![1..m]\!]} a_\ell x_\ell = \sum\nolimits_{\ell \in [\![1..m]\!]} a_\ell \big(\oplus_{k \in [\![1..n]\!]} (i_k, x_{k,\ell}) \big) = \oplus_{k \in [\![1..n]\!]}(i_k, y_k)$$

with $y_k = \sum_{\ell \in [\![1..m]\!]} a_\ell x_{k,\ell}$.

By definition of equality in P, since $\oplus_{k \in [\![1..n]\!]} y_k = 0$, we are in (at least) one of the two following cases:

- all the y_k's are null,
- two indices are equal in I: $i_k =_I i_h$ for h and k distinct in $[\![1..n]\!]$.

The first case is treated like that of a direct sum over a finite I. The second case reduces to the first by induction on n.

Now suppose that P is flat and consider for instance the index $i_1 \in I$ and a syzygy $\sum_{\ell \in [\![1..m]\!]} a_\ell x_\ell = 0$ in M. We explain this syzygy in P by writing

$$(i_1, x_\ell) =_P \sum\nolimits_{j \in [\![1..p]\!]} g_{\ell,j} z_j \text{ with } \sum\nolimits_{\ell \in [\![1..m]\!]} a_\ell g_{\ell,j} =_{\mathbf{A}} 0 \text{ for all } j.$$

We re-express $z_j = \oplus_{k \in [\![1..n]\!]}(i_k, y_{k,j})$, which gives

$$(i_1, x_\ell) =_P \oplus_{k \in [\![1..p]\!]} \big(i_k, \sum\nolimits_{j \in [\![1..p]\!]} g_{\ell,j} y_{k,j}\big).$$

By definition of the equality in P, we are in (at least) one of the two following cases:

- for each ℓ, we have $x_\ell = \sum_{j \in [\![1..n]\!]} g_{\ell,j} y_{1,\ell}$ in M,
- we have in I: $i_1 =_I i_h$ for some $h \neq 1$ in $[\![1..n]\!]$.

In the first case we have in M the equalities that suit us. The second case is reduced to the first by induction on n.

Bibliographic comments

Prüfer domains were introduced by H. Prüfer in 1932 in [153]. Their central place in multiplicative ideal theory is showcased in the book of reference on the subject [Gilmer]. Even though they were introduced in a very concrete way as the integral rings in which every nonzero finitely generated ideal is invertible, this definition is often set aside in the modern literature for the following purely abstract alternative, which only works in the presence of non-constructive principles (**LEM** and the axiom of choice): the localization at any prime ideal gives a valuation ring.

Arithmetic rings were introduced by L. Fuchs in 1949 in [89].

In the case of a non-integral ring, the definition that we have adopted for Prüfer rings is due to Hermida and Sánchez-Giralda [103]. It is the one that seemed the most natural to us, given the central importance of the concept of flatness in commutative algebra. Another name for these rings in the literature is *ring of weak global dimension less than or equal to one*, which is rather inelegant. Moreover, we often find in the literature a Prüfer ring defined as a ring in which every ideal containing a regular element is invertible. They are therefore almost arithmetic rings, but the behavior of the ideals that do not contain regular elements seems utterly random (cf. Exercise 13).

A fairly complete presentation of arithmetic rings and Prüfer rings, written in the style of constructive mathematics, can be found in [71, Ducos&al.] and [128, Lombardi].

A very comprehensive survey on variations of the notion of integral Prüfer rings obtained by deleting the hypothesis of integrity is given in [11, Bazzoni&Glaz], including Gaussian rings (Exercise 12).

Chapter IX

Local rings, or just about

Contents

1. A few constructive definitions

In classical mathematics a local ring is often defined as a ring having a single maximal ideal. In other words the non-invertible elements form an ideal. This second definition has the advantage of being simpler (no quantification over the set of ideals). However, it lends itself fairly poorly to an algorithmic treatment because of the negation contained in "non-invertible elements." This is the reason why we adopt the definition given on page 206 in constructive mathematics: if the sum of two elements is invertible, one of the two is invertible.

We now find ourselves obligated to inflict a few unusual definitions on the classic reader, in line with the definition of a local ring. Rest assured, on other planets, in other solar systems, no doubt the symmetric situation is taking place. There, mathematics has always been constructive and they have just barely discovered the interest of the abstract Cantorian point of view. An author in the new style is in the process of explaining that for them it is much simpler to regard a local ring as a ring having a single maximal ideal. Would the reader then put in the effort to follow what they are saying?

The Jacobson radical, local rings, fields

Recall that for a ring $\mathbf{A}$ we denote by $\mathbf{A}^\times$ the multiplicative group of invertible elements, also called the group of units.

An element x of a ring $\mathbf{A}$ is said to be *non-invertible* if it satisfies[1] the following implication

$$x \in \mathbf{A}^\times \;\Rightarrow\; 1 =_{\mathbf{A}} 0.$$

In the trivial ring the element 0 is both invertible and non-invertible at the same time.

[1] Here we will use a slightly weakened version of negation. For a property P affecting elements of the ring $\mathbf{A}$ or of an $\mathbf{A}$-module M, we consider the property $\mathsf{P}' := (\mathsf{P} \Rightarrow 1 =_{\mathbf{A}} 0)$. It is the negation of P when the ring is not trivial. Yet it often happens that a ring constructed in a proof can be trivial without one knowing. To do an entirely constructive treatment of the usual classical proof in such a situation (the classical proof excludes the case of the trivial ring by an ad hoc argument) our weakened version of negation then turns out to be generally useful. A discrete field does not necessarily satisfy the axiom of discrete sets, $\forall x, y\ \big(x = y \text{ or } \neg(x = y)\big)$, but it satisfies its weak version

$$\forall\, x,\, y,\ \Big(x = y \ \text{ or } \ (x = y)'\Big),$$

since if 0 is invertible, then $1 = 0$.

For an arbitrary commutative ring, the set of elements a of $\mathbf{A}$ which satisfy

$$\forall x \in \mathbf{A} \quad 1 + ax \in \mathbf{A}^{\times} \tag{1}$$

is called the *Jacobson radical* of $\mathbf{A}$. It will be denoted by $\mathrm{Rad}(\mathbf{A})$. It is an ideal because if a, $b \in \mathrm{Rad}\,\mathbf{A}$, we can write, for $x \in \mathbf{A}$

$$1 + (a + b)x = (1 + ax)(1 + (1 + ax)^{-1}bx),$$

which is the product of two invertible elements.

In a local ring the Jacobson radical is equal to the set of non-invertible elements (the reader is invited to find a constructive proof). In classical mathematics the Jacobson radical is characterized as follows.

1.1. Lemma*. *The Jacobson radical is equal to the intersection of the maximal ideals.*

D If $a \in \mathrm{Rad}\,\mathbf{A}$ and $a \notin \mathfrak{m}$ with $\mathfrak{m}$ a maximal ideal, we have $1 \in \langle a \rangle + \mathfrak{m}$ which means that for some x, $1 + xa \in \mathfrak{m}$, so $1 \in \mathfrak{m}$: a contradiction.
If $a \notin \mathrm{Rad}\,\mathbf{A}$, there exists an x such that $1 + xa$ is non-invertible. Therefore there exists a strict ideal containing $1 + xa$. By Zorn's lemma there exists a maximal ideal $\mathfrak{m}$ containing $1 + xa$, and a cannot be in $\mathfrak{m}$ because otherwise we would have $1 = (1 + xa) - xa \in \mathfrak{m}$.
The reader will notice that the proof actually says this: an element x is in the intersection of the maximal ideals if and only if the following implication is satisfied: $\langle x, y \rangle = \langle 1 \rangle \Rightarrow \langle y \rangle = \langle 1 \rangle$. □

Remark. We have reasoned with a nontrivial ring. If the ring is trivial the intersection of the (empty) set of maximal ideals is indeed equal to $\langle 0 \rangle$. ■

A *Heyting field*, or simply a *field*, is by definition a local ring in which every non-invertible element is null, in other words a local ring whose Jacobson radical is reduced to 0.

In particular, a discrete field, therefore also the trivial ring, is a field. The real numbers form a field that *is not* a discrete field.[2] The same remark applies for the field $\mathbb{Q}_p$ of p-adic numbers or that of the formal Laurent series $\mathbf{k}(\!(T)\!)$ when $\mathbf{k}$ is a discrete field.

The reader will check that a field is a discrete field if and only if it is zero-dimensional.

The quotient of a local ring by its Jacobson radical is a field, called the *residual field of the local ring.*

[2] We use the negation in italics to indicate that the corresponding assertion, here it would be "$\mathbb{R}$ is a discrete field," is not provable in constructive mathematics.

1.2. Lemma. *If* $\mathbf{A}$ *is zero-dimensional,* $\mathrm{Rad}\,\mathbf{A} = \mathrm{D}_{\mathbf{A}}(0)$.

D The inclusion $\mathrm{Rad}\,\mathbf{A} \supseteq \mathrm{D}_{\mathbf{A}}(0)$ is always true. Now if $\mathbf{A}$ is zero-dimensional and $x \in \mathrm{Rad}\,\mathbf{A}$, since we have an equality $x^{\ell}(1 - ax) = 0$, it is clear that $x^{\ell} = 0$. □

1.3. Lemma. *For all* $\mathbf{A}$, $\mathrm{Rad}(\mathbf{A}[X]) = \mathrm{D}_{\mathbf{A}}(0)[X]$.

D If $f \in \mathrm{Rad}(\mathbf{A}[X])$, then $1 + Xf(X) \in \mathbf{A}[X]^{\times}$. We conclude with Lemma II-2.6 *4*. □

1.4. Fact. *Let* $\mathbf{A}$ *be a ring and* $\mathfrak{a}$ *be an ideal contained in* $\mathrm{Rad}\,\mathbf{A}$.

1. $\mathrm{Rad}\,\mathbf{A} = \pi_{\mathbf{A},\mathfrak{a}}^{-1}(\mathrm{Rad}\,(\mathbf{A}/\mathfrak{a})) \supseteq \mathrm{D}_{\mathbf{A}}(\mathfrak{a})$.

2. $\mathbf{A}$ *is local if and only if* $\mathbf{A}/\mathfrak{a}$ *is local.*

3. $\mathbf{A}$ *is local and* $\mathfrak{a} = \mathrm{Rad}\,\mathbf{A}$ *if and only if* $\mathbf{A}/\mathfrak{a}$ *is a field.*

The following fact describes a construction that forces a monoid to be inverted and an ideal to be radicalized (for more details, see the subsection "Duality in commutative rings" on page 644 and following, and Section XV-1).

1.5. Fact. *Let* U *be a monoid and* $\mathfrak{a}$ *be an ideal of* $\mathbf{A}$. *Consider the monoid* $S = U + \mathfrak{a}$. *Let* $\mathbf{B} = S^{-1}\mathbf{A}$ *and* $\mathfrak{b} = \mathfrak{a}\mathbf{B}$.

1. The ideal $\mathfrak{b}$ *is contained in* $\mathrm{Rad}\,\mathbf{B}$.

2. The ring $\mathbf{B}/\mathfrak{b}$ *is isomorphic to* $\mathbf{A}_U/\mathfrak{a}\mathbf{A}_U$.

By definition a *residually discrete local ring* is a local ring whose residual field is a discrete field. Such a ring $\mathbf{A}$ can be characterized by the following axiom

$$\forall x \in \mathbf{A} \qquad x \in \mathbf{A}^{\times} \ \text{ or } \ 1 + x\mathbf{A} \subseteq \mathbf{A}^{\times} \tag{2}$$

(the reader is invited to write its constructive proof).

For example the ring of p-adic integers, although *non*-discrete, is residually discrete.

We obtain a *non*-residually discrete local ring when taking $\mathbf{K}[u]_{1+\langle u\rangle}$, where $\mathbf{K}$ is a *non*-discrete field (for example the field of formal series $\mathbf{k}(\!(t)\!)$, where $\mathbf{k}$ is a discrete field).

Comment. The slightly subtle difference that separates local rings from residually discrete local rings can also be found, by permuting addition and multiplication, in the difference that separates rings without zerodivisors from integral rings.

In classical mathematics a ring without zerodivisors is integral; however the two notions do not have the same algorithmic content, and it is for this reason that they are distinguished in constructive mathematics. ■

1.6. Definition. A ring $\mathbf{A}$ is said to be *residually zero-dimensional* when the *residual ring* $\mathbf{A}/\mathrm{Rad}\,\mathbf{A}$ is zero-dimensional. Likewise for *residually connected rings.*

Since a field is zero-dimensional if and only if it is a discrete field, a local ring is residually discrete if and only if it is residually zero-dimensional.

Comment. In classical mathematics a ring $\mathbf{A}$ is said to be semi-local if $\mathbf{A}/\mathrm{Rad}\,\mathbf{A}$ is isomorphic to a finite product of discrete fields. This implies that it is a residually zero-dimensional ring. Actually the hypothesis of finiteness presented in the notion of a semi-local ring is rarely decisive. Most of the theorems from the literature concerning semi-local rings applies to residually zero-dimensional rings, or even to local-global rings (Section 6). For a possible definition of semi-local rings in constructive mathematics see Exercises 18 and 19. ■

Prime and maximal ideals

In constructive mathematics, an ideal of a ring $\mathbf{A}$ is called a *maximal ideal* when the quotient ring is a field.[3] An ideal is called a *prime ideal* when the quotient ring is without zerodivisors.

These definitions coincide with the usual definitions in the context of classical mathematics, except that we tolerate the trivial ring as a field and hence the ideal $\langle 1\rangle$ as a maximal ideal and as a prime ideal.

In a nontrivial ring, an ideal is strict, maximal and detachable if and only if the quotient ring is a nontrivial discrete field, it is strict, prime and detachable if and only if the quotient ring is a nontrivial integral ring.

Comment. It is not without a certain apprehension that we declare the ideal $\langle 1\rangle$ both prime and maximal. This will force us to say "strict prime ideal" or "strict maximal ideal" in order to speak of the "usual" prime ideals and maximal ideals. Fortunately it will be a very rare occurrence.

We actually think that there was *a casting error right at the beginning.* To force a field or an integral ring to be nontrivial, something that seemed eminently reasonable a priori, has unconsciously led mathematicians to transform numerous constructive arguments into reductio ad absurdum arguments. To prove that an ideal constructed in the process of a computation is equal to $\langle 1\rangle$, we have made it a habit to reason as follows: if it wasn't the case, it would be contained in a maximal ideal and the quotient would

[3] We have until now uniquely used the notion of a maximal ideal in the context of proofs in classical mathematics. A constructive definition would have been required sooner or later. Actually this notion is only rarely used in constructive mathematics. As a general rule, it is advantageously replaced by considering the Jacobson radical, for example in the local rings case.

be a field, which case we reach the contradiction $0 = 1$. This argument happens to be a reductio ad absurdum simply because we have made the casting error: we have forbidden the trivial ring from being a field. Without this prohibition, we would present the argument as a direct argument of the following form: let us show that every maximal ideal of the quotient ring contains 1. We will come back to this point in Section XV-6.

Moreover, as we will essentially use prime ideals and maximal ideals heuristically, our transgression of the usual prohibition regarding the trivial ring will have practically no consequence on reading this work. In addition, the reader will be able to see that this unusual convention does not force a modification of most of the results established specifically in classical mathematics, like the abstract local-global principle* II-2.13, Fact* II-2.12 or Lemma* 1.1: it suffices for instance[4] for the localization at a prime ideal $\mathfrak{p}$ to define it as the localization at the filter

$$S \overset{\text{def}}{=} \{\, x \in \mathbf{A} \,|\, x \in \mathfrak{p} \Rightarrow 1 \in \mathfrak{p} \,\}.$$

Fundamentally we think that mathematics is purer and more elegant when we avoid using negation (this radically forbids reductio ad absurdum arguments for example). It is for this reason that you will not find any definitions that use negation in this book.[5] ■

The Jacobson radical and units in an integral extension

1.7. Theorem. *Let* $\mathbf{k} \subseteq \mathbf{A}$ *with* $\mathbf{A}$ *integral over* $\mathbf{k}$*.*

1. *If* $y \in \mathbf{A}^\times$*, then* $y^{-1} \in \mathbf{k}[y]$*.*
2. $\mathbf{k}^\times = \mathbf{k} \cap \mathbf{A}^\times$*.*
3. $\operatorname{Rad}\mathbf{k} = \mathbf{k} \cap \operatorname{Rad}\mathbf{A}$ *and the homomorphism* $\mathbf{A} \to \mathbf{A}/\operatorname{Rad}(\mathbf{k})\mathbf{A}$ *reflects the units.*[6]

D *1.* Let $y, z \in \mathbf{A}$ such that $yz = 1$. We have an integral dependence relation for z: $z^n = a_{n-1}z^{n-1} + \cdots + a_0$ ($a_i \in \mathbf{k}$). By multiplying by y^n we obtain $1 = yQ(y)$ so $z = Q(y) \in \mathbf{k}[y]$.

2. In particular, if $y \in \mathbf{k}$ is invertible in $\mathbf{A}$, its inverse z is in $\mathbf{k}$.

3. Let $x \in \mathbf{k} \cap \operatorname{Rad}\mathbf{A}$, for all $y \in \mathbf{k}$, $1 + xy$ is invertible in $\mathbf{A}$ therefore also in $\mathbf{k}$. This gives the inclusion $\operatorname{Rad}\mathbf{k} \supseteq \mathbf{k} \cap \operatorname{Rad}\mathbf{A}$.

Let $x \in \operatorname{Rad}\mathbf{k}$ and $b \in \mathbf{A}$. We want to show that $y = -1 + xb$ is invertible.

[4] Fact* II-2.2 could also be treated according to the same schema, by deleting the restriction to the nontrivial case.

[5] If such a definition could be found, it would be in a framework where the negation is equivalent to a positive assertion, because the considered property is decidable.

[6] Recall that we say that a homomorphism $\rho : \mathbf{A} \to \mathbf{B}$ reflects the units when $\rho^{-1}(\mathbf{B}^\times) = \mathbf{A}^\times$.

We write an integral dependence relation for b

$$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0,$$

we multiply by x^n and replace bx with $1+y$. We get a polynomial in y with coefficients in $\mathbf{k}$: $y^n + \cdots + (1 + a_{n-1}x + \cdots + a_0x^n) = 0$. Therefore, $yR(y) = 1 + xS(x)$ is invertible in $\mathbf{k}$, and y is invertible in $\mathbf{A}$.
Now let $y \in \mathbf{A}$ which is invertible modulo $\mathrm{Rad}(\mathbf{k})\mathbf{A}$. A fortiori it is invertible modulo $\mathrm{Rad}\,\mathbf{A}$, so it is invertible. □

1.8. Theorem. *Let $\mathbf{k} \subseteq \mathbf{A}$ with $\mathbf{A}$ integral over $\mathbf{k}$.*

1. *$\mathbf{A}$ is zero-dimensional if and only if $\mathbf{k}$ is zero-dimensional.*
2. *$\mathbf{A}$ is residually zero-dimensional if and only if $\mathbf{k}$ is residually zero-dimensional. In this case $\mathrm{Rad}\,\mathbf{A} = \mathrm{D}_{\mathbf{A}}\big(\mathrm{Rad}(\mathbf{k})\mathbf{A}\big)$.*
3. *If $\mathbf{A}$ is local, so is $\mathbf{k}$.*

D *1.* Already known (Lemmas VI-3.14 and IV-8.15).

2. By passage to the quotient, the integral morphism $\mathbf{k} \to \mathbf{A}$ gives an integral morphism $\mathbf{k}/\mathrm{Rad}\,\mathbf{k} \to \mathbf{A}/\mathrm{Rad}\,\mathbf{A}$, which is injective because $\mathrm{Rad}\,\mathbf{k} = \mathbf{k} \cap \mathrm{Rad}\,\mathbf{A}$ (Theorem 1.7). Therefore, the two rings are simultaneously zero-dimensional. In this case, let $\mathfrak{a} = \mathrm{Rad}(\mathbf{k})\,\mathbf{A} \subseteq \mathrm{Rad}\,\mathbf{A}$. We have an integral morphism

$$\mathbf{k}/\mathrm{Rad}\,\mathbf{k} \to \mathbf{A}/\mathfrak{a}\,,$$

so $\mathbf{A}/\mathfrak{a}$ is zero-dimensional, such that its Jacobson radical is equal to its nilpotent radical (Lemma 1.2), i.e. $\mathrm{Rad}(\mathbf{A})/\mathfrak{a} = \mathrm{D}_{\mathbf{A}}(\mathfrak{a})/\mathfrak{a}$, and so $\mathrm{Rad}\,\mathbf{A} = \mathrm{D}_{\mathbf{A}}(\mathfrak{a})$.

3. Results from Theorem 1.7, item *2.* □

2. Four important lemmas

First we give some variants of the “determinant trick” often called “Nakayama’s lemma.” In this lemma the important thing to underline is that the module M is finitely generated.

2.1. Nakayama’s lemma. (The determinant trick)
Let M be a finitely generated $\mathbf{A}$-module and $\mathfrak{a}$ be an ideal of $\mathbf{A}$.

1. *If $\mathfrak{a}M = M$, there exists an $x \in \mathfrak{a}$ such that $(1-x)\,M = 0$.*
2. *If in addition $\mathfrak{a} \subseteq \mathrm{Rad}(\mathbf{A})$, then $M = 0$.*
3. *If $N \subseteq M$, $\mathfrak{a}M + N = M$ and $\mathfrak{a} \subseteq \mathrm{Rad}(\mathbf{A})$, then $M = N$.*
4. *If $\mathfrak{a} \subseteq \mathrm{Rad}(\mathbf{A})$ and $X \subseteq M$ generates $M/\mathfrak{a}M$ as an $\mathbf{A}/\mathfrak{a}$-module, then X generates M as an $\mathbf{A}$-module.*

D We prove item *1* and leave the others as an exercise, as easy consequences. Let $V \in M^{n\times 1}$ be a column vector formed with generators of M. The hypothesis means that there exists a matrix $G \in \mathbb{M}_n(\mathfrak{a})$ satisfying $GV = V$. Therefore $(\mathrm{I}_n - G)V = 0$, and by premultiplying by the cotransposed matrix of $\mathrm{I}_n - G$, we obtain $\det(\mathrm{I}_n - G)V = 0$. However, $\det(\mathrm{I}_n - G) = 1 - x$ with $x \in \mathfrak{a}$. □

Finitely generated projective modules are locally free in the following (weak) sense: they become free when we localize at a prime ideal. Proving this is the same as provinging the *local freeness lemma* (below) which states that a finitely generated projective module over a local ring is free.

2.2. Local freeness lemma. *Let* $\mathbf{A}$ *be a local ring. Every finitely generated projective module over* $\mathbf{A}$ *is free of finite rank. Equivalently, every matrix* $F \in \mathbb{AG}_n(\mathbf{A})$ *is similar to a standard projection matrix*

$$\mathrm{I}_{r,n} = \left[\begin{array}{cc} \mathrm{I}_r & 0_{r,n-r} \\ 0_{n-r,r} & 0_{n-r} \end{array}\right].$$

Remark. The matrix formulation obviously implies the first, more abstract, formulation. Conversely if $M \oplus N = \mathbf{A}^n$, saying that M and N are free (of ranks r and $n - r$) is the same as saying that there is a basis of $\mathbf{A}^n$ whose first r elements form a basis of M and last $n - r$ a basis of N, consequently the projection over M parallel to N is expressed over this basis by the matrix $\mathrm{I}_{r,n}$. ■

First proof, (usual classic proof). We denote by $x \mapsto \overline{x}$ the passage to the residual field. If $M \subseteq \mathbf{A}^n$ is the image of a projection matrix F and if $\mathbf{k}$ is the residual field we consider a basis of $\mathbf{k}^n$ which begins with columns of $\overline{F}$ ($\mathrm{Im}\,\overline{F}$ is a linear subspace of dimension r) and ends with columns of $\mathrm{I}_n - \overline{F}$ ($\mathrm{Im}(\mathrm{I}_n - \overline{F}) = \mathrm{Ker}\,\overline{F}$). When considering the corresponding columns of $\mathrm{Im}\,F$ and $\mathrm{Im}(\mathrm{I}_n - F) = \mathrm{Ker}\,F$ we obtain a lift of the residual basis in n vectors whose determinant is residually invertible, therefore invertible. These vectors form a basis of $\mathbf{A}^n$ and over this basis it is clear that the projection admits as a matrix $\mathrm{I}_{r,n}$.

Note that in this proof we extract a maximal free system among the columns of a matrix with coefficients in a field. This is usually done by the Gauss pivot method. This therefore requires that the residual field be discrete. □

Second proof, (proof by Azumaya). In contrast to the previous proof, this one does not assume that the local ring is residually discrete. We will diagonalize the matrix F. The proof works with a not necessarily commutative local ring.

Let us call f_1 the column vector $F_{1..n,1}$ of the matrix F, $(e_1, \dots, e_n)$ the canonical basis of $\mathbf{A}^n$ and φ the linear map represented by F.

– First case, $f_{1,1}$ is invertible. Then, $(f_1, e_2, \dots, e_n)$ is a basis of $\mathbf{A}^n$. With respect to this basis, the linear map φ has a matrix

$$G = \begin{bmatrix} 1 & L \\ 0_{n-1,1} & F_1 \end{bmatrix}.$$

By writing $G^2 = G$, we obtain $F_1^2 = F_1$ and $LF_1 = 0$. We then define the matrix $P = \begin{bmatrix} 1 & L \\ 0_{n-1,1} & \mathrm{I}_{n-1} \end{bmatrix}$ and we obtain the equalities

$$\begin{aligned} PGP^{-1} &= \begin{bmatrix} 1 & L \\ 0_{n-1,1} & \mathrm{I}_{n-1} \end{bmatrix} \begin{bmatrix} 1 & L \\ 0_{n-1,1} & F_1 \end{bmatrix} \begin{bmatrix} 1 & -L \\ 0_{n-1,1} & \mathrm{I}_{n-1} \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0_{1,n-1} \\ 0_{n-1,1} & F_1 \end{bmatrix}. \end{aligned}$$

– Second case, $1 - f_{1,1}$ is invertible. We apply the previous computation to the matrix $\mathrm{I}_n - F$, which is therefore similar to a matrix

$$A = \begin{bmatrix} 1 & 0_{1,n-1} \\ 0_{n-1,1} & F_1 \end{bmatrix},$$

with $F_1^2 = F_1$, which means that F is similar to a matrix

$$\mathrm{I}_n - A = \begin{bmatrix} 0 & 0_{1,n-1} \\ 0_{n-1,1} & H_1 \end{bmatrix},$$

with $H_1^2 = H_1$.

We finish the proof by induction on n. □

Comment. From the classical point of view, all the sets are discrete, and the corresponding hypothesis is superfluous in the first proof. The second proof must be considered superior to the first as its algorithmic content is more universal than that of the first (which can only be rendered completely explicit when the local ring is residually discrete). ■

The following lemma can be considered as a variant of the local freeness lemma.

2.3. Lemma of the locally simple map. *Let* $\mathbf{A}$ *be a local ring and* ψ *be a linear map between free* $\mathbf{A}$*-modules of finite rank. The following properties are equivalent.*

1. *ψ is simple.*
2. *ψ is locally simple.*
3. *ψ has a finite rank k.*

D *2 ⇒ 3.* The equality $\psi\,\varphi\,\psi = \psi$ implies that the determinantal ideals of ψ are idempotents. By Lemma II-4.6 these ideals are generated by idempotents. Since an idempotent of a local ring is necessarily equal to 0 or 1, and that $\mathcal{D}_0(\psi) = \langle 1 \rangle$ and $\mathcal{D}_r(\psi) = \langle 0 \rangle$ for large enough r, there exists an integer $k \geqslant 0$ such that $\mathcal{D}_k(\psi) = \langle 1 \rangle$ and $\mathcal{D}_{k+1}(\psi) = \langle 0 \rangle$.

3 ⇒ *1.* By hypothesis $\mathcal{D}_k(\psi) = \langle 1 \rangle$, so the minors of order k are comaximal and since the ring is local one of the minors of order k is invertible. As $\mathcal{D}_{k+1}(\psi) = \langle 0 \rangle$, the result is then a consequence of the freeness lemma II-5.10. □

Note that the term locally simple map is partly justified by the previous lemma. Also note that Theorem II-5.26 can be considered as more general than the previous lemma.

2.4. Local number of generators lemma.
Let M be a finitely generated $\mathbf{A}$-module.

1. *Suppose $\mathbf{A}$ is local.*
   - a. *The module M is generated by k elements if and only if its Fitting ideal $\mathcal{F}_k(M)$ is equal to $\mathbf{A}$.*
   - b. *If in addition $\mathbf{A}$ is residually discrete and M is finitely presented, the module admits a presentation matrix whose every coefficient is in the maximal ideal* $\mathrm{Rad}\,\mathbf{A}$*.*
2. *Generally, for any $k \in \mathbb{N}$ the following properties are equivalent.*
   - a. *$\mathcal{F}_k(M)$ is equal to $\mathbf{A}$.*
   - b. *There exist comaximal elements s_j such that after scalar extension to each of the $\mathbf{A}[1/s_j]$, M is generated by k elements.*
   - c. *There exist comaximal monoids S_j such that each of the M_{S_j} is generated by k elements.*
   - d*. *After localization at any prime ideal, M is generated by k elements.*
   - e*. *After localization at any maximal ideal, M is generated by k elements.*

D It suffices to prove the equivalences for a finitely presented module due to Fact IV-9.8.
Suppose M is generated by q elements and let $k' = q - k$.
1. The condition is always necessary, even if the ring is not local. Let $A \in \mathbf{A}^{q\times m}$ be a presentation matrix for M. If the ring is local and if $\mathcal{F}_k(M) = \mathbf{A}$, since the minors of order k' are comaximal, one of them is invertible. By the invertible minor lemma II-5.9, the matrix A is equivalent to a matrix

$$\begin{bmatrix} \mathrm{I}_{k'} & 0_{k',m-k'} \\ 0_{k,k'} & A_1 \end{bmatrix},$$

and so, the matrix $A_1 \in \mathbf{A}^{k\times(m-k')}$ is also a presentation matrix of M. Finally, if the ring is residually discrete, we can reduce the number of generators until the corresponding presentation matrix has all of its coefficients in the radical.

2. *a* ⇒ *b.* The same proof shows that we can take, for s_j, the minors of order k' of A.

b ⇒ *c.* Immediate.
c ⇒ *a.* Saying that $\mathcal{F}_k(M) = \mathbf{A}$ comes down to solving the system of linear equations $\sum_\ell x_\ell s_\ell = 1$, where the unknowns are the x_ℓ's and where the s_ℓ's are the minors of order k' of the matrix A. We can therefore apply the basic local-global principle.
a ⇒ *d.* Results from *1.*
d ⇒ *e.* Trivial.
e ⇒ *a.* This can only be proven in classical mathematics (hence the star that we attached to *d* and *e*). We prove it by reductio ad absurdum, by proving the contrapositive. If $\mathcal{F}_k(M) \neq \mathbf{A}$ let $\mathfrak{p}$ be a strict maximal ideal containing $\mathcal{F}_k(M)$. After localization at $\mathfrak{p}$, we obtain $\mathcal{F}_k(M_\mathfrak{p}) \subseteq \mathfrak{p}\mathbf{A}_\mathfrak{p} \neq \mathbf{A}_\mathfrak{p}$, and so $M_\mathfrak{p}$ is not generated by k elements. □

Comment. This lemma gives the *true meaning* of the equality $\mathcal{F}_k(M) = \mathbf{A}$; we can say that $\mathcal{F}_k(M)$ "measures" the possibility for the module to be locally generated by k elements. Hence the following definition.
See also Exercises IV-19, 11 and 12. ■

2.5. Definition. A finitely generated module is said to be *locally generated by k elements* when it satisfies the equivalent properties of Item *2* in the local number of generators lemma.

3. Localization at $1+\mathfrak{a}$

Let $\mathfrak{a}$ be an ideal of $\mathbf{A}$, $S := 1+\mathfrak{a}$, $\jmath : \mathbf{A} \to \mathbf{B} := \mathbf{A}_{1+\mathfrak{a}}$
be the canonical homomorphism, and $\mathfrak{b} := \jmath(\mathfrak{a})\mathbf{B}$.

Note that $\mathfrak{b}$ is identified with $S^{-1}\mathfrak{a}$ (Fact II-6.4) and that $1+\mathfrak{b} \subseteq \mathbf{B}^\times$ (Fact 1.5).

3.1. Lemma. *(Quotient of powers of* $\mathfrak{a}$ *in the localized ring* $\mathbf{A}_{1+\mathfrak{a}}$*)*
Under the previous hypotheses we have the following results.

1. $\operatorname{Ker}\jmath \subseteq \mathfrak{a}$, $\mathbf{B} = \jmath(\mathbf{A}) + \mathfrak{b}$ *and the canonical homomorphism* $\mathbf{A}/\mathfrak{a} \to \mathbf{B}/\mathfrak{b}$ *is an isomorphism.*
2. *The localization at* $1+\mathfrak{a}$ *is the same as the localization at* $1+\mathfrak{a}^n$ $(n \geqslant 1)$*, so* $\operatorname{Ker}\jmath \subseteq \mathfrak{a}^n$, $\mathbf{B} = \jmath(\mathbf{A}) + \mathfrak{b}^n$ *and* $\mathbf{A}/\mathfrak{a}^n \simeq \mathbf{B}/\mathfrak{b}^n$ *.*
3. *For all* p, $q \in \mathbb{N}$, $\jmath$ *induces an isomorphism* $\mathfrak{a}^p/\mathfrak{a}^{p+q} \xrightarrow{\sim} \mathfrak{b}^p/\mathfrak{b}^{p+q}$ *of* $\mathbf{A}$*-modules.*

D *1.* The inclusion $\operatorname{Ker}\jmath \subseteq \mathfrak{a}$ is immediate.
The fact that the homomorphism $\mathbf{A}/\mathfrak{a} \to \mathbf{B}/\mathfrak{b}$ is an isomorphism relies on two equivalent universal problems being solved: in the first we must annihilate the elements of $\mathfrak{a}$, in the second, we also need to invert the

elements of $1+\mathfrak{a}$, but inverting 1 is costless. Finally, the surjectivity of this morphism means precisely that $\mathbf{B}=\jmath(\mathbf{A})+\mathfrak{b}$.

2. The monoids $1+\mathfrak{a}$ and $1+\mathfrak{a}^n$ are equivalent because $1-a$ divides $1-a^n$.

3. Let $\mathfrak{b}^q=S^{-1}\mathfrak{a}^q=\mathfrak{a}^q\mathbf{B}$. By multiplying $\mathbf{B}=\jmath(\mathbf{A})+\mathfrak{b}^q$ by $\mathfrak{a}^p$, we obtain $\mathfrak{b}^p=\jmath(\mathfrak{a}^p)+\mathfrak{b}^{p+q}$. Therefore, the map $\jmath$ induces a surjection of $\mathbf{A}$-modules $\mathfrak{a}^p\twoheadrightarrow\mathfrak{b}^p/\mathfrak{b}^{p+q}$. It remains to see that its kernel is $\mathfrak{a}^{p+q}$. If $x\in\mathfrak{a}^p$ satisfies $\jmath(x)\in\mathfrak{b}^{p+q}$, there exists an $s\in 1+\mathfrak{a}$ such that $sx\in\mathfrak{a}^{p+q}$, and since s is invertible modulo $\mathfrak{a}$, it is also invertible modulo $\mathfrak{a}^{p+q}$, and so $x\in\mathfrak{a}^{p+q}$. □

3.2. Localized finite ring lemma. *If $\mathfrak{a}$ is a finitely generated ideal and $n\in\mathbb{N}^*$, we have the equivalences*

$$\mathfrak{b}^n=\mathfrak{b}^{n+1}\iff\mathfrak{b}^n=0\iff\mathfrak{a}^n=\mathfrak{a}^{n+1}.$$

In this case,

1. *we have* $\mathfrak{a}^n=\operatorname{Ker}\jmath=\langle 1-e\rangle$ *with e idempotent, such that*
$$\mathbf{B}=\mathbf{A}_{1+\mathfrak{a}}=\mathbf{A}[1/e]=\mathbf{A}/\langle 1-e\rangle\,,$$
2. *if in addition $\mathbf{A}$ is a $\mathbf{k}$-algebra, then $\mathbf{A}/\mathfrak{a}$ is finite over $\mathbf{k}$ if and only if $\mathbf{B}$ is finite over $\mathbf{k}$.*

D If $\mathfrak{b}^n=\mathfrak{b}^{n+1}$, then $\mathfrak{b}^n$ is a finitely generated idempotent ideal, so $\mathfrak{b}^n=\langle\varepsilon\rangle$ with ε being an idempotent. But since $\varepsilon\in\mathfrak{b}$, the idempotent $1-\varepsilon$ is invertible, therefore equal to 1, i.e. $\varepsilon=0$, so $\mathfrak{b}^n=0$. The third equivalence comes from $\mathfrak{b}^n/\mathfrak{b}^{n+1}\simeq\mathfrak{a}^n/\mathfrak{a}^{n+1}$ (Lemma 3.1).

1. Since $\mathfrak{a}^n$ is a finitely generated idempotent, $\mathfrak{a}^n=\langle 1-e\rangle$ with e an idempotent. The rest then stems from Fact II-4.2.

2. If $\mathbf{B}$ is a finitely generated $\mathbf{k}$-module, so is $\mathbf{A}/\mathfrak{a}\simeq\mathbf{B}/\mathfrak{b}$. Conversely, suppose that $\mathbf{A}/\mathfrak{a}$ is a finitely generated $\mathbf{k}$-module and let us consider the filtration of $\mathbf{B}$ by the powers of $\mathfrak{b}$

$$0=\mathfrak{b}^n\subseteq\mathfrak{b}^{n-1}\subseteq\cdots\subseteq\mathfrak{b}^2\subseteq\mathfrak{b}\subseteq\mathbf{B}.$$

Then, each quotient $\mathfrak{b}^i/\mathfrak{b}^{i+1}$ is a $\mathbf{B}/\mathfrak{b}$-finitely generated module, or an $\mathbf{A}/\mathfrak{a}$-finitely generated module, and consequently a finitely generated $\mathbf{k}$-module. We deduce that $\mathbf{B}$ is a finitely generated $\mathbf{k}$-module. □

3.3. Localized zero-dimensional ring lemma.
Let $\mathfrak{a}$ be a finitely generated ideal of $\mathbf{A}$ such that the localized ring $\mathbf{B}=\mathbf{A}_{1+\mathfrak{a}}$ is zero-dimensional. Then, there exist an integer n and an idempotent e such that

$$\mathfrak{a}^n=\langle 1-e\rangle\qquad\textit{and}\qquad\mathbf{A}_{1+\mathfrak{a}}=\mathbf{A}\big[\tfrac{1}{e}\big]=\mathbf{A}/\langle 1-e\rangle\,.$$

If in addition $\mathbf{A}$ is a finitely generated $\mathbf{k}$-algebra with $\mathbf{k}$ zero-dimensional (for example a discrete field), then $\mathbf{B}$ is finite over $\mathbf{k}$.

D We apply the localized finite ring lemma; since $\mathbf{B}$ is zero-dimensional and $\mathfrak{b}$ finitely generated, there exists an integer n such that $\mathfrak{b}^n=\mathfrak{b}^{n+1}$.

We end with the weak Nullstellensatz VI-3.15 because $\mathbf{B}=\mathbf{A}/\langle 1-e\rangle$ is a finitely generated $\mathbf{k}$-algebra. □

Remark. Let $\mathfrak{a}$ be a finitely generated ideal of a ring $\mathbf{A}$ such that the localized ring $\mathbf{A}_{1+\mathfrak{a}}$ is zero-dimensional. The natural map $\mathbf{A}\to\mathbf{A}_{1+\mathfrak{a}}$ is therefore surjective with kernel $\bigcap_{k\geqslant 0}\mathfrak{a}^k=\mathfrak{a}^m$ with m such that $\mathfrak{a}^m=\mathfrak{a}^{m+1}$. In addition, $\mathfrak{a}^m$ is generated by an idempotent $1-e$ and $\mathbf{A}_{1+\mathfrak{a}}=\mathbf{A}[1/e]$. We then have

$$\textstyle\bigcap_{k\geqslant 0}\mathfrak{a}^k=\big(0:(0:\mathfrak{a}^\infty)\big).$$

This remark can be useful for computations. Suppose that $\mathbf{A}=\mathbf{k}[\underline{X}]/\mathfrak{f}$ where $\mathbf{k}[\underline{X}]=\mathbf{k}[X_1,\ldots,X_n]$ is a polynomial ring with n indeterminates over a discrete field $\mathbf{k}$ and $\mathfrak{f}=\langle f_1,\ldots,f_s\rangle$ is a finitely generated ideal. Let $\mathfrak{a}$ be a finitely generated ideal of $\mathbf{k}[\underline{X}]$ and $\overline{\mathfrak{a}}$ be its image in $\mathbf{A}$. Then, if $\mathbf{A}_{1+\overline{\mathfrak{a}}}$ is zero-dimensional, the composition $\mathbf{k}[\underline{X}]\to\mathbf{A}_{1+\overline{\mathfrak{a}}}$ is surjective and its kernel is expressed in two ways

$$\textstyle\bigcap_{k\geqslant 0}(\mathfrak{f}+\mathfrak{a}^k)=\big(\mathfrak{f}:(\mathfrak{f}:\mathfrak{a}^\infty)\big).$$

The right-hand side formula can turn out to be more efficient by computing $(\mathfrak{f}:\mathfrak{a}^\infty)$ as follows

$$(\mathfrak{f}:\mathfrak{a}^\infty)=\textstyle\bigcap_{j=1}^{r}(\mathfrak{f}:g_j^\infty)\text{ if }\mathfrak{a}=\langle g_1,\ldots,g_r\rangle\,.$$

■

Comment. In classical mathematics a prime ideal $\mathfrak{a}$ of the ring $\mathbf{A}$ is said to be *isolated* if it is both minimal and maximal in the set of prime ideals of $\mathbf{A}$. In other words if it does not compare to any other prime ideal for the inclusion relation. Saying that $\mathfrak{a}$ is maximal amounts to saying that $\mathbf{A}/\mathfrak{a}$ is zero-dimensional. Saying that $\mathfrak{a}$ is minimal amounts to saying that $\mathbf{A}_S$ is zero-dimensional, where $S=\mathbf{A}\setminus\mathfrak{a}$. But if $\mathfrak{a}$ is assumed to be maximal, the monoid S is the saturated monoid of $1+\mathfrak{a}$.
Conversely suppose that $\mathbf{B}=\mathbf{A}_{1+\mathfrak{a}}$ is zero-dimensional. Then $\mathbf{A}/\mathfrak{a}$ is also zero-dimensional since $\mathbf{A}/\mathfrak{a}\simeq\mathbf{B}/\mathfrak{a}\mathbf{B}$. Thus, when $\mathfrak{a}$ is also finitely generated, we find ourselves with a special case of the localized zero-dimensional ring lemma 3.3. It is worth noting that in the literature the isolated prime ideals generally intervene in the context of Noetherian rings and that therefore in classical mathematics they are automatically finitely generated. ■

4. Examples of local rings in algebraic geometry

Here we propose to study in a few cases "the local algebra in a zero of a polynomial system." We fix the following context for all of Section 4.

$$\boxed{\begin{array}{c}
\mathbf{k} \text{ is a ring, } \underline{f} = f_1, \dots, f_s \in \mathbf{k}[\underline{X}] = \mathbf{k}[X_1, \dots, X_n], \\
\mathbf{A} = \mathbf{k}[\underline{X}]/\langle \underline{f} \rangle = \mathbf{k}[x_1, \dots, x_n], \\
(\underline{\xi}) = (\xi_1, \dots, \xi_n) \in \mathbf{k}^n \text{ is a zero of the system,} \\
\mathfrak{m}_{\underline{\xi}} = \langle x_1 - \xi_1, \dots, x_n - \xi_n \rangle_{\mathbf{A}} \text{ is the ideal of the point } \underline{\xi}, \\
J(\underline{X}) = \mathrm{JAC}_{\underline{X}}(\underline{f}) \text{ is the Jacobian matrix of the system.}
\end{array}}$$

Recall that $\mathbf{A} = \mathbf{k} \oplus \mathfrak{m}_{\underline{\xi}}$ (Proposition IV-2.7). More precisely, we have with the evaluation at $\underline{\xi}$ a split exact sequence of $\mathbf{k}$-modules

$$0 \to \mathfrak{m}_{\underline{\xi}} \to \mathbf{A} \xrightarrow{\overline{g} \mapsto g(\underline{\xi})} \mathbf{k} \to 0,$$

and two homomorphisms of $\mathbf{k}$-algebras $\mathbf{k} \to \mathbf{A} \to \mathbf{k}$ which when composed give $\mathrm{Id}_{\mathbf{k}}$.

Also recall (Theorem IV-2.8) that $\mathfrak{m}_{\underline{\xi}}$ is a finitely presented $\mathbf{A}$-module (the presentation matrix is explicitly given).

Local algebra at a zero

In the following definition the terminology *local algebra at $\underline{\xi}$* must not be ambiguous. We do not claim that it is a local ring, we simply mimic the construction of the given local algebra in the case where $\mathbf{k}$ is a field.

4.1. Definition. *(Local algebra at a zero of a polynomial system)*
The ring $\mathbf{A}_{1+\mathfrak{m}_{\underline{\xi}}}$ is called *the local algebra at $\underline{\xi}$ of the polynomial system $\underline{f}$*. We also use the shorthand notation $\mathbf{A}_{\underline{\xi}}$ instead of $\mathbf{A}_{1+\mathfrak{m}_{\underline{\xi}}}$.

We denote by $\underline{\xi} : \mathbf{A} \to \mathbf{k}$ the evaluation at $\underline{\xi}$. It is factorized through the localization at $1 + \mathfrak{m}_{\underline{\xi}}$ and we obtain a character $\mathbf{A}_{\underline{\xi}} \to \mathbf{k}$. We therefore have $\mathbf{A}_{\underline{\xi}} = \mathbf{k} \oplus \mathfrak{m}_{\underline{\xi}}\mathbf{A}_{\underline{\xi}}$ and canonical isomorphisms

$$\mathbf{A}_{\underline{\xi}}/(\mathfrak{m}_{\underline{\xi}}\mathbf{A}_{\underline{\xi}}) \simeq \mathbf{A}/\mathfrak{m}_{\underline{\xi}} \simeq \mathbf{k}$$

4.2. Fact. (If $\mathbf{k}$ is a discrete field, the algebra $\mathbf{A}_{\underline{\xi}}$ is a local ring)

1. *Let* $\mathbf{k}$ *be a local ring with* $\mathrm{Rad}\,\mathbf{k} = \mathfrak{p}$, $\mathfrak{M} = \mathfrak{p}\mathbf{A} + \mathfrak{m}_{\underline{\xi}}$ *and* $\mathbf{C} = \mathbf{A}_{1+\mathfrak{M}}$. *Then,* $\mathbf{C}$ *is a local ring with* $\mathrm{Rad}(\mathbf{C}) = \mathfrak{M}\mathbf{C}$ *and* $\mathbf{C}/\mathrm{Rad}\,\mathbf{C} \simeq \mathbf{k}/\mathfrak{p}$ *.*
2. *If* $\mathbf{k}$ *is a discrete field, we have the following results.*
   a. *The ring* $\mathbf{A}_{\underline{\xi}}$ *is a local ring with* $\mathrm{Rad}\,\mathbf{A}_{\underline{\xi}} = \mathfrak{m}_{\underline{\xi}}\mathbf{A}_{\underline{\xi}}$ *and its residual field is (canonically isomorphic to)* $\mathbf{k}$.

b. The rings $\mathbf{A}$ *and* $\mathbf{A}_{\underline{\xi}}$ *are coherent Noetherian, and* $\mathbf{A}$ *is strongly discrete.*

c. $\bigcap_{r\in\mathbb{N}}\big(\mathfrak{m}_{\underline{\xi}}\mathbf{A}_{\underline{\xi}}\big)^r = 0.$

D *1.* We have $\mathbf{C}/\mathfrak{M}\mathbf{C} \simeq \mathbf{A}/\mathfrak{m}_{\xi} = \mathbf{k}/\mathfrak{p}$ by item *2* of Fact 1.5, then use item *3* of Fact 1.4.

2a. Results from *1.*

2b. The ring $\mathbf{A}$ is strongly discrete and coherent by Theorem VII-1.10. We deduce that $\mathbf{A}_{\underline{\xi}}$ is coherent.

For the Noetherianity we refer the reader to [MRR, VIII.1.5].

2c. Given items *2a* and *2b*, this is a special case of Krull's intersection theorem ([MRR, VIII.2.8]). □

Tangent space at a zero

In what follows we write $\partial_j f$ for $\frac{\partial f}{\partial X_j}$. Thus the Jacobian matrix of the system, which we have denoted by $J = J(\underline{X})$, is visualized as follows

$$\begin{array}{c} \\ f_1 \\ f_2 \\ \vdots \\ f_i \\ \vdots \\ f_s \end{array}\begin{array}{c} \begin{array}{cccc} X_1 & X_2 & \cdots & X_n \end{array} \\ \left[\begin{array}{cccc} \partial_1 f_1 & \partial_2 f_1 & \cdots & \partial_n f_1 \\ \partial_1 f_2 & \partial_2 f_2 & \cdots & \partial_n f_2 \\ \vdots & & & \vdots \\ \vdots & & & \vdots \\ \vdots & & & \vdots \\ \partial_1 f_s & \partial_2 f_s & \cdots & \partial_n f_s \end{array}\right] \end{array} = J.$$

The congruence below is immediate, for $f \in \mathbf{k}[\underline{X}]$,

$$f(\underline{X}) \equiv f(\underline{\xi}) + \sum\nolimits_{j=1}^{n} (X_j - \xi_j)\,\partial_j f(\underline{\xi}) \mod \langle X_1 - \xi_1, \ldots, X_n - \xi_n\rangle^2 \quad (3)$$

By specializing $\underline{X}$ in $\underline{x}$ we obtain in $\mathbf{A}$ the fundamental congruence

$$f(\underline{x}) \equiv f(\underline{\xi}) + \sum\nolimits_{j=1}^{n} (x_j - \xi_j)\,\partial_j f(\underline{\xi}) \mod {\mathfrak{m}_{\underline{\xi}}}^2 \quad (4)$$

We leave it up to the reader to verify that the kernel of $J(\underline{\xi})$ only depends on the ideal $\langle f_1, \ldots, f_s\rangle$ and on the point $\underline{\xi}$. It is a $\mathbf{k}$-submodule of $\mathbf{k}^n$ which can be called *the tangent space at* $\underline{\xi}$ *to the affine scheme over* $\mathbf{k}$ *defined by* $\mathbf{A}$. We will denote it by $\mathrm{T}_{\underline{\xi}}(\mathbf{A}/\mathbf{k})$ or $\mathrm{T}_{\underline{\xi}}$.

This terminology is reasonable in algebraic geometry (i.e. when $\mathbf{k}$ is a discrete field), at least in the case where $\mathbf{A}$ is integral. In that case we have a variety defined as an intersection of hypersurfaces $f_i = 0$, and the tangent space at $\underline{\xi}$ of the variety is the intersection of the tangent spaces at the hypersurfaces that define it.

In this same situation (discrete field as the basis), the zero $\underline{\xi}$ of the polynomial system is called a *regular point* or a *non-singular point* (of the affine scheme or yet again of the corresponding variety) when the dimension of the tangent space at $\underline{\xi}$ is equal to the dimension[7] of the variety at the point $\underline{\xi}$. A point that is not regular is called *singular.*

We now give a more abstract interpretation of the tangent space, in terms of derivation spaces. This works with an arbitrary commutative ring $\mathbf{k}$.

For a $\mathbf{k}$-algebra $\mathbf{B}$ and a character $\xi : \mathbf{B} \to \mathbf{k}$ we define a $\mathbf{k}$-*derivation at the point* ξ *of* $\mathbf{B}$ as a $\mathbf{k}$-linear form $d : \mathbf{B} \to \mathbf{k}$ which satisfies Leibniz's rule, i.e. by letting $f(\xi)$ for $\xi(f)$

$$d(fg) = f(\xi)d(g) + g(\xi)d(f).$$

This implies in particular $d(1) = 0$ (writing $1 = 1 \times 1$), and so $d(\alpha) = 0$ for $\alpha \in \mathbf{k}$. We will denote by $\mathrm{Der}_{\mathbf{k}}(\mathbf{B}, \xi)$ the $\mathbf{k}$-module of the $\mathbf{k}$-derivations of $\mathbf{B}$ at the point ξ.

This notation is slightly abusive. Actually if we let $\mathbf{k}'$ be the ring $\mathbf{k}$ provided with the $\mathbf{B}$-module structure given by ξ, the notation of Definition VI-6.5 would be $\mathrm{Der}_{\mathbf{k}}(\mathbf{B}, \mathbf{k}')$, and in fact equipped with the structure of a $\mathbf{B}$-module.

We will see that the tangent space at $\underline{\xi}$ of $\mathbf{A}$ and the $\mathbf{k}$-module of the $\mathbf{k}$-derivations of $\mathbf{A}$ at ξ are naturally isomorphic.

4.3. Proposition. ($\mathrm{T}_{\underline{\xi}}(\mathbf{A}/\mathbf{k})$, $\mathrm{Der}_{\mathbf{k}}(\mathbf{A}, \xi)$, and $(\mathfrak{m}_{\underline{\xi}}/\mathfrak{m}_{\underline{\xi}}{}^2)^\star$)

Let $\mathfrak{m} = \mathfrak{m}_{\underline{\xi}}$ *and recall the notation* $\mathrm{T}_{\underline{\xi}}(\mathbf{A}/\mathbf{k}) = \mathrm{Ker}\, J(\underline{\xi})$.

1. *For* $u = (u_1, \dots, u_n) \in \mathbf{k}^n$, *let* $D_u : \mathbf{k}[\underline{X}] \to \mathbf{k}$ *be the* $\mathbf{k}$-*linear form defined by*
$$D_u(f) = \textstyle\sum_{j=1}^{n} \partial_j f(\underline{\xi})\, u_j.$$
It is a derivation at the point $\underline{\xi}$, *we have* $u_j = D_u(X_j) = D_u(X_j - \xi_j)$, *and the map*
$$u \mapsto D_u,\ \mathbf{k}^n \to \mathrm{Der}_{\mathbf{k}}(\mathbf{k}[\underline{X}], \xi)$$
is a $\mathbf{k}$-*linear isomorphism.*
2. *If* $u \in \mathrm{Ker}\, J(\underline{\xi}) \subseteq \mathbf{k}^n$, *then* D_u *passes to the quotient modulo* $\langle f_1, \dots, f_s \rangle$ *and provides a* $\mathbf{k}$-*derivation at the point* $\underline{\xi}$, $\Delta_u : \mathbf{A} \to \mathbf{k}$.
We have $u_j = \Delta_u(x_j) = \Delta_u(x_j - \xi_j)$, *and the map*
$$u \mapsto \Delta_u,\ \mathrm{Ker}\, J(\underline{\xi}) \to \mathrm{Der}_{\mathbf{k}}(\mathbf{A}, \xi)$$
is a $\mathbf{k}$-*linear isomorphism.*
3. *In addition,* $\Delta_u(\mathfrak{m}^2) = 0$ *and we obtain, by restriction to* $\mathfrak{m}$ *and passage to the quotient modulo* $\mathfrak{m}^2$, *a* $\mathbf{k}$-*linear form* $\delta_u : \mathfrak{m}/\mathfrak{m}^2 \to \mathbf{k}$. *We thus construct a* $\mathbf{k}$-*linear map* $u \mapsto \delta_u$ *of* $\mathrm{Ker}\, J(\underline{\xi})$ *in* $(\mathfrak{m}/\mathfrak{m}^2)^\star$.

[7] If $\mathbf{A}$ is integral, this dimension does not depend on $\underline{\xi}$ and can be defined via a Noether position. In the general case, the Krull dimension of the ring $\mathbf{A}_{\underline{\xi}}$ must be considered.

4. Conversely, to $\delta \in (\mathfrak{m}/\mathfrak{m}^2)^\star$*, we associate* $u \in \mathbf{k}^n$ *defined by*

$$u_j = \delta\big((x_j - \xi_j) \bmod \mathfrak{m}^2\big).$$

Then, u belongs to $\operatorname{Ker} J(\underline{\xi})$*.*

5. The two maps defined in 3 and 4,

$$\operatorname{Ker} J(\underline{\xi}) \to (\mathfrak{m}/\mathfrak{m}^2)^\star \quad \textit{and} \quad (\mathfrak{m}/\mathfrak{m}^2)^\star \to \operatorname{Ker} J(\underline{\xi}),$$

are reciprocal **k***-linear isomorphisms.*

D *1.* Simple verification left to the reader.

2. For any $u \in \mathbf{k}^n$, we easily verify that the set

$$\big\{\, f \in \mathbf{k}[\underline{X}] \mid D_u(f) = 0 \text{ and } f(\underline{\xi}) = 0 \,\big\}$$

is an ideal of $\mathbf{k}[\underline{X}]$. If $u \in \operatorname{Ker} J(\underline{\xi})$, we have $D_u(f_i) = 0$ by definition (and $f_i(\underline{\xi}) = 0$); we deduce that D_u is null over $\langle f_1, \dots, f_s \rangle$.

3. To see that $\Delta_u(\mathfrak{m}^2) = 0$, we use $\Delta_u(fg) = f(\underline{\xi})\Delta_u(g) + g(\underline{\xi})\Delta_u(f)$ and $f(\underline{\xi}) = g(\underline{\xi}) = 0$ for f, $g \in \mathfrak{m}$.

4. The congruence (4) for $f = f_i$ is $\sum_{j=1}^n (x_j - \xi_j)\partial_j f_i(\underline{\xi}) \in \mathfrak{m}^2$. Applying δ, this gives the equality $\sum_{j=1}^n u_j \partial_j f_i(\underline{\xi}) = 0$, i.e. $u \in \operatorname{Ker} J(\underline{\xi})$.

5. Let $\delta \in (\mathfrak{m}/\mathfrak{m}^2)^\star$ and $u \in \operatorname{Ker} J(\underline{\xi})$ be the corresponding element; it must be shown that $\delta_u = \delta$, which is the same as checking, for $f \in \mathfrak{m}$,

$$\delta(f \bmod \mathfrak{m}^2) = \textstyle\sum_{j=1}^n \partial_j f(\underline{\xi}) \delta\big((x_j - \xi_j) \bmod \mathfrak{m}^2\big),$$

but this stems from (4).

Conversely, let $u \in \operatorname{Ker} J(\underline{\xi})$ and $v \in \operatorname{Ker} J(\underline{\xi})$ be the element corresponding to δ_u; it must be shown that $v = u$; which is the same as checking $\delta_u\big((x_j - \xi_j) \bmod \mathfrak{m}^2\big) = u_j$, an equality which has already been observed. □

Remark. Note that the definition which we have given for the tangent space $\mathrm{T}_{\underline{\xi}}(\mathbf{A}/\mathbf{k})$, natural and intuitive, portrays it as a submodule of $\mathbf{k}^n$, where n is the number of generators of the finitely presented **k**-algebra **A**. Therefore, its more abstract definition $\mathrm{Der}_{\mathbf{k}}(\mathbf{A}, \xi)$, or $\mathfrak{m}_{\underline{\xi}}/\mathfrak{m}_{\underline{\xi}}{}^2$, which is more intrinsic, must be preferred since it only depends on the **k**-algebra **A** and on the character $\xi : \mathbf{A} \to \mathbf{k}$, without taking into account the presentation chosen for **A** (actually only the structure of the localized algebra $\mathbf{A}_{\underline{\xi}}$ intervenes). ■

Cotangent space at a zero

Generally, we also have the dual notion of a *cotangent space at* $\underline{\xi}$. We will define it here as the cokernel of the transposed matrix ${}^{\mathrm{t}}J(\underline{\xi})$. Actually, it is a **k**-module which is intrinsically attached to the algebra **A** and to the character ξ, because it can also be defined formally as "the space of differentials at the point $\underline{\xi}$." We will not be developing this notion here.

The fundamental theorem that follows implies that the tangent space is canonically isomorphic to the dual of the cotangent space (Fact II-6.3 *2* applied to ${}^{\mathrm{t}}J$ gives $(\operatorname{Coker} {}^{\mathrm{t}}J)^{\star} \simeq \operatorname{Ker} J$ since ${}^{\mathrm{t}}({}^{\mathrm{t}}J) = J$). However, when we work with an arbitrary ring $\mathbf{k}$, the cotangent space is not necessarily isomorphic to the dual of the tangent space.

When a $\mathbf{B}$-module M admits a presentation matrix W over a generator set $(y_1, \ldots, y_n)$, if $\mathfrak{b}$ is an ideal of $\mathbf{B}$, by the base ring change $\pi_{\mathbf{B},\mathfrak{b}} : \mathbf{B} \to \mathbf{B}/\mathfrak{b}$, we obtain the $\mathbf{B}/\mathfrak{b}$-module $M/\mathfrak{b}M$ with the presentation matrix W mod $\mathfrak{b}$ over the generator set $(\overline{y_1}, \ldots, \overline{y_n})$.
With the $\mathbf{A}$-module $M = \mathfrak{m}_{\underline{\xi}}$ and the ideal $\mathfrak{b} = \mathfrak{m}_{\underline{\xi}}$, we obtain for the presentation matrix of the $\mathbf{k}$-module $\mathfrak{m}_{\underline{\xi}}/\mathfrak{m}_{\underline{\xi}}{}^2$ over $(\overline{x_1 - \xi_1}, \ldots, \overline{x_n - \xi_n})$, the matrix $\overline{W} = W$ mod $\mathfrak{m}_{\underline{\xi}}$, with the matrix W given in Theorem IV-2.8. The latter matrix, up to null columns, is the matrix ${}^{\mathrm{t}}J(\underline{\xi})$. The theorem that follows states the same thing in a precise manner.

4.4. Theorem. (Cotangent space at $\underline{\xi}$ and $\mathfrak{m}_{\underline{\xi}}/\mathfrak{m}_{\underline{\xi}}{}^2$) *Let $(e_i)_{i \in [\![1..n]\!]}$ be the canonical basis of* $\mathbf{k}^n$. *Consider the* $\mathbf{k}$*-linear map*

$$\varphi : \mathbf{k}^n \twoheadrightarrow \mathfrak{m}_{\underline{\xi}}/\mathfrak{m}_{\underline{\xi}}{}^2, \quad e_j \mapsto (x_j - \xi_j) \bmod \mathfrak{m}_{\underline{\xi}}{}^2.$$

Then, φ induces an isomorphism of $\mathbf{k}$*-modules* $\operatorname{Coker} {}^{\mathrm{t}}J(\underline{\xi}) \xrightarrow{\sim} \mathfrak{m}_{\underline{\xi}}/\mathfrak{m}_{\underline{\xi}}{}^2$.
Thus, we have a canonical isomorphism $\operatorname{Coker} {}^{\mathrm{t}}J(\underline{\xi}) \xrightarrow{\sim} \mathfrak{m}_{\underline{\xi}}\mathbf{A}_{\underline{\xi}}/(\mathfrak{m}_{\underline{\xi}}\mathbf{A}_{\underline{\xi}})^2$.

D Suppose without loss of generality that $\underline{\xi} = \underline{0}$ and use the notations of Theorem IV-2.8. The presentation matrix of $\mathfrak{m}_{\underline{0}}$ for the generator set $(x_1, \ldots, x_n)$ is the matrix $W = [\, R_{\underline{x}} \,|\, U \,]$ with $U(\underline{0}) = {}^{\mathrm{t}}J(\underline{0})$. As the matrix $R_{\underline{x}}$ mod $\mathfrak{m}_{\underline{0}}$ is null, we obtain the stated result.
The last assertion is given by Lemma 3.1 *3*. □

4.5. Definition. We define *the cotangent space at $\underline{\xi}$* as being the $\mathbf{k}$-module $\mathfrak{m}_{\underline{\xi}}\mathbf{A}_{\underline{\xi}}/(\mathfrak{m}_{\underline{\xi}}\mathbf{A}_{\underline{\xi}})^2$, for which only the structure of the local algebra at $\underline{\xi}$ intervenes.

In the remainder of Section 4, we will study a few examples of local algebras at zeros of polynomial systems, without assuming that we necessarily have a discrete field to begin with; $\mathbf{k}$ is only a commutative ring. Here we only seek to illustrate the geometric situation by freeing ourselves, if possible, of the hypothesis "discrete field," but without aiming to give the most general framework possible.

Local ring at an isolated point

The idea that drives this subsection comes from algebraic geometry where the local ring at $\underline{\xi}$ is zero-dimensional if and only if the point $\underline{\xi}$ is an isolated zero, and where the isolated zero is simple if and only if the tangent space is reduced to 0.

4.6. Theorem. (A simple isolated zero)
In the context described at the beginning of Section 4, the following properties are equivalent.

1. *The natural morphism* $\mathbf{k} \to \mathbf{A}_{\underline{\xi}}$ *is an isomorphism (in other words, the ideal* $\mathfrak{m}_{\underline{\xi}}$ *is null in* $\mathbf{A}_{\underline{\xi}}$*). In short, we write* $\mathbf{k} = \mathbf{A}_{\underline{\xi}}$*.*
2. *The matrix* ${}^{\mathrm{t}}J(\underline{\xi})$ *is surjective, i.e.* $1 \in \mathcal{D}_n\big(J(\underline{\xi})\big)$*.*
3. *The cotangent space at* $\underline{\xi}$ *is null, i.e.* $\mathfrak{m}_{\underline{\xi}} = \mathfrak{m}_{\underline{\xi}}{}^2$*.*
4. *The ideal* $\mathfrak{m}_{\underline{\xi}}$ *is generated by an idempotent* $1 - e$ *of* $\mathbf{A}$*. In this case the natural morphisms* $\mathbf{k} \to \mathbf{A}[1/e] \to \mathbf{A}_{\underline{\xi}}$ *are isomorphisms.*
5. *There exists a* $g \in \mathbf{A}$ *such that* $g(\underline{\xi}) = 1$ *and* $\mathbf{A}[1/g] = \mathbf{k}$*.*

If in addition $\mathbf{k}$ *is a discrete field (or a reduced zero-dimensional ring), we also have the equivalence with the following property.*

6. *The tangent space* $\mathrm{T}_{\underline{\xi}}$ *is null.*

Here is how we can describe that previous situation more intuitively: the local algebra at $\underline{\xi}$ is a "connected component of $\mathbf{A}$" (i.e. the localization at $\underline{\xi}$ is the same as the localization at an idempotent e) "reduced to a simple point" (i.e. this $\mathbf{k}$-algebra is isomorphic to $\mathbf{k}$). In terms of algebraic varieties, item *5* means that there is a Zariski open set containing the point $\underline{\xi}$ in which the variety is reduced to this point.

D *1* ⇔ *3.* By the localized finite ring lemma 3.2 with $n = 1$.

2 ⇔ *3.* By Theorem 4.4.

3 ⇔ *4.* By the lemma of the finitely generated idempotent ideal II-4.6. We then obtain the desired isomorphisms by Fact II-4.2, and therefore item *5* with $g = e$.

5 ⇒ *1.* The equality $g(\underline{\xi}) = 1$ means that $g \in 1 + \mathfrak{m}_{\underline{\xi}}$. Thus the ring $\mathbf{A}_{\underline{\xi}}$ is a localized ring of $\mathbf{A}[1/g] = \mathbf{k}$, and it is equal to $\mathbf{k}$ since $\mathbf{A}_{\underline{\xi}} = \mathbf{k} \oplus \mathfrak{m}_{\underline{\xi}}\mathbf{A}_{\underline{\xi}}$.

3 ⇔ *6.* (Discrete field case.) Since the tangent space is the dual of the cotangent, *3* always implies *6.* Over a discrete field a matrix is surjective if and only if its transposed matrix is injective, this gives the equivalence of *3* and *6* (when considering the matrix $J(\underline{\xi})$). □

Remark. The difference between the case s (number of equations) $= n$ (number of indeterminates) and the case $s > n$ is scarcely visible in the previous theorem, but it is important. If we tweak a system with $s = n$ and if the base field is algebraically closed, a simple zero continues to exist, slightly tweaked. In the $s > n$ case, a tweak generally makes the zero disappear. But this is another story, because the notion of such a tweak needs to be defined in algebra. ■

For the discrete field case, here is a result in the same style as Theorem 4.6, but more general and more precise. This can also be seen as a local version of Stickelberger's theorem (Theorems IV-8.16 and IV-8.17). Please note however that, unlike what takes place for Stickelberger's theorem, the proof of Theorem 4.7 does not involve the Nullstellensatz or the Noether position. However, a change of variables à la Nagata intervenes in the call of Theorem VI-3.15 for the implication *7* ⇒ *8.*

4.7. Theorem. (Isolated zero) *Suppose that* $\mathbf{k}$ *is a discrete field. The following properties are equivalent.*

1. *The algebra* $\mathbf{A}_{\underline{\xi}}$ *is finite over* $\mathbf{k}$*.*
2. *The algebra* $\mathbf{A}_{\underline{\xi}}$ *is integral over* $\mathbf{k}$*.*
3. *The algebra* $\mathbf{A}_{\underline{\xi}}$ *is zero-dimensional.*
4. *The ideal* $\mathfrak{m}_{\underline{\xi}}$ *is nilpotent in* $\mathbf{A}_{\underline{\xi}}$*.*
5. *There exists an* $r \in \mathbb{N}$ *such that* ${\mathfrak{m}_{\underline{\xi}}}^{r} = {\mathfrak{m}_{\underline{\xi}}}^{r+1}$*.*
6. *There exists an* $r \in \mathbb{N}$ *such that the ideal* ${\mathfrak{m}_{\underline{\xi}}}^{r}$ *is generated by an idempotent* $1-e$*, the morphism* $\mathbf{A} \to \mathbf{A}_{\underline{\xi}}$ *is surjective, and* $\mathbf{A}/\langle 1-e\rangle \simeq \mathbf{A}_{\underline{\xi}} \simeq \mathbf{A}[1/e]$*.*
7. *There exists a* $g \in \mathbf{A}$ *such that* $g(\underline{\xi}) = 1$ *and* $\mathbf{A}[1/g] = \mathbf{A}_{\underline{\xi}}$*.*
8. *There exists a* $g \in \mathbf{A}$ *such that* $g(\underline{\xi}) = 1$ *and* $\mathbf{A}[1/g]$ *is local and zero-dimensional.*
9. *There exists an* $h \in \mathbf{A}$ *such that* $h(\underline{\xi}) = 1$ *and* $\mathbf{A}[1/h]$ *is finite over* $\mathbf{k}$*.*

In this case, $\mathbf{A}_{\underline{\xi}}$ *is strictly finite over* $\mathbf{k}$*,* $(\mathbf{A}_{\underline{\xi}})_{\mathrm{red}} = \mathbf{k}$*, and if* $m = [\mathbf{A}_{\underline{\xi}} : \mathbf{k}]$*, for all* $\ell \in \mathbf{A}_{\underline{\xi}}$*, we have* $\mathrm{C}_{\mathbf{A}_{\underline{\xi}}/\mathbf{k}}(\ell)(T) = \big(T - \ell(\underline{\xi})\big)^{m}$*.*

D The localized finite ring lemma 3.2, applied with $\mathfrak{a} = \mathfrak{m}_{\underline{\xi}}$, shows that *4* is equivalent to *5* and implies *1.*

3 ⇒ *4.* By the localized zero-dimensional ring lemma 3.3.

We have *1* ⇒ *2*, and since $\mathbf{k}$ is a discrete field, *2* ⇒ *3.*

Thus items *1* to *5* are equivalent.

Item *5* implies that $\mathfrak{m}_{\underline{\xi}}^{r}$ is idempotent. Therefore *5* ⇒ *6* by the finitely generated idempotent ideal lemma II-4.6 and Fact II-4.2.

Note that $e \in 1 + \mathfrak{m}_{\underline{\xi}}^{r} \subseteq 1 + \mathfrak{m}_{\underline{\xi}}$, so $e(\underline{\xi}) = 1$. Therefore *6* implies *7* with $g = e$.

7 ⇒ *8.* The algebra $\mathbf{A}[1/g] = \mathbf{A}_{\underline{\xi}}$ is local and finitely generated, and the result follows by Theorem VI-3.15.

8 ⇒ *9.* Take $h = g$.

9 ⇒ *1.* Because $\mathbf{A}_{\underline{\xi}}$ is a localized ring of $\mathbf{A}[1/h]$.

In this case $\mathbf{A}_{\underline{\xi}}$ is strictly finite over $\mathbf{k}$ because it is a finite and finitely presented algebra (Theorem VI-3.17).

Finally, the equality $\mathrm{C}_{\mathbf{A}_{\underline{\xi}}/\mathbf{k}}(\ell)(T) = (T - \ell(\underline{\xi}))^{m}$ comes from the fact that $\ell - \ell(\underline{\xi})$ is in $\mathfrak{m}$, so is nilpotent in $\mathbf{A}_{\underline{\xi}}$, therefore it admits T^{m} as a characteristic polynomial. □

4.8. Definition. *(Isolated zero of a polynomial system over a ring)*

1. The zero $\underline{\xi}$ of the system is a *simple isolated zero* (or *simple zero*) if $\mathbf{A}_{\underline{\xi}} = \mathbf{k}$.
2. The zero $\underline{\xi}$ of the system is an *isolated zero* if $\mathbf{A}_{\underline{\xi}}$ is finite over $\mathbf{k}$.
3. If in addition $\mathbf{k}$ is a discrete field, the dimension of $\mathbf{A}_{\underline{\xi}}$ as a $\mathbf{k}$-vector space is called the *multiplicity* of the isolated zero $\underline{\xi}$.

Remark. Item *1* is an abbreviation by which we mean precisely that the canonical homomorphisms $\mathbf{k} \to \mathbf{A}_{\underline{\xi}} \to \mathbf{k}$ are isomorphisms.

In item *3* we see that over a discrete field, an isolated zero is simple if and only if it is of multiplicity 1. ■

Local ring at a non-singular point of a complete intersection curve

We always consider the context defined at the beginning of Section 4, and we assume $s = n-1$. In other words we now have a system of $n-1$ polynomial equations with n unknowns and we expect the corresponding variety to be "a curve."

We will see that if the zero $\underline{\xi}$ of the curve is non-singular in the intuitive sense that the cotangent space at the point $\underline{\xi}$ is a projective $\mathbf{k}$-module of rank 1, then the "local" situation matches our expectation, i.e. matches what the non-singular points of the curves in differential geometry have accustomed us to.

4.9. Theorem. (The ideal of a non-singular point of a locally complete intersection curve) *When $s = n-1$ the following properties are equivalent.*

1. *The point $\underline{\xi}$ is non-singular in the sense that $J(\underline{\xi})$ is a matrix of rank $n-1$ over $\mathbf{k}$.*
2. *The cotangent space at $\underline{\xi}$, $\mathfrak{m}_{\underline{\xi}}/\mathfrak{m}_{\underline{\xi}}{}^2$, is a projective $\mathbf{k}$-module of rank 1.*
3. *The ideal $\mathfrak{m}_{\underline{\xi}}$ is a projective $\mathbf{A}$-module of rank 1.*
4. *The ideal $\mathfrak{m}_{\underline{\xi}}\mathbf{A}_{\underline{\xi}}$ is a projective $\mathbf{A}_{\underline{\xi}}$-module of rank 1.*
5. *The ideal $\mathfrak{m}_{\underline{\xi}}\mathbf{A}_{\underline{\xi}}$ is a free $\mathbf{A}_{\underline{\xi}}$-module of rank 1.*
6. *The cotangent space at $\underline{\xi}$, $\mathfrak{m}_{\underline{\xi}}/\mathfrak{m}_{\underline{\xi}}{}^2$, is a free $\mathbf{k}$-module of rank 1.*

D Recall that for a ring $\mathbf{B}$, a $\mathbf{B}$-module M and an ideal $\mathfrak{b}$ of $\mathbf{B}$ we obtain by scalar extension $\mathbf{B}/\mathfrak{b} \otimes_{\mathbf{B}} M \simeq M/\mathfrak{b}M$. In particular, if $\mathfrak{c}$ is an ideal of $\mathbf{B}$ we obtain $(\mathbf{B}/\mathfrak{b}) \otimes_{\mathbf{B}} \mathfrak{c} \simeq \mathfrak{c}/\mathfrak{b}\mathfrak{c}$.

But the natural surjective $\mathbf{B}$-linear map $\mathfrak{b} \otimes \mathfrak{c} \to \mathfrak{b}\mathfrak{c}$ is not always an isomorphism (it is the case if one of the two ideals is flat).

1 ⇔ *2.* Indeed, ${}^{\mathrm{t}}J(\underline{\xi})$ is a presentation matrix of the cotangent space.

3 ⇒ *4.* Indeed, the $\mathbf{A}_{\underline{\xi}}$-module $\mathfrak{m}_{\underline{\xi}}\mathbf{A}_{\underline{\xi}}$ is obtained from the $\mathbf{A}$-module $\mathfrak{m}_{\underline{\xi}}$ by scalar extension from $\mathbf{A}$ to $\mathbf{A}_{\underline{\xi}}$.

4 ⇒ *2* and *5* ⇒ *6.* Indeed, the $\mathbf{k}$-module $\mathfrak{m}_{\underline{\xi}}/\mathfrak{m}_{\underline{\xi}}{}^2 \simeq \mathfrak{m}_{\underline{\xi}}\mathbf{A}_{\underline{\xi}}/(\mathfrak{m}_{\underline{\xi}}\mathbf{A}_{\underline{\xi}})^2$ is obtained from the $\mathbf{A}_{\underline{\xi}}$-module $\mathfrak{m}_{\underline{\xi}}\mathbf{A}_{\underline{\xi}}$ by scalar extension from $\mathbf{A}_{\underline{\xi}}$ to $\mathbf{k} \simeq \mathbf{A}_{\underline{\xi}}/\mathfrak{m}_{\underline{\xi}}\mathbf{A}_{\underline{\xi}}$ (see the first sentence of this proof).

2 ⇔ *3.* This results from the consideration of the presentation matrix of $\mathfrak{m}_{\underline{\xi}}$ as an $\mathbf{A}$-module given to Theorem IV-2.8 and to Lemma IV-2.1.
To simplify the presentation let us treat the case $n = 4$ with $\underline{\xi} = \underline{0}$.
We have four variables X_i and three polynomials

$$\begin{aligned} f_1(\underline{X}) &= X_1a_1(\underline{X}) + X_2a_2(\underline{X}) + X_3a_3(\underline{X}) + X_4a_4(\underline{X}),\\ f_2(\underline{X}) &= X_1b_1(\underline{X}) + X_2b_2(\underline{X}) + X_3b_3(\underline{X}) + X_4b_4(\underline{X}),\\ f_3(\underline{X}) &= X_1c_1(\underline{X}) + X_2c_2(\underline{X}) + X_3c_3(\underline{X}) + X_4c_4(\underline{X}). \end{aligned}$$

A presentation matrix of $\mathfrak{m}_{\underline{0}}$ over (x_1, x_2, x_3, x_4) is

$$W(\underline{x}) = \begin{bmatrix} x_2 & x_3 & 0 & x_4 & 0 & 0 & a_1(\underline{x}) & b_1(\underline{x}) & c_1(\underline{x}) \\ -x_1 & 0 & x_3 & 0 & x_4 & 0 & a_2(\underline{x}) & b_2(\underline{x}) & c_2(\underline{x}) \\ 0 & -x_1 & -x_2 & 0 & 0 & x_4 & a_3(\underline{x}) & b_3(\underline{x}) & c_3(\underline{x}) \\ 0 & 0 & 0 & -x_1 & -x_2 & x_3 & a_4(\underline{x}) & b_4(\underline{x}) & c_4(\underline{x}) \end{bmatrix},$$

or yet again $W(\underline{x}) = [\,R_{\underline{x}} \mid U(\underline{x})\,]$ with

$$U(\underline{x}) = \begin{bmatrix} a_1(\underline{x}) & b_1(\underline{x}) & c_1(\underline{x}) \\ a_2(\underline{x}) & b_2(\underline{x}) & c_2(\underline{x}) \\ a_3(\underline{x}) & b_3(\underline{x}) & c_3(\underline{x}) \\ a_4(\underline{x}) & b_4(\underline{x}) & c_4(\underline{x}) \end{bmatrix} \quad \text{and} \quad {}^{\mathrm{t}}J(\underline{0}) = U(\underline{0}).$$

We want to show that $W(\underline{x})$ (presentation matrix of the $\mathbf{A}$-module $\mathfrak{m}_{\underline{0}}$) and $W(\underline{0})$ (presentation matrix of the $\mathbf{k}$-module $\mathfrak{m}_{\underline{0}}/\mathfrak{m}_{\underline{0}}{}^2$) are simultaneously of rank $n - 1 = 3$.
Refer to Lemma IV-2.1. Item *3* gives the equality $\mathcal{D}_4\big(W(\underline{x})\big) = 0$ (because $\mathcal{D}_4\big(U(\underline{x})\big) = 0$), and since $U(\underline{0}) = U(\underline{x}) \bmod \mathfrak{m}_{\underline{0}}$, item *2* gives the equivalence

$$1 \in \mathcal{D}_{\mathbf{A},3}\big(W(\underline{x})\big) \iff 1 \in \mathcal{D}_{\mathbf{k},3}\big(U(\underline{0})\big) \iff 1 \in \mathcal{D}_{\mathbf{k},3}\big(W(\underline{0})\big).$$

1 ⇒ *5.* We reuse the previous notations with $n = 4$ and $\underline{\xi} = \underline{0}$. Since the matrix ${}^{\mathrm{t}}J(\underline{0}) = U(\underline{0})$ is of rank $n - 1$, there exist $\lambda_1, \ldots, \lambda_4 \in \mathbf{k}$ such that

$$\det\big(V(\underline{0})\big) = 1, \quad \text{where} \quad V(\underline{x}) = \begin{bmatrix} a_1(\underline{x}) & b_1(\underline{x}) & c_1(\underline{x}) & \lambda_1 \\ a_2(\underline{x}) & b_2(\underline{x}) & c_2(\underline{x}) & \lambda_2 \\ a_3(\underline{x}) & b_3(\underline{x}) & c_3(\underline{x}) & \lambda_3 \\ a_4(\underline{x}) & b_4(\underline{x}) & c_4(\underline{x}) & \lambda_4 \end{bmatrix}.$$

We deduce that $\det\big(V(\underline{x})\big) \in 1 + \mathfrak{m}_{\underline{\xi}}$, and so $V(\underline{x}) \in \mathbb{GL}_4(\mathbf{A}_{\underline{\xi}})$. However,

$$[\,x_1\ x_2\ x_3\ x_4\,]\,V = [\,0\ \ 0\ \ 0\ \ y\,] \ \text{ with } \ y = \textstyle\sum_i \lambda_i x_i.$$

This shows that $\langle x_1, x_2, x_3, x_4\rangle = \langle y\rangle$ in $\mathbf{A}_{\underline{\xi}}$. Finally, y is regular since the module $\mathfrak{m}_{\underline{\xi}}$ is of rank 1. □

We will denote by $M^{\otimes_{\mathbf{B}} r}$ the r^{th} tensor power of the $\mathbf{B}$-module M.

4.10. Theorem. *Suppose the equivalent properties of Theorem 4.9 satisfied, denote by Ω the cotangent space $\mathfrak{m}_{\underline{\xi}}/\mathfrak{m}_{\underline{\xi}}{}^2$ and consider an element p of $\mathfrak{m}_{\underline{\xi}}$ that is a* **k***-basis of Ω.*

1. *For each $r > 0$, the natural* **k***-linear map $\Omega^{\otimes_{\mathbf{k}} r} \to \mathfrak{m}_{\underline{\xi}}{}^r/\mathfrak{m}_{\underline{\xi}}{}^{r+1}$ is an isomorphism.*
   In other terms, the graded **k***-algebra $\bigoplus_{r\in\mathbb{N}} \mathfrak{m}_{\underline{\xi}}{}^r/\mathfrak{m}_{\underline{\xi}}{}^{r+1}$ associated with the pair $(\mathbf{A}, \mathfrak{m}_{\underline{\xi}})$ is (naturally) isomorphic to the symmetric algebra $\mathbf{S_k}(\Omega)$ of the* **k***-module Ω, itself isomorphic to $\mathbf{k}[X]$ because Ω is free of rank 1.*
2. *If* **k** *is a nontrivial discrete field, $\mathbf{A}_{\underline{\xi}}$ is a* discrete valuation ring (DVR) *in the following sense: every nonzero element of $\mathbf{A}_{\underline{\xi}}$ is uniquely expressed in the form up^ℓ for some $\ell \geqslant 0$ and $u \in \mathbf{A}^\times$.*

D Let $\mathfrak{m} = \mathfrak{m}_{\underline{\xi}}$. Also notice that for some projective **k**-module of rank 1, the symmetric algebra is equal to the tensor algebra.

1. We have a natural isomorphism $\mathfrak{m}^{\otimes_{\mathbf{A}} r} \xrightarrow{\sim} \mathfrak{m}^r$ because $\mathfrak{m}$ is flat. By the scalar extension $\mathbf{A} \to \mathbf{A}/\mathfrak{m} = \mathbf{k}$, the **A**-modules $\mathfrak{m}$ and $\mathfrak{m}^r$ give the **k**-modules $\mathfrak{m}/\mathfrak{m}^2$ and $\mathfrak{m}^r/\mathfrak{m}\mathfrak{m}^r = \mathfrak{m}^r/\mathfrak{m}^{r+1}$.

Since the scalar extension commutes with the tensor product, we deduce that the natural homomorphism $\left(\mathfrak{m}/\mathfrak{m}^2\right)^{\otimes_{\mathbf{k}} r} \to \mathfrak{m}^r/\mathfrak{m}^{r+1}$ is an isomorphism of **k**-modules.

Since the **k**-module $\mathfrak{m}/\mathfrak{m}^2$ admits the **k**-basis p mod $\mathfrak{m}^2$, the **k**-module $\mathfrak{m}^r/\mathfrak{m}^{r+1}$ admits the basis p^r mod $\mathfrak{m}^{r+1}$. Hence an isomorphism of **k**-algebras

$$\mathbf{k}[X] \xrightarrow{\sim} \textstyle\bigoplus_{r\in\mathbb{N}} \mathfrak{m}_{\underline{\xi}}{}^r/\mathfrak{m}_{\underline{\xi}}{}^{r+1} = \mathbf{S_k}(\Omega),$$

given by $X \mapsto p$. In practice, given the filtration

$$\mathfrak{m}^r \subset \cdots \subset \mathfrak{m}^2 \subset \mathfrak{m} \subset \mathbf{A},$$

every quotient of which is a free **k**-module of rank 1, the quotient $\mathbf{A}/\mathfrak{m}^r$ admits as its **k**-basis $(1, p \ldots, p^{r-1})$, with for $\ell < r$ the **k**-submodule $\mathfrak{m}^\ell/\mathfrak{m}^r$ which admits the basis $(p^\ell, \ldots, p^{r-1})$.

2. By Fact 4.2 *2* we obtain the result thanks to the following computation: if $x \in \mathbf{A}_{\underline{\xi}}$ is nonzero, it is nonzero in some $\mathbf{A}_{\underline{\xi}}/\mathfrak{m}^r$. Given the previous filtration there exists a minimum ℓ such that $x \in \mathfrak{m}^\ell$. If $x \equiv ap^\ell \bmod \mathfrak{m}^{\ell+1}$ with $a \in \mathbf{k}^\times$, we write $x = p^\ell(a+vp)$ with $v \in \mathbf{A}$ and $u = a+vp$ is invertible in $\mathbf{A}_{\underline{\xi}}$. □

Example: The monomial curve $t \mapsto (x_1 = t^4, x_2 = t^5, x_3 = t^6)$.

For setwise coprime n_1, n_2, $n_3 \in \mathbb{N}^*$ we define the monomial curve $(x_1 = t^{n_1}, x_2 = t^{n_2}, x_3 = t^{n_3})$, immersed in the affine space of dimension 3.

By definition, the ideal of this parameterized curve is, for a ring **k**, the kernel of the morphism $\mathbf{k}[X_1, X_2, X_3] \to \mathbf{k}[T]$ defined by $X_i \mapsto T^{n_i}$.

We can show that this ideal is always defined over $\mathbb{Z}$ and generated by three generators. Here we have chosen (see the comment at the end) the special case where $(n_1, n_2, n_3) = (4, 5, 6)$, a case for which two relators suffice:

$$x_1^3 = x_3^2 \quad \text{and} \quad x_2^2 = x_1 x_3.$$

(Left as an exercise for the reader.) Let

$$\mathbf{A} = \mathbf{k}[x_1, x_2, x_3] = \mathbf{k}[X_1, X_2, X_3] / \langle X_1^3 - X_3^2, X_2^2 - X_1 X_3 \rangle$$

be the ring of the curve. For $t_0 \in \mathbf{k}$, we consider the point

$$(\underline{\xi}) = (\xi_1, \xi_2, \xi_3) = (t_0^4, t_0^5, t_0^6),$$

with its ideal $\mathfrak{m} = \langle x_1 - \xi_1, x_2 - \xi_2, x_3 - \xi_3 \rangle_{\mathbf{A}}$. The condition for the point $\underline{\xi}$ to be non-singular, in the sense that the Jacobian matrix J evaluated at $\underline{\xi}$ is of rank 2, is given by $t_0 \in \mathbf{k}^\times$, because $\mathcal{D}_2(J) = \langle 4t_0^{11}, 5t_0^{12}, 6t_0^{13} \rangle$. From now on suppose that $t_0 \in \mathbf{k}^\times$. A presentation matrix of $\mathfrak{m}$ for the generator set $(x_1 - \xi_1, x_2 - \xi_2, x_3 - \xi_3)$ is given by

$$W = \begin{bmatrix} x_2 - \xi_2 & x_3 - \xi_3 & 0 & x_1^2 + \xi_1 x_1 + \xi_1^2 & -x_3 \\ -x_1 + \xi_1 & 0 & x_3 - \xi_3 & 0 & x_2 + \xi_2 \\ 0 & -x_1 + \xi_1 & -x_2 + \xi_2 & -x_3 - \xi_3 & -\xi_1 \end{bmatrix}.$$

We know that it is of rank 2. We observe that $W_2, W_3 \in \langle W_1, W_5 \rangle$. We therefore obtain a new, simpler presentation matrix V with only the columns W_1, W_4, W_5. Recall on the one hand that for $B \in \mathbf{A}^{n \times m}$, we have $(\mathbf{A}^n / \operatorname{Im} B)^\star \simeq \operatorname{Ker} {}^{\mathrm{t}}B$ (Fact II-6.3); and on the other hand (Exercise X-11) that for a matrix $A \in \mathbb{M}_n(\mathbf{A})$ of rank $n-1$, $\operatorname{Ker} A = \operatorname{Im} \widetilde{A}$ is a direct summand in $\mathbf{A}^n$. By applying this to $B = V$ and $A = {}^{\mathrm{t}}V$, we obtain

$$\mathfrak{m}^\star \simeq (\mathbf{A}^3 / \operatorname{Im} V)^\star \simeq \operatorname{Ker} {}^{\mathrm{t}}V = \operatorname{Im} {}^{\mathrm{t}}\widetilde{V}$$

with $\operatorname{Im} {}^{\mathrm{t}}\widetilde{V}$ a direct summand in $\mathbf{A}^3$.

We thus explicitly produce the $\mathbf{A}$-module $\mathfrak{m}^\star$ of constant rank 1 as a direct summand in $\mathbf{A}^3$. ∎

Comment. Generally a submonoid M of $(\mathbb{N}, +, 0)$ has a finite complement G if and only if it is generated by a setwise coprime list of integers (for example with the above monomial curve we define $M = n_1\mathbb{N} + n_2\mathbb{N} + n_3\mathbb{N}$ generated by $\{n_1, n_2, n_3\}$). We say that the integers of G are the *holes* of the monoid M.

Their number $g := \#G$ is called the *genus* of M.

We always have $[\,2g, \infty\,[\subseteq M$. The monoids M for which $2g - 1 \in G$ are said to be *symmetric*. This terminology accounts for the fact that, in this case, the interval $[\![0..2g-1]\!]$ contains as many holes as non-holes, and that they are interchanged by the symmetry $x \mapsto (2g-1) - x$.

For example, for coprime a and b, the monoid $a\mathbb{N} + b\mathbb{N}$ is symmetric of genus $g = \frac{(a-1)(b-1)}{2}$. We know how to characterize the monoids $n_1\mathbb{N} + n_2\mathbb{N} + n_3\mathbb{N}$ that are symmetric combinatorially. We prove that this is the case if and only if the ideal of the curve $(x_1 = t^{n_1}, x_2 = t^{n_2}, x_3 = t^{n_3})$ is generated by 2 elements. For example $4\mathbb{N} + 5\mathbb{N} + 6\mathbb{N}$ is symmetric, of genus 4, and its holes are $\{1, 2, 3, 7\}$. ∎

5. Decomposable rings

The rings which are isomorphic to finite products of local rings play an important role in the classical theory of Henselian local rings (for example in [Raynaud] or [Lafon & Marot]). Such rings are called *decomposed rings* and a local ring is said to be Henselian (in classical mathematics) if every finite extension is a decomposed ring.

In this section we give an introductory fragment of the constructive approach for the notion of a decomposed ring. In fact, since we would like to avoid the factorization problems, we will introduce the notion, constructively more pertinent, of a decomposable ring.

Everything begins with this simple but important remark: in a commutative ring the idempotents are always "isolated."

5.1. Lemma. *In a commutative ring* $\mathbf{A}$ *two idempotents equal modulo* $\mathrm{Rad}\,\mathbf{A}$ *are equal.*

D We show that the homomorphism $\mathbb{B}(\mathbf{A}) \to \mathbb{B}(\mathbf{A}/\mathrm{Rad}\,\mathbf{A})$ is injective. If an idempotent e is in $\mathrm{Rad}\,\mathbf{A}$, $1-e$ is idempotent and invertible, therefore equal to 1. □

Remark. This does not hold at all in a noncommutative context; the idempotents of a ring of square matrices $\mathbb{M}_n(\mathbf{A})$ are the projection matrices; over a field we obtain, for instance by fixing the rank to 1, a connected variety of dimension > 0 without any isolated points (if $n \geqslant 2$). ■

Decomposable elements

5.2. Definition. Let $\mathbf{A}$ be a ring and $a \in \mathbf{A}$. The element a is said to be *decomposable*[8] if there exists an idempotent e such that

$$\begin{cases} a \bmod \langle 1-e\rangle \text{ is invertible in } \mathbf{A}/\langle 1-e\rangle \quad \text{and} \\ a \bmod \langle e\rangle \in \mathrm{Rad}(\mathbf{A}/\langle e\rangle). \end{cases}$$

Recall when underlining the analogies that an element a has a quasi-inverse if and only if there exists an idempotent e such that

$$\begin{cases} a \bmod \langle 1-e\rangle \text{ is invertible in } \mathbf{A}/\langle 1-e\rangle \quad \text{and} \\ a \bmod \langle e\rangle = 0 \text{ in } \mathbf{A}/\langle e\rangle\,, \end{cases}$$

and that an element a has as its annihilator an idempotent if and only if there exists an idempotent e such that

$$\begin{cases} a \bmod \langle 1-e\rangle \text{ is regular in } \mathbf{A}/\langle 1-e\rangle \quad \text{and} \\ a \bmod \langle e\rangle = 0 \text{ in } \mathbf{A}/\langle e\rangle\,. \end{cases}$$

[8] Some caution must be exercised here regarding this terminology as it comes into conflict with the notion of an indecomposable idempotent insofar as every idempotent is a decomposable element of the ring.

5.3. Proposition. *An element a of $\mathbf{A}$ is decomposable if and only if there exists a b such that*

1. $b(1-ab)=0$,
2. $a(1-ab)\in \operatorname{Rad}\mathbf{A}$.

In addition, the element b satisfying these conditions is unique, and $ab=e$ is the unique idempotent of $\mathbf{A}$ satisfying $\langle a\rangle=\langle e\rangle \mod \operatorname{Rad}\mathbf{A}$.

D Suppose a is decomposable. Then, in the product $\mathbf{A}=\mathbf{A}_1\times\mathbf{A}_2$, with $\mathbf{A}_1=\mathbf{A}/\langle 1-e\rangle$ and $\mathbf{A}_2=\mathbf{A}/\langle e\rangle$, we have $e=(1,0)$, $a=(a_1,a_2)$, with $a_1\in\mathbf{A}_1^\times$ and $a_2\in\operatorname{Rad}(\mathbf{A}_2)$. We let $b=(a_1^{-1},0)$, and we indeed get

$$b(1-ab)=(b,0)-(b,0)(1,0)=0_\mathbf{A} \ \text{ and } \ a(1-ab)=(0,a_2)\in\operatorname{Rad}\mathbf{A}.$$

Suppose that an element b satisfies

$$\begin{cases} b(1-ab)=0 \quad \text{and} \\ a(1-ab)\in\operatorname{Rad}\mathbf{A}. \end{cases}$$

Then, the element $ab=e$ is an idempotent and a is invertible modulo $1-e$. Moreover, modulo e we have $a=a(1-e)$ which is in $\operatorname{Rad}\mathbf{A}$, so $a \bmod e$ is in $\operatorname{Rad}(\mathbf{A}/\langle e\rangle)$.

Let us take a look at the uniqueness. If $b(1-ab)=0$ and $a(1-ab)\in\operatorname{Rad}\mathbf{A}$, then $e=ab$ is an idempotent such that $\langle a\rangle=\langle e\rangle \mod \operatorname{Rad}\mathbf{A}$. This characterizes it as an idempotent of $\mathbf{A}/\operatorname{Rad}\mathbf{A}$, so as an idempotent of $\mathbf{A}$. The equalities $be=b$ and $ba=e$ imply that $\big(b+(1-e)\big)\big(ae+(1-e)\big)=1$. The element $b+(1-e)$ is therefore uniquely determined as the inverse of $ae+(1-e)$. Consequently, the element b is itself uniquely determined. □

5.4. Definition. We say that the ring $\mathbf{A}$ is *decomposable* if every element is decomposable.

5.5. Fact.

1. *A product of rings is decomposable if and only if each of the factors is decomposable.*
2. *A zero-dimensional ring is decomposable. A residually discrete local ring is decomposable. A connected decomposable ring is local and residually discrete.*
3. *The structure of a decomposable ring is purely equational (it can be defined by means of composition laws subjected to universal axioms).*

D *3.* We add to the laws of commutative rings two laws

$$a\mapsto b \ \text{ and } \ (a,x)\mapsto y,$$

with the axioms $b=b^2a$ and $\big(1+x(a^2b-a)\big)y=1$. Hence $a^2b-a\in\operatorname{Rad}\mathbf{A}$.

1. Results from item *3.* □

Remark. If we let $b=a^\sharp$, then $(a^\sharp)^\sharp=b^\sharp=a^2b$ and $\big((a^\sharp)^\sharp\big)^\sharp=a^\sharp$. In addition, $(a^\sharp)^\sharp$ and $a^\sharp$ are quasi-inverses of one another. ■

Lifting idempotents

5.6. Definition. Let $\mathbf{A}$ be a ring.

1. We say that *the ring* $\mathbf{A}$ *lifts the idempotents* if the natural homomorphism
$$\mathbb{B}(\mathbf{A}) \to \mathbb{B}(\mathbf{A}/\mathrm{Rad}\,\mathbf{A})$$
is bijective, in other words if every idempotent of the quotient $\mathbf{A}/\mathrm{Rad}\,\mathbf{A}$ is lifted at an idempotent of $\mathbf{A}$.
2. We say that the ring $\mathbf{A}$ is *decomposed* if it is decomposable and if $\mathbb{B}(\mathbf{A})$ is bounded.

5.7. Proposition. *The following properties are equivalent.*

1. $\mathbf{A}$ *is residually zero-dimensional and lifts the idempotents.*
2. $\mathbf{A}$ *is decomposable.*

D *1* ⇒ *2.* Since $\mathbf{A}/\mathrm{Rad}\,\mathbf{A}$ is reduced zero-dimensional, there exists an idempotent e of $\mathbf{A}/\mathrm{Rad}\,\mathbf{A}$ such that $\langle a\rangle = \langle e\rangle \mod \mathrm{Rad}\,\mathbf{A}$. This idempotent is lifted at an idempotent of $\mathbf{A}$, that we continue to call e.
The element $a + (1 - e)$ is invertible in $\mathbf{A}/\mathrm{Rad}\,\mathbf{A}$, so in $\mathbf{A}$. Therefore, a is invertible in $\mathbf{A}/\langle 1 - e\rangle$. Finally, since $\langle a\rangle = \langle e\rangle \mod \mathrm{Rad}\,\mathbf{A}$, we obtain $a \in \mathrm{Rad}(\mathbf{A}/\langle e\rangle)$.
2 ⇒ *1.* Let $\pi : \mathbf{A} \to \mathbf{A}/\mathrm{Rad}\,\mathbf{A}$ be the canonical projection. Every element a of $\mathbf{A}$ satisfies $\langle \pi(a)\rangle = \langle \pi(e)\rangle$ for an idempotent e of $\mathbf{A}$. The quotient is therefore zero-dimensional. Let us show that $\mathbf{A}$ lifts the idempotents.
If $\pi(a)$ is idempotent and if e is the idempotent such that $\langle \pi(a)\rangle = \langle \pi(e)\rangle$, then $\pi(a) = \pi(e)$. □

Comment. It is now easy to see that in classical mathematics a ring is decomposed if and only if it is isomorphic to a finite product of local rings. ■

6. Local-global rings

In this section we introduce a notion which generalizes both that of a local ring and that of a zero-dimensional ring. This sheds light on a number of facts that are common to both these classes of rings, such as, for instance, the fact that finitely generated projective modules are quasi-free.

Definitions and the concrete local-global principle

6.1. Definition.

1. We say that a polynomial $f \in \mathbf{A}[X_1, \dots, X_n]$ *represents (in* $\mathbf{A}$*) the element* $a \in \mathbf{A}$ if there exists an $\underline{x} \in \mathbf{A}^n$ such that $f(\underline{x}) = a$.
2. We say that a polynomial $f \in \mathbf{A}[X_1, \dots, X_n]$ is *primitive by values* if the values of f generate the ideal $\langle 1\rangle$ (the variables being evaluated in $\mathbf{A}$).

3. A ring $\mathbf{A}$ is said to be *local-global* if every primitive polynomial by values represents an inverse.

Remark. Every primitive polynomial by values is primitive, therefore if a ring has the property that every primitive polynomial represents an inverse, it is a local-global ring. This corresponds to a definition in the literature (strongly U-irreducible ring) which has preceded that of local-global ring. ■

6.2. Fact.

1. *A ring* $\mathbf{A}$ *is local-global if and only if* $\mathbf{A}/\mathrm{Rad}(\mathbf{A})$ *is local-global.*
2. *A finite product of rings is local-global if and only if each of the rings is local-global.*
3. *A local ring is local-global.*
4. *A residually zero-dimensional ring is local-global.*
5. *A quotient of a local-global ring (resp. residually zero-dimensional) is local-global (resp. residually zero-dimensional).*
6. *Let* $\mathbf{A}$ *be a non-decreasing filtering union ring of subrings* $\mathbf{A}_i$*, i.e. for all* i, j*, there exists a* k *such that* $\mathbf{A}_i \cup \mathbf{A}_j \subseteq \mathbf{A}_k$*. Then, if each* $\mathbf{A}_i$ *is local-global, so is* $\mathbf{A}$*.*

D We leave the first three items as an exercise.

4. Given item *1*, it suffices to treat the case of a reduced zero-dimensional ring. This case reduces to the (obvious) case of a discrete field by the elementary local-global machinery no. 2.

5. Let us consider the local-global case (the other case is obvious). Let $\mathbf{A}$ be a local-global ring, $\mathfrak{a}$ be an ideal and $f \in \mathbf{A}[\underline{X}]$ be a primitive polynomial by values in $\mathbf{A}/\mathfrak{a}$. Therefore there are some values $p_1, \ldots, p_m$ of f and some $a \in \mathfrak{a}$ such that $\langle p_1, \ldots, p_m, a\rangle = \langle 1 \rangle$. The polynomial $g(\underline{X}, T) = Tf(\underline{X}) + (1-T)a$ is therefore primitive by values. Since $\mathbf{A}$ is local-global, there is a value $tf(\underline{x}) + (1-t)a$ of g which is invertible. The value $f(\underline{x})$ is thus invertible modulo $\mathfrak{a}$.

6. Let $P \in \mathbf{A}[X_1, \ldots, X_n]$ be primitive by values: $1 = uP(\underline{x}) + vP(\underline{y}) + \ldots$. By considering u, $\underline{x}$, v, $\underline{y}$, … and the coefficients of P, we see that there is a subring $\mathbf{A}_i$ such that $P \in \mathbf{A}_i[\underline{X}]$ and such that P is primitive by values over $\mathbf{A}_i$. Thus, P represents an inverse over $\mathbf{A}_i$, a fortiori over $\mathbf{A}$. □

For a polynomial the properties of representing an inverse or of being primitive by values are of finite character, as indicated in the following lemma.

6.3. Lemma. *Let S be a monoid of $\mathbf{A}$ and $f \in \mathbf{A}[X_1, \dots, X_m]$ be a polynomial.*

1. *The polynomial f represents an inverse in $\mathbf{A}_S$ if and only if there exists an $s \in S$ such that f represents an inverse in $\mathbf{A}_s$.*
2. *The polynomial f is primitive by values in $\mathbf{A}_S$ if and only if there exists an $s \in S$ such that f is primitive by values in $\mathbf{A}_s$.*

D We only prove item *1.* Let $F(\underline{X}, T) \in \mathbf{A}[\underline{X}, T]$ be the homogenization of $f(\underline{X})$ at a large enough degree. The hypothesis is equivalent to the existence of $\underline{x} \in \mathbf{A}^m$ and t, $u \in S$ such that $F(\underline{x}, t)$ divides u in $\mathbf{A}$. Letting $s = tu$, the elements t and $F(\underline{x}, t)$ are invertible in $\mathbf{A}_s$ so f represents an inverse in $\mathbf{A}_s$. □

6.4. Lemma. *Let $s \in \mathbf{A}$ and $\mathfrak{b}$ be an ideal of $\mathbf{A}$ with $1 \in \langle s \rangle + \mathfrak{b}$.*

1. *If f represents an inverse in $\mathbf{A}_s$ there exists a $\underline{z} \in \mathbf{A}^m$ such that $1 \in \langle f(\underline{z}) \rangle + \mathfrak{b}$.*
2. *If f is primitive by values in $\mathbf{A}_s$ there exists a finite number of elements $\underline{z}_j$, ($j \in [\![1..k]\!]$), in $\mathbf{A}^m$ such that $1 \in \big\langle f(\underline{z}_j) \mid j \in [\![1..k]\!] \big\rangle + \mathfrak{b}$.*

D *1.* Let $F(\underline{X}, T) \in \mathbf{A}[\underline{X}, T]$ be the homogenization of $f(\underline{X})$ at large enough degree d. The hypothesis is that $F(\underline{x}, t)$ divides u in $\mathbf{A}$ for some $\underline{x} \in \mathbf{A}^m$ and $t, u \in s^{\mathbb{N}}$. There exists an a such that $ta \equiv 1 \bmod \mathfrak{b}$ so

$$a^d F(\underline{x}, t) = F(a\underline{x}, at) \equiv F(a\underline{x}, 1) = f(a\underline{x}) \bmod \mathfrak{b},$$

hence $a^d u \in \langle f(\underline{z}) \rangle + \mathfrak{b}$ with $\underline{z} = a\underline{x}$. But $1 \in \big\langle a^d u \big\rangle + \mathfrak{b}$ therefore $1 \in \langle f(\underline{z}) \rangle + \mathfrak{b}$.

We can present the same argument "without computation" as follows.
We have $\mathbf{A}_s/(\mathfrak{b}\mathbf{A}_s) \simeq (\mathbf{A}/\mathfrak{b})_s$. Since $1 \in \langle s \rangle + \mathfrak{b}$, s is invertible in $\mathbf{A}/\mathfrak{b}$, and so $\mathbf{A}_s/(\mathfrak{b}\mathbf{A}_s) \simeq \mathbf{A}/\mathfrak{b}$. Since f represents an inverse in $\mathbf{A}_s$, a fortiori it represents an inverse in $\mathbf{A}_s/(\mathfrak{b}\mathbf{A}_s) \simeq \mathbf{A}/\mathfrak{b}$, i.e. f represents an inverse modulo $\mathfrak{b}$.

2. Similar to Item *1.* □

We will use in the remainder a slightly more subtle concrete local-global principle that we state in the form of a lemma. See also Exercise 15.

6.5. Lemma. *Let S_1, …, S_n be comaximal monoids of $\mathbf{A}$ and $f \in \mathbf{A}[X_1, \dots, X_m]$ be a polynomial. The following properties are equivalent.*

1. *The polynomial f is primitive by values.*
2. *In each of the rings $\mathbf{A}_{S_i}$, the polynomial f is primitive by values.*

3. For every maximal ideal $\mathfrak{m}$ of $\mathbf{A}$, f represents an inverse in $\mathbf{A}/\mathfrak{m}$.*

In particular, if f represents an inverse in each localized ring $\mathbf{A}_{S_i}$, f is primitive by values.

D The implications *1* $\Rightarrow$ *2* $\Rightarrow$ *3** are immediate. The implication *3** $\Rightarrow$ *1* is easy in classical mathematics.

Here is a direct and constructive proof of *2* $\Rightarrow$ *1.* It is a matter of decrypting the classical proof of *3.** $\Rightarrow$ *1*, by using the method that will be explained in Section XV-6. To simplify the notations but without loss of generality, we will prove the special case where f represents an inverse in each localized ring $\mathbf{A}_{S_i}$.
We therefore dispose of comaximal elements $(s_1, \ldots, s_n)$ such that in each localized ring $\mathbf{A}_{s_i}$, the polynomial f represents an inverse (Lemma 6.3). By applying Lemma 6.4 we successively obtain, for $k = 0, \ldots, n$,

$$1 \in \left\langle f(\underline{z_1}), \ldots, f(\underline{z_k}),\ s_{k+1}, \ldots, s_n \right\rangle .$$

After n steps: $1 \in \left\langle f(\underline{z_1}), \ldots, f(\underline{z_n}) \right\rangle$. □

6.6. Proposition. *The following properties are equivalent.*

1. *The ring $\mathbf{A}$ is local-global.*
2. *For every polynomial $f \in \mathbf{A}[X_1, \ldots, X_n]$, if there exists a system of comaximal elements $(s_1, \ldots, s_k)$ such that f represents an inverse in each $\mathbf{A}_{s_i}$, then f represents an inverse.*
3. *For every polynomial $f \in \mathbf{A}[X_1, \ldots, X_n]$, if there exist comaximal monoids S_i such that f is primitive by values in each $\mathbf{A}_{S_i}$, then f represents an inverse.*

D Given Lemmas 6.3 and 6.5, it suffices to show that if f is primitive by values there exist comaximal elements such that f represents an inverse in each localized ring. To simplify the notation, we will write everything using a single variable. We obtain $x_1, \ldots, x_r \in \mathbf{A}$ such that $1 \in \langle f(x_1), \ldots, f(x_r) \rangle$. Let $s_i = f(x_i)$, then the polynomial f represents an inverse in $\mathbf{A}_{s_i}$. □

By the Gauss-Joyal lemma (II-2.6) the primitive polynomials form a filter $U \subseteq \mathbf{A}[X]$. We call the ring $\mathbf{A}(X) = U^{-1}\mathbf{A}[X]$ the *Nagata ring.*

6.7. Fact. *We use the above notation.*

1. *$\mathbf{A}(X)$ is faithfully flat over $\mathbf{A}$.*
2. *$\mathbf{A}(X)$ is a local-global ring.*

D *1.* It is clear that $\mathbf{A}(X)$ is flat over $\mathbf{A}$ (it is a localization of $\mathbf{A}[X]$, which is free with a discrete basis). We then use the characterization *3a* in Theorem VIII-6.1. Let $\mathfrak{a} = \langle a_1, \ldots, a_n \rangle$ be a finitely generated ideal of $\mathbf{A}$ such that $1 \in \mathfrak{a}\mathbf{A}(X)$. We must show that $1 \in \mathfrak{a}$. The hypothesis gives $f_1, \ldots, f_n \in \mathbf{A}[X]$ such that the polynomial $f = \sum_i a_i f_i$ is primitive, i.e. $1 \in \mathrm{c}_{\mathbf{A}}(f)$. However, the ideal $\mathrm{c}_{\mathbf{A}}(f)$ is contained in $\mathfrak{a}$.

2. We proceed in three steps.
a) Let us first show that every primitive polynomial $P(T) \in \mathbf{B}[T]$ where $\mathbf{B} := \mathbf{A}(X)$ represents an invertible element. Indeed, let $P(T) = \sum_i Q_i T^i$ be such a polynomial. We can suppose without loss of generality that the Q_i's are in $\mathbf{A}[X]$. We have polynomials B_i such that $\sum_i B_i(X)Q_i(X)$ is primitive. A fortiori the coefficients of the Q_j's are comaximal.
Then, for $k > \sup_i\big(\deg_X(Q_i)\big)$, since $P(X^k)$ has for coefficients all the coefficients of the Q_j's (Kronecker's trick), it is a primitive polynomial of $\mathbf{A}[X]$, i.e. an invertible element of $\mathbf{B}$.
b) Let us show the same property for an arbitrary number of variables. Consider a primitive polynomial $Q(Y_1, \ldots, Y_m) \in \mathbf{B}[\underline{Y}]$. By Kronecker's trick, by letting $Y_j = T^{n^j}$ with large enough n, we obtain a polynomial $P(T)$ whose coefficients are those of Q, which brings us back to the previous case.
c) Finally, consider a primitive polynomial by values Q with m variables over $\mathbf{B}$. Then, Q is primitive and we can apply item b). □

Remarkable local-global properties

6.8. Concrete local-global principle. *Let S_1, ..., S_r be comaximal monoids of a local-global ring $\mathbf{A}$.*

1. *If two matrices of $\mathbf{A}^{m\times n}$ are equivalent over each of the $\mathbf{A}_{S_i}$, then they are equivalent.*
2. *If two matrices of $\mathbb{M}_n(\mathbf{A})$ are similar over each of the $\mathbf{A}_{S_i}$, then they are similar.*

D *1.* Let F and G be the matrices, then by hypothesis there exists some system of comaximal elements $(s_1, \ldots, s_r)$ and matrices U_1, ..., U_r, V_1, ..., V_r such that for each i we have $U_iF = GV_i$ and $\det(U_i)\det(V_i) = s_i$. Let us introduce indeterminates $(x_1, \ldots, x_r) = (\underline{x})$, and consider the matrices

$$U = U(\underline{x}) = x_1\, U_1 + \cdots + x_r\, U_r \text{ and } V = V(\underline{x}) = x_1\, V_1 + \cdots + x_r\, V_r.$$

We have $UF = GV$, and $\det(U)\det(V)$ is a polynomial in the x_i's that satisfy the hypotheses of Definition 6.1; it suffices to evaluate $(x_1, \ldots, x_r)$ successively at $(1, 0, \ldots, 0)$, ..., $(0, \ldots, 0, 1)$. Therefore there exists some $\underline{\alpha} \in \mathbf{A}^r$ such that the element $\det\big(U(\underline{\alpha})\big)\det\big(V(\underline{\alpha})\big)$ is invertible.

2. The same proof, with $U_i = V_i$ and $U = V$, works. □

We have the following corollary.

6.9. Concrete local-global principle. *Let S_1, …, S_r be comaximal monoids of a local-global ring* $\mathbf{A}$.

1. *If two finitely presented modules are isomorphic over each of the $\mathbf{A}_{S_i}$'s, then they are isomorphic.*
2. *Every finitely generated projective module is quasi-free.*

D *1.* We consider presentation matrices and characterize the fact that the modules are isomorphic by the equivalence of associated matrices (Lemma IV-1.1). We then apply item *1* of the local-global principle 6.8.

2. We apply item *1.* Consider a quasi-free module that has the same Fitting ideals, we know that the two modules become free after localization at comaximal elements (and the rank is the same each time because they have the same Fitting ideals). □

Let us also mention the following principles.

6.10. Concrete local-global principle. *Let* $\mathbf{A}$ *be a local-global ring.*

1. *Let S_1, …, S_r be comaximal monoids, M be a finitely presented module and N a finitely generated module. If N is a quotient of M over each of the $\mathbf{A}_{S_i}$'s, then N is a quotient of M.*
2. *A module locally generated by m elements is generated by m elements.*

D It suffices to prove item *1* because a module is generated by m elements if and only if it is a quotient of a free module of rank m.
We will continue the proof after the next two lemmas. □

6.11. Lemma. *Let M be a finitely presented $\mathbf{A}$-module, N be a finitely generated $\mathbf{A}$-module, S be a monoid of $\mathbf{A}$ and $\varphi : M_S \to N_S$ be a surjective $\mathbf{A}$-linear map.*

1. *There exist $s \in S$ and $\psi \in \mathrm{L}_{\mathbf{A}}(M, N)$ such that $s\varphi =_{\mathbf{A}_S} \psi_S$.*
2. *There exists a $v \in S$ such that $vN \subseteq \psi(M)$.*
3. *There exists a matrix Q of syzygies satisfied by the generators of N such that, when considering the module N' admitting Q as a presentation matrix, the map ψ is decomposed as follows*
$$M \xrightarrow{\theta} N' \xrightarrow{\pi} N,$$
(π is the canonical projection), with in particular $vN' \subseteq \theta(M)$ (a fortiori θ_S is surjective).

D Item *1* is a reformulation of Proposition V-9.3 (which affirms only slightly more, in a more general case). Item *2* easily stems from it.

3. We have $N = \mathbf{A}y_1 + \cdots + \mathbf{A}y_n$, and $M = \mathbf{A}x_1 + \cdots + \mathbf{A}x_m$, with a presentation matrix P.

For the factorization by θ to exist, it suffices that among the columns of the matrix Q we find the sygygies which are "images of the columns of P by ψ" (they are syzygies between the y_k's once we have expressed the $\psi(x_j)$'s in

terms of the y_k's).
For $vN' \subseteq \theta(M)$ to hold, it suffices that among the columns of the matrix Q we find the syzygies expressing that the vy_k's are in $\mathbf{A}\psi(x_1) + \cdots + \mathbf{A}\psi(x_m)$ (once we have expressed the $\psi(x_j)$'s in terms of the y_k's). □

6.12. Lemma. *The concrete local-global principle 6.10 is correct if N is itself a finitely presented module.*

D The hypothesis gives a surjective linear map $\varphi_i : M_{S_i} \to N_{S_i}$. By items *1* and *2* of Lemma 6.11 we have $s_i, v_i \in S_i$ and a linear map $\psi_i : M \to N$ such that $s_i\varphi_i = (\psi_i)_{S_i}$ and $v_iN \subseteq \psi_i(M)$. Each linear map ψ_i is represented by two matrices K_i and G_i which make the suitable diagrams commute (see Section IV-3).

$$\begin{tikzcd}
\mathbf{A}^p \arrow[r, "P"] \arrow[d, "K_i"'] & \mathbf{A}^m \arrow[r, two heads, "\pi_M"] \arrow[d, "G_i"] & M \arrow[d, "\psi_i"] \\
\mathbf{A}^q \arrow[r, "Q"'] & \mathbf{A}^n \arrow[r, two heads, "\pi_N"'] & N
\end{tikzcd}$$

Consider r unknowns a_i in $\mathbf{A}$ and the map $\psi = \sum a_i\psi_i$ corresponding to the matrices $K = \sum a_iK_i$ and $G = \sum a_iG_i$.

$$\begin{tikzcd}
\mathbf{A}^p \arrow[r, "P"] \arrow[d, "K"'] & \mathbf{A}^m \arrow[r, two heads, "\pi_M"] \arrow[d, "G"] & M \arrow[d, "\psi"] \\
\mathbf{A}^q \arrow[r, "Q"'] & \mathbf{A}^n \arrow[r, two heads, "\pi_N"'] & N
\end{tikzcd}$$

The fact that ψ is surjective means that the matrix $H = \boxed{\begin{array}{c|c} G & Q \end{array}}$ is surjective, i.e. $\mathcal{D}_n(H) = \langle 1 \rangle$. We therefore introduce the indeterminates c_ℓ to construct an arbitrary linear combination of the maximal minors δ_ℓ of the matrix H. This linear combination $\sum_\ell c_\ell\delta_\ell$ is a polynomial in the a_i's and c_ℓ's. By hypothesis, this polynomial represents 1 over each of the $\mathbf{A}\big[\frac{1}{s_iv_i}\big]$, thus, since the ring is local-global, it represents an inverse (Proposition 6.6). □

End of the proof of the concrete local-global principle 6.10.
We have $N = \mathbf{A}y_1 + \cdots + \mathbf{A}y_n$, and $M = \mathbf{A}x_1 + \cdots + \mathbf{A}x_m$, with a presentation matrix P. For each $i \in [\![1..r]\!]$ we apply Lemma 6.11 with the monoid S_i and the surjective linear map $\varphi_i : M_{S_i} \to N_{S_i}$ given in the hypothesis. We obtain a linear map $\psi_i : M \to N$, a matrix Q_i of syzygies satisfied by the y_k's, a linear map $\theta_i : M \to N_i'$ (where N_i' is the finitely presented module corresponding to Q_i), elements s_i, $v_i \in S_i$ with $s_i\varphi_i = (\psi_i)_{S_i}$, and finally ψ_i factorizes through $\theta_i : M \to N_i'$ with $v_iN_i' \subseteq \theta_i(M)$.
We then consider the finitely presented module N' corresponding to the matrix of syzygies Q obtained by juxtaposing the matrices Q_i, such that N' is a quotient of each N_i'.

As N is a quotient of N', we have brought the problem back to the case where N is itself finitely presented, a case that has been treated in Lemma 6.12. □

Congruential systems

An important stability property of local-global rings is stability by integral extension.

6.13. Theorem. *Let* $\mathbf{A} \subseteq \mathbf{B}$ *with* $\mathbf{B}$ *integral over* $\mathbf{A}$*. If* $\mathbf{A}$ *is local-global, then so is* $\mathbf{B}$*.*

The proof is left until page 522, after a detour via congruential rings.

6.14. Definition. A subset C of a ring $\mathbf{A}$ is called a *congruential system* if it satisfies the following property: if $s_1 + s_2 = 1$ in $\mathbf{A}$ and if c_1, $c_2 \in C$, then there exists a $c \in C$ such that $c \equiv c_1 \bmod s_1$ and $c \equiv c_2 \bmod s_2$.

Remarks. 1) It amounts to the same thing to say: if $\mathfrak{a}_1$ and $\mathfrak{a}_2$ are two comaximal ideals of $\mathbf{A}$ and if c_1, $c_2 \in C$, then there exists a $c \in C$ such that $c \equiv c_1 \bmod \mathfrak{a}_1$ and $c \equiv c_2 \bmod \mathfrak{a}_2$.
2) The element $c' = c_2 s_1 + c_1 s_2$ is the natural candidate for $c \in \mathbf{A}$ satisfying the congruences $c \equiv c_1 \bmod s_1$ and $c \equiv c_2 \bmod s_2$. We therefore must have some element c of C such that $c \equiv c' \bmod s_1 s_2$. ■

Example. Let $(\underline{b}) = (b_1, \dots, b_n)$ be a sequence in a ring $\mathbf{B}$. The *Suslin set of* $(b_1, \dots, b_n)$ is the following subset of $\mathbf{B}$:

$$\mathrm{Suslin}(\underline{b}) = \{\, u_1 b_1 + \cdots + u_n b_n \mid (u_1, \dots, u_n) \text{ is } \mathbb{E}_n(\mathbf{B})\text{-completable} \,\},$$

($(u_1, \dots, u_n)$ is the first row of a matrix of $\mathbb{E}_n(\mathbf{B})$).

If one of the u_i's is invertible, then $u_1 b_1 + u_2 b_2 + \cdots + u_n b_n \in \mathrm{Suslin}(\underline{b})$ and we therefore have $\{b_1, \dots, b_n\} \subseteq \mathrm{Suslin}(b_1, \dots, b_n) \subseteq \langle b_1, \dots, b_n \rangle$.

Let us show that the set $\mathrm{Suslin}(\underline{b})$ is always congruential.

Indeed, for E, $F \in \mathbb{E}_n(\mathbf{B})$ and two comaximal elements s, t of $\mathbf{B}$, there exists a $G \in \mathbb{E}_n(\mathbf{B})$ satisfying $G \equiv E \bmod s$ and $G \equiv F \bmod t$.

Let f, $g_1, \dots, g_n \in \mathbf{A}[X]$ with f monic, and $\mathbf{B} = \mathbf{A}[X]/\langle f \rangle$. Then the Suslin set of $(\overline{g_1}, \dots, \overline{g_n})$ plays an important role in the study of the unimodular polynomial vectors (cf. Lemma XV-6.1). ■

6.15. Fact. *For every polynomial* $P \in \mathbf{A}[X_1, \dots, X_n]$ *the set* V_P *of values of* P *is a congruential system* ($V_P = \{\, P(\underline{x}) \mid \underline{x} \in \mathbf{A}^n \,\}$)*.*

D Let s, t be two comaximal elements and $\underline{x}$, $\underline{y}$ be in $\mathbf{A}^n$. The Chinese remainder theorem gives us some $\underline{z} \in \mathbf{A}^n$ such that $\underline{z} \equiv \underline{x} \bmod s$ and $\underline{z} \equiv \underline{y} \bmod t$. Then, we have $P(\underline{z}) \equiv P(\underline{x}) \bmod s$ and $P(\underline{z}) \equiv P(\underline{y}) \bmod t$.□

6.16. Fact. *Let C be a congruential system. If $\mathfrak{a}_1, \ldots, \mathfrak{a}_\ell$ are pairwise comaximal ideals and if $c_1, \ldots, c_\ell \in C$, then there exists a $c \in C$ such that $c \equiv c_j \bmod \mathfrak{a}_j$ for $j \in [\![1..\ell]\!]$.*

D This is the usual proof of the Chinese remainder theorem, adapted to the current situation. We proceed by induction on $\ell \geqslant 2$. The base case is by definition. If $\ell > 2$ we consider the pairwise comaximal ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_{\ell-2}$ and $\mathfrak{a}_{\ell-1}\mathfrak{a}_\ell$. Let $e \in C$ such that $e \equiv c_{\ell-1} \bmod \mathfrak{a}_{\ell-1}$ and $e \equiv c_\ell \bmod \mathfrak{a}_\ell$. By induction hypothesis, we find c in C such that $c \equiv c_k \bmod \mathfrak{a}_k$ for $k \in [\![1..\ell-2]\!]$ and $c \equiv e \bmod \mathfrak{a}_{\ell-1}\mathfrak{a}_\ell$. A fortiori, $c \equiv c_{\ell-1} \bmod \mathfrak{a}_{\ell-1}$ and $c \equiv c_\ell \bmod \mathfrak{a}_\ell$. □

6.17. Fact. *Let C be a congruential system, $w_1, \ldots, w_n$ be elements of C and $(e_1, \ldots, e_n)$ be a fundamental system of orthogonal idempotents. Then, the element $w = e_1w_1 + \cdots + e_nw_n$ is in C.*

D We have $w \equiv w_i \bmod 1-e_i$, and the $\langle 1-e_i \rangle$'s are pairwise comaximal, but w is the unique element satisfying these congruences since $\bigcap_i \langle 1-e_i \rangle = \langle 0 \rangle$. It remains to apply the previous fact. □

6.18. Definition. A ring $\mathbf{A}$ is said to be *congruential* if every congruential system that generates the ideal $\langle 1 \rangle$ contains an invertible element.

6.19. Lemma.

1. *Let $\mathfrak{a} \subseteq \operatorname{Rad} \mathbf{A}$. Then, the ring $\mathbf{A}$ is congruential if and only if the ring $\mathbf{A}/\mathfrak{a}$ is congruential.*
2. *Every residually zero-dimensional ring is congruential.*
3. *Every congruential ring is local-global.*

D *1.* We use the fact that elements are comaximal (resp. invertible) in $\mathbf{A}$ if and only if they are comaximal (resp. invertible) in $\mathbf{A}/\mathfrak{a}$.

2. Let us suppose that $\mathbf{A}$ is residually zero-dimensional. It suffices to show that $\mathbf{A}/\operatorname{Rad} \mathbf{A}$ is congruential. Let W be a congruential system of $\mathbf{A}/\operatorname{Rad} \mathbf{A}$ such that $\langle W \rangle = \langle 1 \rangle$. Let $w_1, \ldots, w_n \in W$ with $\langle w_1, \ldots, w_n \rangle = \langle 1 \rangle$. There exists a fundamental system of orthogonal idempotents $(e_1, \ldots, e_n)$ such that we have $\langle e_1w_1 + \cdots + e_nw_n \rangle = \langle 1 \rangle$ (Lemma IV-8.5 item *5*). We conclude with Fact 6.17 that W contains the invertible element $e_1w_1 + \cdots + e_nw_n$.

3. Let us suppose that $\mathbf{A}$ is congruential and let P be a primitive polynomial by values. Since the values of P form a congruential system, a value of P is invertible. □

Stability by integral extension

As an immediate corollary of Lemma 6.19 we have the following result.

6.20. Corollary. *Let* $\mathbf{B}$ *be a strictly finite algebra over a discrete field* $\mathbf{A}$ *and* W *be a congruential system in* $\mathbf{B}$ *such that* $\langle W\rangle = \langle 1\rangle_{\mathbf{B}}$.
Then, the set $\mathrm{N}_{\mathbf{B}/\mathbf{A}}(W)$ *contains an invertible element.*

D We know that $\mathbf{B}$ is zero-dimensional, so it is congruential (Lemma 6.19). Since W is congruential and generates the ideal $\langle 1\rangle$, it contains an invertible element. Finally, the norm of an invertible element is invertible. □

6.21. Proposition. *Let* $\mathbf{B}$ *be a strictly finite algebra over a ring* $\mathbf{A}$ *and* W *be a congruential system in* $\mathbf{B}$. *If* $1 \in \langle W\rangle$, *then,* $1 \in \big\langle \mathrm{N}_{\mathbf{B}/\mathbf{A}}(W)\big\rangle$.

D *1.* A congruential system remains congruential by passage to a quotient ring. If we read the conclusion of Corollary 6.20 in the (weaker) form $1 \in \big\langle \mathrm{N}_{\mathbf{B}/\mathbf{A}}(W)\big\rangle$, we observe that it is in an adequate form to be subjected to the constructive machinery with maximal ideals which will be explained on page 876 in Section XV-6, and which is used to prove that an ideal contains 1. We therefore obtain the desired result. □

Remarks.
1) In classical mathematics we would also say this: if $1 \notin \big\langle \mathrm{N}_{\mathbf{B}/\mathbf{A}}(W)\big\rangle_{\mathbf{A}}$, this ideal would be contained in a maximal ideal $\mathfrak{m}$ of $\mathbf{A}$. But Corollary 6.20, applied with the discrete field $\mathbf{A}/\mathfrak{m}$ and the strictly finite algebra $\mathbf{B}/\mathfrak{m}\mathbf{B}$, shows that it is impossible.
The constructive machinery with maximal ideals precisely aims at decrypting this type of abstract proof and at transforming it into an algorithm which constructs 1 as an element of $\big\langle \mathrm{N}_{\mathbf{B}/\mathbf{A}}(W)\big\rangle_{\mathbf{A}}$ from the hypotheses.

2) As an example, if $(\underline{b}) = (b_1, \ldots, b_q)$ is a system of comaximal elements in $\mathbf{B}$, we have $1 \in \big\langle \mathrm{N}_{\mathbf{B}/\mathbf{A}}(w) \mid w \in \mathrm{Suslin}(\underline{b})\big\rangle_{\mathbf{A}}$, since the set $\mathrm{Suslin}(\underline{b})$ is congruential. But we will refrain from believing that $1 \in \big\langle \mathrm{N}_{\mathbf{B}/\mathbf{A}}(b_1), \ldots, \mathrm{N}_{\mathbf{B}/\mathbf{A}}(b_q)\big\rangle_{\mathbf{A}}$.
A famous instance of this property is a result due to Suslin regarding polynomial vectors, given in Lemma XV-6.1. In this lemma, $\mathbf{B}$ is of the form $\mathbf{A}[X]/\langle v\rangle$ with $v \in \mathbf{A}[X]$ a monic polynomial. A complete decrypting will be provided in the proof of the lemma in question. ■

Proof of Theorem 6.13. Let us first treat the case where $\mathbf{B}$ is free of finite rank, say ℓ, over $\mathbf{A}$. Let $P \in \mathbf{B}[X_1, \ldots, X_n]$ be a primitive polynomial by values. We want some $\underline{b} \in \mathbf{B}^n$ with $P(\underline{b})$ invertible. We consider the congruential system W of the values of P. By hypothesis we have $1 \in \langle W\rangle$. Proposition 6.21 then says that $\big\langle \mathrm{N}_{\mathbf{B}/\mathbf{A}}(W)\big\rangle_{\mathbf{A}} = \langle 1\rangle_{\mathbf{A}}$.
But $\mathrm{N}_{\mathbf{B}/\mathbf{A}}\big(P(b_1, \ldots, b_n)\big)$ is a polynomial with $n\ell$ variables in $\mathbf{A}$ if we express each $b_i \in \mathbf{B}$ over an $\mathbf{A}$-basis of $\mathbf{B}$, and $\mathbf{A}$ is local-global, so there exists a $\underline{b} \in \mathbf{B}^n$ such that $\mathrm{N}_{\mathbf{B}/\mathbf{A}}\big(P(\underline{b})\big)$ is invertible, and this implies that $P(\underline{b})$ is

invertible.
In the general case where $\mathbf{B}$ is only assumed to be integral over $\mathbf{A}$, let us consider in $\mathbf{B}$ the finitely generated $\mathbf{A}$-subalgebras $\mathbf{B}_i$; $\mathbf{B}$ is its increasing filtering union. Since $\mathbf{B}$ is integral over $\mathbf{A}$, so is $\mathbf{B}_i$, therefore it is a quotient of an $\mathbf{A}$-algebra which is a free $\mathbf{A}$-module of finite rank. By the first case, and in virtue of item *5* of Fact 6.2, each $\mathbf{B}_i$ is local-global. Finally, by the last item of Fact 6.2, $\mathbf{B}$ is local-global. □

Exercises and problems

Exercise 1. Prove in classical mathematics that the nilradical of a ring is equal to the intersection of its prime ideals.

Exercise 2. If $\mathfrak{a}$ is an ideal of $\mathbf{A}$ we let $\mathrm{J}_{\mathbf{A}}(\mathfrak{a})$ be its *Jacobson radical*, i.e. the inverse image of $\mathrm{Rad}(\mathbf{A}/\mathfrak{a})$ under the canonical projection $\mathbf{A} \to \mathbf{A}/\mathfrak{a}$. Let $\mathfrak{a}$ be an ideal of $\mathbf{A}$. Show that $\mathrm{J}_{\mathbf{A}}(\mathfrak{a})$ is the greatest ideal $\mathfrak{b}$ such that the monoid $1+\mathfrak{b}$ is contained in the saturated monoid of $1+\mathfrak{a}$.

Exercise 3. Prove in constructive mathematics that the Jacobson radical of a local ring coincides with the set of noninvertible elements, and that it is the unique ideal $\mathfrak{a}$ satisfying

- $\mathfrak{a}$ is maximal
- $1 \in \mathfrak{a}$ implies $1 = 0$.

Exercise 4. Let $\mathbf{A}$ be a noncommutative ring, $a, b \in \mathbf{A}$. Prove the following statements.

1. If a admits a left-inverse c, then c is a right-inverse of a if and only if c is unique as a left-inverse of a.

2. If $1 - ab$ admits a left-inverse u, then $1 - ba$ also admits a left-inverse v. Idea: if ab and ba are "small," u must be equal to $1 + ab + abab + \ldots$, and v equal to $1 + ba + baba + \cdots = 1 + b(1 + ab + abab + \cdots)a$.

3. If for all x, $1 - xa$ is left-invertible, then for all x, $1 - xa$ is right-invertible.

4. The following properties are equivalent.

- For all x, $1 - xa$ is left-invertible.
- For all x, $1 - xa$ is right-invertible.
- For all x, $1 - xa$ is invertible.
- For all x, $1 - ax$ is left-invertible.
- For all x, $1 - ax$ is right-invertible.
- For all x, $1 - ax$ is invertible.
- For all x, y, $1 - xay$ is invertible.

The elements a that satisfy these properties form a two-sided ideal called the Jacobson radical of $\mathbf{A}$.

Exercise 5. *(A freeness lemma)* Let $(\mathbf{A}, \mathfrak{m})$ be an integral local ring with residual field $\mathbf{k}$, with quotient field $\mathbf{K}$. Let E be a finitely generated $\mathbf{A}$-module; suppose that the $\mathbf{k}$-vector space $E/\mathfrak{m}E = \mathbf{k} \otimes_{\mathbf{A}} E$ and the $\mathbf{K}$-vector space $\mathbf{K} \otimes_{\mathbf{A}} E$ have the same dimension n. Show that E is a free $\mathbf{A}$-module of rank n.
Better: if $(x_1, \dots, x_n) \in E^n$ is a residual basis, it is an $\mathbf{A}$-basis of E.

Exercise 6. *(A consequence of Nakayama's lemma)*
Let E be a finitely presented $\mathbf{A}$-module and $a \in \mathrm{Rad}(\mathbf{A})$ be an E-regular element. Suppose that the $\mathbf{A}/a\mathbf{A}$-module E/aE is free of rank n. Show that E is free of rank n. More precisely, let $e_1, \dots, e_n \in E$, if $(\overline{e_1}, \dots, \overline{e_n})$ is an $\mathbf{A}/a\mathbf{A}$-basis of E/aE, then $(e_1, \dots, e_n)$ is an $\mathbf{A}$-basis of E.

Exercise 7. Let $\mathbf{A}$ be a local ring. Prove the following statements. If $\langle b \rangle = \langle a \rangle$, there exists an invertible element u such that $ua = b$. If $\mathfrak{a} = \langle x_1, \dots, x_n \rangle = \langle a \rangle$, there exists an index i such that $\mathfrak{a} = \langle x_i \rangle$.

Exercise 8. Give a detailed direct proof of Theorem 4.6 when $n = s$.

Exercise 9. Here certain items of Theorem V-3.1 are revisited, now supposing that the ring $\mathbf{A}$ is residually zero-dimensional. The reader is invited to provide proofs which are independent from the results obtained for local-global rings.

1. Every finitely generated projective $\mathbf{A}$-module is quasi-free.

2. Every matrix $G \in \mathbf{A}^{q \times m}$ of rank $\geqslant k$ is equivalent to a matrix

$$\begin{bmatrix} \mathrm{I}_k & 0_{k,m-k} \\ 0_{q-k,k} & G_1 \end{bmatrix},$$

with $\mathcal{D}_r(G_1) = \mathcal{D}_{k+r}(G)$ for all $r \geqslant 0$. The matrices are elementarily equivalent if $k < \sup(q, m)$.

3. Every finitely presented module locally generated by k elements is generated by k elements.

Exercise 10. *(If $\mathbf{A}$ is local, $\mathbb{SL}_n(\mathbf{A}) = \mathbb{E}_n(\mathbf{A})$)*
Let $\mathbf{A}$ be a local ring. Show that every matrix $B \in \mathbb{SL}_n(\mathbf{A})$ is produced from elementary matrices (in other words, B is elementarily equivalent to the matrix I_n). Inspiration may come from the proof of the local freeness lemma. See also Exercise 17.

Exercise 11. *1.* Prove that a finitely generated $\mathbf{A}$-module M is locally generated by k elements (Definition 2.5) if and only if $\bigwedge_{\mathbf{A}}^{k+1} M = 0$. Inspiration may come from the case $k = 1$ treated in Theorem V-7.3.

2. Deduce that the annihilator $\mathrm{Ann}\big(\bigwedge_{\mathbf{A}}^{k+1} M\big)$ and the Fitting ideal $\mathcal{F}_k(M)$ have the same radical.

Exercise 12. *(Variation on the locally generated theme)*
Let M be a finitely generated $\mathbf{A}$-module, with two generator sets $(x_1, \ldots, x_n)$ and $(y_1, \ldots, y_r)$ with $r \leqslant n$. We want to explicate a family (s_I) of $\binom{n}{r}$ comaximal elements, indexed by the $I \in \mathcal{P}_{r,n}$, such that $s_I M \subseteq \langle (x_i)_{i \in I} \rangle$. Note that over each localized ring $\mathbf{A}[s_I^{-1}]$, the module M is generated by the $(x_i)_{i\in I}$'s.
1. Let A and $B \in \mathbb{M}_n(\mathbf{A})$.

a. Explicate the membership
$$\det(A + B) \in \mathcal{D}_{n-r}(B) + \mathcal{D}_{r+1}(A).$$
b. Deduce that $1 \in \mathcal{D}_{n-r}(\mathrm{I}_n - A) + \mathcal{D}_{r+1}(A)$.
c. In particular, if $\mathrm{rk}(A) \leqslant r$, then $\mathrm{rk}(\mathrm{I}_n - A) \geqslant n - r$.
d. Let $a_1, \ldots, a_n \in \mathbf{A}$, $\pi_I = \prod_I a_i$, $\pi'_J = \prod_J (1 - a_j)$.
Show that the $(\pi_I)_{\#I=r+1}$'s and $(\pi'_J)_{\#J=n-r}$'s form a system of $\binom{n+1}{r+1}$ comaximal elements.

2. Prove the result stated at the beginning of the exercise by making the family (s_I) explicit.

3. Let E be a finitely generated $\mathbf{A}$-module locally generated by r elements. For any generator set $(x_1, \ldots, x_n)$, there exist comaximal elements t_j such that each of the localized modules E_{t_j} is generated by r elements among the x_i's.

4. Let $E = \langle x_1, \ldots, x_n \rangle$ be a finitely generated $\mathbf{A}$-module and $A \in \mathbb{M}_n(\mathbf{A})$ satisfying $\underline{x}\, A = \underline{x}$ with $\mathrm{rk}(A) \leqslant r$. Show that E is locally generated by r elements. Study a converse.

Exercise 13. If $\mathbf{A}$ and $\mathbf{B}$ are two decomposable rings we say that a ring homomorphism $\varphi : \mathbf{A} \to \mathbf{B}$ is a *decomposable ring morphism* if, for all a, $b \in \mathbf{A}$ satisfying $b(1 - ab) = 0$ and $a(1 - ab) \in \mathrm{Rad}\,\mathbf{A}$, we have in $\mathbf{B}$, with $a' = \varphi(a)$ and $b' = \varphi(b)$, $b'(1 - a'b') = 0$ and $a'(1 - a'b') \in \mathrm{Rad}\,\mathbf{B}$ (cf. Proposition 5.3).

1. Show that φ is a decomposable ring morphism if and only if $\varphi(\mathrm{Rad}\,\mathbf{A}) \subseteq \mathrm{Rad}\,\mathbf{B}$.

2. Study the injective and surjective decomposable ring morphisms. In other terms, precise the notions of a decomposable subring (considered as a single word) and of a decomposable quotient ring.

Exercise 14. *(Elementary local-global machinery of decomposable rings)*
The fact that one can systematically split a decomposable ring into two components leads to the following general method.
Most of the algorithms that work with the residually discrete local rings can be modified to work with the decomposable rings, by splitting the ring into two components each time the algorithm written for the residually discrete local rings uses the test "is this element invertible or in the radical?" In the first component the element in question is invertible, in the second it is in the radical.
Actually we rarely have the occasion to use this elementary machinery, the main reason being that a more general (but less elementary) local-global machinery applies with an arbitrary ring, as it will be explained in Section XV-5.

Exercise 15. *(Polynomial locally representing an inverse, Lemma 6.5)*
Item *3* of this exercise gives a reinforced version of Lemma 6.5. The approach used here is due to Lionel Ducos.
Let $\mathbf{A}$ be a ring, $d \in \mathbb{N}$ and $e = d(d+1)/2$.

1. Here, s is an indeterminate over $\mathbb{Z}$. Construct $d+1$ polynomials $a_i(s) \in \mathbb{Z}[s]$ for $i \in [\![0..d]\!]$, satisfying for every $P \in \mathbf{A}[\underline{X}] = \mathbf{A}[X_1, \dots, X_n]$ of degree $\leqslant d$:

$$(\star_d) \qquad s^e P(s^{-1}\underline{X}) = a_0(s)P(s^0\underline{X}) + a_1(s)P(s^1\underline{X}) + \cdots + a_d(s)P(s^d\underline{X}).$$

2. For $s \in \mathbf{A}$, $\underline{x} \in \mathbf{A}^n$ and $P \in \mathbf{A}[\underline{X}]$ of total degree $\leqslant d$, show that

$$s^e P(\underline{x}/s) \in \left\langle P(\underline{x}), P(s\underline{x}), \dots, P(s^d\underline{x}) \right\rangle \subseteq \mathbf{A}.$$

3. Let S be a monoid and $P \in \mathbf{A}[\underline{X}]$. Suppose that P represents an inverse in $\mathbf{A}_S$. Show that S meets the ideal generated by the values of P.

Exercise 16. (See also Exercise IV-10) Let $\mathbf{A}$ be a local-global ring and M an $\mathbf{A}$-module.

1. For every ideal $\mathfrak{a}$, the canonical homomorphism $\mathbf{A}^\times \to (\mathbf{A}/\mathfrak{a})^\times$ is surjective.

2. If x, $y \in M$ and $\mathbf{A}x = \mathbf{A}y$, there exists an inverse u such that $x = uy$.

Exercise 17. *(If $\mathbf{A}$ is local-global, $\mathbb{SL}_n(\mathbf{A}) = \mathbb{E}_n(\mathbf{A})$)*
Let $\mathbf{A}$ be a local-global ring, and $(a_1, \dots, a_n)$ a unimodular vector ($n \geqslant 2$).
1. Show that there exist x_2, $\dots$, x_n such that $a_1 + \sum_{i \geqslant 2} x_i a_i \in \mathbf{A}^\times$.
2. Deduce (for $n \geqslant 2$) that every unimodular vector transforms into the vector $(1, 0, \dots, 0)$ by elementary manipulations.
3. Deduce that $\mathbb{SL}_n\mathbf{A} = \mathbb{E}_n\mathbf{A}$.

Exercise 18. *(Semi-local rings, 1)*
1. For a ring $\mathbf{B}$, prove that the following properties are equivalent.

a. If $(x_1, \dots, x_k)$ is unimodular, there exists a system of orthogonal idempotents $(e_1, \dots, e_k)$ such that $e_1x_1 + \cdots + e_kx_k$ is invertible.

b. Under the same hypothesis, there exists a splitting $\mathbf{B} \simeq \mathbf{B}_1 \times \cdots \times \mathbf{B}_k$ such that the component of x_i in $\mathbf{B}_i$ is invertible for $i \in [\![1..k]\!]$.

c. Same as in *a*, but with $k = 2$.

d. For all $x \in \mathbf{B}$, there exists an idempotent $e \in \mathbf{B}$ such that $x + e$ is invertible.

Note that at item *a*, $(e_1, \dots, e_k)$ is a fundamental system of orthogonal idempotents since $1 \in \langle e_1, \dots, e_k \rangle$.
The rings satisfying these equivalent properties have been called "clean rings" in [147, Nicholson].

2. Clean rings are stable under quotient and under finite product. Every local ring is clean.
3. If $\mathbf{B}_{\mathrm{red}}$ is clean, the same goes for $\mathbf{B}$. Deduce that a zero-dimensional ring is clean.
4. If $\mathbf{B}_{\mathrm{red}}$ is clean, $\mathbf{B}$ lifts the idempotents of $\mathbf{B}/\operatorname{Rad}\mathbf{B}$.

We say that a ring $\mathbf{A}$ is *semi-local* if the ring $\mathbf{B} = \mathbf{A}/\operatorname{Rad}\mathbf{A}$ is clean. We say that it is *strict semi-local* if it is semi-local and if $\mathbb{B}(\mathbf{A}/\operatorname{Rad}\mathbf{A})$ is a bounded Boolean algebra.

Exercise 19. *(Semi-local rings, 2)* Prove the following statements.

1. A local ring is strict semi-local.
2. A semi-local and residually connected ring is local.
3. A residually zero-dimensional ring is semi-local.
4. A semi-local ring is local-global.
5. The semi-local rings are stable under quotient and under finite product.
6. In classical mathematics, a ring is strict semi-local if and only if it has a finite number of maximal ideals.

Exercise 20. *(Properties of the Nagata ring)* See also Exercise XII-3.
Let $\mathbf{A}$ be a ring and $U \subseteq \mathbf{A}[X]$ be the monoid of primitive polynomials.
Let $\mathbf{B} = U^{-1}\mathbf{A}[X] = \mathbf{A}(X)$ be the Nagata ring of $\mathbf{A}[X]$.

0. Give a direct proof of the fact that $\mathbf{B}$ is faithfully flat over $\mathbf{A}$.

1. $\mathbf{A} \cap \mathbf{B}^\times = \mathbf{A}^\times$.

2. $\mathrm{Rad}\,\mathbf{A} = \mathbf{A} \cap \mathrm{Rad}\,\mathbf{B}$ and $\mathrm{Rad}\,\mathbf{B} = U^{-1}(\mathrm{Rad}\,\mathbf{A})[X]$.

3. $\mathbf{B}/\mathrm{Rad}\,\mathbf{B} \simeq (\mathbf{A}/\mathrm{Rad}\,\mathbf{A})(X)$.

4. If $\mathbf{A}$ is local (resp. local and residually discrete), then $\mathbf{B}$ is local (resp. local and residually discrete).

5. If $\mathbf{A}$ is a field (resp. a discrete field), then $\mathbf{B}$ is a field (resp. a discrete field).

Exercise 21. *(Nagata ring with several indeterminates)*
Let U be the set of primitive polynomials of $\mathbf{A}[X,Y]$.

1. Show that U is a filter.
Let $\mathbf{A}(X,Y) = U^{-1}\mathbf{A}[X,Y]$, we call it the *Nagata ring of* $\mathbf{A}[X,Y]$.

2. Show that the canonical map $\mathbf{A}[X,Y] \to \mathbf{A}(X,Y)$ is injective and that we have a natural isomorphism $\mathbf{A}(X,Y) \xrightarrow{\sim} \mathbf{A}(X)(Y)$.

3. Generalize the results of Exercise 20.

Exercise 22. *(Algebra of a monoid and binomial ideals)*
Let $(\Gamma, \cdot, 1_\Gamma)$ be a commutative monoid denoted multiplicatively, and $\mathbf{k}$ be a commutative ring.
The *algebra of* $(\Gamma, \cdot, 1_\Gamma)$ *over* $\mathbf{k}$, denoted by $\mathbf{k}[(\Gamma, \cdot, 1_\Gamma)]$ or simply $\mathbf{k}[\Gamma]$, is formed from the free $\mathbf{k}$-module over Γ (if Γ is not assumed to be discrete, see Exercise VIII-16). If $\mathbf{k}$ is nontrivial, we identify every element γ of Γ with its image in the free module. In case of doubt regarding $\mathbf{k}$, we should denote by $1_\mathbf{k}\gamma$ instead of γ this element of $\mathbf{k}[\Gamma]$.
The product law $\times$ of $\mathbf{k}[\Gamma]$ is obtained by letting $\gamma \cdot \gamma' = \gamma \times \gamma'$ and by extending by $\mathbf{k}$-bilinearity. Note that $1_\mathbf{A} 1_\Gamma = 1_{\mathbf{k}[\Gamma]}$. In practice, we identify $\mathbf{k}$ with a subring of $\mathbf{k}[\Gamma]$, and we identify the three 1's above.

1. Prove that the $\mathbf{k}$-algebra $\mathbf{k}[\Gamma]$, considered with the map
$$\iota_{\mathbf{k},\Gamma} : \Gamma \to \mathbf{k}[\Gamma],\ \gamma \mapsto 1_\mathbf{k}\gamma,$$
gives the solution to the universal problem summarized in the picture below.

To sum up, we say that $\mathbf{k}[\Gamma]$ *is the* $\mathbf{k}$*-algebra freely generated by the multiplicative monoid* Γ.

$$\begin{tikzcd}
\Gamma \arrow[dd, "\iota_{\mathbf{k},\Gamma}"'] \arrow[ddr, "\psi"] & & \text{commutative monoids} \\
 & & \text{monoids morphisms} \\
\mathbf{k}[\Gamma] \arrow[r, dashed, "\theta\,!"'] & \mathbf{L} & \mathbf{k}\text{-algebras}
\end{tikzcd}$$

When the law of Γ is denoted additively, we denote by X^{γ} the element of $\mathbf{k}[\Gamma]$ image of $\gamma \in \Gamma$ such that we now have the natural expression $X^{\gamma_1}X^{\gamma_2} = X^{\gamma_1+\gamma_2}$. For example, when $\Gamma = \mathbb{N}^r$ is the additive monoid freely generated by a set with r elements, we can see the elements of $\mathbb{N}^r$ as multiexponents and $\mathbf{k}[\Gamma] = \mathbf{k}[(\mathbb{N}^r, +, 0)] \simeq \mathbf{k}[X_1, \ldots, X_r]$. Here $X^{(m_1,\ldots,m_r)} = X_1^{m_1} \cdots X_r^{m_r}$.
When $\Gamma = (\mathbb{Z}^r, +, 0)$, we can again see the elements of $\mathbb{Z}^r$ as multiexponents and $\mathbf{k}[\mathbb{Z}^r] \simeq \mathbf{k}[X_1, \ldots, X_r, \frac{1}{X_1}, \ldots, \frac{1}{X_r}]$ as the Laurent polynomial ring.

Now suppose that $(\Gamma, \cdot, 1)$ is a monoid given by generators and relations. Let G be the set of the generators.
The relations are of the form $\prod_{i\in I} g_i^{k_i} = \prod_{j\in J} h_j^{\ell_j}$ for finite families

$$(g_i)_{i\in I} \text{ and } (h_j)_{j\in J} \text{ in } G, \text{ and } (k_i)_{i\in I} \text{ and } (\ell_j)_{j\in J} \text{ in } \mathbb{N}.$$

Such a relation can be encoded by the pair $\big((k_i, g_i)_{i\in I}, (\ell_j, h_j)_{j\in J}\big)$.
If we hope to control things, G and the set of relations better be enumerable and discrete. From the point of view of the computation, the central role is taken up by the finite presentations.

Notation. To visualize a finite presentation, for instance with $G = \{x, y, z\}$ and relations $xy^2 = yz^3$, $xyz = y^4$ we write in multiplicative notation

$$\boxed{\Gamma =_{\mathrm{CM}} \left\langle x, y, z \,|\, xy^2 = yz^3, xyz = y^4 \right\rangle \qquad (*)},$$

and in additive notation

$$\boxed{\Gamma =_{\mathrm{CM}} \langle x, y, z \,|\, x + 2y = y + 3z, x + y + z = 4y\rangle}.$$

The index CM is added for "commutative monoid."

2. Show that $\mathbf{k}[\Gamma] \simeq \mathbf{k}[(g)_{g\in G}]/\mathfrak{a}$, where $\mathfrak{a}$ is the ideal generated by the differences of monomials $\prod_{i\in I} {g_i}^{k_i} - \prod_{j\in J} {h_j}^{\ell_j}$ (for the relations $\prod_{i\in I} g_i^{k_i} = \prod_{j\in J} h_j^{\ell_j}$ given in the presentation of Γ). Such an ideal is called a *binomial ideal.* With the example $(*)$ above, we can therefore write

$$\boxed{\mathbf{k}[\Gamma] =_{\mathbf{k}-\mathrm{algebras}} \left\langle x, y, z \,|\, xy^2 = yz^3, xyz = y^4 \right\rangle \qquad (**)}.$$

In other words, $\Gamma =_{\mathrm{CM}} \langle \textit{thingy} \,|\, \textit{bob} \rangle$ implies $\mathbf{k}[\Gamma] =_{\mathbf{k}-\mathrm{algebras}} \langle \textit{thingy} \,|\, \textit{bob} \rangle$.

Some solutions, or sketches of solutions

Exercise 4. *1.* If c is right-invertible and left-invertible then it is the unique left-inverse because $c'a = 1$ implies $c' = c'ac = c$.
Conversely, since $ca = 1$, we have $(c + 1 - ac)a = ca + a - aca = 1$. Therefore $c + 1 - ac$ is a left-inverse, and if there is uniqueness, $1 - ac = 0$.

2. We check that $v = 1 + bua$ suits.

3. If $u(1 - xa) = 1$, then $u = 1 + uxa$, therefore it is left-invertible. Thus u is right- and left-invertible, and so is $1 - xa$.

Exercise 5. Let $x_1, \ldots, x_n \in E$ such that $(\overline{x_1}, \ldots, \overline{x_n})$ is a $\mathbf{k}$-basis of $E/\mathfrak{m}E$. By Nakayama, the x_i's generate E. Let $u : \mathbf{A}^n \twoheadrightarrow E$ be the surjection $e_i \mapsto x_i$. By scalar extension to $\mathbf{K}$, we obtain a surjection $U : \mathbf{K}^n \twoheadrightarrow \mathbf{K} \otimes_{\mathbf{A}} E$ between two vector spaces of same dimension n, thus an isomorphism.

Since $\mathbf{A}^n \hookrightarrow \mathbf{K}^n$, we deduce that u is injective. Indeed, if $y \in \mathbf{A}^n$ satisfies $u(y) = 0$, then $1 \otimes u(y) = U(y) = 0$ in $\mathbf{K} \otimes_{\mathbf{A}} E$, therefore $y = 0$, cf. the diagram on the right.

$$\begin{tikzcd}
\mathbf{A}^n \arrow[r, two heads, "u"'] \arrow[d, hook] & E \arrow[d] \\
\mathbf{K}^n \arrow[r, two heads, "U"] & \mathbf{K} \otimes_{\mathbf{A}} E
\end{tikzcd}$$

Recap: u is an isomorphism and $(x_1, \ldots, x_n)$ is an $\mathbf{A}$-basis of E.

Exercise 6. By Nakayama, $(e_1, \ldots, e_n)$ generates the $\mathbf{A}$-module E.
Let $L = \mathbf{A}^n$ and $\varphi : L \twoheadrightarrow E$ be the (surjective) linear map that transforms the canonical basis of L into $(e_1, \ldots, e_n)$. By hypothesis, $\overline{\varphi} : L/aL \to E/aE$ is an isomorphism. Let us show that $\operatorname{Ker}\varphi = a\operatorname{Ker}\varphi$. Let $x \in L$ with $\varphi(x) = 0$; we have $\overline{\varphi}(\overline{x}) = 0$, so $\overline{x} = 0$, i.e. $x \in aL$, say $x = ay$ with $y \in L$. But $0 = \varphi(x) = a\varphi(y)$ and a being E-regular, $\varphi(y) = 0$. We indeed have $\operatorname{Ker}\varphi \subseteq a\operatorname{Ker}\varphi$. Since E is finitely presented, $\operatorname{Ker}\varphi$ is finitely generated, and we can apply Nakayama to the equality $\operatorname{Ker}\varphi = a\operatorname{Ker}\varphi$. We obtain $\operatorname{Ker}\varphi = 0$: φ is an isomorphism.

Exercise 12. *1a., b., c.* The idea is to develop $\det(A + B)$ as a multilinear function of the columns of $A + B$. The result is a sum of 2^n determinants of matrices obtained by mixing columns A_j, B_k of A and B. We write

$$\det(A_1 + B_1, \ldots, A_n + B_n) = \textstyle\sum_{2^n} \det(C_1, \ldots, C_n) \quad \text{with } C_j = A_j \text{ or } B_j.$$

For $J \in \mathcal{P}_n$, let Δ_J^{col} be the determinant when $C_j = B_j$ for $j \in J$ and $C_j = A_j$ otherwise. With this notation, we therefore have

$$\det(A + B) = \textstyle\sum_J \Delta_J^{\mathrm{col}}.$$

If $\#J \geqslant n - r$, then $\Delta_J^{\mathrm{col}} \in \mathcal{D}_{n-r}(B)$; otherwise $\#\overline{J} \geqslant r + 1$ and so $\Delta_J^{\mathrm{col}} \in \mathcal{D}_{r+1}(A)$.

1d. Consider $A = \mathrm{Diag}(a_1, \ldots, a_n)$.

2. We write $\underline{x} = \underline{y}\,U$ with $U \in \mathbf{A}^{r \times n}$, $\underline{y} = \underline{x}\,V$ with $V \in \mathbf{A}^{n \times r}$.

Let $A = VU$, $B = \mathrm{I}_n - A$. We have $\boxed{\underline{x}\,B = 0}$ and $\mathrm{rk}(B) \geqslant n - r$ since $\mathrm{rk}(A) \leqslant r$.

The framed equality shows, for $I \in \mathcal{P}_{r,n}$ and ν minor of B over the rows of $\overline{I}$, the inclusion $\nu M \subseteq \langle (x_i)_{i \in I} \rangle$, and we are done because $1 \in \mathcal{D}_{n-r}(B)$.

Precisely, let Δ_J^{row} be the determinant of the "mixed" matrix whose *rows* of index $i \in J$ are the corresponding *rows* of B and the *rows* of index $i \in \overline{J}$ are those of A. For $J \supseteq \overline{I}$, Δ_J^{row} is a linear combination of minors of B over the rows of $\overline{I}$.

Thus let

$$s_I = \sum\nolimits_{J \mid J \supseteq \overline{I}} \Delta_J^{\mathrm{row}}.$$

Then on the one hand, $s_I M \subseteq \langle (x_i)_{i \in I} \rangle$, and on the other, since $\mathrm{rk}(B) \geqslant n-r$,

$$1 = \sum\nolimits_{I \in \mathcal{P}_{r,n}} s_I.$$

3. Clear by using the successive localizations lemma (Fact V-7.2).

4. If a matrix $A \in \mathbb{M}_n(\mathbf{A})$ exists as indicated, the proof of item *2* applies with $B = \mathrm{I}_n - A$.

The converse is problematic because the constraint $\mathrm{rk}(A) \leqslant r$ is not linear in the coefficients of A. However, we succeed in reaching it for $r = 1$ by other means, (see Theorem V-7.3).

Exercise 13. *1.* The condition $b'(1-a'b') = 0$ is obtained by $\varphi\big(b(1-ab)\big) = 0$. Suppose that φ is a decomposable ring morphism and let us show that $\varphi(\mathrm{Rad}\,\mathbf{A}) \subseteq \mathrm{Rad}\,\mathbf{B}$: let $a \in \mathrm{Rad}\,\mathbf{A}$, then $b = 0$ (by uniqueness of b), thus $b' = 0$ and $a' = a'(1-a'b') \in \mathrm{Rad}\,\mathbf{B}$.

Conversely, suppose $\varphi(\mathrm{Rad}\,\mathbf{A}) \subseteq \mathrm{Rad}\,\mathbf{B}$. If a, $b \in \mathbf{A}$ satisfy $b(1-ab) = 0$ and $a(1-ab) \in \mathrm{Rad}\,\mathbf{A}$, then $\varphi\big(a(1-ab)\big) = a'(1-a'b') \in \mathrm{Rad}\,\mathbf{B}$.

Exercise 15. *1.* It is sufficient and necessary that the a_i's satisfy the equality $(\star_d)$ for the monomials of total degree $\leqslant d$. Let $M = M(\underline{X}) = \underline{X}^\alpha$ be such a monomial with $|\alpha| = j \leqslant d$. Since $M(s^r \underline{X}) = s^{rj} M$, we want to reach

$$s^e s^{-j}\, M = a_0(s)\, M + a_1(s) s^j\, \underline{X} + \cdots + a_d(s) s^{dj}\, M,$$

i.e. after simplification by M and multiplication by s^j

$$s^e = a_0(s) s^j + a_1(s) s^{2j} + \cdots + a_d(s) s^{(d+1)j} = \sum\nolimits_{i=0}^{d} a_i(s) (s^j)^{i+1}.$$

Let us introduce the polynomial $F(T) \in \mathbb{Z}[s][T]$ defined by $F(T) = T\, \sum_{i=0}^{d} a_i(s) T^i$. Then $\deg_T F \leqslant d+1$ and F performs the interpolation $F(0) = 0$ and $F(s^j) = s^e$ for $j \in [\![1..d]\!]$. However, a polynomial $F \in \mathbb{Z}[s][T]$ which satisfies this interpolation is the following

$$(\#_d) \qquad F(T) = s^e - (s^0 - T)(s^1 - T)(s^2 - T) \cdots (s^d - T).$$

Full astern. Consider the polynomial defined by the equality $(\#_d)$. It is of degree $d+1$ in T, null in $T = 0$, therefore it is of the form

$$F(T) = T\, \sum\nolimits_{i=0}^{d} a_i(s) T^i, \quad \text{with } a_0(s), \ldots, a_d(s) \in \mathbb{Z}[s].$$

These polynomials $a_i(s)$ have the desired property.

2. The required membership is deduced from the equality $(\star_d)$ by evaluating $\underline{X}$ at $\underline{x}$.

3. Suppose that P is of total degree $\leqslant d$. The fact that $P(\underline{x}/s) \in (\mathbf{A}_S)^\times$ means, in $\mathbf{A}$, that $y = s^e P(\underline{x}/s)$ divides an element t of S. By item *2*, y is in the ideal generated by the values of P; the same goes for t.

Exercise 16. *1.* Let $b \in \mathbf{A}$ invertible modulo $\mathfrak{a}$. There exists an $a \in \mathfrak{a}$ such that $1 \in \langle b, a \rangle$. The polynomial $aT + b$ takes the comaximal values a, $a+b$, thus it represents an inverse $b' = at + b$. Then, $b' \equiv b \bmod \mathfrak{a}$ with b' invertible.

2. We write $x = ay$, $y = bx$, so $(1-ab)x = 0$.

Since b is invertible modulo $1-ab$, there exists a $u \in \mathbf{A}^\times$ such that $u \equiv b \bmod 1-ab$. Then $ux = bx = y$.

Exercise 18.
For two orthogonal idempotents e, e', we have $\langle ex, e'x'\rangle = \langle ex + e'x'\rangle$.
Therefore for $(e_1, \dots, e_k)$, we have $\langle e_1x_1 + \cdots + e_kx_k\rangle = \langle e_1x_1, \dots, e_kx_k\rangle$.
Thus, $e_1x_1 + \cdots + e_kx_k$ is invertible if and only if e_1x_1, …, e_kx_k are comaximal.
Consequently, in the context of *1a*, let $y_i \in \langle x_i\rangle$ with comaximal $(y_1, \dots, y_k)$ (a fortiori $(x_1, \dots, x_k)$ is comaximal); if idempotents $(e_1, \dots, e_k)$ work for $(y_1, \dots, y_k)$, they also work for $(x_1, \dots, x_k)$. Even if x_i is replaced by u_ix_i. We will therefore be able to assume $\sum x_i = 1$.
For two idempotents e, e', we have $e \perp e'$ if and only if $1 - e$, $1 - e'$ are comaximal.

1. *c* ⇒ *d.* By taking $x_1 = x$, $x_2 = 1+x$, $e = e_2 = 1-e_1$, we have $e_1x_1+e_2x_2 = x+e$.
d ⇒ *c.* We can assume $1 = -x_1 + x_2$; we let $x = x_1$.
Then, $e + x = (1 - e)x + e(1 + x) = (1 - e)x_1 + ex_2$.
a ⇔ *b.* Easily obtained by letting $\mathbf{B}_i = \mathbf{B}/\langle 1 - e_i\rangle$.
c ⇒ *a* (or *d* ⇒ *a*). By induction on k. We can assume $1 = \sum_i x_i$: there exists some idempotent e_1 such that $e_1x_1 + (1 - e_1)(1 - x_1)$ is invertible. We have $1 \in \langle x_2, \dots, x_k\rangle$ in the quotient $\mathbf{B}/\langle e_1\rangle$ that also possesses the property d; therefore, by induction, there exists $(e_2, \dots, e_k)$ in $\mathbf{B}$ forming a fundamental system of orthogonal idempotents in the quotient $\mathbf{B}/\langle e_1\rangle$ with $e_2x_2 + \cdots + e_kx_k$ invertible in $\mathbf{B}/\langle e_1\rangle$. Then, $(e_1, (1-e_1)e_2, \dots, (1-e_1)e_k)$ is a fundamental system of orthogonal idempotents of $\mathbf{B}$ and $e_1x_1 + (1 - e_1)e_2x_2 + \cdots + (1 - e_1)e_kx_k$ is invertible in $\mathbf{B}$.

2. Easy.

3. Let $x \in \mathbf{B}$; there exists some idempotent $e \in \mathbf{B}_{\rm red}$ such that $e + \overline{x}$ is invertible in $\mathbf{B}_{\rm red}$. We lift e at some idempotent $e' \in \mathbf{B}$. Then, $e' + x$ lifts $e + \overline{x}$ so is invertible. Let $\mathbf{B}$ be a zero-dimensional ring; even if we need to replace $\mathbf{B}$ by $\mathbf{B}_{\rm red}$, we can assume that $\mathbf{B}$ is reduced; if $x \in \mathbf{B}$, there exists some idempotent e such that $\langle x\rangle = \langle 1 - e\rangle$; then $e + x$ is invertible.

4. Let $a \in \mathbf{B}$ be an idempotent element in $\mathbf{B}/\mathrm{Rad}\,\mathbf{B}$ and $b = 1 - a$.
Since $\langle a, b\rangle = 1$, there exist two orthogonal idempotents e and f in $\mathbf{B}$ such that $ae + bf$ is invertible. Since $\langle e, f\rangle = 1$, we have $f = 1 - e$. Now, we reason in the quotient. The system (ae, bf, af, be) is a fundamental system of orthogonal idempotents. As $ae + bf$ is invertible, we have $ae + bf = 1$, hence $af = be = 0$. Finally, (in the quotient) $a = e$ and $b = f$.

Exercise 19. A ring $\mathbf{A}$ is local if and only if $\mathbf{A}/\mathrm{Rad}\,\mathbf{A}$ is local; a ring $\mathbf{A}$ is semi-local if and only if $\mathbf{A}/\mathrm{Rad}\,\mathbf{A}$ is semi-local.

1. A local ring satisfies item *1d* of the previous exercise with $e = 0$ or $e = 1$.

2. $\mathbf{A}/\mathrm{Rad}\,\mathbf{A}$ is connected, semi-local thus local (use item *1d* of the previous exercise knowing that $e = 0$ or 1); so $\mathbf{A}$ is local.

4. Is proven for the residual ring and results from the following observation.
If f is a polynomial in n indeterminates and $(e_1, \dots, e_k)$ is a fundamental system of orthogonal idempotents, then for $(x_1, \dots, x_k)$ in $\mathbf{A}^n$, since the evaluation homomorphism commutes with the direct products, we have the equality

$$f(e_1x_1 + \cdots + e_kx_k) = e_1f(x_1) + \cdots + e_kf(x_k).$$

6. A ring $\mathbf{A}$ has a finite number of maximal ideals if and only if it is the case for $\mathbf{A}/\mathrm{Rad}\,\mathbf{A}$. In classical mathematics, $\mathbf{A}/\mathrm{Rad}\,\mathbf{A}$ is a finite product of fields.

Exercise 20.
In the following $f = \sum_i b_i X^i \in \mathbf{A}[X]$ and $g = \sum_i c_i X^i \in U$, with $1 = \sum_i c_i u_i$.

0. Let $\underline{T}$ be a set of indeterminates over $\mathbf{A}$ and $\mathbf{A}(\underline{T})$ be the Nagata ring. We know that $\mathbf{A}(\underline{T})$ is flat over $\mathbf{A}$ and we show that every system of linear equations over $\mathbf{A}$ that admits a solution over $\mathbf{A}(\underline{T})$ admits a solution over $\mathbf{A}$. Thus let the system of linear equations $Ax = b$ with $A \in \mathbf{A}^{n\times m}$ and $b \in \mathbf{A}^n$. Suppose the existence of a solution over $\mathbf{A}(\underline{T})$; it is of the form P/D with $P \in \mathbf{A}[\underline{T}]^m$ and $D \in \mathbf{A}[\underline{T}]$ being a primitive polynomial. We therefore have $A\,P = D\,b$ over $\mathbf{A}[\underline{T}]$.
Let us write $P = \sum_\alpha x_\alpha \underline{T}^\alpha$ with $x_\alpha \in \mathbf{A}^m$ and $D = \sum_\alpha a_\alpha \underline{T}^\alpha$ where the $a_\alpha \in \mathbf{A}$ are comaximal. The equality $A\,P = D\,b$ gives $A\,x_\alpha = a_\alpha b$ for each α.
If $\sum u_\alpha a_\alpha = 1$, the vector $x = \sum_\alpha u_\alpha x_\alpha$ is a solution of the system $Ax = b$.

1. Let $a \in \mathbf{A}$ be invertible in $\mathbf{B}$. There exist f, g such that $af = g$, so a and f are primitive: $a \in \mathbf{A}^\times$.

2. Let us show $\mathrm{Rad}\,\mathbf{A} \subseteq \mathrm{Rad}\,\mathbf{B}$. Let $a \in \mathrm{Rad}\,\mathbf{A}$, we want to show that $1 + a(f/g)$ is invertible in $\mathbf{B}$, i.e. $g + af \in U$. We want $1 \in \langle (c_i + ab_i)_i \rangle$; but this ideal contains $\sum_i u_i(c_i + ab_i) = 1 + az \in \mathbf{A}^\times$.
We therefore know that $\mathrm{Rad}\,\mathbf{B} \supseteq U^{-1}(\mathrm{Rad}\,\mathbf{A})[X]$. Let $h = \sum_{i=0}^n a_i X^i$. Let us show that $h \in \mathrm{Rad}\,\mathbf{B}$ implies $a_n \in \mathrm{Rad}\,\mathbf{A}$.
We will deduce by induction that $h \in (\mathrm{Rad}\,\mathbf{A})[X]$.
Consider $a \in \mathbf{A}$, take $f = a$ and $g = X^n - a(h - a_n X^n)$. Clearly $g \in U$, so $g + fh = (1 + aa_n)X^n$ must be invertible in $\mathbf{B}$, i.e. $1 + aa_n$ must be in $\mathbf{A}^\times$.

Exercise 22. *(Algebra of a monoid and binomial ideals)*
1. First of all we prove that $\mathbf{k}[\Gamma]$ is indeed a $\mathbf{k}$-algebra and that $\iota_{\mathbf{k},\Gamma}$ is a monoid morphism. Then, if $\alpha : \Gamma \to \mathbf{A}$ is a monoid morphism, there is a priori a unique way to extend it to a morphism $\widetilde{\alpha}$ of $\mathbf{k}$-algebras from $\mathbf{k}[\Gamma]$ to $\mathbf{A}$: let $\widetilde{\alpha}\big(\sum_{\gamma\in I} a_\gamma \gamma\big) = \sum_{\gamma\in I} a_\gamma \alpha(\gamma)$ (here, I is a finitely enumerated subset of Γ).
We then prove that $\widetilde{\alpha}$ is indeed a morphism of $\mathbf{k}$-algebras. The readers are invited to prove all the details when Γ is not assumed to be discrete, by basing themselves on Exercise VIII-16.

2. This is a general result of universal algebra, because here we are in the framework of purely equational algebraic structures. To obtain a $\mathbf{k}$-algebra by means of generators and relations given by equalities of monomials, we can first construct the similarly defined monoid, then the algebra freely generated by this monoid.
If we do not want to invoke such a general result, we can simply observe that the computation procedures in $\mathbf{k}[\Gamma]$ with $\Gamma =_{\mathrm{CM}} \langle \textit{thingy} \,|\, \textit{bob} \rangle$ are identical to those in $\mathbf{A} =_{\mathbf{k}-\text{algebras}} \langle \textit{thingy} \,|\, \textit{bob} \rangle$.

Bibliographic comments

The reader will certainly find our will to give to the trivial ring every property under the sun a little arbitrary, especially through our use of a weakened version of negation (cf. footnote 1 page 488). We hope to convince them of the practical use of such a convention by way of the examples. On the proper use of the trivial ring, see [165, Richman].

The "proof by Azumaya" of the local freeness lemma 2.2 is extracted from the proof of the Azumaya theorem III.6.2 in [MRR], in the case that concerns us here. In other words, we have given the "matrix" content of the proof of the local freeness lemma in [MRR].

Monomial curves (example on page 509) are treated in [Kunz], Chapter V, Example 3.13.f.

Decomposed rings play an important role in the classical theory of Henselian local rings for example in the works [Raynaud] or [Lafon & Marot].

A local-global ring is sometimes called a "ring with many units" in the literature. Local-global rings have been particularly studied in [83, Estes & Guralnick]. Other "rings with many units" have appeared long beforehand, under the terminology "unit-irreducible rings" (see for example [117]). Those are the rings $\mathbf{A}$ for which the following property is satisfied: if two polynomials of $\mathbf{A}[X]$ represent an inverse, then their product also represents an inverse. Also introduced were the "primitive" or "strongly U-irreducible" rings which are the rings for which the following property is satisfied: every primitive polynomial represents an inverse. They are special local-global rings. In the proof of Fact 6.7 we have shown that a Nagata ring is always "primitive."

Concerning the Nagata ring $\mathbf{A}(X)$, given Fact 6.7 and the good properties of local-global rings, it is not surprising that this ring plays a crucial role for the uniform solution of systems of linear equations with parameters over a discrete field and more generally for the uniform computations "in a reasonable amount of time" over arbitrary commutative rings (see [60, 61, Díaz-Toca&al.]).

Chapter X

Finitely generated projective modules, 2

Contents

Introduction

Here we continue the study of finitely generated projective modules started in Chapter V.

In Section 1 we readdress the question regarding the characterization of finitely generated projective modules as locally free modules, i.e. regarding the local structure theorem.

Section 2 is dedicated to the ring of ranks over $\mathbf{A}$. In the usual theory in classical mathematics the rank of a finitely generated projective module is defined as a locally constant function over the Zariski spectrum. Here we give an elementary theory of the rank which does not require prime ideals.

In Section 3 we give some simple applications of the local structure theorem.

Section 4 is an introduction to Grassmannians.

In Section 5 we introduce the general problem of completely classifying finitely generated projective modules over a fixed ring $\mathbf{A}$. This classification is a fundamental and difficult problem, which does not admit a general algorithmic solution.

Section 6 presents a nontrivial example for which this classification can be obtained.

1. The finitely generated projective modules are locally free

We continue the theory of finitely generated projective modules after Section V-8. We ask however that the reader forgets what was learnt in Section V-6: the characterization by the Fitting ideals, the local structure theorem V-6.1 and the considerations regarding the rank linked to Fitting ideals as well as Theorem V-8.14 whose proof depends on the local structure theorem.

Actually, all of the results of Sections V-8 and 1 could be obtained by localization arguments at comaximal elements since we have already obtained the local structure theorem for finitely generated projective modules (Theorems II-5.26 and V-6.1) by exterior algebra methods.

We nevertheless think that the "more global" point of view developed in this chapter is itself interesting, and, in a way, simpler, as highlighted by the elementary proof of the matrix theorem 1.7 which summarizes (and specifies) all the previous structure theorems. There also the exterior algebra is an indispensable tool, but it seems better used, in a less invasive way.

Complements on exterior powers of a finitely generated projective module

The following lemma is immediate.

1.1. Lemma. *Let P be a free $\mathbf{A}$-module of rank h and $\varphi \in \mathrm{End}(P)$ be a diagonalizable endomorphism, with a matrix similar to $\mathrm{Diag}(\lambda_1, \ldots, \lambda_h)$, then for the fundamental polynomial of φ we get*

$$\mathrm{F}_\varphi(X) \overset{\mathrm{def}}{=} \det(\mathrm{Id}_{P[X]} + X\varphi) = (1 + \lambda_1 X) \cdots (1 + \lambda_h X).$$

We now establish the crucial result.

1.2. Proposition. (Exterior powers)
Let P be a finitely generated projective module.

1. *The k^{th} exterior power of P, denoted by $\bigwedge^k P$, is also a finitely generated projective module. If $P = \mathrm{Im}(F)$ for $F \in \mathbb{AG}(\mathbf{A})$, the module $\bigwedge^k P$ is (isomorphic to) the image of the projection matrix $\bigwedge^k F$.*
2. *If φ is an endomorphism of P, the fundamental polynomial $\mathrm{F}_{\bigwedge^k \varphi}(X)$ only depends on k and on the polynomial $\mathrm{F}_\varphi(X)$. In particular, the rank polynomial of $\bigwedge^k P$ only depends on k and on the rank polynomial of P.*
3. *a. If P is of constant rank $h < k$, the module $\bigwedge^k P$ is null.*

   b. If P is of constant rank $h \geqslant k$, the module $\bigwedge^k P$ is of constant rank $\binom{h}{k}$.

c. In this case, if φ is an endomorphism whose fundamental polynomial is $\mathrm{F}_\varphi = (1+\lambda_1 X)\,\cdots\,(1+\lambda_h X)$, we have

$$\mathrm{F}_{\bigwedge^k\varphi}(X) = \prod_{1\leqslant i_1<\cdots<i_k\leqslant h}(1+\lambda_{i_1}\cdots\lambda_{i_k}X).$$

4. If a projection matrix F has as its image a projective module of constant rank k, then $\mathcal{D}_{k+1}(F)=0$.

D *1.* Let M and N be two $\mathbf{A}$-modules and consider the first exterior powers of their direct sum $M\oplus N$. By examining the universal problem that the k^{th} exterior power of a module solves, we obtain the canonical isomorphisms

$$\begin{aligned}
&\textstyle\bigwedge^2(M\oplus N) \simeq \bigwedge^2 M\oplus(M\otimes N)\oplus\bigwedge^2 N\\
&\textstyle\bigwedge^3(M\oplus N) \simeq \bigwedge^3 M\oplus\big((\bigwedge^2 M)\otimes N\big)\oplus\big(M\otimes(\bigwedge^2 N)\big)\oplus\bigwedge^3 N,
\end{aligned}$$

and more generally

$$\textstyle\bigwedge^m(M\oplus N) \;\simeq\; \bigoplus_{k=0}^m\big((\bigwedge^k M)\otimes(\bigwedge^{m-k}N)\big) \tag{1}$$

(with $\bigwedge^0 M=\mathbf{A}$ and $\bigwedge^1 M = M$). In particular, if $P\oplus Q\simeq\mathbf{A}^m$, $\bigwedge^k P$ is a direct summand in $\bigwedge^k\mathbf{A}^m\simeq\mathbf{A}^{\binom{m}{k}}$. We also see that if $P=\mathrm{Im}(F)$ for some projection matrix F, $\bigwedge^k P$ is (isomorphic to) the image of the projection matrix $\bigwedge^k F$, because this matrix represents the identity over $\bigwedge^k P$ and 0 over all the other summands of the direct sum.

2. We can assume $P=\mathrm{Im}(F)$, where $F\in\mathbb{AG}_n(\mathbf{A})$, and $n\geqslant k$.
We therefore have $P\oplus Q=\mathbf{A}^n$ with $Q=\mathrm{Ker}(F)$. The endomorphism φ extends into an endomorphism $\varphi_1:\mathbf{A}^n\to\mathbf{A}^n$, null over Q, with matrix H satisfying $FHF=H$, and we have $\mathrm{F}_\varphi(X)=\mathrm{F}_{\varphi_1}(X)=\det(\mathrm{I}_n+XH)$. Then, we see that $\bigwedge^k\varphi_1$ is an extension of $\bigwedge^k\varphi$, null over the terms distinct from $\bigwedge^k P$ in the direct sum explicated in the proof of item *1.* The matrix of $\bigwedge^k\varphi_1$ is none other than $\bigwedge^k H$.
We therefore want to show that $\det\big(\mathrm{I}_{\binom{n}{k}}+X\ \bigwedge^k H\big)$ only depends on k and on $\det(\mathrm{I}_n+XH)$. We are therefore brought back to the case of a free module, and this case has been treated in Proposition III-5.6.

3. This item results from the previous one, since the "projective of rank k" case can be deducted from the "free of rank k" case. Note that items *3a* and *3b* both say that when P is of constant rank h, $\bigwedge^k P$ is of constant rank $\binom{h}{k}$ (which is equal to 0 if $h<k$). We have only separated them in order to give the result in a more visible form.

4. This is equivalent to the fact that $\bigwedge^{k+1}P$ is null, which is item *3a.* □

Remarks. (Consequences of Proposition 1.2.)

1) Let $\mathrm{R}_P(X)=r_0+r_1X+\cdots+r_nX^n$. Each r_hP is a projective module of constant rank h over $A[1/r_h]$, which gives, as a consequence of item *3*,

for $k > 0$,

$$\mathrm{R}_{\bigwedge^k (r_h P)}(X) = X^{\binom{h}{k}} \text{ over } \mathbf{A}[1/r_h].$$

By writing $P = \bigoplus_h r_h P$ and $\mathbf{A} = \prod_h \mathbf{A}[1/r_h]$ we obtain

$$\begin{aligned}\mathrm{R}_{\bigwedge^k P}(X) &= r_0 + \cdots + r_{k-1} + r_k X + \cdots + r_{k+j} X^{\binom{k+j}{k}} + \cdots + r_n X^{\binom{n}{k}} \\ &= \textstyle\sum_{h=0}^{n} r_h X^{\binom{h}{k}}.\end{aligned}$$

We also have by convention $\bigwedge^0 P = \mathbf{A}$ and thus also $\mathrm{R}_{\bigwedge^0 P}(X) = X$ (so that the previous formula applies it must be agreed that $\binom{n}{0} = 1$ for all $n \geqslant 0$).
2) If we let $\bigwedge P$ be the exterior algebra of P, the reader will show by an analogous computation that

$$\mathrm{R}_{\bigwedge P}(X) = r_0 X + r_1 X^2 + \cdots + r_k X^{2^k} + \cdots + r_n X^{2^n}.$$

3) We can compute $\mathrm{F}_{\bigwedge^k (\varphi)}$ from F_φ as follows.
Since $\mathrm{F}_\varphi(0) = 1$ and $\deg(\mathrm{F}_\varphi) \leqslant n$, if ψ is the endomorphism of $\mathbf{A}^n$ having as its matrix the companion matrix C of $X^n\,\mathrm{F}_\varphi(-1/X)$, we obtain $\mathrm{F}_\varphi = \mathrm{F}_\psi$.
Therefore

$$\mathrm{F}_{\bigwedge^k \varphi} = \mathrm{F}_{\bigwedge^k \psi} = \det\left(\mathrm{I}_{\binom{n}{k}} + X \bigwedge^k C\right) \qquad \blacksquare$$

From the previous remarks we deduce the following proposition.

1.3. Proposition. *Let P be a finitely generated projective module, and $k \leqslant h$ be two integers > 0. The following properties are equivalent.*

1. *The module P is of constant rank h.*
2. *The module $\bigwedge P$ is of constant rank 2^h.*
3. *The module $\bigwedge^k P$ is of constant rank $\binom{h}{k}$.*

With $h = 0$, the properties 1 and 2 are equivalent.

Case of the modules of constant rank

1.4. Theorem. *Let P be a projective $\mathbf{A}$-module of constant rank h with n generators, (isomorphic to the) image of a projector $F \in \mathbb{AG}_n(\mathbf{A})$. Then the $\binom{n}{h}$ principal minors (s_i) of order h of F satisfy*

- *$\sum_i s_i = 1$, and*
- *each $\mathbf{A}_{s_i}$-module P_{s_i} is free of rank h, the matrix F seen as a matrix with coefficients in $\mathbf{A}_{s_i}$ is similar to the standard projection matrix $\mathrm{I}_{h,n}$.*

D The sum of the principal minors s_i of order h of F is equal to 1 since $\det(\mathrm{I}_n + XF) = (1 + X)^h$.
Moreover, since every minor of order $h + 1$ is null (Proposition 1.2), we can apply the freeness lemma II-5.10 to each localized module P_{s_i}, which is

isomorphic to the image of the matrix F seen as a matrix with coefficients in P_{s_i} (by Proposition V-5.1). □

Remark. In the previous theorem, it is possible that s_i is nilpotent for certain values of i, therefore that $\mathbf{A}_{s_i}$ is trivial. The fact of not excluding these zero localizations is inevitable when we do not dispose of a test to know whether an element of $\mathbf{A}$ is nilpotent or not. This justifies the natural convention given in the remark on page 276. ■

General case

1.5. Theorem. *Let P be a finitely generated projective $\mathbf{A}$-module with n generators. Then for each idempotent $\mathrm{e}_h(P)$ there exist $\binom{n}{h}$ elements $(s_{h,i})$ of $\mathbf{A}$ with the following properties*

- $\sum_i s_{h,i} = \mathrm{e}_h(P)$,
- *each $\mathbf{A}_{s_{h,i}}$-module $P_{s_{h,i}}$ is free of rank h.*

In particular, for every finitely generated projective module with n generators, there exist 2^n comaximal elements v_ℓ such that each P_{v_ℓ} is free.

D We first localize by inverting $\mathrm{e}_h(P)$ to be reduced to Theorem 1.4. We then localize a little more in accordance with the latter theorem. Fact V-7.2 regarding the successive localizations applies. □

The following theorem summarizes Theorems 1.4 and 1.5, and the converse given by the local-global principle V-2.4.

1.6. Theorem. *An $\mathbf{A}$-module P is finitely generated projective if and only if there exist comaximal elements $s_1, \dots, s_\ell$ such that each P_{s_i} is free over $\mathbf{A}_{s_i}$. It is projective of rank k if and only if there exist comaximal elements $s_1, \dots, s_\ell$ such that each P_{s_i} is free of rank k over $\mathbf{A}_{s_i}$.*

A practical form of Theorem 1.5 is its matrix form.

1.7. Theorem. (Explicit matrix form of Theorems V-1.1 and V-1.3)
Let $\mathbf{A}$ be a ring, $F \in \mathbb{M}_n(\mathbf{A})$ with $F^2 = F$ and P be the finitely generated projective module image of F in $\mathbf{A}^n$. We define the elements r_h of $\mathbf{A}$ for $h \in [\![0..n]\!]$ by the equalities

$$\mathrm{R}_P(1+X) := \det(\mathrm{I}_n + XF), \quad \mathrm{R}_P(X) =: r_0 + r_1X + \cdots + r_nX^n.$$

We have the following results.

1. *The family $(r_h)_{h=0,\dots,n}$ is a fundamental system of orthogonal idempotents of $\mathbf{A}$.*
2. *For $h \in [\![0..n-1]\!]$ and for any minor u of order $h+1$ of F, we have $r_hu = 0$.*
3. *If the $t_{h,i}$'s are principal minors of order h of F, by letting $s_{h,i} = r_ht_{h,i}$ we obtain the following,*

- *the sum (for fixed h) of the $s_{h,i}$'s is equal to r_h,*
- *each $\mathbf{A}_{s_{h,i}}$-module $P_{s_{h,i}}$ is free of rank h,*
- *the matrix F is similar to the matrix $\mathrm{I}_{h,n}$, over $\mathbf{A}_{s_{h,i}}$*
- *the $s_{h,i}$'s are comaximal, precisely $\sum_{h,i} s_{h,i} = 1$.*

Remark. Theorem 1.7 summarizes Theorems V-8.13, 1.4 and 1.5 which have preceded it. It is even slightly more precise. Thus it is not uninteresting to provide a purely matrix proof of it that concentrates all of the previous proofs together, especially since it is particularly elementary.

Matrix proof of the matrix theorem.
1. This results from $\mathrm{R}_P(1) = 1$ (obvious) and $\mathrm{R}_P(XY) = \mathrm{R}_P(X)\,\mathrm{R}_P(Y)$ which becomes apparent as follows

$$\begin{array}{rcl} \mathrm{R}_P(1+X)\,\mathrm{R}_P(1+Y) & = & \det(\mathrm{I}_n + XF)\det(\mathrm{I}_n + YF) \quad = \\ \det\big((\mathrm{I}_n + XF)(\mathrm{I}_n + YF)\big) & = & \det(\mathrm{I}_n + (X+Y)F + XYF^2) = \\ \det(\mathrm{I}_n + (X+Y+XY)F) & = & \mathrm{R}_P\big((1+X)(1+Y)\big). \end{array}$$

2. The matrix r_hF has as its fundamental polynomial $\det(\mathrm{I}_n + r_hXF)$. In the ring $\mathbf{A}_{r_h}$, we have $1 = r_h$ and

$$\det(\mathrm{I}_n + r_hXF) = \det(\mathrm{I}_n + XF) = \mathrm{R}_P(1+X) = (1+X)^h.$$

Within the ring $\mathbf{A}_{r_h}$ we are therefore reduced to proving item *2* for the case where $r_h = 1$ and $\det(\mathrm{I}_n + XF) = (1+X)^h$, which we assume from now on. We must show that the minors of order $h+1$ of F are all null. The minors of order $h+1$ are the coefficients of the matrix $\bigwedge^{h+1} F = G$. Since $F^2 = F$, we also have $G^2 = G$. Moreover, for any square matrix H, the characteristic polynomial of $\bigwedge^k H$ only depends on k and on the characteristic polynomial of H (Proposition III-5.6). By applying this to compute the characteristic polynomial of G, we can replace F with the matrix $\mathrm{I}_{h,n}$ which has the same characteristic polynomial as F. Since the matrix $\bigwedge^{h+1} \mathrm{I}_{h,n}$ is null, its characteristic polynomial is $X^{\binom{h+1}{n}}$, so, by Cayley-Hamilton, the matrix G is nilpotent, and since it is idempotent, it is null.

3. Results from *1*, *2* and from the freeness lemma II-5.10. □

Modules of constant rank: some precisions

The following two results are now easy and we leave their proof as an exercise.

1.8. Proposition. (Projective modules of constant rank)
For some $\mathbf{A}$-module P the following properties are equivalent.

1. *P is projective of constant rank h.*
2. *There exist comaximal elements s_i of $\mathbf{A}$ such that each P_{s_i} is free of rank h over $\mathbf{A}_{s_i}$.*

3. *P is finitely generated projective and for every element s of $\mathbf{A}$, if P_s is free over $\mathbf{A}_s$, it is of rank h.*

4. *P is finitely presented, $\mathcal{F}_h(P) = \langle 1 \rangle$ and $\mathcal{F}_{h-1}(P) = 0$.*

5. *P is isomorphic to the image of a projection matrix of rank h.*

In addition, if P is generated by n elements, the number of comaximal elements in item *2* is bounded above by $\binom{n}{h}$.

1.9. Proposition. (Localized modules of constant rank and uniqueness of the fundamental system of orthogonal idempotents)
Let P be a finitely generated projective $\mathbf{A}$-module. Let $r_h = \mathrm{e}_h(P)$. Let s be an element of $\mathbf{A}$.

1. *The localized module P_s is projective of rank h if and only if $r_h/1 = 1$ in $\mathbf{A}_s$, i.e. if $r_h s^m = s^m$ in $\mathbf{A}$ for some exponent m.*

2. *If s is an idempotent, that means that r_h divides s, or yet again that $1 - r_h$ and s are two orthogonal idempotents.*

3. *Finally, if $(s_0, \ldots, s_n)$ is a fundamental system of orthogonal idempotents such that each P_{s_h} is of rank h over $\mathbf{A}_{s_h}$, then $r_h = s_h$ for each $h \in [\![0..n]\!]$.*

In the following proposition we make the link between our definition and the usual definition (in classical mathematics) of a projective module of rank k. The proof of this equivalence is however not constructive (nor can it be).

1.10. Proposition. *Let k be a non-negative integer, P be a finitely generated projective module over a nontrivial ring $\mathbf{A}$ and $\mathfrak{a}$ be an ideal contained in $\operatorname{Rad}\mathbf{A}$. Then the following properties are equivalent.*

1. *P is of rank k, i.e. $\mathrm{R}_P(X) = X^k$*

*2.** *For all maximal ideal $\mathfrak{m}$ of $\mathbf{A}$, the vector space obtained from P by extending the scalars to the residual field $\mathbf{A}/\mathfrak{m}$ has dimension k.*

3. *$\mathrm{R}_P(X) \equiv X^k$ modulo $\mathfrak{a}[X]$.*

D From a classical point of view, the implication *2* ⇒ *3* is immediate; it suffices to recall that the intersection of the maximal ideals is the Jacobson radical of $\mathbf{A}$. Note that from a constructive point of view, condition *2* is a priori too weak, for lack of maximal ideals.
Moreover, *1* trivially implies *2* and *3*.
Conversely, if $\mathrm{R}_P(X) = X^k$ modulo $\mathfrak{a}[X]$, since the idempotents are always isolated (Lemma IX-5.1), the equality takes place in $\mathbf{A}[X]$. □

1.11. Theorem. (Modules of constant rank k as submodules of $\mathbf{A}^k$)
Suppose that over $\operatorname{Frac}\mathbf{A}$ *every projective module of constant rank k is free. Then every projective* $\mathbf{A}$*-module of constant rank k is isomorphic to a submodule of* $\mathbf{A}^k$*.*

D By the enlargement lemma V-2.10, we can assume that the module is an image of a projector $F \in \mathbb{AG}_n(\mathbf{A})$ of rank k and that there exists a matrix P in $\mathbb{GL}_n(\operatorname{Frac}\mathbf{A})$ such that $PFP^{-1} = \mathrm{I}_{k,n}$. We have $P = Q/a$ with $Q \in \mathbb{M}_n(\mathbf{A})$ and $a \in \operatorname{Reg}\mathbf{A}$; thus $\det Q = a^n \det P$ is also regular in $\mathbf{A}$. We define a matrix Q_1 as

$$Q \cdot F = \mathrm{I}_{k,n} \cdot Q = \begin{array}{|c|c|}\hline \mathrm{I}_k & 0 \\ \hline 0 & 0 \\ \hline \end{array} \cdot Q = \begin{array}{|c|}\hline Q_1 \\ \hline 0 \\ \hline \end{array}.$$

However, the image of $Q \cdot F$ is isomorphic to the image of F because Q is injective, and the image of $\mathrm{I}_{k,n} \cdot Q$ is clearly isomorphic to the image of $Q_1 = Q_{1..k,1..n}$. □

Remark. 1) The previous theorem applies to the pp-rings and more generally to every ring $\mathbf{A}$ such that $\operatorname{Frac}\mathbf{A}$ is zero-dimensional, or even simply local-global. This is the case, for example, for reduced strongly discrete coherent Noetherian rings (see Problem XIII-1). In classical mathematics one proves that for every Noetherian ring $\mathbf{A}$, $\operatorname{Frac}\mathbf{A}$ is residually zero-dimensional, so we can apply the theorem to it. We do not know of a constructive analogue of this theorem.
2) For further details regarding the $k = 1$ case see Theorem 5.8.

Generic case

What do we call the generic case, regarding a projective module with n generators? We consider the ring

$$\mathbf{G}_n = \mathbb{Z}[(f_{i,j})_{i,j\in[\![1..n]\!]}]/\mathcal{G}_n,$$

where the $f_{i,j}$'s are indeterminates, F is the matrix $(f_{i,j})_{i,j\in[\![1..n]\!]}$ and $\mathcal{G}_n$ is the ideal defined by the n^2 relations obtained when writing $F^2 = F$. With coefficients in this ring $\mathbf{G}_n$, we have the matrix F whose image in $\mathbf{G}_n^n$ is what deserves to be called *the generic projective module with n generators.*

Let us reuse the notations of Theorem 1.7 in this particular case.
Saying that $r_h r_k = 0$ in $\mathbf{G}_n$ (for $0 \leqslant h \neq k \leqslant n$) signifies that we have a membership

$$r_h(F)r_k(F) \in \mathcal{G}_n \qquad (*)$$

in the ring $\mathbb{Z}[(f_{i,j})_{i,j\in[\![1..n]\!]}]$. This implies an algebraic identity that allows us to express this membership. This algebraic identity is naturally valid in all the commutative rings. It is therefore clear that if the membership $(*)$

is satisfied in the generic case, it implies $r_h r_k = 0$ for any projection matrix over an arbitrary commutative ring.

The same holds for the equalities $r_h u = 0$ when u is a minor of order $h + 1$.

In short: if Theorem 1.7 is satisfied in the generic case, it is satisfied in every case. As is often the case, we therefore observe that important theorems of commutative algebra do nothing other than affirm the existence of certain particular types of algebraic identities.

2. The semiring $\mathsf{H}_0^+(\mathbf{A})$, and the ring of generalized ranks $\mathsf{H}_0(\mathbf{A})$

For a free module, by passing from the rank k to the rank polynomial X^k, we pass from the additive notation to the multiplicative notation. For a general finitely generated projective module, we can conversely consider a "generalized rank" of the module, which is the (purely formal) logarithm in base X of its rank polynomial. Although this is just a simple play on notation, it so happens that computations with the ranks are facilitated by it. Let us explain how this works.

The semiring of ranks

Recall that we say that a polynomial $R(X) = r_0 + r_1X + \cdots + r_nX^n$ is multiplicative when $R(1) = 1$ and $R(XY) = R(X)R(Y)$. It amounts to the same to say that the r_i's form a fundamental system of orthogonal idempotents, or that $R(X)$ is the rank polynomial of a finitely generated projective module.

2.1. Notation. We denote by $\mathsf{H}_0^+(\mathbf{A})$ the set of isomorphism classes of quasi-free modules over $\mathbf{A}$, and $[P]_{\mathsf{H}_0^+(\mathbf{A})}$ (or $[P]_{\mathbf{A}}$, or even $[P]$) the class of such a module P in $\mathsf{H}_0^+(\mathbf{A})$. The set $\mathsf{H}_0^+(\mathbf{A})$ is equipped with a *semiring structure*[1] *for the inherited laws of* $\oplus$ *and* $\otimes$*:* $[P \oplus Q] = [P] + [Q]$ *and* $[P \otimes Q] = [P] \cdot [Q]$*. For an idempotent e we will also write* $[e]$ *instead of* $[e\mathbf{A}]$*, when the context is clear. The neutral element for the multiplication is* $[1]$*.*

[1] This means that the structure is given by an addition, commutative and associative, a multiplication, commutative, associative and distributive with respect to addition, with a neutral 0 for the addition and a neutral 1 for the multiplication. For example $\mathbb{N}$ is a semiring.

Every quasi-free module P is isomorphic to a unique module[2]

$$(r_1\mathbf{A}) \oplus (r_2\mathbf{A})^2 \oplus \cdots \oplus (r_n\mathbf{A})^n,$$

where the r_i's are orthogonal idempotents, because then $\mathrm{e}_i(P) = r_i$. We therefore have= $[P] = \sum_{k=1}^{n} k\,[r_k]$ and its rank polynomial is

$$\mathrm{R}_P(X) = r_0 + r_1X + \cdots + r_nX^n$$

with $r_0 = 1 - (r_1 + \cdots + r_n)$.

But while $\mathrm{R}_{P\oplus Q} = \mathrm{R}_P\,\mathrm{R}_Q$, we have $[P \oplus Q] = [P] + [Q]$: this assures the passage from the multiplicative notation to the additive notation. Thus the "logarithm in base X" of the multiplicative polynomial $r_0{+}r_1X{+}\cdots{+}r_nX^n$is defined as the element $\sum_{k=1}^{n} k\,[r_k]$ of $\mathsf{H}_0^+(\mathbf{A})$.

2.2. Definition. If M is a finitely generated projective $\mathbf{A}$-module we call *(generalized) rank* and we denote by $\mathrm{rk}_{\mathbf{A}}(M)$ or $\mathrm{rk}(M)$ the unique element of $\mathsf{H}_0^+(\mathbf{A})$ which has the same rank polynomial.

Thus if $\mathrm{R}_M(X) = r_0 + r_1X + \cdots + r_nX^n$, then $\mathrm{rk}(M) = \sum_{k=1}^{n} k\,[r_k]$.

The zero module is characterized by $\mathrm{rk}(M) = 0$ (Theorem V-8.4).

If $\mathbf{A}$ is nontrivial, then $[1] \neq [0]$ and $\mathbb{N}$ is identified with the subsemiring of $\mathsf{H}_0^+(\mathbf{A})$ generated by $[1]$ by means of the injection $n \mapsto n\,[1]$. The above definition therefore does not conflict with the notion of rank for projective modules of constant rank, previously defined.

Also note that when $\mathbf{A}$ is trivial we have $\mathsf{H}_0^+(\mathbf{A}) = 0$: this indeed conforms with the convention according to which the zero module over the trivial ring has for rank any integer, since in $\mathsf{H}_0^+(\mathbf{A})$, $k = 0$, or if we prefer, the two rank polynomials 1 and X^k are equal over the trivial ring.

Remark. A rule of practical computation regarding ranks is the following

$$[r] + [r'] = [r + r'] \quad \text{if} \quad rr' = 0,$$

i.e. more generally

$$[r] + [r'] = [r \vee r'] + [r \wedge r'] = [r \oplus r'] + 2\,[r \wedge r'] \tag{2}$$

where the laws $\vee$, $\wedge$ and $\oplus$ are those of the Boolean algebra of the idempotents of the ring: $r \oplus r' = r + r' - 2rr'$, $r \vee r' = r + r' - rr'$ and $r \wedge r' = rr'$. Note that the two idempotents $r \oplus r'$ and $r \wedge r'$ are orthogonal, of sum $r \vee r'$, and that the meaning of the equality (2) is given by the following isomorphisms

$$r\mathbf{A} \oplus r'\mathbf{A} \;\simeq\; (r \vee r')\mathbf{A} \oplus (r \wedge r')\mathbf{A} \;\simeq\; (r \oplus r')\mathbf{A} \oplus \big((r \wedge r')\mathbf{A}\big)^2. \qquad \blacksquare$$

[2] We also have (Exercise II-14) $P \simeq e_1\mathbf{A} \oplus \cdots \oplus e_n\mathbf{A}$ with $e_k = \sum_{j=k}^{n} r_j$, and e_k divides e_{k+1} for $1 \leqslant k < n$.

Exponential notation

Please note that a^n is the result of evaluating the multiplicative polynomial X^n at the point a: $X^n(a) = a^{\log_X(X^n)}$.

Thus, for a multiplicative polynomial $R(X) = \sum_{k=0}^{n} e_k X^k$, whose logarithm in base X is the element $r = \sum_{k=0}^{n} k\,[e_k]$, we adopt the following legitimate notations

- $a^r = \sum_{k=0}^{n} e_k a^k = R(a)$,
- and for an $\mathbf{A}$-module M, $M^r = \bigoplus_{k=0}^{n} e_k M^k$.

This is not a fancy: we indeed have

- $a^{r+r'} = a^r a^{r'}$, $a^{rr'} = (a^r)^{r'}$,
- $M^{r+r'} \simeq M^r \times M^{r'}$ and $M^{rr'} \simeq M^r \otimes M^{r'} \simeq (M^r)^{r'}$,

for arbitrary r, r' in $\mathsf{H}_0^+\,\mathbf{A}$.

Symmetrization

The additive monoid $\mathsf{H}_0^+(\mathbf{A})$ is regular: either by McCoy's lemma (Corollary III-2.3), or by one of the two uniqueness theorems IV-5.1 and IV-5.2 (page 202), or finally by item *3* of Theorem V-8.4.

The semiring $\mathsf{H}_0^+(\mathbf{A})$ can therefore be considered as a subsemiring of the ring obtained by symmetrization. This ring is called the *ring of (generalized) ranks of finitely generated projective modules* over $\mathbf{A}$, and we denote it by $\mathsf{H}_0(\mathbf{A})$.

Every element of $\mathsf{H}_0(\mathbf{A})$ is expressed in the form $\sum_{k\in J} k\,[r_k]$ where the r_k's are pairwise orthogonal idempotents and J is a finite subset of $\mathbb{Z} \setminus \{0\}$. The expression is unique in the following sense: if $\sum_{k\in J} k\,[r_k] = \sum_{k\in J'} k\,[r'_k]$, then $r_k = r'_k$ if $k \in J \cap J'$, and the others are null.

Multiplication of the ranks

We have defined a multiplication on $\mathsf{H}_0^+\,\mathbf{A}$, as the law inherited from the tensor product. This implies that for two idempotents e and e' we have $[e]\cdot[e'] = [ee']$. The other product computations are deducted from it by distributivity. Hence the following fact.

2.3. Fact. *The element* 1 *is the only invertible element of* $\mathsf{H}_0^+(\mathbf{A})$*.*

D If $r = \sum_k k[r_k]$ and $s = \sum_k k[s_k]$, then $rs = \sum_k k(\sum_{i,j,ij=k} [r_i s_j])$. By uniqueness of the expression, if $rs = 1 = 1[1]$, then $r_1 s_1 = 1$ therefore $r_1 = s_1 = 1$. □

We can ask ourselves which is the corresponding law on multiplicative polynomials; the readers will convince themselves that is it the law

$$\big(R(X), R'(X)\big) \mapsto R\big(R'(X)\big) = R'\big(R(X)\big).$$

We also have the following fact which stems from the upcoming Proposition 3.3.

2.4. Fact. *If P and Q are two finitely generated projective modules, then $P \otimes Q$ is a finitely generated projective module and* $\mathrm{rk}(P \otimes Q) = \mathrm{rk}(P) \cdot \mathrm{rk}(Q)$.

Order relation over ranks

The natural order relation associated with the monoid structure of $\mathsf{H}_0^+ \mathbf{A}$ is described in the following proposition.

2.5. Proposition and definition.

1. *For s, $t \in \mathsf{H}_0 \mathbf{A}$ we define $s \leqslant t$ by $\exists r \in \mathsf{H}_0^+ \mathbf{A}$, $s + r = t$.*
2. *This relation gives to $\mathsf{H}_0 \mathbf{A}$ an* ordered ring *structure,*[3] *and $\mathsf{H}_0^+ \mathbf{A}$ is the non-negative subset of $\mathsf{H}_0 \mathbf{A}$.*
3. *Let P and Q be finitely generated projective modules, the following properties are equivalent.*
   - *a.* $\mathrm{rk}(P) \leqslant \mathrm{rk}(Q)$.
   - *b.* R_P *divides* R_Q *in* $\mathbf{A}[X]$.
   - *c.* R_P *divides* R_Q *in* $\mathbb{B}(\mathbf{A})[X]$.
   - *d. For all $s \in \mathbf{A}$, if P_s and Q_s are free, then the rank of P_s is less or equal to that of Q_s.*
   - *e. For all $k > i$,* $\mathrm{e}_k(P) \cdot \mathrm{e}_i(Q) = 0$.
   - *f. For all k,* $\mathrm{e}_k(P) \cdot \sum_{i \geqslant k} \mathrm{e}_i(Q) = \mathrm{e}_k(P)$.

Example. Let us suppose that $P \oplus R = Q$ and that we know the ranks of P and Q, we want to compute the rank of R.
We have $\mathrm{rk}\, P = \sum_{i=0}^{n} i\,[r_i]$ and $\mathrm{rk}\, Q = \sum_{j=0}^{m} j\,[s_j]$. We write

$$\begin{aligned} \mathrm{rk}\, P &= \big(\textstyle\sum_{i=0}^{n} i\,[r_i]\big)\big(\sum_{j=0}^{m} [s_j]\big) = \sum_{i,j} i\,[r_i s_j] \leqslant \\ \mathrm{rk}\, Q &= \big(\textstyle\sum_{j=0}^{m} j\,[s_j]\big)\big(\sum_{i=0}^{n} [r_i]\big) = \sum_{i,j} j\,[r_i s_j]. \end{aligned}$$

The $r_i s_j$'s form a fundamental system of orthogonal idempotents and we obtain by subtraction, without having to think, the equalities

$$\mathrm{rk}(Q) - \mathrm{rk}(P) = \mathrm{rk}(R) = \textstyle\sum_{i \leqslant j} (j - i)\,[r_i s_j] = \sum_{k=0}^{m} k\big(\sum_{j-i=k} [r_i s_j]\big). \qquad \blacksquare$$

[3] This means that $\geqslant$ is a partial order relation *compatible* with the laws $+$ and $\times$, more precisely
- $1 \geqslant 0$,
- $x \geqslant 0$ and $y \geqslant 0$ imply $x + y$ and $xy \geqslant 0$,
- $x \geqslant y \Leftrightarrow x - y \geqslant 0$.

In the remainder of the text, we definitively drop the use of the word "generalized" when we speak of the rank of a finitely generated projective module.

Remark. In classical mathematics, $\mathsf{H}_0(\mathbf{A})$ is often defined as the ring of locally constant (i.e. continuous) functions from $\mathsf{Spec}\,\mathbf{A}$ to $\mathbb{Z}$. A more detailed comment on the subject can be found on page 573. ■

Other uses for the rank

2.6. Notations.

1. If $\varphi \in \mathrm{L}_{\mathbf{A}}(P,Q)$ with P, Q finitely generated projective, and if $\mathrm{Im}\,\varphi$ is a direct summand in Q we will denote $\mathrm{rk}(\mathrm{Im}\,\varphi)$ by $\mathrm{rk}\,\varphi$.
2. If $p(X)$ is a pseudomonic polynomial of $\mathbf{A}[X]$, we can define its degree $\deg p$ as an element of $\mathsf{H}_0^+(\mathbf{A})$.

For item *1* we have $\mathrm{Ker}\,\varphi$ which is a direct summand in P and we obtain the generalizations of well-known equalities in the case of vector spaces over a discrete field

$$\mathrm{rk}(\mathrm{Ker}\,\varphi) + \mathrm{rk}\,\varphi = \mathrm{rk}\,P \quad \text{and} \quad \mathrm{rk}(\mathrm{Ker}\,\varphi) + \mathrm{rk}\,Q = \mathrm{rk}(\mathrm{Coker}\,\varphi) + \mathrm{rk}\,P\,.$$

In addition, in case of free modules, and for some rank $r \in \mathbb{N}$, we indeed find the notion of rank of a matrix as defined in II-5.7.

As for item *2*, note that for two pseudomonic polynomials p and q we have the equality $\deg pq = \deg p + \deg q$.

This notion of degree is naturally extended to locally monic polynomials defined in Exercise 14.

3. Some applications of the local structure theorem

In this section we consider results regarding finitely generated projective modules and some linear maps between those.

Given the local structure theorem for finitely generated projective modules, and since the determinant and the related polynomials are well-behaved by change of base ring (Fact V-8.8), we have almost systematically all the desired results by means of the proof given in the following frame.

D In the free module case, the result is easy to establish. □

We will not always mention it in this section.

NB: if in the hypothesis there is a locally simple linear map between two different modules, by the local structure theorem we are reduced to the case of a simple linear map.

The proof works each time the result to be established is true if and only if it is true after localization at comaximal elements.

Remark. If we must prove a result which, in the case of free modules, comes down to algebraic identities we can also suppose that the endomorphisms are diagonalizable. The argument here is different from the local structure theorem. The fact is that to check an algebraic identity it suffices to do so on a Zariski open set of the parameter space, and a generic matrix is diagonalizable by Proposition III-5.3. ■

Trace of an endomorphism and new expression for the fundamental polynomial

Recall that if M and N are two $\mathbf{A}$-modules, we denote by $\theta_{M,N}$ the canonical linear map

$$\theta_{M,N} : M^\star \otimes_{\mathbf{A}} N \to \mathrm{L}_{\mathbf{A}}(M,N),\ (\alpha \otimes y) \mapsto (x \mapsto \alpha(x)y).$$

Also recall the following results (Fact V-2.2 and Proposition V-5.4).

Let P be a finitely generated projective module.

1. *$\theta_{P,N}$ is an isomorphism of $P^\star \otimes_{\mathbf{A}} N$ in $\mathrm{L}_{\mathbf{A}}(P,N)$.*
2. *$\theta_{N,P}$ is an isomorphism of $N^\star \otimes_{\mathbf{A}} P$ in $\mathrm{L}_{\mathbf{A}}(N,P)$.*
3. *The canonical homomorphism $P \to P^{\star\star}$ is an isomorphism.*
4. *The canonical homomorphism*
$$\varphi \mapsto {}^{\mathrm{t}}\varphi\ ;\ \mathrm{L}_{\mathbf{A}}(N,P) \to \mathrm{L}_{\mathbf{A}}(P^\star,N^\star),$$
is an isomorphism.

If P is a finitely generated projective module, recall that the *trace* of the endomorphism φ of P (denoted by $\mathrm{Tr}_P(\varphi)$) is the coefficient in X of the fundamental polynomial $\mathrm{F}_\varphi(X)$. It can also be defined from the natural linear map

$$\mathrm{tr}_P : P^\star \otimes_{\mathbf{A}} P \to \mathbf{A}\ :\ \alpha \otimes y \mapsto \alpha(y),$$

and of the canonical isomorphism $\theta_P : P^\star \otimes_{\mathbf{A}} P \to \mathrm{End}(P)$, as follows

$$\mathrm{Tr}_P = \mathrm{tr}_P \circ {\theta_P}^{-1}.$$

(The reader will be able to observe that the two definitions coincide in the case of a free module, or to refer to Fact V-8.9.)

When P and Q are finitely generated projective, the trace also allows us to define a canonical duality between $\mathrm{L}_{\mathbf{A}}(P,Q)$ and $\mathrm{L}_{\mathbf{A}}(Q,P)$ by means of the bilinear map $(\varphi,\psi) \mapsto \mathrm{Tr}(\varphi \circ \psi) = \mathrm{Tr}(\psi \circ \varphi)$. This duality can also be defined by the canonical isomorphism $(P^\star \otimes_{\mathbf{A}} Q)^\star \simeq P \otimes_{\mathbf{A}} Q^\star$.

3.1. Proposition. *Let φ be an endomorphism of a finitely generated projective module P with n generators. The coefficients of the fundamental polynomial of φ are given by*

$$\mathrm{F}_\varphi(X) = 1 + \textstyle\sum_{h \in [\![1..n]\!]} \mathrm{Tr}\left(\bigwedge^h \varphi \right) X^h .$$

3.2. Proposition. *If P is a faithful finitely generated projective module, then the trace $\mathbf{A}$-linear map $\mathrm{Tr}_P : \mathrm{End}(P) \to \mathbf{A}$ is surjective.*

Tensor product

3.3. Proposition. *We consider two finitely generated projective $\mathbf{A}$-modules P and Q. Let φ and ψ be endomorphisms of P and Q. The module $P \otimes_{\mathbf{A}} Q$ is a finitely generated projective module.*

1. *We have the equality*
$$\det(\varphi \otimes \psi) = (\det \varphi)^{\mathrm{rk}\, Q}\, (\det \psi)^{\mathrm{rk}\, P} \overset{\mathrm{def}}{=} \mathrm{R}_Q(\det \varphi)\, \mathrm{R}_P(\det \psi).$$
2. *The fundamental polynomial $\mathrm{F}_{\varphi\otimes\psi}(X)$ of $\varphi \otimes_{\mathbf{A}} \psi$ only depends on $\mathrm{rk}(P)$, on $\mathrm{rk}(Q)$, on F_φ, and on F_ψ.*
3. *If $\mathrm{F}_\varphi = (1 + \lambda_1 X) \cdots (1 + \lambda_m X)$, and $\mathrm{F}_\psi = (1 + \mu_1 X) \cdots (1 + \mu_n X)$, we have the equality $\mathrm{F}_{\varphi\otimes\psi}(X) = \prod_{i,j}(1 + \lambda_i \mu_j X)$.*
4. *In particular, $\mathrm{rk}(P \otimes Q) = \mathrm{rk}(P)\, \mathrm{rk}(Q)$.*

Please note that the last equality can be rewritten as

$$\mathrm{e}_h(P \otimes Q) = \textstyle\sum_{jk=h} \mathrm{e}_j(P)\mathrm{e}_k(Q).$$

Also note that the previous proposition could be "directly" proven without making use of the local structure theorem, with a proof copied from that which was given for exterior powers (Proposition 1.2).

Ranks and linear maps

3.4. Proposition. *Let $\varphi : P \to Q$ be a linear map between finitely generated projective modules.*

1. *If φ is surjective, then $P \simeq \mathrm{Ker}\, \varphi \oplus Q$. If in addition $\mathrm{rk}(P) = \mathrm{rk}(Q)$, then φ is an isomorphism.*
2. *If φ is injective, then $\mathrm{rk}(P) \leqslant \mathrm{rk}(Q)$.*

D In item *2*, it suffices to prove the inequality after localization at an element s which renders the two modules free. As localization preserves injectivity, we can conclude by the free module case (see Corollary II-5.23 and the remark that follows). □

3.5. Corollary. *Let $P_1 \subseteq P_2 \subseteq P$ with P_1 a direct summand in P. Then P_1 is a direct summand in P_2. Consequently, if the modules are finitely generated projective, we have the equivalence*

$$\mathrm{rk}(P_1) = \mathrm{rk}(P_2) \iff P_1 = P_2.$$

If in addition $P_1 \oplus Q_1 = P_2 \oplus Q_2 = P$, we have the equivalences

$$\mathrm{rk}(P_1) = \mathrm{rk}(P_2) \iff \mathrm{rk}(Q_1) = \mathrm{rk}(Q_2) \iff P_1 = P_2.$$

Transitivity formulas

3.6. Notation. Let $\mathbf{B}$ be an $\mathbf{A}$-algebra , strictly finite over $\mathbf{A}$. Then $[\mathbf{B} : \mathbf{A}] = \mathrm{rk}_{\mathbf{A}}(\mathbf{B})$.

Recall that by Fact VI-4.4, if $\mathbf{B}$ is strictly finite over $\mathbf{A}$, and if P is a finitely generated projective $\mathbf{B}$-module, then P is also a finitely generated projective $\mathbf{A}$-module.

When we take P to be a quasi-free module over $\mathbf{B}$, by considering its rank over $\mathbf{A}$ it defines a homomorphism from the additive group $\mathsf{H}_0\,\mathbf{B}$ to the additive group $\mathsf{H}_0\,\mathbf{A}$. This homomorphism is called the *restriction homomorphism* and it is denoted by $\mathrm{Rs}_{\mathbf{B}/\mathbf{A}}$. We thus obtain a contravariant functor from a subcategory of commutative rings to that of Abelian groups. This is the category whose morphisms are the $\rho : \mathbf{A} \to \mathbf{B}$ which make of $\mathbf{B}$ a strictly finite algebra over $\mathbf{A}$.

Moreover, H_0 defines a covariant functor from the category of commutative rings to that of semirings, since by scalar extension, a quasi-free module gives a quasi-free module.

As $\mathsf{H}_0(\mathbf{C})$ is completely characterized by $\mathbb{B}(\mathbf{C})$ (for a categorical formulation, see Exercise 17), items *1* and *2* of the following fact completely describe the two functors which we have just spoken of.

3.7. Fact. *Let $\rho : \mathbf{A} \to \mathbf{B}$ be an algebra.*

1. *For $e \in \mathbb{B}(\mathbf{A})$, we have $\mathsf{H}_0(\rho)([e]_{\mathbf{A}}) = \big[\rho(e)\big]_{\mathbf{B}}$ in $\mathsf{H}_0\,\mathbf{B}$.*
   In particular $\mathsf{H}_0(\rho)$ is injective (resp. surjective, bijective) if and only if the restriction of ρ to $\mathbb{B}(\mathbf{A})$ and $\mathbb{B}(\mathbf{B})$ is injective (resp. surjective, bijective).

Now suppose that $\mathbf{B}$ is strictly finite over $\mathbf{A}$.

2. *For $e \in \mathbb{B}(\mathbf{B})$, $\mathrm{Rs}_{\mathbf{B}/\mathbf{A}}([e]_{\mathbf{B}}) = \mathrm{rk}_{\mathbf{A}}(e\mathbf{B})$, and $\mathrm{Rs}_{\mathbf{B}/\mathbf{A}}(1) = [\mathbf{B} : \mathbf{A}]$.*
3. *If a $\mathbf{B}$-module P is quasi-free over both $\mathbf{A}$ and $\mathbf{B}$, we simply obtain $\mathrm{Rs}_{\mathbf{B}/\mathbf{A}}([P]_{\mathbf{B}}) = [P]_{\mathbf{A}}$.*

Remark. If $\mathbf{A}$ is connected and contains $\mathbb{Z}$, we may pretend to consider $\mathsf{H}_0(\mathbf{A}) \simeq \mathbb{Z}$ as a subring of $\mathbf{A}$. In item *2* above we then see that $\mathrm{Rs}_{\mathbf{B}/\mathbf{A}}([e]_{\mathbf{B}}) = \big[\mathrm{Tr}_{\mathbf{B}/\mathbf{A}}(e)\big]_{\mathbf{A}}$ (it suffices to consider the case where $e\mathbf{B}$ is free and has a free direct complement within $\mathbf{B}$). ∎

The following lemma generalizes Theorem II-5.29 (which handled the free case).

3.8. Lemma. (Transitivity formulas for the trace and the determinant) *Let* $\mathbf{B}$ *be a strictly finite* $\mathbf{A}$*-algebra and* P *be a finitely generated projective* $\mathbf{B}$*-module. Let* $u_{\mathbf{B}} : P \to P$ *be a* $\mathbf{B}$*-linear map, that we denote as* $u_{\mathbf{A}}$ *when we consider it as an* $\mathbf{A}$*-linear map. Then we have the fundamental equalities*

$$\det_{\mathbf{A}}(u_{\mathbf{A}}) = \mathrm{N}_{\mathbf{B}/\mathbf{A}}\big(\det_{\mathbf{B}}(u_{\mathbf{B}})\big) \;\; \textit{and} \;\; \mathrm{Tr}(u_{\mathbf{A}}) = \mathrm{Tr}_{\mathbf{B}/\mathbf{A}}\big(\mathrm{Tr}(u_{\mathbf{B}})\big).$$

D Localizing at comaximal elements of $\mathbf{A}$ we can assume that $\mathbf{B}$ is a free $\mathbf{A}$-module, of rank k. We write

$$P \oplus N = L \simeq \mathbf{B}^n \simeq \mathbf{A}^{nk},$$

(the last isomorphism is an isomorphism of $\mathbf{A}$-modules). We consider $v = u \oplus \mathrm{Id}_N \in \mathrm{End}_{\mathbf{B}}(L)$. Then, by definition of the determinant, we obtain the equalities $\det_{\mathbf{B}}(u_{\mathbf{B}}) = \det_{\mathbf{B}}(v_{\mathbf{B}})$ and $\det_{\mathbf{A}}(u_{\mathbf{A}}) = \det_{\mathbf{A}}(v_{\mathbf{A}})$. We can therefore apply the transitivity formula of Theorem II-5.29.
The reasoning for the trace is similar. □

3.9. Corollary. *Let* $\mathbf{A} \xrightarrow{\rho} \mathbf{B}$ *be a strictly finite algebra,* P *a finitely generated projective* $\mathbf{B}$*-module and* $u_{\mathbf{B}} \in \mathrm{End}_{\mathbf{B}}(P)$*.*

1. $\mathrm{C}_{u_{\mathbf{A}}}(X) = \mathrm{N}_{\mathbf{B}[X]/\mathbf{A}[X]}\big(\mathrm{C}_{u_{\mathbf{B}}}(X)\big)$.
2. $\mathrm{F}_{u_{\mathbf{A}}}(X) = \mathrm{N}_{\mathbf{B}[X]/\mathbf{A}[X]}\big(\mathrm{F}_{u_{\mathbf{B}}}(X)\big)$.
3. *In particular, the rank polynomials of* P *over* $\mathbf{A}$ *and* $\mathbf{B}$ *are linked by* $$\mathrm{R}_{P_{\mathbf{A}}}(X) = \mathrm{N}_{\mathbf{B}[X]/\mathbf{A}[X]}\big(\mathrm{R}_{P_{\mathbf{B}}}(X)\big)$$
4. *The restriction homomorphism satisfies* $$\mathrm{Rs}_{\mathbf{B}/\mathbf{A}}\big(\mathrm{rk}_{\mathbf{B}}(P)\big) = \mathrm{rk}_{\mathbf{A}}(P).$$
5. *If* P *is a finitely generated projective* $\mathbf{A}$*-module, then* $$\mathrm{rk}_{\mathbf{B}}\big(\rho_\star(P)\big) = \mathsf{H}_0(\rho)\big(\mathrm{rk}_{\mathbf{A}}(P)\big), \;\; \textit{and} \;\; \mathrm{rk}_{\mathbf{A}}\big(\rho_\star(P)\big) = [\mathbf{B} : \mathbf{A}]\,\mathrm{rk}_{\mathbf{A}}(P).$$

D Items *1*, *2*, *3* result from the previous lemma.
4. Item *3* tells us that the rank polynomial of P over $\mathbf{A}$ only depends on the rank polynomial of P over $\mathbf{B}$. We can therefore assume that P is quasi-free over $\mathbf{B}$ and we apply the definition of the homomorphism $\mathrm{Rs}_{\mathbf{B}/\mathbf{A}}$.
Item *5* is left to the reader. □

Another corollary is given by the following theorem.

3.10. Theorem. *Let* $\mathbf{B}$ *be a strictly finite* $\mathbf{A}$*-algebra and* $\mathbf{C}$ *be a strictly finite* $\mathbf{B}$*-algebra. Then* $\mathbf{C}$ *is a strictly finite* $\mathbf{A}$*-algebra and*

$$[\mathbf{C} : \mathbf{A}] = \mathrm{Rs}_{\mathbf{B}/\mathbf{A}}([\mathbf{C} : \mathbf{B}]).$$

In particular, if $\mathsf{H}_0(\mathbf{A})$ *is identified with a subring of* $\mathsf{H}_0(\mathbf{B})$*, and if the rank of* $\mathbf{C}$ *over* $\mathbf{B}$ *is an element of* $\mathsf{H}_0(\mathbf{A})$*, we have*

$$[\mathbf{C} : \mathbf{A}] = [\mathbf{B} : \mathbf{A}]\,[\mathbf{C} : \mathbf{B}].$$

Projective modules of rank 1

3.11. Fact. *A matrix $F \in \mathbb{M}_n(\mathbf{A})$ is idempotent and of rank* 1 *if and only if* $\mathrm{Tr}(F) = 1$ *and* $\bigwedge^2 F = 0$.

D The proof is left to the reader. □

3.12. Proposition. *Let P be a projective $\mathbf{A}$-module of constant rank* 1.

1. *The canonical homomorphisms*
$$\mathbf{A} \to \mathrm{End}(P),\ a \mapsto \mu_{P,a} \ \text{ and } \ \mathrm{End}(P) \to \mathbf{A},\ \varphi \mapsto \mathrm{Tr}(\varphi)$$
are two reciprocal isomorphisms.
2. *For all $\varphi \in \mathrm{End}(P)$, we have* $\det(\varphi) = \mathrm{Tr}(\varphi)$.
3. *The canonical homomorphism $P^\star \otimes_{\mathbf{A}} P \to \mathbf{A}$ is an isomorphism.*

3.13. Proposition. *Let M and N be two $\mathbf{A}$-modules.*
If $N \otimes_{\mathbf{A}} M$ is isomorphic to $\mathbf{A}$, then M is a projective module of rank 1 *and N is isomorphic to $M^\star$.*

D Let φ be an isomorphism of $N \otimes_{\mathbf{A}} M$ over $\mathbf{A}$. Let $u = \sum_{i=1}^n c_i \otimes a_i$ be the element of $N \otimes M$ such that $\varphi(u) = 1$. We have two isomorphisms from $N \otimes M \otimes M$ to M, constructed from φ.
$$c \otimes a \otimes b \mapsto \varphi(c \otimes a)\, b \quad \text{and} \quad c \otimes a \otimes b \mapsto \varphi(c \otimes b)\, a.$$
This gives an isomorphism $\sigma : M \to M$ satisfying
$$\sigma\big(\varphi(c \otimes a)\, b\big) = \varphi(c \otimes b)\, a \ \text{ for all } c \in N,\ a, b \in M, \text{ hence}$$
$$\sigma(x) = \sigma\big(\textstyle\sum_i \varphi(c_i \otimes a_i)x\big) = \sum_i \varphi(c_i \otimes x)a_i, \text{ and } x = \sum_i \varphi(c_i \otimes x)\sigma^{-1}(a_i).$$
This shows that M is finitely generated projective, with the coordinate system $\big((u_1, \ldots, u_n), (\alpha_1, \ldots, \alpha_n)\big)$, where $u_i = \sigma^{-1}(a_i)$ and $\alpha_i(x) = \varphi(c_i \otimes x)$. Similarly, N is finitely generated projective.
But $1 = \mathrm{rk}(N \otimes M) = \mathrm{rk}(N)\,\mathrm{rk}(M)$, so M and N are of rank 1 (Fact 2.3).
Finally, $N \otimes M^\star \otimes M \simeq N \simeq M^\star$. □

4. Grassmannians

The generic rings $\mathbf{G}_n$ and $\mathbf{G}_{n,k}$

We have defined the ring $\mathbf{G}_n = \mathbf{G}_n(\mathbb{Z}) = \mathbb{Z}[(f_{ij})_{i,j \in [\![1..n]\!]}]/\mathcal{G}_n$ on page 543.

Actually the construction is functorial and we can define $\mathbf{G}_n(\mathbf{A})$ for every commutative ring $\mathbf{A}$: $\mathbf{G}_n(\mathbf{A}) = \mathbf{A}[(f_{ij})_{i,j \in [\![1..n]\!]}]/\mathcal{G}_n \simeq \mathbf{A} \otimes_{\mathbb{Z}} \mathbf{G}_n$.
Let $r_k = \mathrm{e}_k(\mathrm{Im}\ F)$ where F is the matrix $(f_{i,j})$ in $\mathbf{G}_n(\mathbf{A})$.

If we impose in addition that the rank must be equal to k, we introduce the ideal $\mathcal{G}_{n,k} = \mathcal{G}_n + \langle 1 - r_k \rangle$ and we obtain the ring
$$\mathbf{G}_{n,k} = \mathbb{Z}[F]/\mathcal{G}_{n,k} \simeq \mathbf{G}_n[1/r_k] \simeq \mathbf{G}_n/\langle 1 - r_k \rangle\,.$$

We also have the version relativized to $\mathbf{A}$:

$$\mathbf{G}_{n,k}(\mathbf{A}) = \mathbf{A}[F]/\mathcal{G}_{n,k} \simeq \mathbf{G}_n(\mathbf{A})[1/r_k] \simeq \mathbf{A} \otimes_{\mathbb{Z}} \mathbf{G}_{n,k}.$$

The ring $\mathbf{G}_n(\mathbf{A})$ is isomorphic to the product of the rings $\mathbf{G}_{n,k}(\mathbf{A})$.

$$\boxed{\text{In the present subsection devoted to } \mathbf{G}_{n,k} \text{ we let } h = n - k.}$$

If $\mathbf{K}$ is a field, the ring $\mathbf{G}_{n,k}(\mathbf{K})$ can be considered as the ring of coordinates of the affine variety $\mathbb{AG}_{n,k}(\mathbf{K})$ whose points are the pairs (E_1, E_2) of subspaces of $\mathbf{K}^n$ satisfying the equalities $\dim(E_1) = k$ and $\mathbf{K}^n = E_1 \oplus E_2$. In algebraic geometry, there are a few forceful arguments to affirm that the ring $\mathbf{G}_{n,k}(\mathbf{K})$ has all the right properties that we can imagine, with respect to the fact that the variety $\mathbb{AG}_{n,k}(\mathbf{K})$ is a homogeneous space for an action of the linear group.

We will find these results again "by hand" and by freeing ourselves of the hypothesis "$\mathbf{K}$ is a field."

By using the suitable localizations at the principal minors of order k of the matrix $F = (f_{ij})$ (the sum of these minors is equal to 1 in $\mathbf{G}_{n,k}(\mathbf{A})$), we will establish a few essential properties of the functor $\mathbf{G}_{n,k}$.

4.1. Theorem. (The functor $\mathbf{G}_{n,k}$)

1. *There exist comaximal elements μ_i of the ring $\mathbf{G}_{n,k}(\mathbf{A})$ such that each localized ring $\mathbf{G}_{n,k}(\mathbf{A})[1/\mu_i]$ is isomorphic to the ring*
$$\mathbf{A}[(X_j)_{j\in[\![1..2hk]\!]}][1/\delta]$$
for some δ which satisfies $\delta(\underline{0}) = 1$.
2. *The natural homomorphism $\mathbf{A} \to \mathbf{G}_{n,k}(\mathbf{A})$ is injective.*
3. *If $\varphi : \mathbf{A} \to \mathbf{B}$ is a homomorphism, the kernel of $\mathbf{G}_{n,k}(\varphi)$ is generated by* Ker φ. *In particular, if φ is injective, so is $\mathbf{G}_{n,k}(\varphi)$.*

4.2. Corollary. *Let $\mathbf{K}$ be a discrete field and $\mathbf{A}$ be a ring.*

1. *The ring $\mathbf{G}_{n,k}(\mathbf{K})$ is integral, integrally closed, coherent, Noetherian regular, of Krull dimension $2kh$.*
2. *If $\mathbf{A}$ is an integral ring (resp. reduced, pp-ring, pf-ring, normal, coherent Noetherian, coherent Noetherian regular) the same goes for $\mathbf{G}_{n,k}(\mathbf{A})$.*
3. *The Krull dimension of $\mathbf{G}_{n,k}(\mathbf{A})$ is equal to that of $\mathbf{A}[X_1, \ldots, X_{2hk}]$.*
4. *The ring $\mathbf{G}_{n,k} = \mathbf{G}_{n,k}(\mathbb{Z})$ is integral, integrally closed, coherent Noetherian, regular, of (Krull) dimension $2kh + 1$.*

Comment. In the corollary we have used the notion of a normal ring and that of a Krull dimension that we have not yet defined (see Sections XII-2 and XIII-2). Finally, a coherent ring is called regular when every finitely presented module admits a finite projective resolution (for this last notion see Problem 8). ■

Proof sketch. If we make a principal minor of order k of F invertible, then the ring $\mathbf{G}_{n,k}(\mathbf{A})$ becomes isomorphic to a localized ring of a polynomial ring over $\mathbf{A}$, therefore inherits all of the nice properties of $\mathbf{A}$. For the fact that $\mathbf{G}_{n,k}(\mathbb{Z})$ is integral there is an added subtleness, because this is not a local property. □

We now develop the above sketch. For the discrete field case we start with the following result.

4.3. Lemma. *Let $\mathbf{K}$ be a discrete field and (E_1, E_2) be a pair of complementary subspaces of dimensions k and h in $\mathbf{K}^n$.*

Suppose that in the matrix $\begin{bmatrix} \mathrm{I}_k & L \\ C & \mathrm{I}_h \end{bmatrix}$, the first k columns generate E_1 and the last h columns generate E_2.

1. *The matrices L and C are entirely determined by the pair (E_1, E_2).*
2. *The matrix $\mathrm{I}_k - LC$ is invertible (we denote its inverse by V).*
3. *The projection matrix over E_1 parallel to E_2 is equal to*
$$F = \begin{bmatrix} V & -VL \\ CV & -CVL \end{bmatrix}.$$

D The uniqueness is clear. Let $F = \begin{bmatrix} V & L' \\ C' & W \end{bmatrix}$ be the matrix of the considered projection. It is characterized by the equality

$$F \begin{bmatrix} \mathrm{I}_k & L \\ C & \mathrm{I}_h \end{bmatrix} = \begin{bmatrix} \mathrm{I}_k & 0 \\ C & 0 \end{bmatrix},$$

i.e.

$$V + L'C = \mathrm{I}_k,\ VL + L' = 0,\ C' + WC = C \ \text{ and } \ C'L + W = 0,$$

which is equivalent to

$$L' = -VL,\ W = -C'L,\ C'(\mathrm{I}_k - LC) = C \ \text{ and } \ V(\mathrm{I}_k - LC) = \mathrm{I}_k,$$

or $(\mathrm{I}_k - LC)^{-1} = V$, $C' = CV$, $L' = -VL$, and $W = -CVL$. □

This can be generalize to the case of a projection matrix of rank k over an arbitrary commutative ring as follows, which is a variant common to both the freeness lemma and the local freeness lemma.

4.4. Second freeness lemma.
Let F be a projector in $\mathbb{AG}_n(\mathbf{A})$; recall that $k + h = n$.

1. *If $\mathrm{rk}(F) \leqslant k$ and if a principal minor of order k is invertible, then the matrix F is similar to a standard projection matrix $\mathrm{I}_{k,n}$.*
2. *More precisely, suppose that $F = \begin{bmatrix} V & L' \\ C' & W \end{bmatrix}$ with $V \in \mathbb{GL}_k(\mathbf{A})$. Let*
$$B = \begin{bmatrix} V & -L' \\ C' & \mathrm{I}_h - W \end{bmatrix}.$$

Then, by letting $L = V^{-1}L'$ *and* $C = -C'V^{-1}$*, the matrix* B *is invertible, with inverse* $\begin{bmatrix} \mathrm{I}_k & L \\ C & \mathrm{I}_h \end{bmatrix}$*. In addition, we have the equalities*

$$B^{-1}\,F\,B = \mathrm{I}_{k,n},\ W = C'V^{-1}L',\ V = (\mathrm{I}_k - LC)^{-1},$$
$$\det V = \det(\mathrm{I}_h - W) \ \textit{and}\ \mathrm{I}_h - W = (\mathrm{I}_h - CL)^{-1}.$$

3. Conversely, if $L \in \mathbf{A}^{k\times h}$*,* $C \in \mathbf{A}^{h\times k}$ *and if* $\mathrm{I}_k - LC$ *is invertible with inverse* V*, then the matrix*

$$F = \begin{bmatrix} V & V\,L \\ -C\,V & -C\,V\,L \end{bmatrix}$$

is a projection of rank k*; it is the projection over the free submodule* E_1 *generated by the first* k *columns of* $\begin{bmatrix} \mathrm{I}_k & L \\ C & \mathrm{I}_h \end{bmatrix}$*, parallel to the free submodule* E_2 *generated by the last* h *columns of this matrix.*

D See Exercise 2 and its solution. □

What we have gained relative to the first freeness lemma II-5.10 is that F is similar to $\mathrm{I}_{k,n}$ instead of simply being equivalent (however, see Exercise V-3), and most importantly, the precisions obtained here will be useful to us.

The previous lemma can be reformulated as follows, in a more abstract form, but essentially equivalent (albeit less precise).

4.5. Lemma. (The ring $\mathbf{G}_{n,k}(\mathbf{A})$ is almost a polynomial ring)
We consider the generic matrix $F = (f_{ij})_{i,j\in[\![1..n]\!]}$ *in the ring* $\mathbf{G}_{n,k}(\mathbf{A})$*. Let* $\mu = \det\big((f_{ij})_{i,j\in[\![1..k]\!]}\big)$ *be its leading principal minor of order* k*. Moreover let* $\mathbf{A}[L,C]$ *be the polynomial ring in* $2kh$ *indeterminates, seen as coefficients of two matrices* L *and* C *of respective types* $k\times h$ *and* $h\times k$*. Finally, let* $\delta = \det(\mathrm{I}_k - LC) \in \mathbf{A}[L,C]$*.*
Then the localized rings $\mathbf{G}_{n,k}(\mathbf{A})[1/\mu]$ *and* $\mathbf{A}[L,C][1/\delta]$ *are naturally isomorphic.*

D Let us write F in the form $\begin{bmatrix} V & L' \\ C' & W \end{bmatrix}$ with $V \in \mathbb{M}_k(\mathbf{A})$. When we invert $\mu = \det(V)$ we get $V \in \mathbb{GL}_k(\mathbf{A}[1/\mu])$.
Let $L = V^{-1}L'$ and $C = -C'V^{-1}$. By item *2* of Lemma 4.4, we have $\delta = \det(\mathrm{I}_k - LC) \in \mathbf{A}^\times$. This defines a morphism of $\mathbf{A}$-algebras from $\mathbf{A}[L,C][1/\delta]$ to $\mathbf{G}_{n,k}(\mathbf{A})[1/\mu]$.
In the other direction: to L and C with δ being invertible we associate the matrix $F = \begin{bmatrix} V & V\,L \\ -C\,V & -C\,V\,L \end{bmatrix}$ (with $V = (\mathrm{I}_k - LC)^{-1}$).
The corresponding homomorphism goes from $\mathbf{G}_{n,k}(\mathbf{A})[1/\mu]$ to $\mathbf{A}[L,C][1/\delta]$.
By composing these morphisms we find the identity in both cases. □

Proof of Theorem 4.1.
1. This item is deducted from the previous lemma since the sum of the principal minors of order k of F is equal to 1 in $\mathbf{G}_{n,k}(\mathbf{A})$.

2. Consider the **A**-homomorphism $\psi : \mathbf{A}[(f_{i,j})] \to \mathbf{A}$ with specialization at $\mathrm{I}_{k,n}$ defined by $\psi(f_{i,j}) = 1$ if $i = j \in [\![1..k]\!]$ and $= 0$ otherwise.
It is clear that $\psi\big(\mathcal{G}_{n,k}(\mathbf{A})\big) = 0$. This proves that $\mathbf{A} \cap \mathcal{G}_{n,k}(\mathbf{A}) = 0$ because if a is in this intersection, $a = \psi(a) = 0$.

3. The kernel of $\varphi_{L,C} : \mathbf{A}[L, C] \to \mathbf{B}[L, C]$ (the natural extension of φ) is generated by the kernel of φ. The property remains true after localization. Then it remains true by gluing localizations at comaximal monoids. Therefore in our case we glue by saying that Ker $\mathbf{G}_{n,k}(\varphi)$ is generated by Ker φ. □

Proof of Corollary 4.2.
2. Besides the integrality question this results from item *1* of Theorem 4.1, because all the considered notions are stable by $\mathbf{A} \rightsquigarrow \mathbf{A}[X]$ and stem from the basic local-global principle. As for the integrality, it is deducted from the result in the case of a discrete field; if **A** is integral and $S = \mathrm{Reg}(\mathbf{A})$, then $\mathbf{K} = \mathrm{Frac}\,\mathbf{A} = \mathbf{A}_S$ is a discrete field and item *3* of Theorem 4.1 allows us to conclude.

3. Given the concrete local-global principle for the Krull dimension (page 760), it suffices to show that $\mathbf{A}[L, C]$ and $\mathbf{A}[L, C][1/\delta]$ have the same dimension, which result from Lemma 4.6 below.

1. Given items *2* and *3* it remains to show that $\mathbf{G}_{n,k}(\mathbf{K})$ is integral. In order to do so recall that $\mathbb{SL}_n(\mathbf{K})$ operates transitively over $\mathbb{AG}_{n,k}(\mathbf{K})$, which means that every projection matrix of rank k and of order n can be expressed in the form $S \cdot \mathrm{I}_{k,n} \cdot S^{-1}$ with $S \in \mathbb{SL}_n(\mathbf{K})$. Let us introduce the ring of coordinates of the variety $\mathbb{SL}_n(\mathbf{K}) \subseteq \mathbb{M}_n(\mathbf{K})$:

$$\mathbf{SL}_n(\mathbf{K}) = \mathbf{K}[(s_{i,j})_{i,j \in [\![1..n]\!]}]/\langle 1 - \det\, S \rangle \,.$$

To the surjective map

$$\theta_{\mathbf{K}} : \mathbb{SL}_n(\mathbf{K}) \to \mathbb{AG}_{n,k}(\mathbf{K}) \;:\; S \mapsto S \cdot \mathrm{I}_{k,n} \cdot S^{-1},$$

corresponds the **K**-homomorphism

$$\widetilde{\theta}_{\mathbf{K}} : \mathbf{G}_{n,k}(\mathbf{K}) \to \mathbf{SL}_n(\mathbf{K}),$$

which sends each $f_{i,j}$ onto the coefficient i, j of the matrix $S \cdot \mathrm{I}_{k,n} \cdot S^{-1}$.
It is well-known that $\mathbf{SL}_n(\mathbf{K})$ is integral, and it therefore suffices to show that $\widetilde{\theta}_{\mathbf{K}}$ is injective. As $\theta_{\mathbf{L}}$ is surjective for every finite extension **L** of **K**, every element of Ker $\widetilde{\theta}_{\mathbf{K}}$ is nilpotent (by the Nullstellensatz[4]). However, $\mathbf{G}_{n,k}(\mathbf{K})$ is reduced, so $\widetilde{\theta}_{\mathbf{K}}$ is injective.

4. Results from the other items (for the Krull dimension, Theorem XIII-8.20 is also required). □

[4] Here we give a constructive proof by assuming that **K** is contained in an algebraically closed discrete field. We could adapt it to the general case.

4.6. Lemma. *Using the previous notations the ring* $\mathbf{A}[L,C][1/\delta]$ *is a monogenic integral extension of a polynomial ring over* $\mathbf{A}$ *with* $2kh$ *indeterminates. Consequently* $\mathsf{Kdim}\,\mathbf{A}[L,C][1/\delta] = \mathsf{Kdim}\,\mathbf{A}[X_1,\ldots,X_{2kh}]$.

D Let $L = (l_{ij})_{i\in[\![1..k]\!],j\in[\![1..h]\!]}$, $C = (c_{ij})_{i\in[\![1..h]\!],j\in[\![1..k]\!]}$. The polynomial δ is of degree $2m$ with $m = \min(h,k)$ and contains the monomial

$$(-1)^m l_{11}\ldots l_{mm}c_{11}\ldots c_{mm}.$$

The localized ring $\mathbf{A}' = \mathbf{A}[L,C][1/\delta]$ can be obtained by adjoining an indeterminate t: $\mathbf{A}' = \mathbf{A}[L,C,t]/\langle t\delta-1\rangle$. We can put the polynomial $g = t\delta - 1$ in Noether position. Indeed, with the change of variables

$$l'_{ii} = l_{ii}+t,\ c'_{ii} = c_{ii}+t,\ i\in[\![1..m]\!],\quad l'_{ij} = l_{ij},\ c'_{ij} = c_{ij} \text{ if } i\neq j,$$

the polynomial g becomes, up to sign, monic in t. Therefore $\mathbf{A}'$ is a monogenic integral extension of $\mathbf{A}[L',C']$. We conclude with Theorem XIII-7.16.□

We will now study tangent spaces to grassmannians. For this we need to define the concept itself.

We therefore begin with a heuristic introduction to abstract categorical and functorial notions. The readers unfamiliar with the language of categories will have to skip this introduction, in which we give practically no proofs, and simply try to convince themselves from the given examples that the notion of a tangent space to a functor at a point is, all in all, quite reasonable, which will allow us them to then see the beautiful application of this concept to grassmannians.

Affine schemes, tangent spaces

Nullstellensatz and equivalence of two categories

Let $(\underline{f}) = (f_1,\ldots,f_s)$ be a polynomial system in $\mathbf{k}[X_1,\ldots,X_n] = \mathbf{k}[\underline{X}]$, and let $\mathbf{A} = \mathbf{k}[x_1,\ldots,x_n] = \mathbf{k}[\underline{x}]$ be the corresponding quotient algebra.

We have seen on page 317 the crucial identification

$$\boxed{\mathrm{Hom}_{\mathbf{k}}(\mathbf{A},\mathbf{k}) = \mathscr{Z}(\underline{f},\mathbf{k}) \subseteq \mathbf{k}^n}$$

between the zeros over $\mathbf{k}$ of the polynomial system $(\underline{f})$ and the characters of the algebra $\mathbf{A}$. If $\mathbf{k}$ is reduced, we obviously have $\mathrm{Hom}_{\mathbf{k}}(\mathbf{A},\mathbf{k}) = \mathrm{Hom}_{\mathbf{k}}(\mathbf{A}_{\mathrm{red}},\mathbf{k})$.

Now suppose that $\mathbf{k}$ is a discrete algebraically closed field.

Such a set of zeros $\mathscr{Z}(\underline{f},\mathbf{k}) \subseteq \mathbf{k}^n$ is then called an *algebraic variety over* $\mathbf{k}$.

Let $\mathbf{A}$ and $\mathbf{B}$ be two quotient $\mathbf{k}$-algebras corresponding to two polynomial systems $(\underline{f})$ and $\underline{g}$ in $\mathbf{k}[\underline{X}] = \mathbf{k}[X_1,\ldots,X_n]$. The Nullstellensatz (Corollary III-9.8) tells us that the two reduced algebras $\mathbf{A}_{\mathrm{red}}$ and $\mathbf{B}_{\mathrm{red}}$ are equal if and only if they have the same variety of zeros in $\mathbf{k}^n$:

$$\boxed{\mathscr{Z}(\underline{f},\mathbf{k}) = \mathscr{Z}(\underline{g},\mathbf{k}) \iff \mathrm{D}_{\mathbf{k}[\underline{X}]}(\underline{f}) = \mathrm{D}_{\mathbf{k}[\underline{X}]}(\underline{g}) \iff \mathbf{A}_{\mathrm{red}} = \mathbf{B}_{\mathrm{red}}}$$

This observation is the first step in the development of the equivalence between the category of finitely presented reduced **k**-algebras on the one hand, and that of algebraic varieties over **k** on the other.

For the equivalence to be complete, we must also treat the morphisms. Therefore we provide a preliminary study regarding the algebra $\mathbf{A}_{\mathrm{red}}$.

Notice that every element p of $\mathbf{k}[\underline{X}]$ defines a polynomial function $\mathbf{k}^n \to \mathbf{k}$, $\underline{\xi} \mapsto p(\underline{\xi})$, and that an element of $\mathbf{A}_{\mathrm{red}}$ defines (by restriction) a function $\mathscr{Z}(\underline{f},\mathbf{k}) \to \mathbf{k}$; indeed, if $p \equiv q \bmod \mathrm{D}_{\mathbf{k}[\underline{X}]}(\underline{f})$, a power of $p - q$ is in the ideal $\langle \underline{f} \rangle$, so the restrictions of the polynomial functions p and q to $\mathscr{Z}(\underline{f},\mathbf{k})$ are equal. But in the case where **k** is an algebraically closed field, we have the converse; if the restrictions of p and q to $\mathscr{Z}(\underline{f},\mathbf{k})$ are equal, $p - q$ vanishes over $\mathscr{Z}(\underline{f},\mathbf{k})$, and by Nullstellensatz, a power of $p - q$ is in the ideal $\langle \underline{f} \rangle$.

Thus, $\mathbf{A}_{\mathrm{red}}$ can be interpreted as an algebra of functions over the algebraic variety that it defines, namely $A = \mathscr{Z}(\underline{f},\mathbf{k}) = \mathrm{Hom}_{\mathbf{k}}(\mathbf{A},\mathbf{k})$. The **k**-algebra structure of $\mathbf{A}_{\mathrm{red}}$ is indeed that of this algebra of functions. These functions $\mathscr{Z}(\underline{f},\mathbf{k}) \to \mathbf{k}$ are called the *regular functions.*

Similarly, if $\mathbf{A} = \mathbf{k}[x_1,\ldots,x_n]$ and $\mathbf{C} = \mathbf{k}[y_1,\ldots,y_m]$ are the quotient algebras corresponding to two polynomial systems

$$(\underline{f}) \text{ in } \mathbf{k}[X_1,\ldots,X_n] \text{ and } (\underline{h}) \text{ in } \mathbf{k}[Y_1,\ldots,Y_m],$$

if $A = \mathscr{Z}(\underline{f},\mathbf{k}) \subseteq \mathbf{k}^n$ and $C = \mathscr{Z}(\underline{h},\mathbf{k}) \subseteq \mathbf{k}^m$ are the corresponding algebraic varieties, we define a *regular map* from A to C as the restriction to A and C of a polynomial map $\varphi : \mathbf{k}^n \to \mathbf{k}^m$ which sends A to C.

The regular maps are, by definition, *the morphisms from A to C in category of the algebraic varieties over* **k**. We will denote by $\mathrm{Mor}_{\mathbf{k}}(A,C)$ the set of these morphisms.

The above map φ is given by a system $(F_1,\ldots,F_m)$ in $\mathbf{k}[\underline{X}]$, or by the homomorphism $F : \mathbf{k}[\underline{Y}] \to \mathbf{k}[\underline{X}]$, $Y_j \mapsto F_j$.

Let $\varphi_1 : A \to C$ be the restriction of φ; if $\gamma : C \to \mathbf{k}$ is a regular function, then the composite function $\gamma \circ \varphi_1 : A \to \mathbf{k}$ is a regular function, and the map $\psi_1 : \gamma \mapsto \gamma \circ \varphi_1$ can be seen as a map from $\mathbf{C}_{\mathrm{red}}$ to $\mathbf{A}_{\mathrm{red}}$. Actually, this map is none other than the homomorphism which comes from F by passage to the quotients.

In the opposite direction, we can see that every homomorphism $\psi_1 : \mathbf{C}_{\mathrm{red}} \to \mathbf{A}_{\mathrm{red}}$ comes from a homomorphism $\psi : \mathbf{C} \to \mathbf{A}$, and that ψ defines a regular map $\varphi : A \to C$, sometimes called the *co-morphism* of ψ. This takes place as follows: via the identifications $A = \mathrm{Hom}_{\mathbf{k}}(\mathbf{A},\mathbf{k})$ and $C = \mathrm{Hom}_{\mathbf{k}}(\mathbf{C},\mathbf{k})$, we simply have the equality $\varphi(\underline{\xi}) = \underline{\xi} \circ \psi$ (which makes of φ the "transpose" of ψ).

Finally, $\mathrm{Mor}_{\mathbf{k}}(A,C)$, is naturally identified with $\mathrm{Hom}_{\mathbf{k}}(\mathbf{C}_{\mathrm{red}},\mathbf{A}_{\mathrm{red}})$, identification that we express under the form of an equality:

$$\boxed{\mathrm{Mor}_{\mathbf{k}}(A,C)=\mathrm{Hom}_{\mathbf{k}}(\mathbf{C}_{\mathrm{red}},\mathbf{A}_{\mathrm{red}}).}$$

However, note that the direction of the arrows is reversed.

Let us consider as a special case the case where A is the algebraic variety reduced to a point, associated with the algebra $\mathbf{k}$, corresponding to the empty polynomial system over *the variable-free polynomial algebra* $\mathbf{k}$. If preferred, here we can see $\mathbf{k}$ as the quotient $\mathbf{k}[X]/\langle X\rangle$, corresponding to the point $\{0\}$, subvariety of the algebraic variety $V=\mathbf{k}$ associated with the algebra $\mathbf{k}[X]$.
In these conditions, the framed equality above admits as a special case $C=\mathrm{Mor}_{\mathbf{k}}(\{0\},C)=\mathrm{Hom}_{\mathbf{k}}(\mathbf{C}_{\mathrm{red}},\mathbf{k})$. We have come full circle!

The summary of this study is the following: we can entirely reduce the consideration of algebraic varieties over an algebraically closed field to the study of finitely presented reduced $\mathbf{k}$-algebras. This is an interpretation in finite terms (finite polynomial systems over $\mathbf{k}$ for the objects as well as for the morphisms) of objects a priori slightly more mysterious, and certainly more infinite. In categorical terms: we can advantageously replace the category of algebraic varieties over $\mathbf{k}$ with the opposite category to that of finitely presented reduced $\mathbf{k}$-algebras. There is a natural equivalence between these two categories.

Affine schemes

Now we take a big leap into abstraction. First of all we admit that varieties can have multiplicities. For example the intersection of a circle with a line must be a double point, and not only a point, when the line is tangent to the circle. Consequently, it is sometimes counterproductive to limit ourselves to reduced $\mathbf{k}$-algebras.

We also admit that our ring is not necessarily an algebraically closed field but an arbitrary commutative ring. In which case the points of the variety over $\mathbf{k}$ are not sufficient to characterize what we want to consider as an abstract algebraic variety defined over $\mathbf{k}$ (by allowing multiplicities). For example the abstract circle is certainly represented by the $\mathbb{Z}$-algebra

$$\mathbb{Z}[x,y]=\mathbb{Z}[X,Y]\big/\big\langle X^2+Y^2-1\big\rangle,$$

but it is not its points over $\mathbb{Z}$ that will give us much information. On the contrary, it is its points over all the $\mathbb{Z}$-algebras (i.e. over all the commutative rings) that matter. Similarly an abstract *double circle* is certainly represented by the $\mathbb{Z}$-algebra

$$\mathbb{Z}[x',y']=\mathbb{Z}[X,Y]\big/\big\langle (X^2+Y^2-1)^2\big\rangle,$$

but we would not know how to distinguish a simple circle from a double circle if we only consider the points over the reduced rings (the rings without multiplicity).

We now can define the category of *affine schemes over the commutative ring* $\mathbf{k}$. This could simply be the opposite category to the category of $\mathbf{k}$-algebras; that whose objects are the $\mathbf{k}$-algebras and whose arrows are the homomorphisms of $\mathbf{k}$-algebras.

But there exists a strictly more meaningful (and elegant?) equivalent description: *an affine scheme over the commutative ring* $\mathbf{k}$ *is known when its zeros over all the* $\mathbf{k}$*-algebras are known.* In other words, the $\mathbf{k}$-algebra $\mathbf{A}$ defines an affine scheme which is nothing other that the functor $\mathrm{Hom}_{\mathbf{k}}(\mathbf{A}, \bullet)$ from the category of $\mathbf{k}$-algebras to the category of sets.

A homomorphism of $\mathbf{k}$-algebras $\mathbf{B} \to \mathbf{A}$ defines a natural transformation from the functor $\mathrm{Hom}_{\mathbf{k}}(\mathbf{A}, \bullet)$ to the functor $\mathrm{Hom}_{\mathbf{k}}(\mathbf{B}, \bullet)$: natural transformations of functors are “in the right direction,” i.e. from the zeros of $\mathbf{A}$ to the zeros of $\mathbf{B}$.

If we do not want to abstract up too high, we can limit ourselves to finitely presented $\mathbf{k}$-algebras, which is quite enough to make very beautiful abstract algebraic geometry (i.e. not limited to algebraic geometry over discrete fields).

Tangent space at a point of a functor

First of all recall the notion of a tangent space to a polynomial system at a zero of the system introduced in Section IX-4.

Take the example of the sphere as an affine scheme defined over $\mathbb{Q}$. This scheme is associated with the $\mathbb{Q}$-algebra

$$\mathbf{A} = \mathbb{Q}[x, y, z] = \mathbb{Q}[X, Y, Z]\big/\big\langle X^2 + Y^2 + Z^2 - 1\big\rangle .$$

If $\underline{\xi} = (\alpha, \beta, \gamma) \in \mathbb{Q}^3$ is a zero of $\mathbf{A}$ over $\mathbb{Q}$, i.e. a rational point of the sphere, we associate to it

- the ideal $\mathfrak{m}_{\underline{\xi}} = \langle x - \alpha, y - \beta, z - \gamma\rangle_{\mathbf{A}}$,
- the local algebra $\mathbf{A}_{\underline{\xi}} = \mathbf{A}_{1+\mathfrak{m}_{\underline{\xi}}}$, and
- the tangent space $\mathrm{T}_{\underline{\xi}}(\mathbf{A}/\mathbb{Q}) \simeq \mathrm{Der}_{\mathbb{Q}}(\mathbf{A}, \underline{\xi})$,

which is a $\mathbb{Q}$-vector space canonically isomorphic to $(\mathfrak{m}_{\underline{\xi}}/\mathfrak{m}_{\underline{\xi}}{}^2)^{\star}$ or to $(\mathfrak{m}_{\underline{\xi}}\mathbf{A}_{\underline{\xi}}/\mathfrak{m}_{\underline{\xi}}\mathbf{A}_{\underline{\xi}}{}^2)^{\star}$.

More intuitively but equivalently (Proposition IX-4.3), a tangent vector to the sphere at $\underline{\xi}$ is simply given by a $(u, v, w) \in \mathbb{Q}^3$ which satisfies

$u\alpha + v\beta + w\gamma = 0$, i.e. by letting $f = X^2 + Y^2 + Z^2 - 1$,

$$u\frac{\partial f}{\partial X}(\underline{\xi}) + v\frac{\partial f}{\partial Y}(\underline{\xi}) + w\frac{\partial f}{\partial Z}(\underline{\xi}) = 0.$$

Here is now a new way to see this tangent space, which we express in terms of corresponding affine schemes, i.e. of the functor $\mathrm{Hom}_{\mathbb{Q}}(\mathbf{A}, \bullet) = \mathscr{Z}(f, \bullet)$. For this we must formally introduce an infinitesimal which we denote by ε, i.e. consider the $\mathbb{Q}$-algebra $\mathbb{Q}[\varepsilon] = \mathbb{Q}[T]/\langle T^2 \rangle$ (ε is the class of T modulo T^2).

The point $\underline{\xi}$ is seen as a character of $\mathbf{A}$, i.e. as the element $\widetilde{\underline{\xi}} : g \mapsto g(\underline{\xi})$ of $\mathrm{Hom}_{\mathbb{Q}}(\mathbf{A}, \mathbb{Q})$. We then ask ourselves what are the λ elements of the set $\mathrm{Hom}_{\mathbb{Q}}(\mathbf{A}, \mathbb{Q}[\varepsilon])$ that "lift $\widetilde{\underline{\xi}}$," in the sense that when composed with the evaluation of ε at 0, from $\mathbb{Q}[\varepsilon]$ to $\mathbb{Q}$, we once again obtain $\widetilde{\underline{\xi}}$.

$$\begin{tikzcd} & \mathbb{Q}[\varepsilon] \arrow[d, "\varepsilon:=0"] \\ \mathbf{A} \arrow[ru, dashed] \arrow[r, "\widetilde{\underline{\xi}}"] & \mathbb{Q} \end{tikzcd}$$

Such an element is a priori given by a zero of f over $\mathbb{Q}[\varepsilon]$ which recovers $\underline{\xi}$ when we evaluate ε at 0, i.e. a triple $(\alpha + a\varepsilon, \beta + b\varepsilon, \gamma + c\varepsilon)$, with $f(\alpha + a\varepsilon, \beta + b\varepsilon, \gamma + c\varepsilon) = 0$ in $\mathbb{Q}[\varepsilon]$. But this means precisely that (a, b, c) is a tangent vector to the sphere at $\underline{\xi}$.

It is simply the substance of the mundane observation which states that "the differential is the linear component of the increase in the function":

$$f(\underline{\xi} + \varepsilon V) = f(\underline{\xi}) + \varepsilon\, \mathrm{d}f(\underline{\xi})(V) \bmod \varepsilon^2.$$

This zero $\underline{\xi} + \varepsilon(a, b, c)$ of $\mathbf{A}$ in $\mathbf{k}[\varepsilon]$ defines a homomorphism $\mathbf{A} \to \mathbf{k}[\varepsilon]$ via $x \mapsto \alpha + a\varepsilon$, $y \mapsto \beta + b\varepsilon$, $z \mapsto \gamma + c\varepsilon$.

This homomorphism sends g to $g(\underline{\xi}) + a\frac{\partial g}{\partial X}(\underline{\xi}) + b\frac{\partial g}{\partial Y}(\underline{\xi}) + c\frac{\partial g}{\partial Z}(\underline{\xi})$, since

$$g\big(\underline{\xi} + \varepsilon(a, b, c)\big) = g(\underline{\xi}) + \varepsilon\, \mathrm{d}g(\underline{\xi})(a, b, c) \bmod \varepsilon^2.$$

The reader will be able to check that this little computation, which we have just performed on a small example, works for any zero of any polynomial system based on any commutative ring.

However, we need to at least add how to interpret the $\mathbf{k}$-module structure over the tangent space at a zero of a polynomial system over a ring $\mathbf{k}$ in terms of the functor $\mathrm{Hom}_{\mathbf{k}}(\mathbf{A}, \bullet)$.

Here also the use of our small example shall be sufficient.

In the category of $\mathbb{Q}$-algebras, the fiber product of the "restriction arrow"

$$\mathbb{Q}[\varepsilon] \to \mathbb{Q},\ \varepsilon \mapsto 0$$

which itself is the algebra

$$\mathbb{Q}[\varepsilon] \times_{\mathbb{Q}} \mathbb{Q}[\varepsilon] \simeq \mathbb{Q}[\varepsilon_1, \varepsilon_2] \quad \text{with } \varepsilon_1^2 = \varepsilon_1\varepsilon_2 = \varepsilon_2^2 = 0,$$

equipped with the two "projection " homomorphisms

$$\mathbb{Q}[\varepsilon_1, \varepsilon_2] \xrightarrow{\pi_1} \mathbb{Q}[\varepsilon],\ \varepsilon_1 \mapsto \varepsilon,\ \varepsilon_2 \mapsto 0 \quad \text{and}$$
$$\mathbb{Q}[\varepsilon_1, \varepsilon_2] \xrightarrow{\pi_2} \mathbb{Q}[\varepsilon],\ \varepsilon_2 \mapsto \varepsilon,\ \varepsilon_1 \mapsto 0,$$

and with the “restriction” arrow

$$\mathbb{Q}[\varepsilon_1, \varepsilon_2] \to \mathbb{Q}, \quad \varepsilon_1 \mapsto 0,\ \varepsilon_2 \mapsto 0.$$

There is also a natural homomorphism “of addition”

$$\mathbb{Q}[\varepsilon_1, \varepsilon_2] \to \mathbb{Q}[\varepsilon], \quad \varepsilon_1 \mapsto \varepsilon,\ \varepsilon_2 \mapsto \varepsilon,$$

which commutes with the restrictions.

When we give two zeros $\underline{\xi} + \varepsilon V_1$ and $\underline{\xi} + \varepsilon V_2$ of $\mathbf{A}$ in $\mathbb{Q}[\varepsilon]$, given the characteristic property of the fiber product in the category of $\mathbb{Q}$-algebras, the two corresponding homomorphisms $\mathbf{A} \to \mathbb{Q}[\varepsilon]$ uniquely factorize to give a homomorphism from $\mathbf{A}$ to $\mathbb{Q}[\varepsilon_1, \varepsilon_2]$, the “fiber product of the two,” which corresponds to the zero $\underline{\xi} + \varepsilon_1 V_1 + \varepsilon_2 V_2$ of $\mathbf{A}$ in $\mathbb{Q}[\varepsilon_1, \varepsilon_2]$.

Finally, by composing this fiber product homomorphism with the addition homomorphism $\mathbb{Q}[\varepsilon_1, \varepsilon_2] \to \mathbb{Q}[\varepsilon]$, we obtain the homomorphism corresponding to the zero $\underline{\xi} + \varepsilon(V_1 + V_2)$. We have therefore come full circle, the addition of tangent vectors has been described in purely categorical terms.

Let us recap. In the case of the functor that is an affine scheme defined by a polynomial system over a ring $\mathbf{k}$ with its quotient algebra $\mathbf{A}$, there is a canonical identification between $\mathrm{T}_{\underline{\xi}}(\mathbf{A}/\mathbf{k})$ and the set of points of $\mathbf{A}$ over $\mathbf{k}[\varepsilon]$ that lift $\underline{\xi}$, when we identify $\underline{\xi}$ and $\underline{\xi} + \varepsilon V$ with the corresponding elements of $\mathrm{Hom}_{\mathbf{k}}(\mathbf{A}, \mathbf{k})$ and $\mathrm{Hom}_{\mathbf{k}}(\mathbf{A}, \mathbf{k}[\varepsilon])$. In addition, the $\mathbf{k}$-module structure in the second interpretation is given by the “addition” provided by the homomorphism

$$\mathbf{k}[\varepsilon_1, \varepsilon_2] \simeq \mathbf{k}[\varepsilon] \times_{\mathbf{k}} \mathbf{k}[\varepsilon] \to \mathbf{k}[\varepsilon], \quad \varepsilon_1 \mapsto \varepsilon,\ \varepsilon_2 \mapsto \varepsilon,$$

$(\varepsilon^2 = \varepsilon_1^2 = \varepsilon_2^2 = \varepsilon_1\varepsilon_2 = 0)$.

Note that the “external law,” multiplication by the scalar a, comes from the homomorphism

$$\mathbf{k}[\varepsilon] \xrightarrow{\lambda_a} \mathbf{k}[\varepsilon], \quad b + \varepsilon c \mapsto b + \varepsilon ac.$$

The formal mechanism of addition described thus will work with any other functor which will itself be willing to transform the fiber products (in the category of $\mathbb{Q}$-algebras) into fiber products (in the category of sets).

Thus the notion of a tangent space at a point of a functor[5] generalizes to the other schemes over a ring $\mathbf{k}$, because they are “good functors.” That is, the Grothendieck schemes (that we will not define here) are good functors. The Grassmannian functors (which have already been defined) are such schemes.

[5] Functor from category of $\mathbf{k}$-algebras to the category of sets.

Tangent spaces to the Grassmannians

Projectors and ranks

Two easy facts before entering the heart of the matter. Consider a module E. Two projectors π_1, $\pi_2 : E \to E$ are said to be *orthogonal* if they satisfy $\pi_1 \circ \pi_2 = \pi_2 \circ \pi_1 = 0$.

4.7. Fact. *If π_1, $\pi_2 : E \to E$ are orthogonal projectors of images E_1 and E_2, then $\pi_1 + \pi_2$ is a projector and its image is $E_1 \oplus E_2$. Consequently, when E is a finitely generated projective module, we obtain*

$$\operatorname{rk}(\pi_1 + \pi_2) = \operatorname{rk}(E_1 \oplus E_2) = \operatorname{rk} E_1 + \operatorname{rk} E_2.$$

4.8. Fact. *Let π_1, $\pi_2 \in \operatorname{End}_{\mathbf{A}}(E)$ be two projectors of images E_1 and E_2. Then the $\mathbf{A}$-linear map*

$$\Phi : \operatorname{End}(E) \to \operatorname{End}(E),\ \varphi \mapsto \pi_2 \circ \varphi \circ \pi_1,$$

is a projector whose image is isomorphic to $\mathrm{L}_{\mathbf{A}}(E_1, E_2)$. Consequently, when E is a finitely generated projective module, we obtain the equality

$$\operatorname{rk} \Phi = \operatorname{rk} E_1 \cdot \operatorname{rk} E_2.$$

Affine Grassmannian

This subsection is dedicated to the determination of the tangent space at a point to the functor $\mathbf{A} \mapsto \mathbb{AG}_n(\mathbf{A})$. Recall that the acronym $\mathbb{AG}$ is used for “Affine Grassmannian.” The geometric interpretation of a point P of $\mathbb{AG}_n(\mathbf{A})$ is given by the ordered pair $(E, F) = (\operatorname{Im} P, \operatorname{Ker} P)$ of submodules as a direct sum in $\mathbf{A}^n$.

More generally, if $\mathbf{k}$ is a ring given as a reference (in usual geometry it would be a discrete field) and if M is a fixed finitely generated projective $\mathbf{k}$-module, we can consider the category of $\mathbf{k}$-algebras and the functor $\mathbf{A} \mapsto \mathbb{AG}_M(\mathbf{A})$, where $\mathbb{AG}_M(\mathbf{A})$ designates the set of ordered pairs (E, F) of submodules as a direct sum in the extended module $\mathbf{A} \otimes_{\mathbf{k}} M$, which we will denote by $M_{\mathbf{A}}$. Such a pair can be represented by the projection $\pi : M_{\mathbf{A}} \to M_{\mathbf{A}}$ over E parallel to F. The affine Grassmannian $\mathbb{AG}_M(\mathbf{A})$ can therefore be seen as the subset of idempotent elements in $\operatorname{End}_{\mathbf{A}}(M_{\mathbf{A}})$. It is this point of view that we adopt in the following.

To study the tangent space we must consider the $\mathbf{A}$-algebra $\mathbf{A}[\varepsilon]$ where ε is the generic element with null square. First of all we give the statement of the usual Grassmannian $\mathbb{AG}_n(\mathbf{A})$.

4.9. Theorem. (Tangent space to an affine Grassmannian)
Let $P \in \mathbb{AG}_n(\mathbf{A})$ be a projector of image E and of kernel F. For $H \in \mathbb{M}_n(\mathbf{A})$ we have the following equivalence.

$$P + \varepsilon H \in \mathbb{AG}_n(\mathbf{A}[\varepsilon]) \quad \Longleftrightarrow \quad H = HP + PH.$$

Let us associate to P the $\mathbf{A}$-linear map $\widehat{P} : \mathbb{M}_n(\mathbf{A}) \to \mathbb{M}_n(\mathbf{A})$ defined by

$$\widehat{P}(G) = P\,G\,(\mathrm{I}_n - P) + (\mathrm{I}_n - P)\,G\,P.$$

We have the following results.

- *The $\mathbf{A}$-linear maps*
  $$\pi_1 : G \mapsto P\,G\,(\mathrm{I}_n - P) \ \text{ and } \ \pi_2 : G \mapsto (\mathrm{I}_n - P)\,G\,P$$
  are orthogonal projectors. In particular, $\widehat{P}$ is a projector.
- *For $H \in \mathbb{M}_n(\mathbf{A})$, we have $H = PH + HP$ if and only if $H \in \operatorname{Im}\widehat{P}$.*
- *The module $\operatorname{Im}\widehat{P}$ is canonically isomorphic to $\mathrm{L}_{\mathbf{A}}(E,F) \oplus \mathrm{L}_{\mathbf{A}}(F,E)$. In particular, $\operatorname{rk}(\operatorname{Im}\widehat{P}) = 2\operatorname{rk}E \cdot \operatorname{rk}F$.*

In brief, the tangent space at the $\mathbf{A}$-point P to the functor $\mathbb{AG}_n$ is canonically isomorphic to the finitely generated projective module $\operatorname{Im}\widehat{P}$ (via $H \mapsto P + \varepsilon H$), itself canonically isomorphic to $\mathrm{L}_{\mathbf{A}}(E,F) \oplus \mathrm{L}_{\mathbf{A}}(F,E)$.

D The first item is immediate. Let V_P be the submodule of matrices H which satisfy $H = HP + PH$. This module is canonically isomorphic to the tangent space that we are looking for. A simple computation shows that π_1 and π_2 are orthogonal projectors. Therefore $\widehat{P}$ is a projector. The following equality is clear: $P\widehat{P}(G) + \widehat{P}(G)P = \widehat{P}(G)$. Therefore $\operatorname{Im}\widehat{P} \subseteq V_P$. Moreover, if $H = PH + HP$, we have $PHP = 0$, so $\widehat{P}(H) = PH + HP = H$. Thus $V_P \subseteq \operatorname{Im}\widehat{P}$. In brief $V_P = \operatorname{Im}\widehat{P} = \operatorname{Im}\pi_1 \oplus \operatorname{Im}\pi_2$: the result follows by applying Fact 4.8. □

We now give the general statement (the proof is identical).

4.10. Proposition. *Let $\pi \in \mathbb{AG}_M(\mathbf{A})$ be a projector of image E and of kernel F. For $\eta \in \operatorname{End}_{\mathbf{A}}(M_{\mathbf{A}})$ we have the equivalence*

$$\pi + \varepsilon\eta \in \mathbb{AG}_M(\mathbf{A}[\varepsilon]) \quad \Longleftrightarrow \quad \eta = \pi\eta + \eta\pi.$$

We associate to π the $\mathbf{A}$-linear map $\widehat{\pi} : \operatorname{End}(M_{\mathbf{A}}) \to \operatorname{End}(M_{\mathbf{A}})$ defined by $\widehat{\pi}(\psi) = \pi\,\psi\,(\mathrm{I} - \pi) + (\mathrm{I} - \pi)\,\psi\,\pi$. Then

- *The linear maps $\pi_1 : \psi \mapsto \pi\,\psi\,(\mathrm{I} - \pi)$ and $\pi_2 : \psi \mapsto (\mathrm{I} - \pi)\,\psi\,\pi$ are orthogonal projectors. In particular, $\widehat{\pi}$ is a projector.*
- *An $\mathbf{A}$-linear map $\eta \in \operatorname{End}(M_{\mathbf{A}})$ satisfies $\eta = \pi\eta + \eta\pi$ if and only if $\eta \in \operatorname{Im}\widehat{\pi}$.*
- *The module $\operatorname{Im}\widehat{\pi}$ is canonically isomorphic to $\mathrm{L}_{\mathbf{A}}(E,F) \oplus \mathrm{L}_{\mathbf{A}}(F,E)$. In particular, $\operatorname{rk}(\operatorname{Im}\widehat{\pi}) = 2\operatorname{rk}E \cdot \operatorname{rk}F$.*

In short the tangent space at the $\mathbf{A}$-point π to the functor $\mathbb{AG}_M$ is canonically isomorphic to the finitely generated projective module $\operatorname{Im}\widehat{\pi}$ (via $\eta \xrightarrow{\sim} \pi + \varepsilon\eta$), itself canonically isomorphic to $\mathrm{L}_{\mathbf{A}}(E,F) \oplus \mathrm{L}_{\mathbf{A}}(F,E)$.

Projective Grassmannian

This subsection is dedicated to the determination of the tangent space at a point to the functor $\mathbf{A} \mapsto \mathbb{G}_n(\mathbf{A})$, where $\mathbb{G}_n(\mathbf{A})$ designates the set of submodules which are direct summands in $\mathbf{A}^n$.

4.11. Fact. (The space of projectors that have the same image as a given projector) *Let $P \in \mathbb{G}_n(\mathbf{A})$ be a projector of image E. Let Π_E be the set of projectors that have E as their image, and $V = \mathbf{A}^n$. Then Π_E is an affine subspace of $\mathbb{M}_n(\mathbf{A})$, having for "direction" the finitely generated projective $\mathbf{A}$-module $\mathrm{L}_{\mathbf{A}}(V/E, E)$ (naturally identified with an $\mathbf{A}$-submodule of $\mathbb{M}_n(\mathbf{A})$). We specify the result as follows.*

1. *Let $Q \in \mathbb{G}_n(\mathbf{A})$ be another projector.*
   Then $Q \in \Pi_E$ if and only if $PQ = Q$ and $QP = P$.
   In this case, the difference $N = Q - P$ satisfy the equalities $PN = N$ and $NP = 0$, and so $N^2 = 0$.
2. *Conversely, if $N \in \mathbb{M}_n(\mathbf{A})$ satisfy $PN = N$ and $NP = 0$ (in which case $N^2 = 0$), then $Q := P + N$ is in Π_E.*
3. *In short, the set Π_E is identified with the $\mathbf{A}$-module $\mathrm{L}_{\mathbf{A}}(V/E, E)$ via the affine map*
   $$\mathrm{L}_{\mathbf{A}}(V/E, E) \to \mathbb{M}_n(\mathbf{A}),\ \varphi \mapsto P + j \circ \varphi \circ \pi,$$
   where $j : E \to V$ is the canonical injection and $\pi : V \to V/E$ is the canonical projection.

Additional information.

4. *If $Q \in \Pi_E$, P and Q are conjugated in $\mathbb{M}_n(\mathbf{A})$. More precisely, by letting $N = Q - P$, we have $(\mathrm{I}_n + N)(\mathrm{I}_n - N) = \mathrm{I}_n$ and $(\mathrm{I}_n - N)P(\mathrm{I}_n + N) = Q$.*
5. *If $Q \in \Pi_E$, then for all $t \in \mathbf{A}$, we have $tP + (1 - t)Q \in \Pi_E$.*

D *1.* $N^2 = 0$ as seen when multiplying $PN = N$ by N on the left-hand side.

3. The conditions $PN = N$ and $NP = 0$ over the matrix N is equivalent to the inclusions $\operatorname{Im} N \subseteq E = \operatorname{Im} P$ and $E \subseteq \operatorname{Ker} N$.
The matrices N of this type form an $\mathbf{A}$-module $\widetilde{E}$ which can be identified with the module $\mathrm{L}_{\mathbf{A}}(\operatorname{Ker} P, \operatorname{Im} P)$ "by restriction of the domain and of the image."
More intrinsically, this module $\widetilde{E}$ is also identified with $\mathrm{L}_{\mathbf{A}}(V/E, E)$ via the linear map $\mathrm{L}_{\mathbf{A}}(V/E, E) \to \mathbb{M}_n(\mathbf{A})$, $\varphi \mapsto j \circ \varphi \circ \pi$, which is injective and admits $\widetilde{E}$ as its image.

4. $(\mathrm{I}_n - N)\, P\, (\mathrm{I}_n + N) = P\, (\mathrm{I}_n + N) = P + PN = P + N = Q.$ □

4.12. Fact. *Let $E \in \mathbb{G}_n(\mathbf{A})$ and $E' \in \mathbb{G}_n(\mathbf{A}[\varepsilon])$ which gives E by the specialization $\varepsilon \mapsto 0$ (in other words E' is a point of the tangent space at E to the functor $\mathbb{G}_n$). Then E' is isomorphic to the module obtained from E by scalar extension: $E' \simeq \mathbf{A}[\varepsilon] \otimes_{\mathbf{A}} E$.*

D By Theorem 5.10, a finitely generated projective module M over a ring $\mathbf{B}$ is characterized, up to isomorphism, by its "reduction" M_{red} (i.e. the module obtained by scalar extension to $\mathbf{B}_{\mathrm{red}}$). However, E' and $\mathbf{A}[\varepsilon] \otimes_{\mathbf{A}} E$ have the same reduction E_{red} to $(\mathbf{A}[\varepsilon])_{\mathrm{red}} \simeq \mathbf{A}_{\mathrm{red}}$. □

4.13. Theorem. (Tangent space to a projective Grassmannian)
Let $E \in \mathbb{G}_n(\mathbf{A})$ be an $\mathbf{A}$-submodule which is a direct summand in $\mathbf{A}^n = V$. Then the tangent space at the $\mathbf{A}$-point E to the functor $\mathbb{G}_n$ is canonically isomorphic to $\mathrm{L}_{\mathbf{A}}(E, V/E)$. More precisely, if $\varphi \in \mathrm{L}_{\mathbf{A}}(E, V/E)$ and if we let

$$E_\varphi = \{\, x + \varepsilon h \mid x \in E,\ h \in V,\ h \equiv \varphi(x) \bmod E \,\},$$

then $\varphi \mapsto E_\varphi$ is a bijection from the module $\mathrm{L}_{\mathbf{A}}(E, V/E)$ to the set of matrices $E' \in \mathbb{G}_n(\mathbf{A}[\varepsilon])$ that give E when we specialize ε at 0.

D Let $E \in \mathbb{G}_n(\mathbf{A})$ and $\varphi \in \mathrm{L}_{\mathbf{A}}(E, V/E)$.
Let us first show that E_φ is in $\mathbb{G}_n(\mathbf{A}[\varepsilon])$ and above E. Let us fix a matrix $P \in \mathbb{AG}_n(\mathbf{A})$ satisfying $E = \operatorname{Im} P$. We therefore have $V = E \oplus \operatorname{Ker} P$ and an isomorphism $V/E \simeq \operatorname{Ker} P \subseteq V$. We can therefore lift the linear map φ at a matrix $H \in \mathbb{M}_n(\mathbf{A}) = \operatorname{End}(V)$ in accordance with the diagram

$$\begin{tikzcd}
V \arrow[r, "H"] \arrow[d, two heads] & V \\
E \arrow[r, "\varphi"] & V/E \arrow[u, hook]
\end{tikzcd}$$

The matrix H satisfies $PH = 0$ and $H(\mathrm{I}_n - P) = 0$, i.e. $HP = H$.
It suffices to show that $P + \varepsilon H$ is a projector of image E_φ.
For the inclusion $\operatorname{Im}(P + \varepsilon H) \subseteq E_\varphi$, let $(P + \varepsilon H)(y + \varepsilon z)$ with $y, z \in V$:

$$(P + \varepsilon H)(y + \varepsilon z) = Py + \varepsilon(Hy + Pz) = Py + \varepsilon(HPy + Pz) = x + \varepsilon h,$$

with $x = Py \in E$, $h = Hx + Pz$. Since $x \in E$, we have $\varphi(x) = Hx$, and so $h \equiv \varphi(x) \bmod E$. For the converse inclusion, let $x + \varepsilon h \in E_\varphi$ and let us show that $(P + \varepsilon H)(x + \varepsilon h) = x + \varepsilon h$:

$$(P + \varepsilon H)(x + \varepsilon h) = Px + \varepsilon(Hx + Ph).$$

As $x \in E$, we have $Px = x$. We need to see that $Hx + Ph = h$, but h is of the form $h = Hx + y$ with $y \in E$, so $Ph = 0 + Py = y$ and we indeed have the equality $h = Hx + Ph$.
Finally, it is clear that $P + \varepsilon H$ is a projector

$$(P + \varepsilon H)(P + \varepsilon H) = P^2 + \varepsilon(HP + PH) = P + \varepsilon H.$$

Let us show the surjectivity of $\varphi \mapsto E_\varphi$. Let $E' \subseteq \mathbf{A}[\varepsilon]^n$, a direct summand, above E. Then E' is the image of a projector $P + \varepsilon H$ and we have

$$(P + \varepsilon H)(P + \varepsilon H) = P^2 + \varepsilon(HP + PH), \text{ so } P^2 = P \text{ and } HP + PH = H,$$

which gives $PHP = 0$ (multiply $HP+PH = H$ by P on the right-hand side, for instance). We therefore see that P is a projector of image E (because E', for $\varepsilon := 0$, it is E). We replace H with $K = HP$, which satisfies

$$KP = (HP)P = K, \qquad PK = P(HP) = 0.$$

This does not change the image of $P + \varepsilon H$, i.e. $\mathrm{Im}(P + \varepsilon H) = \mathrm{Im}(P + \varepsilon K)$. To see this, it suffices (and is necessary) to show that

$$(P + \varepsilon H)(P + \varepsilon K) = P + \varepsilon K, \qquad (P + \varepsilon K)(P + \varepsilon H) = P + \varepsilon H.$$

On the left-hand side, we obtain $P+\varepsilon(HP+PK) = P+\varepsilon(HP+0) = P+\varepsilon K$; On the right-hand side, $P + \varepsilon(KP + PH) = P + \varepsilon(K + PH) = P + \varepsilon(HP + PH) = P + \varepsilon H$.

The matrix K satisfies $KP = K$, $PK = 0$ and represents a linear map $\varphi : E \to \mathbf{A}^n/E$ with $E' = \mathrm{Im}(P + \varepsilon K) = E_\varphi$.

Let us prove the injectivity of $\varphi \mapsto E_\varphi$. Therefore suppose $E_\varphi = E_{\varphi'}$. We fix a projector $P \in \mathbb{G}_n(\mathbf{A})$ with image E and we encode φ as H, φ' as H' with

$$HP = H, \quad PH = 0, \qquad H'P = H', \quad PH' = 0.$$

As $P + \varepsilon H$ and $P + \varepsilon H'$ have the same image, we have the equalities

$$(P + \varepsilon H)(P + \varepsilon H') = P + \varepsilon H' \quad \text{and} \quad (P + \varepsilon H')(P + \varepsilon H) = P + \varepsilon H.$$

The equality on the right gives $H = H'$, so $\varphi = \varphi'$. □

Remark. The projection $\mathbb{A}\mathbb{G}_n \to \mathbb{G}_n$ associates to P its image $E = \mathrm{Im}\, P$. Here is how the tangent spaces and the projection (with $F = \mathrm{Ker}\, P$) are organised

$$\begin{tikzcd}
\mathrm{T}_P(\mathbb{A}\mathbb{G}_n, \mathbf{A}) \arrow[r, dash, "\sim"] \arrow[d] & \mathrm{L}_{\mathbf{A}}(E, F) \oplus \mathrm{L}_{\mathbf{A}}(F, E) \arrow[r, dash, "\sim"] & \{H \in \mathbb{M}_n(\mathbf{A}) \mid H = HP + PH\} \arrow[d, "H \mapsto K = HP"] \\
\mathrm{T}_E(\mathbb{G}_n, \mathbf{A}) \arrow[r, dash, "\sim"] & \mathrm{L}_{\mathbf{A}}(E, \mathbf{A}^n/E) \arrow[r, dash, "\sim"] & \{K \in \mathbb{M}_n(\mathbf{A}) \mid KP = K,\ PK = 0\}
\end{tikzcd}$$

■

5. Grothendieck and Picard groups

Here we tackle the general problem of the complete classification of finitely generated projective modules over a fixed ring $\mathbf{A}$.

This classification is a fundamental but difficult problem, which does not admit a general algorithmic solution.

We start by stating some waymarks for the case where all the projective modules of constant rank are free.

In the following subsections we give a very small introduction to classic tools that allow us to apprehend the general problem.

When the projective modules of constant rank are free

Let us begin with an elementary remark.

5.1. Fact. *A projective* $\mathbf{A}$*-module of rank* k *is free if and only if it is generated by* k *elements.*

D The condition is clearly necessary. Now suppose the module generated by k elements. The module is therefore the image of a projection matrix $F \in \mathbb{M}_k(\mathbf{A})$. By hypothesis $\det(\mathrm{I}_k + XF) = (1+X)^k$. In particular, $\det F = 1$, so F is invertible, and since $F^2 = F$, this gives $F = \mathrm{I}_k$. □

Here is another easy remark.

5.2. Fact. *Every projective* $\mathbf{A}$*-module of constant rank is free if and only if every projective* $\mathbf{A}$*-module is quasi-free.*

D The condition is clearly sufficient. If every projective $\mathbf{A}$-module of constant rank is free and if P is projective, let $(r_0, \ldots, r_n)$ be the corresponding fundamental system of orthogonal idempotents. Then $P_k = r_kP \oplus (1-r_k)\mathbf{A}^k$ is a projective $\mathbf{A}$-module of rank k therefore free. Let B_k be a base, the "component" r_kB_k is in r_kP, and $r_kP \simeq (r_k\mathbf{A})^k$. Since P is the direct sum of the r_kP, it is indeed quasi-free. □

5.3. Proposition. *Every projective module of constant rank over a local-global ring is free.*

D Already seen in Theorem IX-6.9. □

5.4. Theorem. *Every finitely generated projective module over a Bézout domain is free. Every finitely generated projective module of constant rank over a Bézout pp-ring is free.*

D Let us consider the integral case. A presentation matrix of the module can be reduced to the form $\begin{bmatrix} T & 0 \\ 0 & 0 \end{bmatrix}$ where T is triangular with regular elements over the diagonal (see Exercise IV-6). As the determinantal ideals of this matrix are idempotents the determinant δ of T is a regular element which satisfies $\delta\mathbf{A} = \delta^2\mathbf{A}$. Thus δ is invertible and the presentation matrix is equivalent to $\begin{bmatrix} \mathrm{I}_k & 0 \\ 0 & 0 \end{bmatrix}$.

For the pp-ring case we apply the elementary local-global machinery explained on page 204. □

Let us take note of another important case: $\mathbf{A} = \mathbf{B}[X_1, \ldots, X_n]$ where $\mathbf{B}$ is a Bézout domain. This is a remarkable extension of the Quillen-Suslin theorem, due to Bass (for $n = 1$), then Lequain and Simis [126]. The theorem will be proved in Section XVI-6.

$\mathsf{GK}_0(\mathbf{A})$, $\mathsf{K}_0(\mathbf{A})$ and $\widetilde{\mathsf{K}}_0(\mathbf{A})$

Let $\mathsf{GK}_0\,\mathbf{A}$ be the set of isomorphism classes of finitely generated projective modules over $\mathbf{A}$. It is a semiring for the inherited laws of $\oplus$ and $\otimes$. The G of GK_0 is in tribute to Grothendieck.

Every element of $\mathsf{GK}_0\,\mathbf{A}$ can be represented by an idempotent matrix with coefficients in $\mathbf{A}$. Every ring homomorphism $\varphi : \mathbf{A} \to \mathbf{B}$ induces a homomorphism $\mathsf{GK}_0\,\varphi : \mathsf{GK}_0\,\mathbf{A} \to \mathsf{GK}_0\,\mathbf{B}$. So GK_0 is a covariant functor from the category of commutative rings to the category of semirings. We have $\mathsf{GK}_0(\mathbf{A}_1 \times \mathbf{A}_2) \simeq \mathsf{GK}_0\,\mathbf{A}_1 \times \mathsf{GK}_0\,\mathbf{A}_2$. The passage from a projective module to its dual defines an involutive automorphism of $\mathsf{GK}_0\,\mathbf{A}$.

If P is a finitely generated projective $\mathbf{A}$-module we can denote by $[P]_{\mathsf{GK}_0\,\mathbf{A}}$ the element of $\mathsf{GK}_0\,\mathbf{A}$ that it defines.

The subsemiring of $\mathsf{GK}_0\,\mathbf{A}$ generated by 1 (the class of the finitely generated projective module $\mathbf{A}$) is isomorphic to $\mathbb{N}$, except in the case where $\mathbf{A}$ is the trivial ring. As a subsemiring of $\mathsf{GK}_0\,\mathbf{A}$ we also have the one generated by the isomorphism classes of the modules $r\mathbf{A}$ where $r \in \mathbb{B}(\mathbf{A})$, isomorphic to $\mathsf{H}_0^+(\mathbf{A})$. We easily obtain the isomorphism $\mathsf{H}_0^+(\mathbf{A}) \simeq \mathsf{GK}_0\big(\mathbb{B}(\mathbf{A})\big)$. Moreover, the rank defines a surjective homomorphism of semirings $\mathsf{GK}_0\,\mathbf{A} \to \mathsf{H}_0^+(\mathbf{A})$, and the two homomorphisms $\mathsf{H}_0^+(\mathbf{A}) \to \mathsf{GK}_0\,\mathbf{A} \to \mathsf{H}_0^+(\mathbf{A})$ are composed according to the identity.

The *Picard group* $\mathsf{Pic}\,\mathbf{A}$ is the subset of $\mathsf{GK}_0\,\mathbf{A}$ formed by the isomorphism classes of the projective modules of constant rank 1. By Propositions 3.12 and 3.13 this is the group of invertible elements of the semiring $\mathsf{GK}_0\,\mathbf{A}$ (the "inverse" of P is the dual of P).

The (commutative) additive monoid of $\mathsf{GK}_0\,\mathbf{A}$ is not always regular. To obtain a group, we symmetrize the additive monoid $\mathsf{GK}_0\,\mathbf{A}$ and we obtain the *Grothendieck group* that we denote by $\mathsf{K}_0\,\mathbf{A}$.

The class of the finitely generated projective module P in $\mathsf{K}_0\,\mathbf{A}$ is denoted by $[P]_{\mathsf{K}_0(\mathbf{A})}$, or $[P]_{\mathbf{A}}$, or even $[P]$ if the context allows it. Every element of $\mathsf{K}_0\,\mathbf{A}$ is written in the form $[P] - [Q]$. More precisely, it can be represented under the two forms

- [projective] - [free] on the one hand,
- [free] - [projective] on the other hand.

Indeed

$$[P] - [Q] = [P \oplus P'] - [Q \oplus P'] = [P \oplus Q'] - [Q \oplus Q'],$$

with a choice of $P \oplus P'$ or $Q \oplus Q'$ being free.

The defined product in $\mathsf{GK}_0\,\mathbf{A}$ gives by passage to the quotient a product in $\mathsf{K}_0\,\mathbf{A}$, which therefore has a commutative ring structure.[6]

The classes of two finitely generated projective modules P and P' are equal in $\mathsf{K}_0\,\mathbf{A}$ if and only if there exists an integer k such that $P \oplus \mathbf{A}^k \simeq P' \oplus \mathbf{A}^k$. We say in this case that P and P' are *stably isomorphic* .

Two stably isomorphic quasi-free modules are isomorphic, so that $\mathsf{H}_0\,\mathbf{A}$ is identified with a subring of $\mathsf{K}_0\,\mathbf{A}$, and when P is quasi-free, there is no conflict between the two notations $[P]_{\mathbf{A}}$ (above and page 544).

Two stably isomorphic finitely generated projective modules P and P' have the same rank since $\mathrm{rk}(P\oplus\mathbf{A}^k) = k+\mathrm{rk}(P)$. Consequently, the (generalized) rank of the finitely generated projective modules defines a surjective ring homomorphism $\mathrm{rk}_{\mathbf{A}} : \mathsf{K}_0\,\mathbf{A} \to \mathsf{H}_0\,\mathbf{A}$. Let $\widetilde{\mathsf{K}}_0\,\mathbf{A}$ be its kernel. The two homomorphisms $\mathsf{H}_0\,\mathbf{A} \to \mathsf{K}_0\,\mathbf{A} \to \mathsf{H}_0\,\mathbf{A}$ are composed in terms of the identity, in other words the map $\mathrm{rk}_{\mathbf{A}}$ is a character of the $\mathsf{H}_0(\mathbf{A})$-algebra $\mathsf{K}_0\,\mathbf{A}$ and we can write

$$\mathsf{K}_0(\mathbf{A}) = \mathsf{H}_0(\mathbf{A}) \oplus \widetilde{\mathsf{K}}_0(\mathbf{A}).$$

The structure of the ideal $\widetilde{\mathsf{K}}_0\,\mathbf{A}$ of $\mathsf{K}_0\,\mathbf{A}$ concentrates a good part of the mystery of classes of stable isomorphism of finitely generated projective modules, since $\mathsf{H}_0\,\mathbf{A}$ presents no mystery (it is completely decrypted by $\mathbb{B}(\mathbf{A})$). In this framework the following result can be useful (cf. Problem 2).

5.5. Proposition. *The ideal* $\widetilde{\mathsf{K}}_0\,\mathbf{A}$ *is the nilradical of* $\mathsf{K}_0\,\mathbf{A}$.

Finally, note that if $\rho : \mathbf{A} \to \mathbf{B}$ is a ring homomorphism, we obtain correlative homomorphisms

$$\mathsf{K}_0\,\rho : \mathsf{K}_0\,\mathbf{A} \to \mathsf{K}_0\,\mathbf{B}, \quad \widetilde{\mathsf{K}}_0\,\rho : \widetilde{\mathsf{K}}_0\,\mathbf{A} \to \widetilde{\mathsf{K}}_0\,\mathbf{B} \quad \text{and} \quad \mathsf{H}_0\,\rho : \mathsf{H}_0\,\mathbf{A} \to \mathsf{H}_0\,\mathbf{B}.$$

And K_0, $\widetilde{\mathsf{K}}_0$ and H_0 are functors.

The Picard group

The Picard group is not affected by the passage to the classes of stable isomorphism, because of the following fact.

5.6. Fact. *Two stably isomorphic projective modules of constant rank* 1 *are isomorphic. In particular, a stably free module of rank* 1 *is free. More precisely, for a projective module* P *of consant rank* 1 *we have*

$$P \simeq \bigwedge^{k+1}(P \oplus \mathbf{A}^k). \tag{3}$$

In particular, $\mathsf{Pic}\,\mathbf{A}$ *is identified with a subgroup of* $(\mathsf{K}_0\,\mathbf{A})^\times$.

[6] When the ring $\mathbf{A}$ is not commutative, there is no more multiplicative structure over $\mathsf{GK}_0\,\mathbf{A}$. This explains why the usual terminology is Grothendieck group and not Grothendieck ring.

D Let us prove the isomorphism: it results from general isomorphisms given in the proof of Proposition 1.2 (equation (1)). For arbitrary **A**-modules P, Q, R, …, the consideration of the universal property that defined the exterior powers leads to

$$\textstyle\bigwedge^2(P \oplus Q) \simeq \bigwedge^2 P \oplus (P \otimes Q) \oplus \bigwedge^2 Q,$$

$$\textstyle\bigwedge^3(P\oplus Q\oplus R) \simeq \bigwedge^3 P \oplus \bigwedge^3 Q \oplus \bigwedge^3 R \oplus \big(\bigwedge^2 P \otimes Q\big) \oplus \cdots \oplus (P \otimes Q \otimes R),$$

with the following general formula by agreeing that $\bigwedge^0(P_i) = \mathbf{A}$

$$\bigwedge^k \big(\textstyle\bigoplus_{i=1}^m P_i\big) \simeq \displaystyle\bigoplus_{\sum_{i=1}^m k_i = k} \Big(\big(\bigwedge^{k_1} P_1\big) \otimes \cdots \otimes \big(\bigwedge^{k_m} P_m\big)\Big). \qquad (4)$$

In particular, if P_1, …, P_r are projective modules of constant rank 1 we obtain

$$\bigwedge^r (P_1 \oplus \cdots \oplus P_r) \simeq P_1 \otimes \cdots \otimes P_r. \qquad (5)$$

It remains to apply this with the direct sum $P \oplus \mathbf{A}^k = P \oplus \mathbf{A} \oplus \cdots \oplus \mathbf{A}$. The isomorphism of Equation (3) is then obtained with the **A**-linear map $P \to \bigwedge^{k+1}(P \oplus \mathbf{A}^k)$, $x \mapsto x \wedge 1_1 \wedge 1_2 \wedge \cdots \wedge 1_k$, where the index represents the position in the direct sum $\mathbf{A} \oplus \cdots \oplus \mathbf{A}$.
The last affirmation is then clear since we have just shown that the map $\mathsf{GK}_0\,\mathbf{A} \to \mathsf{K}_0\,\mathbf{A}$, restricted to $\mathsf{Pic}\,\mathbf{A}$, is injective. □

Remark. The reader will be able to compare the previous result and its proof with Exercise V-13. ■

We deduce the following theorem.

5.7. Theorem. ($\mathsf{Pic}\,\mathbf{A}$ and $\widetilde{\mathsf{K}}_0\,\mathbf{A}$) *Suppose that every* **A**-*projective module of constant rank* $k+1$ *(*$k \geqslant 1$*) is isomorphic to a module* $\mathbf{A}^k \oplus Q$*. Then the map from* $(\mathsf{Pic}\,\mathbf{A}, \times)$ *to* $(\widetilde{\mathsf{K}}_0\,\mathbf{A}, +)$ *defined by*

$$[P]_{\mathsf{Pic}\,\mathbf{A}} \mapsto [P]_{\mathsf{K}_0\mathbf{A}} - 1_{\mathsf{K}_0\mathbf{A}}$$

is a group isomorphism. In addition, $\mathsf{GK}_0\,\mathbf{A} = \mathsf{K}_0\,\mathbf{A}$ *and its structure is entirely known from that of* $\mathsf{Pic}\,\mathbf{A}$*.*

D The map is injective by Fact 5.6, and surjective by hypothesis. It is a group homomorphism because $\mathbf{A} \oplus (P \otimes Q) \simeq P \oplus Q$, also in virtue of Fact 5.6, since

$$\bigwedge^2 \big(\mathbf{A} \oplus (P \otimes Q)\big) \simeq P \otimes Q \simeq \bigwedge^2 (P \oplus Q).$$

□

Note that the law of $\mathsf{Pic}\,\mathbf{A}$ is inherited from the tensor product whilst that of $\widetilde{\mathsf{K}}_0\,\mathbf{A}$ is inherited from the direct form. We will see in Chapter XIII that the hypothesis of the theorem is satisfied for rings of Krull dimension $\leqslant 1$.

Comment. We have seen in Section 2 how the structure of $\mathsf{H}_0(\mathbf{A})$ directly stems from that of the Boolean algebra $\mathbb{B}(\mathbf{A})$.
From the classical mathematics' point of view the Boolean algebra $\mathbb{B}(\mathbf{A})$ is the algebra of the open and closed sets in $\mathsf{Spec}\,\mathbf{A}$ (the set of prime ideals of $\mathbf{A}$ equipped with a suitable topology, cf. Chapter XIII). An element of $\mathbb{B}(\mathbf{A})$ can therefore be seen as the characteristic function of an open-closed set of $\mathsf{Spec}\,\mathbf{A}$. Then the way in which we construct $\mathsf{H}_0(\mathbf{A})$ from $\mathbb{B}(\mathbf{A})$ shows that $\mathsf{H}_0(\mathbf{A})$ can be seen as the ring of functions with integer values, integral linear combinations of elements in $\mathbb{B}(\mathbf{A})$. It follows that $\mathsf{H}_0(\mathbf{A})$ is identified with the algebra of locally constant functions, with integer values, over $\mathsf{Spec}\,\mathbf{A}$. Still from the point of view of classical mathematics the (generalized) rank of a finitely generated projective $\mathbf{A}$-module P can be seen as the function (with values in $\mathbb{N}$) defined over $\mathsf{Spec}\,\mathbf{A}$ as follows: to a prime ideal $\mathfrak{p}$ we associate the rank of the free module $P_{\mathfrak{p}}$ (over a local ring all the finitely generated projective modules are free). The ring $\mathsf{H}_0(\mathbf{A})$ is indeed obtained simply by symmetrizing the semiring $\mathsf{H}_0^+(\mathbf{A})$ of the ranks of finitely generated projective $\mathbf{A}$-modules. ■

Picard group and class group of a ring

Let us consider the multiplicative monoid of the *finitely generated fractional ideals* of the ring $\mathbf{A}$, formed by the finitely generated $\mathbf{A}$-submodules of the total ring of fractions $\mathrm{Frac}\,\mathbf{A}$. We will denote this monoid by $\mathrm{Ifr}\,\mathbf{A}$.

More generally a *fractional ideal* of $\mathbf{A}$ is an $\mathbf{A}$-submodule $\mathfrak{b}$ of $\mathrm{Frac}\,\mathbf{A}$ such that there exists some regular b in $\mathbf{A}$ satisfying $b\,\mathfrak{b} \subseteq \mathbf{A}$.

In short we can see $\mathrm{Ifr}\,\mathbf{A}$ as the monoid obtained from that of the finitely generated ideals of $\mathbf{A}$ by forcing the invertibility of the principal ideals generated by regular elements.

An ideal $\mathfrak{a} \in \mathrm{Ifr}\,\mathbf{A}$ is sometimes said to be *integral* if it is contained in $\mathbf{A}$, in which case it is a finitely generated ideal of $\mathbf{A}$ in the usual sense.

An arbitrary ideal $\mathfrak{a}$ of $\mathbf{A}$ is invertible like an ideal of $\mathbf{A}$ (in the sense of Definition III-8.19) if and only if it is an invertible element in the monoid $\mathrm{Ifr}\,\mathbf{A}$. Conversely every ideal of $\mathrm{Ifr}\,\mathbf{A}$ invertible in this monoid is of the form $\mathfrak{a}/b$, where $b \in \mathbf{A}$ is regular and $\mathfrak{a}$ is an invertible ideal of $\mathbf{A}$. The invertible elements of $\mathrm{Ifr}\,\mathbf{A}$ form a group, the *group of invertible fractional ideals of* $\mathbf{A}$, which we will denote by $\mathrm{Gfr}\,\mathbf{A}$.

As an $\mathbf{A}$-module, an invertible fractional ideal is projective of constant rank 1. Two invertible ideals are isomorphic as $\mathbf{A}$-modules if they are equal modulo the subgroup of invertible principal ideals (i.e. generated by a regular element of $\mathrm{Frac}\,\mathbf{A}$). We denote by $\mathrm{Cl}\,\mathbf{A}$ the quotient group, that we call the *group of classes of invertible ideals*, or simply the *class group* of the ring $\mathbf{A}$, and we obtain a well-defined natural map $\mathrm{Cl}\,\mathbf{A} \to \mathsf{Pic}\,\mathbf{A}$.

Moreover, let us consider an integral and invertible ideal $\mathfrak{a}$. Since $\mathfrak{a}$ is flat, the natural map $\mathfrak{a} \otimes_{\mathbf{A}} \mathfrak{b} \to \mathfrak{a}\mathfrak{b}$ is an isomorphism, for any ideal $\mathfrak{b}$ (Theorem VIII-1.11). Thus, the map $\mathrm{Cl}\,\mathbf{A} \to \mathsf{Pic}\,\mathbf{A}$ is a group homomorphism, and it is clearly an injective homomorphism, so $\mathrm{Cl}\,\mathbf{A}$ is identified with a subgroup of $\mathsf{Pic}\,\mathbf{A}$.

These two groups are often identical as the following theorem shows, which results from the previous considerations and from Theorem 1.11.

5.8. Theorem. (Modules of constant rank 1 as ideals of $\mathbf{A}$)
Suppose that over $\mathrm{Frac}\,\mathbf{A}$ *every projective module of rank* 1 *is free.*

1. *Every projective* $\mathbf{A}$*-module of rank* 1 *is isomorphic to an invertible ideal of* $\mathbf{A}$*.*
2. *Every projective ideal of rank* 1 *is invertible.*
3. *The group of classes of invertible ideals is naturally isomorphic to the Picard group.*

D Theorem 1.11 shows that every projective module of rank 1 is isomorphic to an ideal $\mathfrak{a}$. It therefore remains to see that such an ideal is invertible. Since it is locally principal it suffices to show that it contains a regular element. For this we consider an integral ideal $\mathfrak{b}$ isomorphic to the inverse of $\mathfrak{a}$ in $\mathsf{Pic}\,\mathbf{A}$. The product of these two ideals is isomorphic to their tensor product (because $\mathfrak{a}$ is flat) so it is a free module, thus it is a principal ideal generated by a regular element. □

NB: With regard to the comparison of $\mathsf{Pic}\,\mathbf{A}$ and $\mathrm{Cl}\,\mathbf{A}$ we will find a more general result in Exercise 16.

The semirings $\mathsf{GK}_0(\mathbf{A})$, $\mathsf{GK}_0(\mathbf{A}_{\mathrm{red}})$ and $\mathsf{GK}_0(\mathbf{A}/\mathrm{Rad}\,\mathbf{A})$

In this subsection we use $\mathrm{Rad}\,\mathbf{A}$, the Jacobson radical of $\mathbf{A}$, which is defined on page 489. We compare the finitely generated projective modules defined over $\mathbf{A}$, those defined over $\mathbf{A}' = \mathbf{A}/\mathrm{Rad}\,\mathbf{A}$ and those defined over $\mathbf{A}_{\mathrm{red}}$.

The scalar extension from $\mathbf{A}$ to $\mathbf{B}$ transforms a finitely generated projective module defined over $\mathbf{A}$ into a finitely generated projective module over $\mathbf{B}$. From a projection matrix point of view, this corresponds to considering the matrix transformed by the homomorphism $\mathbf{A} \to \mathbf{B}$.

5.9. Proposition.
The natural homomorphism from $\mathsf{GK}_0(\mathbf{A})$ *to* $\mathsf{GK}_0(\mathbf{A}/\mathrm{Rad}\,\mathbf{A})$ *is injective, which means that if two finitely generated projective modules E, F over* $\mathbf{A}$ *are isomorphic over* $\mathbf{A}' = \mathbf{A}/\mathrm{Rad}\,\mathbf{A}$*, they also are over* $\mathbf{A}$*. More precisely, if two idempotents matrices P, Q of the same format are conjugated over* $\mathbf{A}'$*, they also are over* $\mathbf{A}$*, with an automorphism which lifts the residual conjugation automorphism.*

D Denote by $\overline{x}$ the object x seen modulo $\text{Rad}\,\mathbf{A}$. Let $C \in \mathbb{M}_n(\mathbf{A})$ be a matrix such that $\overline{C}$ conjugates $\overline{P}$ with $\overline{Q}$. Since $\det C$ is invertible modulo $\text{Rad}\,\mathbf{A}$, $\det C$ is invertible in $\mathbf{A}$ and $C \in \mathbb{GL}_n(\mathbf{A})$. So we have $\overline{Q} = \overline{C\,P\,C^{-1}}$. Even if it means replacing P with $C\,P\,C^{-1}$ we can assume $\overline{Q} = \overline{P}$ and $\overline{C} = \mathrm{I}_n$. In this case we search an invertible matrix A such that $\overline{A} = \mathrm{I}_n$ and $APA^{-1} = Q$.

We remark that QP encodes an $\mathbf{A}$-linear map from $\text{Im}\,P$ to $\text{Im}\,Q$ that residually gives the identity. Similarly $(\mathrm{I}_n - Q)(\mathrm{I}_n - P)$ encodes an $\mathbf{A}$-linear map from $\text{Ker}\,P$ to $\text{Ker}\,Q$ that residually gives the identity. Taking inspiration from the enlargement lemma (Lemma V-2.10), this leads us to the matrix $A = QP + (\mathrm{I}_n - Q)(\mathrm{I}_n - P)$ which realizes $AP = QP = QA$ and $\overline{A} = \mathrm{I}_n$, so A is invertible and $APA^{-1} = Q$.

For two residually isomorphic finitely generated projective modules E and F we use the enlargement lemma which allows us to realize $\overline{E}$ and $\overline{F}$ as images of idempotents conjugated matrices of the same format. □

As for the reduction modulo the nilpotents, we obtain in addition the possibility to lift every finitely generated projective module on account of Corollary III-10.4. Hence the following theorem.

5.10. Theorem. *The natural homomorphism* $\mathsf{GK}_0(\mathbf{A}) \to \mathsf{GK}_0(\mathbf{A}_{\text{red}})$ *is an isomorphism. More precisely, we have the following results.*

1. a. *Every idempotent matrix over* $\mathbf{A}_{\text{red}}$ *is lifted to an idempotent matrix over* $\mathbf{A}$.

   b. *Every finitely generated projective module over* $\mathbf{A}_{\text{red}}$ *comes from a finitely generated projective module over* $\mathbf{A}$.

2. a. *If two idempotent matrices of the same format are conjugated over* $\mathbf{A}_{\text{red}}$*, they also are over* $\mathbf{A}$*, with an automorphism which lifts the residual conjugation automorphism.*

   b. *Two finitely generated projective modules over* $\mathbf{A}$ *isomorphic over* $\mathbf{A}_{\text{red}}$*, are also isomorphic over* $\mathbf{A}$.

The Milnor square

A commutative square (in an arbitrary category) of the following style

$$\begin{tikzcd} A \arrow[r, "i_2"] \arrow[d, "i_1"] & A_2 \arrow[d, "j_2"] \\ A_1 \arrow[r, "j_1"] & A' \end{tikzcd}$$

is called a *Cartesian square* if it defines (A, i_1, i_2) as the limit (or inverse limit, or projective limit) of (A_1, j_1, A'), (A_2, j_2, A'). In an equational category we can take

$$A = \{\, (x_1, x_2) \in A_1 \times A_2 \,|\, j_1(x_1) = j_2(x_2) \,\}\,.$$

The reader will verify for example that given $\mathbf{A} \subseteq \mathbf{B}$ and an ideal $\mathfrak{f}$ of $\mathbf{A}$ which is also an ideal of $\mathbf{B}$ (in other words, $\mathfrak{f}$ is contained in the conductor of $\mathbf{B}$ into $\mathbf{A}$), we have a Cartesian square of commutative rings, defined below.

$$\begin{tikzcd}
\mathbf{A} \arrow[r] \arrow[d, two heads] & \mathbf{B} \arrow[d, two heads] \\
\mathbf{A}/\mathfrak{f} \arrow[r] & \mathbf{B}/\mathfrak{f}
\end{tikzcd}$$

Let $\rho : \mathbf{A} \to \mathbf{B}$ be a homomorphism, M be an $\mathbf{A}$-module and N be a $\mathbf{B}$-module. Recall that an $\mathbf{A}$-linear map $\alpha : M \to N$ is a *scalar extension morphism* (cf. Definition IV-4.10) if and only if the natural $\mathbf{B}$-linear map $\rho_\star(M) \to N$ is an isomorphism.

In the entirety of this subsection we consider in the category of commutative rings the "Milnor square" below on the left, denoted by $\mathcal{A}$, in which j_2 is surjective,

$$\begin{tikzcd}
\mathbf{A} \arrow[r, "i_2"] \arrow[d, "i_1"'] \arrow[dr, phantom, "\textcircled{$\mathcal{A}$}"] & \mathbf{A}_2 \arrow[d, two heads, "j_2"] \\
\mathbf{A}_1 \arrow[r, "j_1"] & \mathbf{A}'
\end{tikzcd}
\qquad
\begin{tikzcd}
M \arrow[r, "\psi_2"] \arrow[d, "\psi_1"] & M_2 \arrow[d, two heads, "\varphi_2"] \\
M_1 \arrow[r, "\varphi_1"] & M'
\end{tikzcd}
\qquad
\begin{tikzcd}
E \arrow[r] \arrow[d] & E_2 \arrow[d, two heads, "{j_2}_\star"] \\
E_1 \arrow[r, "h \circ {j_1}_\star"] & E'
\end{tikzcd}$$

Given an $\mathbf{A}$-module M, an $\mathbf{A}_1$-module M_1, an $\mathbf{A}_2$-module M_2, an $\mathbf{A}'$-module M' and a Cartesian square of $\mathbf{A}$-modules as the one illustrated in the center above, the latter is said to be *adapted to* $\mathcal{A}$, if the ψ_i's and φ_i's are scalar extension morphisms.

Given an $\mathbf{A}_1$-module E_1, an $\mathbf{A}_2$-module E_2, and an isomorphism of $\mathbf{A}'$-modules

$$h : {j_1}_\star(E_1) \to {j_2}_\star(E_2) = E',$$

let $M(E_1, h, E_2) = E$ (above on the right-hand side) be the $\mathbf{A}$-module limit of the diagram

$$\big(E_1, h \circ {j_1}_\star, {j_2}_\star(E_2)\big), \big(E_2, {j_2}_\star, {j_2}_\star(E_2)\big)$$

Note that a priori the obtained Cartesian square is not necessarily adapted to $\mathcal{A}$.

5.11. Theorem. (Milnor's theorem)

1. *Suppose that E_1 and E_2 are finitely generated projective, then*
   a. *E is finitely generated projective,*
   b. *the Cartesian square is adapted to $\mathcal{A}$: the natural homomorphisms ${j_k}_\star(E) \to E_k$ $(k = 1, 2)$ are isomorphisms.*
2. *Every finitely generated projective module over $\mathbf{A}$ is obtained (up to isomorphism) by this procedure.*

We will need the following lemma.

5.12. Lemma. *Let $A \in \mathbf{A}^{m\times n}$, $A_k = i_k(A)$ ($k = 1, 2$), $A' = j_1(A_1) = j_2(A_2)$, $K = \operatorname{Ker} A \subseteq \mathbf{A}^n$, $K_i = \operatorname{Ker} A_i$ ($i = 1, 2$), $K' = \operatorname{Ker} A'$. Then K is the limit (as an $\mathbf{A}$-module) of $K_1 \to K'$ and $K_2 \to K'$.*

D Let $x \in \mathbf{A}^n$, $x_1 = j_{1\star}(x) \in \mathbf{A}_1^n$, $x_2 = j_{2\star}(x) \in \mathbf{A}_2^n$. Since $x \in K$ if and only if $x_i \in K_i$ for $i = 1, 2$, K is indeed the desired limit. □

The reader will notice that the lemma does not apply in general to the submodules that are images of matrices.

Proof of Theorem 5.11. 2. If $V \oplus W = \mathbf{A}^n$, let P be the projective matrix over V parallel to W. If V_1, V_2, V' are the modules obtained by scalar extension to $\mathbf{A}_1$, $\mathbf{A}_2$ and $\mathbf{A}'$, they are identified with kernels of the matrices $P_1 = i_1(\mathrm{I}_n - P)$, $P_2 = i_2(\mathrm{I}_n - P)$, $P' = j_2(\mathrm{I}_n - P_2) = j_1(\mathrm{I}_n - P_1)$, and the lemma applies: V is the limit of $V_1 \to V'$ and $V_2 \to V'$. The isomorphism h is then $\mathrm{Id}_{V'}$. This "miracle" takes place thanks to the identification of $j_{i\star}(V_i)$ and $\operatorname{Ker} P_i$.

1a. Let $P_i \in \mathbb{M}_{n_i}(\mathbf{A}_i)$ be a projector with image isomorphic to E_i ($i = 1, 2$). We dispose of an isomorphism of $\mathbf{A}'$-modules from $\operatorname{Im}\big(j_1(P_1)\big) \in \mathbb{M}_{n_1}(\mathbf{A}')$ to $\operatorname{Im}\big(j_2(P_2)\big) \in \mathbb{M}_{n_2}(\mathbf{A}')$. Let $n = n_1 + n_2$. By the enlargement lemma V-2.10 there exists a matrix $C \in \mathbb{E}_n(\mathbf{A}')$ realizing the conjugation

$$\operatorname{Diag}(j_1(P_1), 0_{n_2}) = C\ \operatorname{Diag}\big(0_{n_1}, j_2(P_2)\big)\ C^{-1}.$$

Since j_2 is surjective (ha ha!), C is lifted to a matrix $C_2 \in \mathbb{E}_n(\mathbf{A}_2)$. Let

$$Q_1 = \operatorname{Diag}(P_1, 0_{n_2}),\ \ Q_2 = C_2\ \operatorname{Diag}(0_{n_1}, P_2)\, C_2^{-1},$$

such that $j_1(Q_1) = j_2(Q_2)$ (not bad, right?). There then exists a unique matrix $Q \in \mathbb{M}_n(\mathbf{A})$ such that $i_1(Q) = Q_1$ and $i_2(Q) = Q_2$. The uniqueness of Q assures $Q^2 = Q$, and the previous lemma applies to show that $\operatorname{Im} Q$ is isomorphic to E (hats off to you, Mr Milnor!).

1b. Results from the fact that $Q_k = i_k(Q)$ and $\operatorname{Im} Q_k \simeq \operatorname{Im} P_k \simeq E_k$ for $k = 1, 2$. □

The following fact is purely categorical and left to the good will of the reader.

5.13. Fact. *Given two Cartesian squares adapted to $\mathcal{A}$ as found below, it amounts to the same thing to take a linear map θ from E to F or to take three linear maps (for the corresponding rings) $\theta_1 : E_1 \to F_1$, $\theta_2 : E_2 \to F_2$*

and $\theta' : E' \to F'$ which make the adequate squares commutative.

$$\begin{tikzcd}
E \arrow[r] \arrow[dd] \arrow[drr, dashed, "\theta"'] & E_1 \arrow[dd] \arrow[drr, "\theta_1"] & & \\
& & F \arrow[r] \arrow[dd] & F_1 \arrow[dd] \\
E_2 \arrow[r] \arrow[drr, "\theta_2"'] & E' \arrow[drr, "\theta'"] & & \\
& & F_2 \arrow[r] & F'
\end{tikzcd}$$

5.14. Corollary.
Consider two modules $E = M(E_1, h, E_2)$ and $F = M(F_1, k, F_2)$ like in Theorem 5.11. Every homomorphism ψ of E in F is obtained using two $\mathbf{A}_i$-module homomorphisms $\psi_i : E_i \to F_i$ compatibles with h and k in the sense that the diagram below is commutative. The homomorphism ψ is an isomorphism if and only if ψ_1 and ψ_2 are isomorphisms.

$$\begin{tikzcd}
{j_1}_\star(E_1) \arrow[r, "{j_1}_\star(\psi_1)"] \arrow[d, "h"] & {j_1}_\star(F_1) \arrow[d, "k"] \\
{j_2}_\star(E_2) \arrow[r, "{j_2}_\star(\psi_2)"] & {j_2}_\star(F_2)
\end{tikzcd}$$

6. A nontrivial example: identification of points on the affine line

Preliminaries

Consider a commutative ring $\mathbf{k}$, the affine line over $\mathbf{k}$ *corresponds to* the $\mathbf{k}$-algebra $\mathbf{k}[t] = \mathbf{B}$. Given s points $\alpha_1, \ldots, \alpha_s$ of $\mathbf{k}$ and orders of multiplicity $e_1, \ldots, e_s \geqslant 1$, we formally define a $\mathbf{k}$-algebra $\mathbf{A}$ which represents the result of the identification of these points with the given multiplicities.

$$\mathbf{A} = \left\{ f \in \mathbf{B} \;\middle|\; f(\alpha_1) = \cdots = f(\alpha_s),\ f^{[\ell]}(\alpha_i) = 0,\, \ell \in [\![1, e_i]\!],\, i \in [\![1..s]\!] \right\}$$

In this definition $f^{[\ell]}$ represents the *Hasse derivative* of the polynomial $f(t)$, i.e. $f^{[\ell]} = f^{(\ell)}/\ell!$ (formally, because the characteristic can be finite). The Hasse derivatives allow us to write a Taylor formula for any ring $\mathbf{k}$.

Let $e = \sum_i e_i$, $x_0 = \prod_i (t - \alpha_i)^{e_i}$ and $x_\ell = t^\ell x_0$ for $\ell \in [\![0..e-1]\!]$. Suppose $e > 1$ without which $\mathbf{A} = \mathbf{B}$. It is clear that the x_ℓ's are in $\mathbf{A}$.

We also assume that the $\alpha_i - \alpha_j$'s are invertible for $i \neq j$. We then have by the Chinese remainder theorem a surjective homomorphism

$$\varphi : \mathbf{B} \to \textstyle\prod_i \big(\mathbf{k}[t]/\langle (t - \alpha_i)^{e_i} \rangle\big)$$

whose kernel is the product of the principal ideals $(t-\alpha_i)^{e_i}\mathbf{B}$, i.e. the ideal $x_0\mathbf{B}$.

6.1. Lemma.

1. *$\mathbf{A}$ is a finitely generated $\mathbf{k}$-algebra, more precisely, $\mathbf{A}=\mathbf{k}[x_0,\dots,x_{e-1}]$.*
2. *$\mathbf{B}=\mathbf{A}\oplus\bigoplus_{1\leqslant\ell<e}\mathbf{k}\,t^\ell$ as a $\mathbf{k}$-module.*
3. *The conductor of $\mathbf{B}$ into $\mathbf{A}$, $\mathfrak{f}=(\mathbf{A}:\mathbf{B})$ is given by*

$$\mathfrak{f}=\langle x_0\rangle_{\mathbf{B}}=\langle x_0,\dots,x_{e-1}\rangle_{\mathbf{A}}\,.$$

D Let $f\in\mathbf{B}$, we express it "in base x_0," $f=r_0+r_1x_0+r_2x_0^2+\cdots$ with $\deg r_i<\deg x_0=e$. For $i\geqslant 1$, by writing $r_ix_0^i=(r_i\,x_0)x_0^{i-1}$ we see that $r_ix_0^i\in\mathbf{k}[x_0,\dots,x_{e-1}]$. This proves that

$$\mathbf{B}=\mathbf{k}[x_0,\dots,x_{e-1}]+\left(\bigoplus\nolimits_{1\leqslant\ell<e}\mathbf{k}\,t^\ell\right).$$

Let $f\in\mathbf{A}$ which we write $g+h$ in the previous decomposition.. We therefore have h in $\mathbf{A}$, and if β is the common value of the $h(\alpha_i)$'s, we obtain the equality $\varphi(h-\beta)=0$. Therefore $h-\beta\in x_0\mathbf{B}$, and since $h\in\bigoplus_{1\leqslant\ell<e}\mathbf{k}\,t^\ell$ (the $\mathbf{k}$-module of the polynomials of degree $<e$ and without a constant term), we obtain $h-\beta=0$ then $h=\beta=0$, so $f\in\mathbf{k}[x_0,\dots,x_{e-1}]$.
In conclusion $\mathbf{A}=\mathbf{k}[x_0,\dots,x_{e-1}]$, items *1* and *2* are proven.
By multiplying the equality of item *2* by x_0 we obtain

$$x_0\mathbf{B}=x_0\,\mathbf{A}\;\oplus\;\bigoplus\nolimits_{\ell\in[\![1..e-1]\!]}x_\ell\,\mathbf{k},$$

then the equality $x_0\,\mathbf{B}=\langle x_0,\dots,x_{e-1}\rangle_{\mathbf{A}}$, which implies $x_0\,\mathbf{B}\subseteq\mathfrak{f}$. Finally, let $f\in\mathfrak{f}$, and so $f\in\mathbf{A}$, and $f=\lambda+g$ with $\lambda\in\mathbf{k}$ and $g\in\langle x_0,\dots,x_{e-1}\rangle_{\mathbf{A}}$. We deduce that $\lambda\in\mathfrak{f}$, which implies $\lambda=0$; indeed, $\lambda t\in\mathbf{A}$, if β is the common value of the $\lambda\alpha_i$'s, we have $\varphi(\lambda t-\beta)=0$, so $\lambda t-\beta\in x_0\,\mathbf{B}$, and since x_0 is a monic polynomial of degree $\geqslant 2$, $\lambda=0$. □

A Milnor square

In the situation described in the previous subsection we have the following Milnor square

$$\begin{tikzcd}
\mathbf{A} \arrow[r] \arrow[d, two heads] & \mathbf{B}=\mathbf{k}[t] \arrow[d, two heads, "\varphi"] \\
\mathbf{k}=\mathbf{A}/\mathfrak{f} \arrow[r, tail, "\Delta"] & \mathbf{B}/\mathfrak{f}\simeq\prod_i\left(\mathbf{k}[t]/\langle(t-\alpha_i)^{e_i}\rangle\right)
\end{tikzcd}$$

In what follows we are interested in projective $\mathbf{A}$-modules of constant rank r obtained by gluing the $\mathbf{B}$-module $\mathbf{B}^r$ and the $\mathbf{k}$-module $\mathbf{k}^r$ together using a $(\mathbf{B}/\mathfrak{f})$-isomorphism

$$h:\Delta_\star(\mathbf{k}^r)\to\varphi_\star(\mathbf{B}^r),$$

as described before Theorem 5.11.
We have denoted by $M(\mathbf{k}^r,h,\mathbf{B}^r)$ such an $\mathbf{A}$-module.

Actually, $\Delta_\star(\mathbf{k}^r)$ and $\varphi_\star(\mathbf{B}^r)$ are both identified with $(\mathbf{B}/\mathfrak{f})^r$, and the isomorphism h is identified with an element of

$$\mathbb{GL}_r(\mathbf{B}/\mathfrak{f}) \simeq \prod_{i=1}^{s} \mathbb{GL}_r(\mathbf{k}[t]/\langle (t-\alpha_i)^{e_i}\rangle).$$

We will use these identifications in the remainder of the text without mentioning them, and, for the sake of convenience, we will encode h^{-1} (and not h) by the s corresponding matrices H_i (with $H_i \in \mathbb{GL}_r(\mathbf{k}[t]/\langle (t-\alpha_i)^{e_i}\rangle)$). The module $M(\mathbf{k}^r, h, \mathbf{B}^r)$ will be denoted by $M(H_1, \dots, H_s)$.

In the case where the projective modules of constant rank over $\mathbf{k}$ and $\mathbf{B} = \mathbf{k}[t]$ are always free, Milnor's theorem affirms that we thus obtain (up to isomorphism) all the projective modules of constant rank r over $\mathbf{A}$.

In the following subsection we give a complete description of the category of projective modules of constant rank over $\mathbf{A}$ obtained by such gluings, in a special case. The one where all the multiplicities are equal to 1.

Identification of points without multiplicities

We now apply the previous conventions by supposing that the multiplicities e_i are all equal to 1.

6.2. Theorem. *With the previous conventions.*

1. *The module $M(H_1, \dots, H_s)$, (with $H_i \in \mathbb{GL}_r(\mathbf{k}[t]/\langle t-\alpha_i\rangle) \simeq \mathbb{GL}_r(\mathbf{k})$) is identified with the $\mathbf{A}$-submodule $M'(H_1, \dots, H_s)$ of $\mathbf{B}^r$ consisting of the elements f of $\mathbf{B}^r$ such that*
$$\forall 1 \leqslant i < j \leqslant s,\ \ H_i \cdot f(\alpha_i) = H_j \cdot f(\alpha_j).$$
In particular, $M'(H_1, \dots, H_s) = M'(HH_1, \dots, HH_s)$ if $H \in \mathbb{GL}_r(\mathbf{k})$.
2. *Let, for $i \in [\![1..s]\!]$,*
$$G_i \in \mathbb{GL}_{r_1}(\mathbf{k}[t]/\langle t-\alpha_i\rangle) \simeq \mathbb{GL}_{r_1}(\mathbf{k}) \quad \text{and}$$
$$H_i \in \mathbb{GL}_{r_2}(\mathbf{k}[t]/\langle t-\alpha_i\rangle) \simeq \mathbb{GL}_{r_2}(\mathbf{k}).$$
An $\mathbf{A}$-linear map ϕ from $M(G_1, \dots, G_s)$ to $M(H_1, \dots, H_s)$ can be encoded by a matrix $\Phi \in \mathbf{B}^{r_2 \times r_1}$ satisfying, for $1 \leqslant i < j \leqslant s$,
$$H_i \cdot \Phi(\alpha_i) \cdot G_i^{-1} = H_j \cdot \Phi(\alpha_j) \cdot G_j^{-1}. \tag{6}$$
Such a matrix sends $M'(G_1, \dots, G_s)$ to $M'(H_1, \dots, H_s)$. The $\mathbf{A}$-linear map ϕ is an isomorphism if and only if $r_1 = r_2$ and the $\Phi(\alpha_i)$'s are invertible.

D The first item has no incidence on the results that follow, and it is left to the reader. The second item is an immediate consequence of Lemma 5.12 and of Corollary 5.14. □

In the following theorem we suppose that

- $\mathbf{k}$ is reduced,

- the projective modules of constant rank over $\mathbf{k}[t]$ are all free,
- the square matrices with determinant 1 are products of elementary matrices, i.e. $\mathbb{SL}_n(\mathbf{k}) = \mathbb{E}_n(\mathbf{k})$ for every n.

For example $\mathbf{k}$ can be a discrete field, a reduced zero-dimensional ring or an integral Euclidean ring. Also note that if the projective modules of constant rank over $\mathbf{k}[t]$ are free, it is a fortiori true for the projective modules of constant rank over $\mathbf{k}$.

6.3. Theorem. *For $a \in \mathbf{k}$ let $J_{r,a} \overset{\text{def}}{=} \mathrm{Diag}(1, \dots, 1, a) \in \mathbb{M}_r(\mathbf{k})$. Under the previous hypotheses we obtain the complete classification of the projective modules of constant rank over the ring $\mathbf{A}$ (we use the previous notations and conventions).*

1. *The modules of constant rank $M(H_1, \dots, H_s)$ and $M(G_1, \dots, G_s)$ are isomorphic if and only if $\det(H_j^{-1} \cdot H_1) = \det(G_j^{-1} \cdot G_1)$ for all j.*
2. *Every projective $\mathbf{A}$-module of constant rank r is isomorphic to a unique module*
$$M_r(a_2, \dots, a_s) \overset{\text{def}}{=} M(\mathrm{I}_r, J_{r,a_2}, \dots, J_{r,a_s}),$$
where the a_i's are in $\mathbf{k}^\times$. In addition
$$M_r(a_2, \dots, a_s) \simeq \mathbf{A}^{r-1} \oplus M_1(a_2, \dots, a_s).$$
3. *Finally, the structure of $\mathsf{GK}_0\,\mathbf{A}$ is specified by*
$$\begin{aligned} M_1(a_2, \dots, a_s) \otimes M_1(b_2, \dots, b_s) &\simeq M_1(a_2 b_2, \dots, a_s b_s) \\ M_1(a_2, \dots, a_s) \oplus M_1(b_2, \dots, b_s) &\simeq \mathbf{A} \oplus M_1(a_2 b_2, \dots, a_s b_s) \end{aligned}$$
In particular, $\mathsf{Pic}(\mathbf{A}) \simeq (\mathbf{k}^\times)^{s-1}$.

D *1.* In case of an isomorphism all the matrices in Equations (6) are invertible, and it amounts to the same thing to ask
$$H_j^{-1} \cdot H_1 \cdot \Phi(\alpha_1) \cdot G_1^{-1} \cdot G_j = \Phi(\alpha_j)$$
for $j \in [\![2..s]\!]$. Since $\Phi = \Phi(t)$ is invertible, its determinant is an invertible element of $\mathbf{k}[t]$, so of $\mathbf{k}$, and all the $\det \Phi(\alpha_i)$'s are equal to $\det \Phi$. Consequently the two modules can only be isomorphic if
$$\det(H_j^{-1} \cdot H_1) = \det(G_j^{-1} \cdot G_1)$$
for all j (this proves in particular the uniqueness of the sequence $a_2, \dots, a_s$ when $M_r(a_2, \dots, a_s)$ is isomorphic to a given projective module of constant rank). Conversely if this condition is satisfied, we can find an elementary matrix Φ which realizes the above conditions. It indeed suffices to have
$$\Phi(\alpha_1) = \mathrm{I}_r \text{ and } \Phi(\alpha_j) = H_j^{-1} \cdot H_1 \cdot G_1^{-1} \cdot G_j,$$
which we obtain by applying the following lemma.

The end of the proof is left to the reader. Recall: if $Q = P_1 \oplus P_2 \simeq \mathbf{A} \oplus P$ (the P_i's are projective of constant rank 1), we have $P \simeq \bigwedge_{\mathbf{A}}^2 Q \simeq P_1 \otimes_{\mathbf{A}} P_2$. □

6.4. Lemma. *Let $\alpha_1, \dots, \alpha_s$ in a commutative ring $\mathbf{k}$ with the invertible differences $\alpha_i - \alpha_j$ for $i \neq j$. Given $A_1, \dots, A_s \in \mathbb{E}_r(\mathbf{k})$, there exists a matrix $A \in \mathbb{E}_r(\mathbf{k}[t])$ such that $A(\alpha_i) = A_i$ for each i.*

D If a matrix $A \in \mathbb{E}_r(\mathbf{k}[t])$ is evaluated in s matrices $A_1, \dots, A_s$, and a matrix $B \in \mathbb{E}_r(\mathbf{k}[t])$ is evaluated in s matrices $B_1, \dots, B_s$, then AB is evaluated in $A_1B_1, \dots, A_sB_s$. Consequently, it suffices to prove the lemma when the A_i's are all equal to I_r except for one which is an elementary matrix. In this case we can make an interpolation à la Lagrange since the elements $\alpha_i - \alpha_j$ are invertible. □

Exercises and problems

Exercise 1. We recommend that the proofs which are not given, or are sketched, or left to the reader, etc, be done. But in particular, we will cover the following cases.

- Prove Propositions 1.8 and 1.9.
- Prove the equivalences in Proposition 2.5 *3*.
- Prove Corollary 3.9.
- Prove Facts 4.7 and 4.8.

Exercise 2. Check the computations in the second local freeness lemma 4.4.

Exercise 3. *(Magic formula to diagonalize a projection matrix)*
Let n be a fixed integer. If $\alpha \in \mathcal{P}_n$ (set of finite subsets of $[\![1..n]\!]$), we consider the canonical projector obtained from I_n by annihilating the diagonal elements whose index is not in α. We denote it by I_α. Let $F \in \mathbb{AG}_n(\mathbf{A})$ be a projector, we will explicate a family (F_α) indexed by $\mathcal{P}_n$ with matrices satisfying the "conjugations"

$$F F_\alpha = F_\alpha \mathrm{I}_\alpha \tag{†}$$

as well as the algebraic identity

$$\sum\nolimits_\alpha \det F_\alpha = 1 \tag{‡}$$

This result provides a new uniform method to explicate the local freeness of a finitely generated projective module: we take the localizations at the comaximal elements $\det(F_\alpha)$, since over the ring $\mathbf{A}[1/\det(F_\alpha)]$ we have $F_\alpha^{-1} F F_\alpha = \mathrm{I}_\alpha$.
We will see that this is realized by the family defined as follows

$$F_\alpha = F\,\mathrm{I}_\alpha + (\mathrm{I}_n - F)(\mathrm{I}_n - \mathrm{I}_\alpha).$$

For example if $\alpha = [\![1..k]\!]$, we have the following block decompositions

$$\mathrm{I}_\alpha = \mathrm{I}_{k,n} = \begin{bmatrix} \mathrm{I}_k & 0 \\ 0 & 0 \end{bmatrix}, \quad F = \begin{bmatrix} F_1 & F_2 \\ F_3 & F_4 \end{bmatrix}, \quad F_\alpha = \begin{bmatrix} F_1 & -F_2 \\ F_3 & \mathrm{I}_{n-k} - F_4 \end{bmatrix}.$$

1. Show (‡). Hint: for two square matrices A and B of order n, we develop the determinant $\det(A+B)$ as a multilinear function of the columns of $A+B$. We obtain a sum of 2^n determinants of matrices obtained by shuffling columns of A and columns of B. We apply this remark with $A = F$ and $B = \mathrm{I}_n - F$.
2. If f and e are two idempotents in a not necessarily commutative ring, and if we let $f * e = fe + (1-f)(1-e)$, show that $f(f*e) = fe = (f*e)e$. With $f = F$ and $e = \mathrm{I}_\alpha$, we obtain $f * e = F_\alpha$ which gives equality (†) above.
3. We now study a few equalities which make $\det F_\alpha$ intervene. Let β be the complementary of α
   - Show that $(1-2f)(1-e-f) = (1-e-f)(1-2e) = f * e$
   - Show that $(1-2e)^2 = (1-2f)^2 = 1$.
   - With $f = F$ and $e = \mathrm{I}_\alpha$, we obtain $(\det F_\alpha)^2 = \big(\det(\mathrm{I}_\beta - F)\big)^2$.
   - Verify that $(1-e)f(1-e) + e(1-f)e = (e-f)^2$.
   - If we let μ_α be the principal minor extracted from F on the indices belonging to α, and μ'_β be the principal minor extracted from $\mathrm{I} - F$ on the indices belonging to β, show that $(\det F_\alpha)^2 = \mu_\alpha \mu'_\beta$.
   Hint: for the above example with $f = F$ and $e = \mathrm{I}_\beta$ the equality in the previous item gives
   $$\begin{bmatrix} F_1 & 0 \\ 0 & \mathrm{I}_{n-k} - F_4 \end{bmatrix} = (\mathrm{I}_\beta - F)^2$$

NB. This uniform method of diagonalization of projection matrices gives a shortcut for the local freeness lemma and for the structure theorem which affirms that a finitely generated projective module is locally free in the strong sense. We have taken the time to prove this structure theorem twice. Once by the Fitting ideals in Chapter V, the other more structurally, in the previous chapter. We hope that the readers will not hold it against us for subjecting them to substantially less elementary proofs in the course than that of Exercise 3. It is because magic formulas certainly are nice things, but they sometimes hide the profound meaning of more elaborate proofs.

Exercise 4. *(Generalization of the previous exercise to the diagonalization of matrices annihilating a split separable polynomial)*
Let a, b, $c \in \mathbf{A}$ such that $(a-b)(a-c)(b-c) \in \mathbf{A}^\times$, i.e. the polynomial
$$f(T) = (T-a)(T-b)(T-c)$$
is separable, and let $A \in \mathbb{M}_n(\mathbf{A})$ be a matrix such that $f(A) = 0$. Consider the Lagrange polynomials $f_a(T) = \frac{(T-b)(T-c)}{(a-b)(a-c)}, \ldots$ that satisfy $f_a + f_b + f_c = 1$. Let $A_a = f_a(A)$, $A_b = f_b(A)$, $A_c = f_c(A)$.

1. Show that $AA_a = aA_a$, i.e. every column vector C of A_a satisfies $AC = aC$.
2. Deduce that if a matrix P has column vectors of A_a or A_b or A_c as its column vectors, then $AP = PD$, where D is a diagonal matrix with a, b or c as its diagonal elements.

3. Using $1 = \det(\mathrm{I}_n) = \det(A_a + A_b + A_c)$ and using the multilinearity of the determinant as a function of the column vectors, show that there exist 3^n matrices P_i that satisfy
   - $\sum_i \det(P_i) = 1$.
   - In $\mathbf{A}[1/\det(P_i)]$, the matrix A is similar to a diagonal matrix with a, b or c as its diagonal elements.
4. If the characteristic polynomial of A is equal to $(T-a)^m(T-b)^p(T-c)^q$, show that several matrices P_i are null and that the sum $\sum_i \det(P_i) = 1$ can be restricted to a family of matrices indexed by a finite set with $\frac{(m+p+q)!}{m!p!q!}$ elements.

Exercise 5. *(Jacobian of the system $P^2 - P = 0$)*
Let $\mathbb{M}_n(\mathbf{A}) \to \mathbb{M}_n(\mathbf{A})$ be the map defined by $P \mapsto P^2 - P$. Its differential at a point$P \in \mathbb{AG}_n(\mathbf{A})$ is

$$\varphi_P : \mathbb{M}_n(\mathbf{A}) \to \mathbb{M}_n(\mathbf{A}),\ H \mapsto HP + PH - H.$$

If we identify $\mathbb{M}_n(\mathbf{A})$ and $\mathbf{A}^{n^2}$, φ_P is given by the Jacobian matrix at the point P of the n^2 equations $P^2 - P = 0$.
By considering

$$\mathbf{A} = \mathbf{G}_n(\mathbb{Z}) = \mathbb{Z}[(X_{ij})_{i,j \in [\![1..n]\!]}] \big/ \big\langle P^2 - P \big\rangle \text{ with } P = (X_{ij}),$$

by Theorem 4.9, the tangent space of the affine scheme $\mathbb{AG}_n$ at the point P is canonically identified with

$$\operatorname{Ker} \varphi_P = \{\, H \in \mathbb{M}_n(\mathbf{A}) \mid HP + PH = H \,\} = \operatorname{Im} \pi_P,$$

where $\pi_P \in \mathbb{AG}_n(\mathbf{A})$ is the projector defined by

$$\pi_P(H) = PH(\mathrm{I}_n - P) + (\mathrm{I}_n - P)HP = PH + HP - 2PHP.$$

This brings us to studying the relations between φ_P and π_P. Illustrate what is stated regarding the Jacobian matrix and the identification of $\mathbb{M}_n(\mathbf{A})$ and $\mathbf{A}^{n^2}$ for $n = 2$. In general show the equalities

$$\varphi_P \circ \pi_P = \pi_P \circ \varphi_P = 0,\ \ (\varphi_P)^2 = \mathrm{I}_n - \pi_P,\ \ (\varphi_P)^3 = \varphi_P,$$
$$\operatorname{Ker} \varphi_P = \operatorname{Ker}(\varphi_P)^2 = \operatorname{Im} \pi_P \ \text{ and } \ \operatorname{Im} \varphi_P = \operatorname{Im}(\varphi_P)^2 = \operatorname{Ker} \pi_P.$$

Exercise 6. Prove the following local characterization of faithful finitely generated projective modules. For some $\mathbf{A}$-module P, the following properties are equivalent.

(a) P is finitely generated projective and faithful.

(b) There exist comaximal elements s_i of $\mathbf{A}$ such that each P_{s_i} is free of rank $h \geqslant 1$ over $\mathbf{A}_{s_i} = \mathbf{A}[1/s_i]$.

(c) P is finitely generated projective and for every element s of $\mathbf{A}$, if P_s is free over the ring $\mathbf{A}_s$, it is of rank $h \geqslant 1$.

Exercise 7. Let $\varphi : P \to Q$ be an $\mathbf{A}$-linear map between finitely generated projective modules and $r \in \mathsf{H}_0^+\,\mathbf{A}$. Express $\operatorname{rk}(P) \leqslant r$ and $\operatorname{rk}(P) \geqslant r$ in terms of the determinantal ideals of a projection matrix with image P.

Exercise 8. *(Projective line and rational fractions)*
1. Let $\mathbf{k}$ be a ring, P, $Q \in \mathbf{k}[u,v]$ be two homogeneous polynomials of degrees p, q. Define

$$g(t) = P(t,1), \quad \widetilde{g}(t) = P(1,t), \quad h(t) = Q(t,1), \quad \widetilde{h}(t) = Q(1,t).$$

a. Show that $\mathrm{Res}(g,p,h,q) = (-1)^{pq}\mathrm{Res}(\widetilde{g},p,\widetilde{h},q)$, value that we denote by $\mathrm{Res}(P,Q)$.

b. Show the inclusion

$$\mathrm{Res}(P,Q)\,\langle u,v\rangle^{p+q-1} \subseteq \langle P,Q\rangle$$

2. Recall that $\mathbb{AG}_{2,1}(\mathbf{k})$ is the subset of $\mathbb{AG}_2(\mathbf{k})$ formed by the projectors of rank 1; we have a projection $F \mapsto \mathrm{Im}\, F$ from $\mathbb{AG}_{2,1}(\mathbf{k})$ to $\mathbb{P}^1(\mathbf{k})$.
When $\mathbf{k}$ is a discrete field and $f \in \mathbf{k}(t)$ is a rational fraction, we associate to f the "morphism," denoted also by f, $\mathbb{P}^1(\mathbf{k}) \xrightarrow{f} \mathbb{P}^1(\mathbf{k})$, which realizes $t \mapsto f(t)$ (for the usual inclusion $\mathbf{k} \subseteq \mathbb{P}^1(\mathbf{k})$).
How do we generalize to an arbitrary ring $\mathbf{k}$?
Explain how we can lift this morphism f to a polynomial map, illustrated below by a doted arrow.

$$\begin{tikzcd}
\mathbb{AG}_{2,1}(\mathbf{k}) \arrow[r, dashed] \arrow[d] \arrow[dr] & \mathbb{AG}_{2,1}(\mathbf{k}) \arrow[d] \\
\mathbb{P}^1(\mathbf{k}) \arrow[r, "f"] & \mathbb{P}^1(\mathbf{k})
\end{tikzcd}$$

3. Treat the examples $f(t) = t^2$, $f(t) = t^d$ and $f(t) = (t^2+1)/t^2$. How is a homography $f(t) = \frac{at+b}{ct+d}$ lifted ($ad - bc \in \mathbf{k}^\times$)?

Exercise 9. *(The fundamental conic or Veronese embedding $\mathbb{P}^1 \to \mathbb{P}^2$)*
When $\mathbf{k}$ is a discrete field, the Veronese embedding $\mathbb{P}^1(\mathbf{k}) \to \mathbb{P}^2(\mathbf{k})$ is defined by

$$(u : v) \mapsto (X = u^2 : Y = uv : Z = v^2).$$

Its image is the "fundamental conic" of $\mathbb{P}^2$ with equation

$$\begin{vmatrix} X & Y \\ Y & Z \end{vmatrix} = XZ - Y^2 = 0.$$

Analogously to Exercise 8 (see also Problem 6), show that we can lift the Veronese morphism to a polynomial map, illustrated below by a dotted arrow.

$$\begin{tikzcd}
\mathbb{AG}_{2,1}(\mathbf{k}) \arrow[r, dashed] \arrow[d, "F\mapsto\mathrm{Im}\,F"'] \arrow[dr] & \mathbb{AG}_{3,1}(\mathbf{k}) \arrow[d, "F\mapsto\mathrm{Im}\,F"] \\
\mathbb{P}^1(\mathbf{k}) \arrow[r, "\text{Veronese}"] & \mathbb{P}^2(\mathbf{k})
\end{tikzcd}$$

Your obtained lift must apply to an arbitrary ring $\mathbf{k}$.

Exercise 10. *(Projection matrices of corank* 1*)* Let $n \geqslant 2$.

1. Let $P \in \mathbb{AG}_{n,n-1}(\mathbf{A})$. Show that $P + \widetilde{P} = \mathrm{I}_n$.

2. If $P \in \mathbb{AG}_n(\mathbf{A})$ satisfies $P + \widetilde{P} = \mathrm{I}_n$, then P is of rank $n-1$.

3. If $P \in \mathbb{M}_n(\mathbf{A})$ satisfies $\det(P) = 0$ and $P + \widetilde{P} = \mathrm{I}_n$, then $P \in \mathbb{AG}_{n,n-1}(\mathbf{A})$.

Exercise 11. In this exercise, $A \in \mathbb{M}_n(\mathbf{A})$ is a matrix of *corank* 1, i.e. of rank $n-1$. Using Exercise 10, show the following items.

1. $\mathrm{Im}\, A = \mathrm{Ker}\, \widetilde{A}$ (projective module of rank $n-1$).

2. $\mathrm{Im}\, \widetilde{A} = \mathrm{Ker}\, A$ (projective module of rank 1).

3. $\mathrm{Im}\ {}^{\mathrm{t}}A = \mathrm{Ker}\ {}^{\mathrm{t}}\widetilde{A}$ (projective module of rank $n-1$).

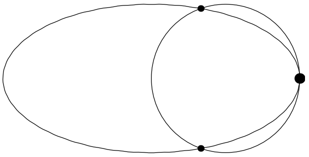
4. $\mathrm{Im}\ {}^{\mathrm{t}}\widetilde{A} = \mathrm{Ker}\ {}^{\mathrm{t}}A$ (projective module of rank 1).

5. The projective modules of rank 1, $\mathbf{A}^n / \mathrm{Im}\, A$ and $\mathbf{A}^n / \mathrm{Im}\ {}^{\mathrm{t}}A$, are duals of one another. In short, from a matrix A of corank 1, we construct two dual projective modules of rank 1

$$\mathbf{A}^n / \mathrm{Im}\, A = \mathbf{A}^n / \mathrm{Ker}\, \widetilde{A} \simeq \mathrm{Im}\, \widetilde{A} = \mathrm{Ker}\, A,$$
$$\mathbf{A}^n / \mathrm{Im}\ {}^{\mathrm{t}}A = \mathbf{A}^n / \mathrm{Ker}\ {}^{\mathrm{t}}\widetilde{A} \simeq \mathrm{Im}\ {}^{\mathrm{t}}\widetilde{A} = \mathrm{Ker}\ {}^{\mathrm{t}}A.$$

Exercise 12. *(Intersection of two affine schemes over* $\mathbf{k}$*)*
This exercise belongs to the informal setting of affine schemes over a ring $\mathbf{k}$ "defined" on page 560. Let $\mathbf{A} = \mathbf{k}[x_1, \dots, x_n]$, $\mathbf{B} = \mathbf{k}[y_1, \dots, y_n]$ be two quotient $\mathbf{k}$-algebras corresponding to two polynomial systems $(\underline{f})$, $(\underline{g})$ in $\mathbf{k}[X_1, \dots, X_n]$. Let A and B be the corresponding affine schemes. The intersection scheme $A \cap B$ is defined as being associated with the $\mathbf{k}$-algebra $\mathbf{k}[\underline{X}] \big/ \left\langle \underline{f}, \underline{g} \right\rangle \simeq \mathbf{A} \otimes_{\mathbf{k}[\underline{X}]} \mathbf{B}$ (note that the tensor product is taken over $\mathbf{k}[\underline{X}]$).

"Justify" this definition by basing yourself on the picture opposite.
In a "Euclidean" coordinate system, the picture includes the ellipse $\left(\frac{x}{a}\right)^2 + y^2 = 1$, i.e. $f(x,y) = 0$ with $f = x^2 + a^2y^2 - a^2$, and the circle $g(x,y) = 0$ with $g = (x-c)^2 + y^2 - (c-a)^2$.



Exercise 13. *(Pseudomonic polynomials)*
Recall that a polynomial $p(t) = \sum_{k \geqslant 0} a_k T^k \in \mathbf{k}[T]$ is said to be pseudomonic if there exists a fundamental system of orthogonal idempotents $(e_0, \dots, e_r)$ such that over each $\mathbf{k}[1/e_j]$, p is a polynomial of degree j with its coefficient of degree j being invertible (see page 391). Such a polynomial is primitive and this notion is stable under product and morphism.

1. Verify that $a_k = 0$ for $k > r$ and that $\left\langle (1 - \sum_{j>k} e_j) a_k \right\rangle = \langle e_k \rangle$ for $k \in [\![0..r]\!]$. In particular, $\langle a_r \rangle = \langle e_r \rangle$ and the e_k's are unique or rather the polynomial $\sum_k e_k X^k$ is unique (we can add null idempotents).

2. Let $P = \mathbf{A}[T]/\langle p \rangle$. Show that P is a finitely generated projective $\mathbf{A}$-module whose polynomial rank is $\mathrm{R}_P(X) = \sum_{k=0}^{r} e_k X^k$; we also have $\deg p = \sum_{k=1}^{r} k[e_k]$ (cf. item *2* of 2.6). In a similar vein, see Exercise 14.

Exercise 14. *(Locally monic polynomials)*
1. Let $\mathfrak{a} \subseteq \mathbf{A}[T]$ be an ideal such that $\mathbf{A}[t] = \mathbf{A}[T]/\mathfrak{a}$ is a free $\mathbf{A}$-module of rank n. Let $f \in \mathbf{A}[T]$ be the characteristic polynomial of t in $\mathbf{A}[t]$. Show that $\mathfrak{a} = \langle f \rangle$. In particular, $1, t, \ldots, t^{n-1}$ is an $\mathbf{A}$-basis of $\mathbf{A}[t]$.

2. Analogous result by replacing the hypothesis "$\mathbf{A}[T]/\mathfrak{a}$ is a free $\mathbf{A}$-module of rank n" with "$\mathbf{A}[T]/\mathfrak{a}$ is a projective module of constant rank n."

A polynomial $f \in \mathbf{A}[T]$ of degree $\leqslant r$ is said to be *locally monic* if there exists a fundamental system of orthogonal idempotents $(e_0, \ldots, e_r)$ such that f is monic of degree d in $\mathbf{A}[1/e_d][T]$ for each $d \in [\![0..r]\!]$. Thus, for each $d \in [\![0..r]\!]$, the polynomial $f_d := e_d f$ is monic of degree d modulo $\langle 1 - e_d \rangle$. It is clear that this definition does not depend on the formal degree r chosen for f, and that over a connected ring, a locally monic polynomial is monic.

3. Characterize a locally monic polynomial using its coefficients.

4. The characteristic polynomial of an endomorphism of a finitely generated projective module M is locally monic and the corresponding fundamental system of orthogonal idempotents is given by the $\mathrm{e}_i(M)$'s.

5. Let $S_1, \ldots, S_m$ be comaximal monoids of $\mathbf{A}$. Show that if f is locally monic (for example monic) over each $S_i^{-1}\mathbf{A}$, it also is locally monic over $\mathbf{A}$.

6. If $f \in \mathbf{A}[T]$ is locally monic, show that the ring $\mathbf{A}[t] = \mathbf{A}[T]/\langle f \rangle$ is a quasi-free $\mathbf{A}$-module and that f is the characteristic polynomial of t.

7. Conversely, if $\mathfrak{a} \subseteq \mathbf{A}[T]$ is an ideal such that the ring $\mathbf{A}[t] = \mathbf{A}[T]/\mathfrak{a}$ is a finitely generated projective $\mathbf{A}$-module, then $\mathfrak{a} = \langle f \rangle$. In particular, if a monogenic $\mathbf{A}$-algebra is a finitely generated projective $\mathbf{A}$-module, it is a quasi-free $\mathbf{A}$-module.

8. For $g \in \mathbf{A}[T]$ the following properties are equivalent.

- g can be written as uf with $u \in \mathbf{A}^\times$ and f locally monic.
- g is pseudomonic.
- $\mathbf{A}[T]/\langle g \rangle$ is a finitely generated projective $\mathbf{A}$-module.

*9**. Prove in classical mathematics that a polynomial is locally monic if and only if it becomes monic after localization at any prime ideal.

Exercise 15. *(Invertible modules and projective modules of constant rank* 1*)*
We propose a slight variation with respect to Theorem 5.8.
1. Let there be two commutative rings $\mathbf{A} \subseteq \mathbf{B}$. The $\mathbf{A}$-submodules of $\mathbf{B}$ form a multiplicative monoid, with neutral element $\mathbf{A}$. Show that an $\mathbf{A}$-submodule M of $\mathbf{B}$ *invertible* in this monoid is finitely generated and that for every $\mathbf{A}$-submodule M' of $\mathbf{B}$ the canonical homomorphism $M \otimes_{\mathbf{A}} M' \to M.M'$ is an isomorphism. Consequently, the invertible $\mathbf{A}$-submodules of $\mathbf{B}$ are projective $\mathbf{A}$-modules of constant rank 1.
2. Let $S \subseteq \mathrm{Reg}(\mathbf{A})$ be a monoid and $\mathfrak{a}$ be a locally principal ideal. Suppose that $S^{-1}\mathfrak{a}$ is an invertible ideal of $S^{-1}\mathbf{A}$; show that $\mathfrak{a}$ is an invertible ideal of $\mathbf{A}$. This is the case, for example, if $S^{-1}\mathfrak{a}$ is a free $S^{-1}\mathbf{A}$-module.

Exercise 16. *(The exact sequence with* $\mathsf{Pic}\,\mathbf{A}$ *and* $\mathsf{Pic}\,\mathbf{K}$*, where* $\mathbf{K} = \mathrm{Frac}\,\mathbf{A}$*)*
Let $\mathbf{A}$ be a ring and $\mathbf{K} = \mathrm{Frac}\,\mathbf{A}$. Define natural group morphisms

$$1 \to \mathbf{A}^{\times} \to \mathbf{K}^{\times} \to \mathrm{Gfr}(\mathbf{A}) \to \mathsf{Pic}\,\mathbf{A} \to \mathsf{Pic}\,\mathbf{K},$$

and show that the obtained sequence is exact. Consequently, we have an exact sequence

$$1 \to \mathrm{Cl}(\mathbf{A}) \to \mathsf{Pic}\,\mathbf{A} \to \mathsf{Pic}\,\mathbf{K}.$$

If $\mathsf{Pic}\,\mathbf{K}$ is trivial, we obtain an isomorphism $\mathrm{Cl}(\mathbf{A}) \simeq \mathsf{Pic}\,\mathbf{A}$, and thus we once again find Theorem 5.8.

Exercise 17. Show that $\mathsf{H}_0\,\mathbf{A}$ is the ring "generated by" $\mathbb{B}(\mathbf{A})$, the Boolean algebra of idempotents of $\mathbf{A}$, in the sense of adjoint functors.
More precisely, if B is a Boolean algebra, the ring $\widetilde{B}$ freely generated by B is given with a homomorphism of Boolean algebras $\eta_B : B \to \mathbb{B}(\widetilde{B})$ such that for every ring $\mathbf{C}$ the map described below is a bijection:

$$\begin{aligned} \mathrm{Hom}_{\mathrm{Rings}}(\widetilde{B}, \mathbf{C}) &\longrightarrow \mathrm{Hom}_{\mathrm{Boolean\ alg.}}\big(B, \mathbb{B}(\mathbf{C})\big) \\ \varphi &\longmapsto \mathbb{B}(\varphi) \circ \eta_B \end{aligned}$$

$$\begin{tikzcd}
\widetilde{B} \arrow[dd, "\varphi"', ""{name=F}] & B \arrow[dd, ""{name=G}] \arrow[dr, "\eta_B"] & \\
& & \mathbb{B}(\widetilde{B}) \arrow[dl, "\mathbb{B}(\varphi)"] \\
\mathbf{C} & \mathbb{B}(\mathbf{C}) &
\arrow[from=F, to=G, squiggly]
\end{tikzcd}$$

Then show that $\widetilde{\mathbb{B}(\mathbf{A})} \simeq \mathsf{H}_0\,\mathbf{A}$.

Exercise 18. Prove in classical mathematics that $\mathsf{H}_0(\mathbf{A})$ is canonically isomorphic to the ring of locally constant (i.e. continuous) functions from $\mathsf{Spec}\,\mathbf{A}$ to $\mathbb{Z}$.

Exercise 19. *(The determinant as a functor)*
We have defined the determinant of an endomorphism of a finitely generated projective module. We will see that more generally we can define the determinant as a functor from the category of projective modules to that of projective modules of rank 1. No doubt, the simplest definition of the determinant of a finitely generated projective module is the following.

Definition:

(*a*) *Let M be a finitely generated projective* $\mathbf{A}$*-module generated by n elements. Let $r_h = \mathrm{e}_h(M)$ ($h \in [\![0..n]\!]$) and $M^{(h)} = r_h M$. Define* $\det(M)$ *by*

$$\det(M) := r_0\mathbf{A} \oplus M^{(1)} \oplus \bigwedge\nolimits^2 M^{(2)} \oplus \cdots \oplus \bigwedge\nolimits^n M^{(n)}.$$

We will also use the suggestive notation $\det(M) = \bigwedge^{\mathrm{rk}(M)} M$ *by using the rank* $\mathrm{rk}(M) = \sum_{k=1}^{n} k\,[\mathrm{e}_k(M)] \in \mathsf{H}_0\,\mathbf{A}$.

(*b*) *If $\varphi : M \to N$ is a homomorphism of finitely generated projective* $\mathbf{A}$*-modules, with $s_h = \mathrm{e}_h(N)$, we define* $\det(\varphi)$ *as a homomorphism of* $\det(M)$ *in* $\det(N)$ *sending $\bigwedge^h M^{(h)}$ to $\bigwedge^h N^{(h)}$ by $x \mapsto s_h(\bigwedge^h \varphi)(x)$.*

We will note that when $x \in \bigwedge^h M^{(h)}$ we have $x = r_h x$.

1. The module $\det(M)$ is a projective module of constant rank 1, and we have the equalities $r_h \det(M) = \det(M)_{r_h} = \bigwedge^h M^{(h)}$. More generally, for every idempotent e, we have $e\det(M) = \det(M_e)$.

2. The previous definition provides a functor that commutes with the localization and transforms the direct sums into tensor products. Deduce that the functor det induces a surjective morphism from $(\mathsf{K}_0\,\mathbf{A},+)$ to $\mathsf{Pic}\,\mathbf{A}$.
3. A homomorphism between finitely generated projective modules is an isomorphism if and only if its determinant is an isomorphism.
4. For an endomorphism of a finitely generated projective module, the new definition of the determinant coincides with the previous one if we identify $\mathrm{End}(L)$ with $\mathbf{A}$ when L is a projective module of constant rank 1.

Exercise 20. Show that, up to isomorphism, the determinant functor is the only functor from the category of finitely generated projective $\mathbf{A}$-modules in itself which possesses the following properties:

- it transforms every arrow $\varphi : \mathbf{A} \to \mathbf{A}$ in itself,
- it transforms the direct sums into tensor products,
- it commutes to the scalar extension for every change of basis $\alpha : \mathbf{A} \to \mathbf{B}$.

Exercise 21. *(Determinantal ideals of a linear map between finitely generated projective modules)* Let $\varphi : M \to N$ be a homomorphism between finitely generated projective modules. Let us write $M \oplus M' \simeq \mathbf{A}^m$, $N \oplus N' \simeq \mathbf{A}^n$, and extend φ to

$$\psi : M \oplus M' \to N \oplus N' \ \text{ with } \ \psi(x + x') = \varphi(x)\ (x \in M,\, x' \in M').$$

Show that, for each integer h, the determinantal ideal $\mathcal{D}_h(\psi)$ only depends on h and on φ. We denote it by $\mathcal{D}_h(\varphi)$ and we call it *the determinantal ideal of order h of φ*.

6.5. Notation. Let $r = \sum_{k=1}^{n} k\,[r_k] \in \mathsf{H}_0^+(\mathbf{A})$. Applying the previous exercise, we call *determinantal ideal of type r for φ* and we denote by $\mathcal{D}_r(\varphi)$ the ideal

$$r_0\mathbf{A} + r_1\mathcal{D}_1(\varphi) + \cdots + r_n\mathcal{D}_n(\varphi).$$

The notations $\mathrm{rk}(\varphi) \geqslant k$ and $\mathrm{rk}(\varphi) \leqslant k$ for the linear maps between free modules of finite rank are generalized as follows to the linear maps between finitely generated projective modules: let $\mathrm{rk}(\varphi) \geqslant r$ if $\mathcal{D}_r(\varphi) = \langle 1 \rangle$, $\mathrm{rk}(\varphi) \leqslant r$ if $\mathcal{D}_{1+r}(\varphi) = \langle 0 \rangle$, and $\mathrm{rk}(\varphi) = r$ if $\mathrm{rk}(\varphi) \leqslant r$ and $\mathrm{rk}(\varphi) \geqslant r$.
NB: see Exercise 23.

Exercise 22. (Continuation of Exercise 21) Let $r \in \mathbb{N}^*$.

1. If $M \xrightarrow{\varphi} N \xrightarrow{\varphi'} L$ are linear maps between finitely generated projective modules, we have $\mathcal{D}_r(\varphi'\varphi) \subseteq \mathcal{D}_r(\varphi')\mathcal{D}_r(\varphi)$.
2. If S is a monoid of $\mathbf{A}$, then $\big(\mathcal{D}_r(\varphi)\big)_S = \mathcal{D}_r(\varphi_S)$.
3. For every $s \in \mathbf{A}$ such that M_s and N_s are free, we have $\big(\mathcal{D}_r(\varphi)\big)_s = \mathcal{D}_r(\varphi_s)$. In addition, this property characterizes the ideal $\mathcal{D}_r(\varphi)$.

Let $r = \sum_{k\in[\![1..n]\!]} k[r_k] \in \mathsf{H}_0^+\,\mathbf{A}$.

4. Redo the previous items of the exercise in this new context.

Exercise 23. (With notations 6.5) Let $\varphi : M \to N$ be a linear map between finitely generated projective $\mathbf{A}$-modules. Prove that the following properties are equivalent.
1. φ is locally simple.
2. φ has a well-defined rank in $\mathsf{H}_0^+(\mathbf{A})$.
3. After localization at comaximal elements, the modules are free and the linear map is simple.

Exercise 24. Let $A \in \mathbf{A}^{n\times m}$; if A is of rank $m-1$, we can explicate a finite system of generators of the submodule $\operatorname{Ker} A \subseteq \mathbf{A}^n$ without using neither an equality test nor a membership test. In fact, under the only (weaker) hypothesis $n \geqslant m-1$, we uniformly define a matrix $A' \in \mathbf{A}^{m\times N}$ with $N = \binom{n}{m-1}$ which is "a kind of comatrix of $\mathbf{A}$." This matrix satisfies $\operatorname{Im} A' \subseteq \operatorname{Ker} A$ as soon as A is of rank $\leqslant m-1$, with equality when A is of rank $m-1$.

We can define $A' \in \mathbf{A}^{m\times N}$ via the exterior algebra: we see A as a linear map $u : \mathbf{A}^m \to \mathbf{A}^n$ and we consider $u' = \bigwedge^{m-1}({}^{\mathrm{t}}u) : \bigwedge^{m-1}(\mathbf{A}^n) \to \bigwedge^{m-1}(\mathbf{A}^m)$. In the canonical bases, $\bigwedge^{m-1}(\mathbf{A}^n) = \mathbf{A}^N$ and $\bigwedge^{m-1}(\mathbf{A}^m) = \mathbf{A}^m$, so u' is represented by a matrix $A' \in \mathbf{A}^{m\times N}$. To explicate this matrix A', we order the set of $N = \binom{n}{m-1}$ subsets I of $⟦1..n⟧$ of cardinality $m-1$ such that their complements are in increasing lexicographic order; the columns of A' are indexed by this set of subsets, as follows

$$a'_{j,I} = (-1)^{k_I + j} \det(A_{I,\{1..m\}\setminus\{j\}}), \qquad k_I \text{ being the number of } I.$$

For example, if $m = 2$, then $N = n$, and $A' = \begin{bmatrix} a_{n,2} & -a_{n-1,2} & \cdots & \pm a_{1,2} \\ -a_{n,1} & a_{n-1,1} & \cdots & \mp a_{1,1} \end{bmatrix}$.

1. For $i \in ⟦1..n⟧$, we have $(AA')_{i,I} = (-1)^{k_I+1} \det(A_{\{i\}\cup I,\{1..m\}})$. In particular, if $\mathcal{D}_m(A) = 0$, then $AA' = 0$.

2. If $n = m$, then $A' = \widetilde{A}$ (the comatrix of A).

3. If A is of rank $m-1$, then $\operatorname{Im} A' = \operatorname{Ker} A$; in particular, A' is of rank 1.

4. Every stably free module of rank 1 is free. We will be able to compare with Fact 5.6 and with Exercise V-13.

5. If B is a matrix satisfying $ABA = A$, then $P = BA$ is a projection matrix satisfying $\operatorname{Im}(\mathrm{I}_n - P) = \operatorname{Ker} P = \operatorname{Ker} A$. This provides another way to answer the question: give a finite system of generators of $\operatorname{Ker} A$. Compare this other solution to that of the current exercise. To compute the matrix P, we will be able to use the method explained in Section II-5 (Theorem II-5.14). Another method, considerably more economical, can be found in [61, Díaz-Toca&al.] (based on [143, Mulmuley]).

Exercise 25. *(Homogeneous polynomials and* $\mathbb{P}^n(\mathbf{k})$*)*
Let $(f_1, \ldots, f_s) = (\underline{f})$ in $\mathbf{k}[X_0, \ldots, X_n]$ be a homogeneous polynomial system. We seek to define the zeros of $(\underline{f})$ in $\mathbb{P}^n(\mathbf{k})$. Let P be a point of $\mathbb{P}^n(\mathbf{k})$, i.e. a projective $\mathbf{k}$-module of rank 1 which is a direct summand in $\mathbf{k}^{n+1}$. Show that if a generator set of P annihilates $(\underline{f})$, then every element of P annihilates $(\underline{f})$.

Exercise 26. *(Tangent space to $\mathbb{GL}_n$)*
Determine the tangent space at a point to the functor $\mathbf{k} \mapsto \mathbb{GL}_n(\mathbf{k})$.

Exercise 27. *(Tangent space to $\mathbb{SL}_n$)*
Determine the tangent space at a point to the functor $\mathbf{k} \mapsto \mathbb{SL}_n(\mathbf{k})$.

Exercise 28. *(Tangent space at J_0 to the nilpotent cone)* Let $\mathbf{k}$ be a ring. Let $(e_{ij})_{i,j\in[\![1..n]\!]}$ be the canonical basis of $\mathbb{M}_n(\mathbf{k})$ and $J_0 \in \mathbb{M}_n(\mathbf{k})$ be the standard Jordan matrix. For example, for $n = 3$, $J_0 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}$.

1. We define $\varphi : \mathbb{M}_n(\mathbf{k}) \to \mathbb{M}_n(\mathbf{k})$ by $\varphi(H) = \sum_{i+j=n-1} J_0^i H J_0^j$.
Determine $\operatorname{Im}\varphi$.

2. Give a direct complement of $\operatorname{Im}\varphi$ in $\mathbb{M}_n(\mathbf{k})$, then give $\psi : \mathbb{M}_n(\mathbf{k}) \to \mathbb{M}_n(\mathbf{k})$ satisfying $\varphi \circ \psi \circ \varphi = \varphi$. Show that $\operatorname{Ker}\varphi$ is free of rank $n^2 - n$ and give a basis of this module.

3. Consider the functor $\mathbf{k} \mapsto \{N \in \mathbb{M}_n(\mathbf{k}) \mid N^n = 0\}$. Determine the tangent space at J_0 to this functor.

Exercise 29. *(Complement of Theorem 4.9)* Let $\mathbf{A}[\varepsilon] = \mathbf{A}[T]/\langle T^2 \rangle$.
Let P, $H \in \mathbb{M}_n(\mathbf{A})$. Show that the matrix $P + \varepsilon H$ is idempotent if and only if

$$P^2 = P \quad \text{and} \quad H = HP + PH.$$

Generalize to an abstract noncommutative ring with an idempotent ε in the center of the ring.

Comment. The example of the ring $\mathbb{M}_n(\mathbf{A})$ shows that in the noncommutative case the situation for the idempotents is quite different from the one in the commutative case where $\mathbb{B}(\mathbf{A}) = \mathbb{B}(\mathbf{A}_{\text{red}})$ (Corollary III-10.4) and where the idempotents are "isolated" (Lemma IX-5.1). ■

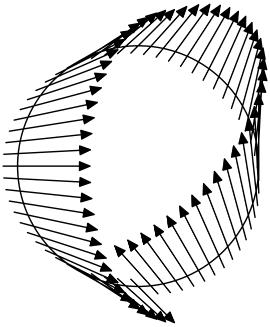
Problem 1. *(The ring of the circle)*
Let $\mathbf{k}$ be a discrete field of characteristic $\neq 2$, $f(X,Y) = X^2 + Y^2 - 1 \in \mathbf{k}[X,Y]$. It is an irreducible and smooth polynomial, i.e. $1 \in \langle f, \frac{\partial f}{\partial X}, \frac{\partial f}{\partial Y} \rangle$ (explicitly, we have $-2 = 2f - X\frac{\partial f}{\partial X} - Y\frac{\partial f}{\partial Y}$).
It is therefore licit to think that the ring $\mathbf{A} = \mathbf{k}[X,Y]/\langle f \rangle = \mathbf{k}[x,y]$ is an integral Prüfer ring. This will be proven in Problem XII-1 (item *4*).
Let $\mathbf{K}$ be its field of fractions and let $t = \frac{y}{x-1} \in \mathbf{K}$.

1. Show that $\mathbf{K} = \mathbf{k}(t)$; geometrically justify how to find t (parameterization of a conic having a $\mathbf{k}$-rational point) and make x, y explicit in terms of t.
2. Let $u = (1+t^2)^{-1}$, $v = tu$. Verify that the integral closure of $\mathbf{k}[u]$ in $\mathbf{K} = \mathbf{k}(t)$ is

$$\mathbf{k}[x,y] = \mathbf{k}[u,v] = \left\{ h(t)/(1+t^2)^s \,|\, h \in \mathbf{k}[t],\ \deg(h) \leqslant 2s \right\}.$$

   In particular, $\mathbf{A} = \mathbf{k}[x,y]$ is integrally closed. Explain how the $\mathbf{k}$-circle $x^2 + y^2 = 1$ is the projective line $\mathbb{P}^1(\mathbf{k})$ deprived "of the $\mathbf{k}$-point" $(x,y) = (1, \pm i)$.

3. If -1 is a square in $\mathbf{k}$, show that $\mathbf{k}[x,y]$ is a localized ring $\mathbf{k}[w,w^{-1}]$ (for some w to explicate) of a polynomial ring over $\mathbf{k}$, therefore a Bézout ring.
4. Let $P_0=(x_0,y_0)$ be a $\mathbf{k}$-point of the circle $x^2+y^2=1$ and $\langle x-x_0,y-y_0\rangle\subseteq\mathbf{A}$ be its maximal ideal. Verify that $\langle x-x_0,y-y_0\rangle^2$ is a principal ideal of generator xx_0+yy_0-1. Geometric interpretation of xx_0+yy_0-1?
5. Here $(x_0,y_0)=(1,0)$. Describe the computations allowing to explicate the (projection) matrix
$$P=\tfrac{1}{2}\begin{bmatrix}1-x & -y\\ -y & 1+x\end{bmatrix}$$
as a principal localization matrix for the pair $(x-1,y)$. The exact sequence
$$\mathbf{A}^2\xrightarrow{\mathrm{I}_2-P}\mathbf{A}^2\xrightarrow{(x-1,y)}\langle x-1,y\rangle\to 0$$
allows us to realize the (invertible) ideal of the point $(1,0)$ as the image of the projector P of rank 1.
Comment on the opposite picture which is its geometric counterpart (vector line bundle of the circle).



6. Suppose that -1 is not a square in $\mathbf{k}$ and that we see $\mathbf{k}[x,y]$ as a free $\mathbf{k}[x]$-algebra of rank 2, with basis $(1,y)$. Explicate the norm and verify, for $z=a(x)+b(x)y\neq 0$, the equality
$$\deg \mathrm{N}_{\mathbf{k}[x,y]/\mathbf{k}[x]}(z)=2\max(\deg a,1+\deg b).$$
In particular, $\deg \mathrm{N}_{\mathbf{k}[x,y]/\mathbf{k}[x]}(z)$ is even. Deduce the group $\mathbf{k}[x,y]^\times$, the fact that y and $1\pm x$ are irreducible in $\mathbf{k}[x,y]$, and that the ideal $\langle x-1,y\rangle$ of the point $(1,0)$ is not principal (i.e. the line bundle above is not trivial).

Problem 2. *(The operations λ_t and γ_t over $\mathsf{K}_0(\mathbf{A})$)*
If P is a finitely generated projective module over $\mathbf{A}$, let, for $n\in\mathbb{N}$, $\lambda^n(P)$ or $\lambda^n([P])$ be the class of $\bigwedge^n P$ in $\mathsf{K}_0(\mathbf{A})$ and we have the fundamental equality
$$\lambda^n(P\oplus Q)=\textstyle\sum_{p+q=n}\lambda^p(P)\lambda^q(Q).\qquad (*)$$
We also define the polynomial $\lambda_t(P)\in\mathsf{K}_0(A)[t]$ by $\lambda_t(P)=\sum_{n\geqslant 0}\lambda^n(P)t^n$. It is a polynomial of constant term 1 that we consider in the ring of formal series $\mathsf{K}_0(A)[[t]]$. Then
$$\lambda_t(P)\ \in\ 1+t\,\mathsf{K}_0(\mathbf{A})[[t]]\ \subseteq\ (\mathsf{K}_0(\mathbf{A})[[t]])^\times.$$
By $(*)$ we have $\lambda_t(P\oplus Q)=\lambda_t(P)\lambda_t(Q)$, which allows us to extend λ_t to a morphism $(\mathsf{K}_0(\mathbf{A}),+)\to(1+t\,\mathsf{K}_0(\mathbf{A})[[t]],\times)$. Thus if P, Q are two finitely generated projective modules, for $x=[P]-[Q]$, we have by definition
$$\lambda_t(x)=\frac{\lambda_t(P)}{\lambda_t(Q)}=\frac{1+\lambda^1(P)t+\lambda^2(P)t^2+\cdots}{1+\lambda^1(Q)t+\lambda^2(Q)t^2+\cdots}$$
sequence that we will denote by $\sum_{n\geqslant 0}\lambda^n(x)t^n$, with $\lambda^0(x)=1$, $\lambda^1(x)=x$.

Grothendieck has also defined over $\mathsf{K}_0(\mathbf{A})$ another operation γ_t by the equality

$$\gamma_t(x) = \lambda_{t/(1-t)}(x),$$

for $x \in \mathsf{K}_0(\mathbf{A})$. This is licit because the multiplicative subgroup $1 + t\,\mathsf{K}_0(\mathbf{A})[[t]]$ is stable by the substitution $t \leftarrow t/(1-t)$. This substitution $t \leftarrow t/(1-t)$ leaves the term invariant in t, let

$$\gamma_t(x) \;=\; 1 + tx + t^2\big(x + \lambda^2(x)\big) + \cdots \;=\; \textstyle\sum_{n \geqslant 0} \gamma^n(x) t^n.$$

1. Give $\lambda_t(p)$ and $\gamma_t(p)$ for $p \in \mathbb{N}^*$. Let $x \in \widetilde{\mathsf{K}}_0\,\mathbf{A}$. Show that $\gamma_t(x)$ is a polynomial t. By using $\gamma_t(-x)$, deduce that x is nilpotent.

2. Show that $\widetilde{\mathsf{K}}_0(\mathbf{A})$ is the nilradical of the ring $\mathsf{K}_0(\mathbf{A})$.

We have $\operatorname{rk}\big(\lambda^n(x)\big) = \lambda^n(\operatorname{rk} x)$ and thus we dispose of a formal sequence $\operatorname{rk}_t^\lambda(x)$ with coefficients in $\mathsf{H}_0\,\mathbf{A}$ defined by

$$\operatorname{rk}_t^\lambda(x) = \lambda_t(\operatorname{rk} x) = \textstyle\sum_{n \geqslant 0} \operatorname{rk}\big(\lambda^n(x)\big) t^n.$$

If $x \in \mathsf{H}_0\,\mathbf{A}$ this simply gives $\operatorname{rk}_t^\lambda(x) = \lambda_t(x)$.

3. If $x = [P]$, recall that $(1+t)^{\operatorname{rk} x} = \mathrm{R}_P(1+t) = \mathrm{F}_{\mathrm{Id}_P}(t) \in \mathbb{B}(\mathbf{A})[t]$. Show that, when we identify $\mathbb{B}(\mathbf{A})$ with $\mathbb{B}(\mathsf{H}_0\,\mathbf{A})$ by letting $e = [e\mathbf{A}] = [e]$ for $e \in \mathbb{B}(\mathbf{A})$, we obtain $\operatorname{rk}_t^\lambda(x) = 1 + t \operatorname{rk} x = (1+t)^{\operatorname{rk} x}$ if $0 \leqslant \operatorname{rk} x \leqslant 1$.
Then show that $\operatorname{rk}_t^\lambda(x) = (1+t)^{\operatorname{rk} x}$ for every $x \in \mathsf{K}_0(\mathbf{A})$.

4. We define $\operatorname{rk}_t^\gamma(x) = \gamma_t(\operatorname{rk} x) = \sum_{n \geqslant 0} \operatorname{rk}\big(\gamma^n(x)\big) t^n$.
Show that $\operatorname{rk}_t^\gamma(x) = (1-t)^{-\operatorname{rk} x}$ for every $x \in \mathsf{K}_0(\mathbf{A})$, or for $x = [P]$ that $\operatorname{rk}_t^\gamma(x) = \mathrm{R}_P\big(1/(1-t)\big) = \mathrm{R}_P(1-t)^{-1}$. In addition, if $0 \leqslant \operatorname{rk} x \leqslant 1$, we obtain the equality $\operatorname{rk}_t^\gamma(x) = 1 + xt/(1-t) = 1 + xt + xt^2 + \ldots$

5. For all x of $\mathsf{K}_0\,\mathbf{A}$, $\gamma_t(x)(1-t)^{\operatorname{rk}(x)}$ is a polynomial.

6. Show the reciprocity formulas between λ^n and γ^n for $n \geqslant 1$

$$\gamma^n(x) = \textstyle\sum_{p=0}^{n-1} \binom{n-1}{p} \lambda^{p+1}(x), \qquad \lambda^n(x) = \sum_{q=0}^{n-1} \binom{n-1}{q} (-1)^{n-1-q} \gamma^{q+1}(x).$$

Problem 3. *(The projective map of Noether and the projective modules of constant rank* 1 *direct summands in* $\mathbf{k}^2$*)*
Fix a ring $\mathbf{k}$, two indeterminates X, Y over $\mathbf{k}$ and an integer $n \geqslant 1$. Given two n-sequences of elements of $\mathbf{k}$, $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$, we associate with them an $(n+1)$-sequence $z = z(x,y) = (z_0, \ldots, z_n)$ as follows

$$\textstyle\prod_{i=1}^n (x_i X + y_i Y) = z_0 X^n + z_1 X^{n-1} Y + \cdots + z_{n-1} X Y^{n-1} + z_n Y^n.$$

Thus, we have $z_0 = x_1 \cdots x_n$, $z_n = y_1 \cdots y_n$, and for example, for $n = 3$,

$$z_1 = x_1 x_2 y_3 + x_1 x_3 y_2 + x_2 x_3 y_1, \quad z_2 = x_1 y_2 y_3 + x_2 y_1 y_3 + x_3 y_1 y_2.$$

For $d \in [\![0..n]\!]$, we easily check that $z_d(y,x) = z_{n-d}(x,y)$ and that we have the following formal expression thanks to the elementary symmetric functions with n indeterminates $(S_0 = 1, S_1, \ldots, S_n)$:

$$z_d = x_1 \cdots x_n S_d(y_1/x_1, \ldots, y_n/x_n).$$

In particular, z_d is homogeneous in x of degree $n - d$, and homogeneous in y of degree d. We can give a direct definition of z_d as follows

$$z_d = \textstyle\sum_{\#I = n-d} \prod_{i \in I} x_i \prod_{j \in [\![1..n]\!] \setminus I} y_j.$$

If $\mathbf{k}$ is a discrete field, we have a map $\psi : (\mathbb{P}^1)^n = \mathbb{P}^1 \times \cdots \times \mathbb{P}^1 \to \mathbb{P}^n$, said to be Noetherian, defined by

$$(\star) \qquad \psi : \big((x_1 : y_1), \ldots, (x_n : y_n)\big) \mapsto (z_0 : \cdots : z_n)$$

We make the symmetric group S_n act on the product $(\mathbb{P}^1)^n$ by permutation of the coordinates; then the map $(\star)$ above, which is S_n-invariant, intervenes in algebraic geometry to make $(\mathbb{P}^1)^n/\mathrm{S}_n$ and $\mathbb{P}^n$ isomorphic.

1. Show that for $P_1, \ldots, P_n, Q_1, \ldots, Q_n$ in $\mathbb{P}^1$, we have

$$\psi(P_1, \ldots, P_n) = \psi(Q_1, \ldots, Q_n) \iff (Q_1, \ldots, Q_n) \text{ is a permutation of } (P_1, \ldots, P_n).$$

We now want, $\mathbf{k}$ being an arbitrary ring, to formulate the map $(\star)$ in terms of projective $\mathbf{k}$-modules of constant rank 1.

Precisely, let $L = \mathbf{k}X \oplus \mathbf{k}Y \simeq \mathbf{k}^2$, and let

$$S_n(L) = \mathbf{k}X^n \oplus \mathbf{k}X^{n-1}Y \oplus \cdots \oplus \mathbf{k}XY^{n-1} \oplus \mathbf{k}Y^n \simeq \mathbf{k}^{n+1}$$

be the homogeneous component of degree n of $\mathbf{k}[X, Y]$. If $P_1, \ldots, P_n \subset L$ are n projective $\mathbf{k}$-submodules of constant rank 1 which are direct summands, we want to associate with them, functorially, a $\mathbf{k}$-submodule $P = \psi(P_1, \ldots, P_n)$ of $S_n(L)$, projective of constant rank 1 and a direct summand. Of course, we must have

$$\psi(P_1, \ldots, P_n) = \psi(P_{\sigma(1)}, \ldots, P_{\sigma(n)})$$

for every permutation $\sigma \in \mathrm{S}_n$. In addition, if each P_i is free with basis $x_iX + y_iY$, then P must be free with basis $\sum_{i=0}^{n} z_i X^{n-i} Y^i$, in order to find $(\star)$.

2. Show that if each (x_i, y_i) is unimodular, the same holds for $(z_0, \ldots, z_n)$.

3. Define $\psi(P_1, \ldots, P_n) \subset S_n(L)$ thanks to the module $P_1 \otimes_{\mathbf{k}} \cdots \otimes_{\mathbf{k}} P_n$ and to the $\mathbf{k}$-linear map $\pi : L^{n\otimes} \twoheadrightarrow S_n(L)$,

$$\pi : \textstyle\bigotimes_{i=1}^{n} (x_iX + y_iY) \longmapsto \prod_{i=1}^{n} (x_iX + y_iY).$$

4. Let $\mathbf{k}[\underline{Z}] = \mathbf{k}[Z_0, \ldots, Z_n]$, $\mathbf{k}[\underline{X}, \underline{Y}] = \mathbf{k}[X_1, Y_1, \ldots, X_n, Y_n]$.

What to say about the $\mathbf{k}$-morphism $\varphi : \mathbf{k}[\underline{Z}] \to \mathbf{k}[\underline{X}, \underline{Y}]$ defined by

$$Z_d \longmapsto z_d = \textstyle\sum_{\#I=n-d} \prod_{i \in I} X_i \prod_{j \in [\![1..n]\!] \setminus I} Y_j \quad ?$$

NB: φ is the co-morphism of ψ.

Problem 4. *(Hilbert's theorem 90, multiplicative form)*

Let G be a finite group acting on a commutative ring $\mathbf{B}$; a 1-*cocycle* of G over $\mathbf{B}^\times$ is a family $(c_\sigma)_{\sigma \in G}$ such that $c_{\sigma\tau} = c_\sigma \sigma(c_\tau)$; consequently, $c_{\mathrm{Id}} = 1$. For every element $b \in \mathbf{B}^\times$, $(\sigma(b)b^{-1})_{\sigma \in G}$ is a 1-cocycle called a 1-*coboundary.*

Let $Z^1(G, \mathbf{B}^\times)$ be the set of 1-cocycles of G over $\mathbf{B}^\times$; it is a subgroup of the (commutative) group of all the maps of G in $\mathbf{B}^\times$ equipped with the final product. The map $\mathbf{B}^\times \to Z^1(G, \mathbf{B}^\times)$, $b \mapsto (\sigma(b)b^{-1})_{\sigma \in G}$, is a morphism; let $B^1(G, \mathbf{B}^\times)$ be its image and we define *the first group of cohomology of G over* $\mathbf{B}^\times$

$$H^1(G, \mathbf{B}^\times) = Z^1(G, \mathbf{B}^\times) \big/ B^1(G, \mathbf{B}^\times)\ .$$

Finally, we define the (generally noncommutative) ring $\mathbf{B}\{G\}$ as being the $\mathbf{B}$-module with basis G, equipped with the product $(b\sigma) \cdot (b'\sigma') = b\sigma(b')\sigma\sigma'$. Then $\mathbf{B}$ becomes a $\mathbf{B}\{G\}$-algebra via $\left(\sum_\sigma b_\sigma \sigma\right) \cdot b = \sum_\sigma b_\sigma \sigma(b)$.

We call $\mathbf{B}\{G\}$ *the twisted group algebra of the group G.*

Let $(\mathbf{A}, \mathbf{B}, G)$ be a Galois algebra. The aim of the problem is to associate with every 1-cocycle $c = (c_\sigma)_{\sigma \in G}$ a projective $\mathbf{A}$-module of constant rank 1 denoted by $\mathbf{B}_c^G$ and to show that $c \mapsto \mathbf{B}_c^G$ defines an injective morphism of $H^1(G, \mathbf{B}^\times)$ in $\mathsf{Pic}(\mathbf{A})$. In particular, if $\mathsf{Pic}(\mathbf{A})$ is trivial, then every 1-cocycle of G over $\mathbf{B}^\times$ is a coboundary.

1. Show that $\mathbf{B}\{G\} \to \mathrm{End}_\mathbf{A}(\mathbf{B})$, $\sigma \mapsto \sigma$ is an isomorphism of $\mathbf{A}$-algebras.

2. Let $c \in Z^1(G, \mathbf{B}^\times)$. We define $\theta_c : \mathbf{B}\{G\} \to \mathbf{B}\{G\}$ by $\theta_c(b\sigma) = bc_\sigma\sigma$.

- *a.* Verify $\theta_c \circ \theta_d = \theta_{cd}$; deduce that θ_c is an $\mathbf{A}$-automorphism of $\mathbf{B}\{G\}$.
- *b.* Show that if $c \in B^1(G, \mathbf{B}^\times)$, then θ_c is an interior automorphism.

3. Let $c \in Z^1(G, \mathbf{B}^\times)$. Consider the action from $\mathbf{B}\{G\}$ to $\mathbf{B}$ "twisted" by θ_c, i.e. $z \cdot b = \theta_c(z)\, b$; let $\mathbf{B}_c$ be this $\mathbf{B}\{G\}$-module, $\mathbf{B}_c^G$ be the set of elements of $\mathbf{B}$ invariant under G (for this action twisted by θ_c), and

$$\pi_c = \textstyle\sum_{\sigma \in G} c_\sigma\, \sigma \in \mathrm{End}_\mathbf{A}(\mathbf{B}).$$

Verify that $\mathbf{B}_c^G$ is an $\mathbf{A}$-submodule of $\mathbf{B}$. Show that π_c is a surjection from $\mathbf{B}$ to $\mathbf{B}_c^G$ by explicating a section; deduce that $\mathbf{B}_c^G$ is a direct summand in $\mathbf{B}$ (as an $\mathbf{A}$-module).

4. We will show that for every $c \in Z^1(G, \mathbf{B}^\times)$, $\mathbf{B}_c^G$ is a projective $\mathbf{A}$-module of constant rank 1.

- *a.* Verify that $\mathbf{B}_c^G\mathbf{B}_d^G \simeq \mathbf{B}_{cd}^G$ and $\mathbf{B}_c^G \otimes_\mathbf{A} \mathbf{B}_d^G \simeq \mathbf{B}_{cd}^G$.
- *b.* Show that if $c \in B^1(G, \mathbf{B}^\times)$, then $\mathbf{B}_c^G \simeq \mathbf{A}$. Conclude the result.
- *c.* Show that $c \mapsto \mathbf{B}_c^G$ induces an injective morphism from $H^1(G, \mathbf{B}^\times)$ into $\mathsf{Pic}(\mathbf{A})$.

5. In the case where $\mathbf{A}$ is a zero-dimensional ring (for example a discrete field), show that every 1-cocycle $(c_\sigma)_{\sigma \in G}$ is the coboundary of some $b \in \mathbf{B}^\times$.

6. Suppose that G is cyclic of order n, $G = \langle \sigma \rangle$, and that $\mathsf{Pic}(\mathbf{A}) = 0$.
Let $x \in B$; show that $\mathrm{N}_{\mathbf{B}/\mathbf{A}}(x) = 1$ if and only if there exists a $b \in \mathbf{B}^\times$ such that $x = \sigma(b)/b$.

Problem 5. *(The Segre morphism in a special case)*
Let $\mathbf{A}[\underline{X}, \underline{Y}] = \mathbf{A}[X_1, \ldots, X_n, Y_1, \ldots, Y_n]$. Consider the ideal $\mathfrak{a} = \langle X_iY_j - X_jY_i \rangle$, i.e. the ideal $\mathcal{D}_2(A)$, where A is the generic matrix $\begin{bmatrix} X_1 & X_2 & \cdots & X_n \\ Y_1 & Y_2 & \cdots & Y_n \end{bmatrix}$. We want to show that $\mathfrak{a}$ is the kernel of the morphism

$$\varphi : \mathbf{A}[\underline{X}, \underline{Y}] \to \mathbf{A}[T, U, \underline{Z}] = \mathbf{A}[T, U, Z_1, \ldots, Z_n], \quad X_i \to TZ_i, \ \ Y_i \to UZ_i,$$

where T, U, Z_1, …, Z_n are new indeterminates. Let us agree to say that a monomial $m \in \mathbf{A}[\underline{X}, \underline{Y}]$ is normalized if m is equal to $X_{i_1} \cdots X_{i_r} Y_{j_1} \cdots Y_{j_s}$ with $1 \leqslant i_1 \leqslant \cdots \leqslant i_r \leqslant j_1 \leqslant \cdots \leqslant j_s \leqslant n$ (the indices of $\underline{X}$ are smaller than that of $\underline{Y}$). Let $\mathfrak{a}_{\mathrm{nor}}$ be the $\mathbf{A}$-submodule of $\mathbf{A}[\underline{X}, \underline{Y}]$ generated by the normalized monomials.

1. If m, m' are normalized, show that $\varphi(m) = \varphi(m') \Rightarrow m = m'$. Deduce that $\mathrm{Ker}\, \varphi \cap \mathfrak{a}_{\mathrm{nor}} = \{0\}$.

2. Show that we have a direct sum of $\mathbf{A}$-modules: $\mathbf{A}[\underline{X},\underline{Y}] = \mathfrak{a} \oplus \mathfrak{a}_{\rm nor}$
3. Deduce that $\mathfrak{a} = \operatorname{Ker}\varphi$. In particular, if $\mathbf{A}$ is reduced (resp. without zerodivisors), then $\mathfrak{a}$ is radical (resp. prime).

Comment. The morphism φ induces, by co-morphism, a morphism between affine spaces

$$\psi : \mathbb{A}^2(\mathbf{A}) \times \mathbb{A}^n(\mathbf{A}) \to \mathbb{M}_{2,n}(\mathbf{A}) \simeq \mathbb{A}^{2n}(\mathbf{A}),\ \big((t,u),z\big) \mapsto \begin{bmatrix} tz_1 & \cdots & tz_n \\ uz_1 & \cdots & uz_n \end{bmatrix}.$$

If $\mathbf{A}$ is a field, the image of ψ is the zero set $\mathcal{Z}(\mathfrak{a})$, and ψ induces at the projective spaces level an inclusion $\mathbb{P}^1(\mathbf{A}) \times \mathbb{P}^{n-1}(\mathbf{A}) \to \mathbb{P}^{2n-1}(\mathbf{A})$ (called “embedding”).
More generally, by completely changing the notations, with indeterminates $X_1, \ldots,$ X_n, $Y_1, \ldots, Y_m$, Z_{ij}, $i \in [\![1..n]\!]$, $j \in [\![1..m]\!]$, consider the morphism $\varphi : \mathbf{A}[\underline{Z}] \to \mathbf{A}[\underline{X},\underline{Y}]$, $Z_{ij} \to X_iY_j$. We show that $\operatorname{Ker}\varphi = \mathcal{D}_2(A)$ where $A \in \mathbb{M}_{n,m}(\mathbf{A}[\underline{Z}])$ is the generic matrix. The morphism φ induces, by co-morphism, a morphism between affine spaces

$$\psi : \mathbb{A}^n(\mathbf{A}) \times \mathbb{A}^m(\mathbf{A}) \to \mathbb{M}_{n,m}(\mathbf{A}) \simeq \mathbb{A}^{nm}(\mathbf{A}),\ \big((x_i)_i,(y_j)_j\big) \mapsto (x_iy_j)_{ij},$$

whose image is the zero set $\mathcal{Z}\big(\mathcal{D}_2(A)\big)$. If $\mathbf{A}$ is a discrete field, ψ induces an injection $\mathbb{P}^{n-1}(\mathbf{A}) \times \mathbb{P}^{m-1}(\mathbf{A}) \to \mathbb{P}^{nm-1}(\mathbf{A})$: it is the Segre embedding. This allows us to realise $\mathbb{P}^{n-1} \times \mathbb{P}^{m-1}$ *as a projective algebraic subvariety of* $\mathbb{P}^{nm-1}$ (in a precise sense that we do not specify here).
If $\mathbf{A}$ is arbitrary, let $E \in \mathbb{P}^{n-1}(\mathbf{A})$, $F \in \mathbb{P}^{m-1}(\mathbf{A})$; E is thus a direct summand in $\mathbf{A}^n$, of rank 1; similarly for F. Then $E \otimes_{\mathbf{A}} F$ is canonically identified with a submodule of $\mathbf{A}^n \otimes_{\mathbf{A}} \mathbf{A}^m \simeq \mathbf{A}^{nm}$, a direct summand, of rank 1. By letting $\psi(E,F) = E \otimes_{\mathbf{A}} F$, we thus obtain a map from $\mathbb{P}^{n-1}(\mathbf{A}) \times \mathbb{P}^{m-1}(\mathbf{A})$ to $\mathbb{P}^{nm-1}(\mathbf{A})$ which “extends” the map previously defined: if $x \in \mathbf{A}^n$, $y \in \mathbf{A}^m$ are unimodular, the same holds for $x \otimes y \in \mathbf{A}^n \otimes_{\mathbf{A}} \mathbf{A}^m$, and by letting $E = \mathbf{A}x$, $F = \mathbf{A}y$, we have $E \otimes_{\mathbf{A}} F = \mathbf{A}(x \otimes y)$. ∎

Problem 6. *(The Veronese morphism in a special case)*
Let $d \geqslant 1$, $\mathbf{A}[\underline{X}] = \mathbf{A}[X_0, \ldots, X_d]$ and $\mathfrak{a} = \langle X_iX_j - X_kX_\ell, i+j = k+\ell\rangle$. We will show that the ideal $\mathfrak{a}$ is the kernel of the morphism

$$\varphi : \mathbf{A}[\underline{X}] \to \mathbf{A}[U,V], \qquad \varphi(X_i) = U^{d-i}V^i.$$

where U, V are two new indeterminates. We define another ideal $\mathfrak{b}$

$$\mathfrak{b} = \langle X_iX_j - X_{i-1}X_{j+1}, 1 \leqslant i \leqslant j \leqslant d-1\rangle$$

1. Show that
$$\operatorname{Ker}\varphi \cap (\mathbf{A}[X_0,X_d] + \mathbf{A}[X_0,X_d]X_1 + \cdots + \mathbf{A}[X_0,X_d]X_{d-1}) = \{0\}$$
2. Show that we have a direct sum of $\mathbf{A}$-modules
$$\mathbf{A}[\underline{X}] = \mathfrak{b} \oplus \mathbf{A}[X_0,X_d] \oplus \mathbf{A}[X_0,X_d]X_1 \oplus \cdots \oplus \mathbf{A}[X_0,X_d]X_{d-1}$$
3. Deduce that $\mathfrak{a} = \mathfrak{b} = \operatorname{Ker}\varphi$. In particular, if $\mathbf{A}$ is reduced (resp. without zerodivisors), then $\mathfrak{a}$ is radical (resp. prime).

Comment. More generally, let $N = \binom{n+d}{d} = \binom{n+d}{n}$ and $n+1+N$ indeterminates $U_0, \ldots, U_n$, $(X_\alpha)_\alpha$, where the indices $\alpha \in \mathbb{N}^{n+1}$ are such that $|\alpha| = d$. We dispose of a morphism $\varphi : \mathbf{A}[\underline{X}] \to \mathbf{A}[\underline{U}]$, $X_\alpha \mapsto \underline{U}^\alpha$ (the special case studied here is

$n = 1 \mapsto N = d+1$); its kernel is the ideal

$$\mathfrak{a} = \left\langle X_\alpha X_\beta - X_{\alpha'} X_{\beta'}, \alpha + \beta = \alpha' + \beta' \right\rangle .$$

By co-morphism, φ induces a morphism between affine spaces

$$\psi : \mathbb{A}^{n+1}(\mathbf{A}) \to \mathbb{A}^N(\mathbf{A}),\ u = (u_0, \ldots, u_n) \mapsto (u^\alpha)_{|\alpha|=d}.$$

If $\mathbf{A}$ is a discrete field, the image of ψ is the zero set $\mathscr{Z}(\mathfrak{a})$ and we can show that ψ induces an injection $\mathbb{P}^n(\mathbf{A}) \to \mathbb{P}^{N-1}(\mathbf{A})$: it is the Veronese embedding of degree d. Even more generally, let E be a direct summand in $\mathbf{A}^{n+1}$, of rank 1., The homogeneous component of degree d of the symmetric algebra $\mathbf{S}_\mathbf{A}(E)$, which we denote by $\mathbf{S}_\mathbf{A}(E)_d$, is identified with a submodule of $\mathbf{S}_\mathbf{A}(\mathbf{A}^{n+1})_d \simeq \mathbf{A}[U_0, \ldots, U_n]_d$ (homogeneous component of degree d), a direct summand of rank 1.
If we let $\psi(E) = \mathbf{S}_\mathbf{A}(E)_d$, we thus "extend" the map ψ previously defined. ■

Problem 7. *(Veronese matrices)*
Let two polynomial rings $\mathbf{k}[\underline{X}] = \mathbf{k}[X_1, \ldots, X_n]$ and $\mathbf{k}[\underline{Y}] = \mathbf{k}[Y_1, \ldots, Y_m]$. To every matrix $A \in \mathbf{k}^{m\times n}$, which represents a linear map $\mathbf{k}^n \to \mathbf{k}^m$, we can associate (watch the reversal), a $\mathbf{k}$-morphism $\varphi_A : \mathbf{k}[\underline{Y}] \to \mathbf{k}[\underline{X}]$ constructed as follows: let $X'_1, \ldots, X'_m$ be the m linear forms of $\mathbf{k}[\underline{X}]$ defined as follows.

$$\text{If} \quad \begin{bmatrix} X'_1 \\ \vdots \\ X'_m \end{bmatrix} = A \begin{bmatrix} X_1 \\ \vdots \\ X_n \end{bmatrix}, \quad \text{then} \quad \varphi_A : f(Y_1, \ldots, Y_m) \mapsto f(X'_1, \ldots, X'_m).$$

It is clear that φ_A induces a $\mathbf{k}$-linear map $A_d : \mathbf{k}[\underline{Y}]_d \to \mathbf{k}[\underline{X}]_d$ between the homogeneous components of degree $d \geqslant 0$, and that the restriction $A_1 : \mathbf{k}[\underline{Y}]_1 \to \mathbf{k}[\underline{X}]_1$ has as its matrix in the bases $(Y_1, \ldots, Y_m)$ and $(X_1, \ldots, X_n)$, the *transpose* of A. The $\mathbf{k}$-module $\mathbf{k}[\underline{X}]_d$ is free of rank $n' = \binom{n-1+d}{d}$; it possesses a natural bases, that of the monomials of degree d, which we can choose to order lexicographically with $X_1 > \cdots > X_n$. Similarly for $\mathbf{k}[\underline{Y}]_d$ with its basis of $m' = \binom{m-1+d}{m-1}$ monomials. Let $V_d(A) \in \mathbf{k}^{m'\times n'}$ be the *transpose* of the matrix of the endomorphism A_d in these bases (such that $V_1(A) = A$) and we say that $V_d(A)$ is the Veronese extension of A in degree d.
For example, let $n = 2$, $d = 2$, so $n' = 3$; if $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, we obtain the matrix $V_2(A) \in \mathbb{M}_3(\mathbf{k})$ as follows

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = A \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} ax+by \\ cx+dy \end{bmatrix}, \begin{bmatrix} x'^2 \\ x'y' \\ y'^2 \end{bmatrix} = \begin{bmatrix} a^2 & 2ab & b^2 \\ ac & ad+bc & bd \\ c^2 & 2cd & d^2 \end{bmatrix} \begin{bmatrix} x^2 \\ xy \\ y^2 \end{bmatrix}.$$

1. If A, B are two matrices for which the product AB has a meaning, check the equalities $\varphi_{AB} = \varphi_B \circ \varphi_A$ and $V_d(AB) = V_d(A)V_d(B)$ for every $d \geqslant 0$. Also check that $V_d({}^{\mathrm{t}}A) = {}^{\mathrm{t}}V_d(A)$.

2. If E is a $\mathbf{k}$-module, the *d-Veronese transform of E* is the $\mathbf{k}$-module $\mathbf{S}_\mathbf{k}(E)_d$, homogeneous component of degree d of the symmetric algebra $\mathbf{S}_\mathbf{k}(E)$.
If E is a direct summand in $\mathbf{k}^n$, then $\mathbf{S}_\mathbf{k}(E)_d$ is identified with a direct summand in $\mathbf{S}_\mathbf{k}(\mathbf{k}^n)_d \simeq \mathbf{k}[X_1, \ldots, X_n]_d$ (see also Problem 6). Show that the image under

V_d of a projector is a projector and that we have a commutative diagram

$$\begin{tikzcd}
\mathbb{AG}_n(\mathbf{k}) \arrow[r, "V_d"] \arrow[d, "\mathrm{Im}"'] & \mathbb{AG}_{n'}(\mathbf{k}) \arrow[d, "\mathrm{Im}"] \\
\mathbb{G}_n(\mathbf{k}) \arrow[r, "d-\text{Veronese}"] & \mathbb{G}_{n'}(\mathbf{k})
\end{tikzcd} \qquad \text{with} \quad n' = \binom{n-1+d}{d} = \binom{n-1+d}{n-1}$$

3. Show that if A is a projector of rank 1, the same holds for $V_d(A)$. More generally, if A is a projector of rank r, then $V_d(A)$ is a projector of rank $\binom{d+1-r}{r-1}$.

Problem 8. *(Some examples of finite projective resolutions)*
Given $2n+1$ elements z, x_1, …, x_n, y_1, …, y_n, of a ring $\mathbf{A}$, we define a sequence of matrices $F_k \in \mathbb{M}_{2^k}(\mathbf{A})$, for $k \in [\![0..n]\!]$, as follows

$$F_0 = \begin{bmatrix} z \end{bmatrix}, \qquad F_k = \begin{bmatrix} F_{k-1} & x_k \mathrm{I}_{2^{k-1}} \\ y_k \mathrm{I}_{2^{k-1}} & \mathrm{I}_{2^{k-1}} - F_{k-1} \end{bmatrix}.$$

Thus with $\overline{z} = 1 - z$,

$$F_1 = \begin{bmatrix} z & x_1 \\ y_1 & \overline{z} \end{bmatrix}, \qquad F_2 = \begin{bmatrix} z & x_1 & x_2 & 0 \\ y_1 & \overline{z} & 0 & x_2 \\ y_2 & 0 & \overline{z} & -x_1 \\ 0 & y_2 & -y_1 & z \end{bmatrix}.$$

1. Check that $F_k^2 - F_k$ is the scalar matrix with the term $z(z-1) + \sum_{i=1}^{k} x_i y_i$. Also show that ${}^{\mathrm{t}}F_n$ is similar to $\mathrm{I}_{2^n} - F_n$ for $n \geqslant 1$. Consequently, if $z(z-1) + \sum_{i=1}^{n} x_i y_i = 0$, then F_n is a projector of rank 2^{n-1}.

2. We define three sequences of matrices

$$U_k, V_k \in \mathbb{M}_{2^{k-1}}(\mathbf{A})\ (k \in [\![1..n]\!]), \quad G_k \in \mathbb{M}_{2^k}(\mathbf{A})\ (k \in [\![0..n]\!]),$$

as follows: $U_1 = \begin{bmatrix} x_1 \end{bmatrix}$, $V_1 = \begin{bmatrix} y_1 \end{bmatrix}$, $G_0 = \begin{bmatrix} z \end{bmatrix}$ and

$$U_k = \begin{bmatrix} U_{k-1} & x_k \mathrm{I} \\ y_k \mathrm{I} & -V_{k-1} \end{bmatrix}, \; V_k = \begin{bmatrix} V_{k-1} & x_k \mathrm{I} \\ y_k \mathrm{I} & -U_{k-1} \end{bmatrix}, \; G_k = \begin{bmatrix} z\mathrm{I} & U_k \\ V_k & \overline{z}\mathrm{I} \end{bmatrix}.$$

Thus,

$$U_2 = \begin{bmatrix} x_1 & x_2 \\ y_2 & -y_1 \end{bmatrix}, \; V_2 = \begin{bmatrix} y_1 & x_2 \\ y_2 & -x_1 \end{bmatrix}, \; G_2 = \begin{bmatrix} z & 0 & x_1 & x_2 \\ 0 & z & y_2 & -y_1 \\ y_1 & x_2 & \overline{z} & 0 \\ y_2 & -x_1 & 0 & \overline{z} \end{bmatrix}.$$

a. Verify that G_n and F_n are conjugated by a permutation matrix.

b. Verify that $U_k V_k$ is the scalar $\sum_{i=1}^{k} x_i y_i$ and that $U_k V_k = V_k U_k$.

c. For $n \geqslant 1$, if $z(z-1) + \sum_{i=1}^{n} x_i y_i = 0$, show that G_n (therefore F_n) is a projector of rank 2^{n-1}.

3. Let M be an $\mathbf{A}$-module. A *finite projective resolution* of M is an exact sequence of finitely generated projective modules $0 \to P_n \to \cdots \to P_1 \to P_0 \twoheadrightarrow M \to 0$; we say that n is *the length of the resolution.* In this case, M is finitely presented.

a. Consider two finite projective resolutions of M that we can assume to be of the same length,

$$0 \to P_n \to P_{n-1} \to \cdots \to P_1 \to P_0 \to M \to 0,$$
$$0 \to P'_n \to P'_{n-1} \to \cdots \to P'_1 \to P'_0 \to M \to 0.$$

By using Exercise V-4, show that we have in $\mathsf{K}_0(\mathbf{A})$ the following equality

$$(\star) \qquad \textstyle\sum_{i=0}^{n}(-1)^i[P_i] = \sum_{i=0}^{n}(-1)^i[P'_i].$$

Note. Exercise V-4 provides a much more precise result. ■

Definition and notation. For a module M which admits a finite projective resolution we let $[M] \in \mathsf{K}_0(\mathbf{A})$ be the common value of $(\star)$ (even if M is not finitely generated projective). We then define *the rank of* M as that of $[M]$ and we have $\operatorname{rk} M = \sum_{i=0}^{n}(-1)^i \operatorname{rk} P_i \in \mathsf{H}_0(\mathbf{A})$.

b. Let M be an $\mathbf{A}$-module admitting a finite projective resolution; suppose that $aM = 0$ with $a \in \operatorname{Reg}(\mathbf{A})$. Show that $\operatorname{rk}(M) = 0$ i.e. that $[M] \in \widetilde{\mathsf{K}}_0(\mathbf{A})$.

If $\mathbf{k}$ is an arbitrary ring, we define the ring

$$\mathbf{B}_n = \mathbf{k}[z,\underline{x},\underline{y}] = \mathbf{k}[Z, X_1, \dots, X_n, Y_1, \dots, Y_n]\big/\big\langle Z(Z-1) + \textstyle\sum_{i=1}^{n} X_iY_i \big\rangle$$

Thus $\mathbf{B}_0 \simeq \mathbf{k} \times \mathbf{k}$. Let $\mathfrak{b}_n$ be the ideal $\langle z, x_1, \dots, x_n\rangle$.

4. Show that the localized rings $\mathbf{B}_n[1/z]$ and $\mathbf{B}_n[1/(1-z)]$ are elementary localized rings (i.e. obtained by inverting a single element) of a polynomial ring over $\mathbf{k}$ with $2n$ indeterminates. Show that $\mathbf{B}_n/\langle x_n\rangle \simeq \mathbf{B}_{n-1}[y_n] \simeq \mathbf{B}_{n-1}[Y]$.

5. For $n = 1$, define a projective resolution of the $\mathbf{B}_1$-module $\mathbf{B}_1/\mathfrak{b}_1$ of length 2 and verify that $[\mathbf{B}_1/\mathfrak{b}_1] \in \widetilde{\mathsf{K}}_0(\mathbf{B}_1)$.

6. For $n = 2$, define a projective resolution of the $\mathbf{B}_2$-module $\mathbf{B}_2/\mathfrak{b}_2$ of length 3

$$0 \to \operatorname{Im} F_2 \to \mathbf{B}_2^4 \to \mathbf{B}_2^3 \xrightarrow{[z,x_1,x_2]} \mathbf{B}_2 \twoheadrightarrow \mathbf{B}_2/\mathfrak{b}_2 \to 0,$$

and verify that $[\mathbf{B}_2/\mathfrak{b}_2] \in \widetilde{\mathsf{K}}_0(\mathbf{B}_2)$.

7. Explicate a permutation $\sigma \in \mathrm{S}_{2^n}$ such that the $n+1$ first coefficients of the first row of the matrix $F'_n = P_\sigma F_n P_\sigma^{-1}$ are z, x_1, …, x_n (P_σ is the permutation matrix σ).

8. For $n = 3$, define a projective resolution of the $\mathbf{B}_3$-module $\mathbf{B}_3/\mathfrak{b}_3$ of length 4

$$0 \to \operatorname{Im}(\mathrm{I}_8 - F'_3) \to \mathbf{B}_3^8 \to \mathbf{B}_3^7 \to \mathbf{B}_3^4 \xrightarrow{[z,x_1,x_2,x_3]} \mathbf{B}_3 \twoheadrightarrow \mathbf{B}_3/\mathfrak{b}_3 \to 0,$$

and verify that $[\mathbf{B}_3/\mathfrak{b}_3] \in \widetilde{\mathsf{K}}_0(\mathbf{B}_3)$.

9. And in general?

Some solutions, or sketches of solutions

Exercise 2. We roughly rewrite the second proof of the local freeness lemma. Let φ be the linear map which has as its matrix F. Let f_j be the column j of the matrix F, and $(e_1, \dots, e_n)$ be the canonical basis of $\mathbf{A}^n$.

By hypothesis, $(f_1,\dots,f_k,e_{k+1},\dots,e_n)$ is a basis of $\mathbf{A}^n$. The corresponding change of coordinate matrix is $B_1 = \begin{bmatrix} V & 0 \\ C' & \mathrm{I}_h \end{bmatrix}$. Since $\varphi(f_i) = \varphi\big(\varphi(e_i)\big) = \varphi(e_i) = f_i$, with respect to this basis, φ has a matrix of the type $\begin{bmatrix} \mathrm{I}_k & X \\ 0 & Y \end{bmatrix}$. The computation gives

$$B_1^{-1} = \begin{bmatrix} V^{-1} & 0 \\ C & \mathrm{I}_h \end{bmatrix}, \qquad G = B_1^{-1}\, F\, B_1 = \begin{bmatrix} \mathrm{I}_k & L \\ 0 & -C'V^{-1}L' + W \end{bmatrix},$$

where $L = V^{-1}L'$, and $C = -C'V^{-1}$.

Since $\mathcal{D}_{k+1}(G) = 0$, we have $G = \begin{bmatrix} \mathrm{I}_k & L \\ 0 & 0 \end{bmatrix}$, therefore $W = C'V^{-1}L'$.

Let $B_2 = \begin{bmatrix} \mathrm{I}_k & -L \\ 0 & \mathrm{I}_h \end{bmatrix}$, we have $B_2^{-1} = \begin{bmatrix} \mathrm{I}_k & L \\ 0 & \mathrm{I}_h \end{bmatrix}$, then $B_2^{-1}\, G\, B_2 = \mathrm{I}_{k,n}$.

Finally, we obtain $B^{-1}\, F\, B = \mathrm{I}_{k,n}$ with

$$B = B_1\, B_2 = \begin{bmatrix} V & 0 \\ C' & \mathrm{I}_h \end{bmatrix} \cdot \begin{bmatrix} \mathrm{I}_k & -L \\ 0 & \mathrm{I}_h \end{bmatrix} = \begin{bmatrix} V & -L' \\ C' & \mathrm{I}_h - W \end{bmatrix}$$

and

$$B^{-1} = B_2^{-1}\, B_1^{-1} = \begin{bmatrix} \mathrm{I}_k & L \\ 0 & \mathrm{I}_h \end{bmatrix} \cdot \begin{bmatrix} V^{-1} & 0 \\ C & \mathrm{I}_h \end{bmatrix} = \begin{bmatrix} V^{-1} + LC & L \\ C & \mathrm{I}_h \end{bmatrix}.$$

The equality $F^2 = F$ gives in particular $V = V^2 + L'C'$.
Therefore $\mathrm{I}_k = V\,(\mathrm{I}_k + L'C'V^{-1}) = V\,(\mathrm{I}_k - LC)$, and finally $V^{-1} = \mathrm{I}_k - LC$.
Therefore as stated $B^{-1} = \begin{bmatrix} \mathrm{I}_k & L \\ C & \mathrm{I}_h \end{bmatrix}$.
Before proving the statement regarding $\mathrm{I}_h - W$, let us prove the converse.
The double equality

$$\begin{bmatrix} \mathrm{I}_k & L \\ C & \mathrm{I}_h \end{bmatrix} = \begin{bmatrix} \mathrm{I}_k - LC & L \\ 0 & \mathrm{I}_h \end{bmatrix} \begin{bmatrix} \mathrm{I}_k & 0 \\ C & \mathrm{I}_h \end{bmatrix} = \begin{bmatrix} \mathrm{I}_k & L \\ 0 & \mathrm{I}_h \end{bmatrix} \begin{bmatrix} \mathrm{I}_k & 0 \\ C & \mathrm{I}_h - CL \end{bmatrix}$$

shows that $\mathrm{I}_k - LC$ is invertible if and only if $\mathrm{I}_h - CL$ is invertible if and only if $\begin{bmatrix} \mathrm{I}_k & L \\ C & \mathrm{I}_h \end{bmatrix}$ is invertible. This also gives

$$\det \begin{bmatrix} \mathrm{I}_k & L \\ C & \mathrm{I}_h \end{bmatrix} = \det(\mathrm{I}_k - LC) = \det(\mathrm{I}_h - CL)\,.$$

The computation then gives

$$\begin{bmatrix} \mathrm{I}_k & L \\ C & \mathrm{I}_h \end{bmatrix}^{-1} = \begin{bmatrix} V & -VL \\ -CV & \mathrm{I}_h + CVL \end{bmatrix},$$

hence

$$\begin{bmatrix} \mathrm{I}_k & L \\ C & \mathrm{I}_h \end{bmatrix}^{-1} \cdot \begin{bmatrix} \mathrm{I}_k & 0 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} \mathrm{I}_k & L \\ C & \mathrm{I}_h \end{bmatrix} = \begin{bmatrix} V & VL \\ -CV & -CVL \end{bmatrix},$$

which establishes the converse. Finally, the equality $B^{-1}\, F\, B = \mathrm{I}_{k,n}$ implies $B^{-1}\,(\mathrm{I}_n - F)\, B = \mathrm{I}_n - \mathrm{I}_{k,n}$, which gives

$$\begin{bmatrix} \mathrm{I}_k - V & -L' \\ -C' & \mathrm{I}_h - W \end{bmatrix} = \begin{bmatrix} \mathrm{I}_k & L \\ C & \mathrm{I}_h \end{bmatrix}^{-1} \cdot \begin{bmatrix} 0 & 0 \\ 0 & \mathrm{I}_h \end{bmatrix} \cdot \begin{bmatrix} \mathrm{I}_k & L \\ C & \mathrm{I}_h \end{bmatrix}$$

and we find ourselves in the symmetric situation, therefore $(\mathrm{I}_h - W)^{-1} = \mathrm{I}_h - CL$ and $\det V = \det(\mathrm{I}_h - W)$.

Exercise 5. Note g (resp. d) as the left-multiplication (resp. right-multiplication) by P. We then have $g^2 = g$, $d^2 = d$, $gd = dg$, $\varphi = g + d - 1$ and $\pi = g + d - 2gd$.

Exercise 8. *1a.* The "homogeneous Sylvester matrix" S is defined as that of the linear map $(A, B) \mapsto PA + QB$ over the bases $(u^{q-1}, \ldots, v^{q-1})$ for A (homogeneous polynomial of degree $q-1$), $(u^{p-1}, \ldots, v^{p-1})$ for B (homogeneous polynomial of degree $p-1$) and $(u^{p+q-1}, \ldots, v^{p+q-1})$ for $PA+QB$ (homogeneous polynomial of degree $p+q-1$).
By making $v = 1$, we see that ${}^{\mathrm{t}}S = \mathrm{Syl}(g, p, h, q)$, hence $\det(S) = \mathrm{Res}(g, p, h, q)$.
By making $u = 1$, we see that ${}^{\mathrm{t}}S$ is almost the matrix $\mathrm{Syl}(\widetilde{g}, p, \widetilde{h}, q)$: the order of the rows, the order of the q first columns and the order of the last p must be reversed. Hence the stated result because $(-1)^{\lfloor q/2 \rfloor + \lfloor p/2 \rfloor + \lfloor (p+q)/2 \rfloor} = (-1)^{pq}$.

1b. The equality $S\widetilde{S} = \mathrm{Res}(P, Q)\,\mathrm{I}_{p+q}$ means that, if $k + \ell = p + q - 1$, $u^k v^\ell \mathrm{Res}(P, Q)$ is a linear combination of the column vectors of the matrix S. That therefore exactly gives the required inclusion, which is after all just the homogeneous version of the usual inclusion.

2. We write f in the irreducible form $f = a/b$ with a, $b \in \mathbf{k}[t]$, and we homogenize a and b in degree d (maximum of the degrees of a and b) to obtain two homogeneous polynomials A, $B \in \mathbf{k}[u, v]$ of degree d.
If $\mathbf{k}$ is an arbitrary ring, we ask that $\mathrm{Res}(A, B)$ be invertible. That is necessary for the fraction to remain well-defined after every scalar extension. Let us then see that the morphism f is first defined at the unimodular vector level

$$(\xi : \zeta) \mapsto \big(A(\xi, \zeta) : B(\xi, \zeta)\big).$$

This makes sense because if $1 \in \langle \xi, \zeta \rangle$, then $1 \in \langle A(\xi, \zeta), B(\xi, \zeta) \rangle$ after item *1b.*
To get back up to level $\mathbb{AG}_{2,1}(\mathbf{k})$, we take two new indeterminates x, y by thinking about the matrix $\begin{bmatrix} xu & yu \\ xv & yv \end{bmatrix}$. As $\langle u, v \rangle^{2d-1} \subseteq \langle A, B \rangle$, we can write

$$(xu + yv)^{2d-1} = E(x, y, u, v)A(u, v) + F(x, y, u, v)B(u, v)$$

with E and F homogeneous in (x, y, u, v).
Actually, E and F are bihomogeneous in $\big((x, y), (u, v)\big)$, of degree $2d-1$ in (x, y), of degree $d-1$ in (u, v). As EA is bihomogeneous, of bidegree $(2d-1, 2d-1)$, there exists (see the justification below) some homogeneous polynomial α' in 4 variables, $\alpha' = \alpha'(\alpha, \beta, \gamma, \delta)$, such that:

$$EA = \alpha'(xu, yu, xv, yv), \quad \deg(\alpha') = 2d - 1.$$

Likewise with FA, EB, FB to produce β', γ', δ'. We then consider the matrices

$$\begin{bmatrix} xu & yu \\ xv & yv \end{bmatrix} \rightsquigarrow \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}, \qquad \begin{bmatrix} EA & FA \\ EB & FB \end{bmatrix} \rightsquigarrow \begin{bmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{bmatrix}.$$

The lifting we are looking for is then $\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \mapsto \begin{bmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{bmatrix}$.

Note: α', β', γ', δ' are homogeneous polynomials in $(\alpha, \beta, \gamma, \delta)$, of degree $2d-1$, such that

$$\begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix} \text{ divides } \begin{vmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{vmatrix}, \qquad \alpha+\delta-1 \text{ divides } \alpha'+\delta'-1.$$

Justification of the existence of α'.

This rests on the following simple fact: $u^i v^j x^k y^\ell$ is a monomial in (xu, yu, xv, yv) if and only if $i+j=k+\ell$; indeed, if this equality is satisfied, there is a matrix $\begin{bmatrix} m & n \\ r & s \end{bmatrix} \in \mathbb{M}_2(\mathbb{N})$ such that the sums of rows are (i,j) and the sums of columns are (k,l). A schema to help with the reading:

$$\begin{array}{cc} & \begin{array}{cc} k & \ell \end{array} \\ \begin{array}{c} i \\ j \end{array} & \begin{bmatrix} m & n \\ r & s \end{bmatrix} \end{array} \qquad \begin{bmatrix} xu & yu \\ xv & yv \end{bmatrix},$$

and then

$$u^i v^j x^k y^\ell = u^{m+n} v^{r+s} x^{m+r} y^{n+s} = (xu)^m (yu)^n (xv)^r (yv)^s.$$

We deduce that a bihomogeneous polynomial in $\big((x,y),(u,v)\big)$, of bidegree (d,d), is the evaluation at (xu, yu, xv, yv) of a homogeneous polynomial of degree d.

3. For $f(t)=t^2$, we obtain the lift

$$\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \mapsto \begin{bmatrix} \alpha^2(\alpha+3\delta) & \beta^2(3\alpha+\delta) \\ \gamma^2(\alpha+3\delta) & \delta^2(3\alpha+\delta) \end{bmatrix}.$$

More generally, we develop $(\alpha+\delta)^{2d-1}$ in the form $\alpha^d S_d(\alpha,\delta)+\delta^d S_d(\delta,\alpha)$, and we obtain the lift

$$\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \mapsto \begin{bmatrix} \alpha^d S_d(\alpha,\delta) & \beta^d S_d(\delta,\alpha) \\ \gamma^d S_d(\alpha,\delta) & \delta^d S_d(\delta,\alpha) \end{bmatrix}.$$

If $H = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, we obtain the following lift of $f(t)=\frac{at+b}{ct+d}$:

$$\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \mapsto H \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} H^{-1}.$$

Exercise 9. *(The fundamental conic or Veronese embedding $\mathbb{P}^1 \to \mathbb{P}^2$)*

We proceed as in Exercise 8, but it is simpler because, since $\langle u,v\rangle^2 = \left\langle u^2, uv, v^2\right\rangle$, the map $(u:v) \mapsto (u^2:uv:v^2)$ is well-defined at the unimodular vector level.

We introduce (x,y) with the matrix $\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \leftrightarrow \begin{bmatrix} xu & yu \\ xv & yv \end{bmatrix}$ in mind. We develop $(xu+yv)^2 = x^2u^2+2xyuv+y^2v^2$, sum of 3 terms which will be the 3 diagonal terms of a matrix of $\mathbb{AG}_{3,1}(\mathbf{k})$, then we complete such that each column the ad-hoc multiple of the vector ${}^{\mathrm{t}}[\,u^2\ uv\ v^2\,]$. Which gives

$$\begin{bmatrix} x^2u^2 & 2xyu^2 & y^2u^2 \\ x^2uv & 2xyuv & y^2uv \\ x^2v^2 & 2xyv^2 & y^2v^2 \end{bmatrix} \qquad F = \begin{bmatrix} \alpha^2 & 2\alpha\beta & \beta^2 \\ \alpha\gamma & 2\alpha\delta & \beta\delta \\ \gamma^2 & 2\gamma\delta & \delta^2 \end{bmatrix}.$$

The lift $\mathbb{AG}_{2,1}(\mathbf{k}) \to \mathbb{AG}_{3,1}(\mathbf{k})$ is $\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \mapsto F$.

We of course have $\mathrm{Tr}(F) = (\alpha + \delta)^2 = 1$, $\mathcal{D}_2(F) \subseteq \langle \alpha\delta - \beta\gamma \rangle = 0$, and F is a projector of rank 1.

Exercise 10. *(Projection matrices of corank* 1*)*

1. We provide two solutions for this question. The first consists of using the expression of the adjoint in terms of the starting matrix; the second proof uses the localization.

For $A \in \mathbb{M}_n(\mathbf{A})$ we have the classical expression of $\widetilde{A}$ as a polynomial in A

$$\widetilde{A} = (-1)^{n-1} Q(A) \quad \text{with} \quad XQ(X) = \mathrm{C}_A(X) - \mathrm{C}_A(0).$$

Apply this to a projector P of rank $n-1$. We get

$$\mathrm{C}_P(X) = (X-1)^{n-1} X,\ Q(X) = (X-1)^{n-1} \text{ and } (P - \mathrm{I}_n)^{n-1} = (-1)^{n-1}\widetilde{P}.$$

Since $(\mathrm{I}_n - P)^{n-1} = \mathrm{I}_n - P$, we obtain $P + \widetilde{P} = \mathrm{I}_n$.

Here is the proof by localization. By the local structure theorem for finitely generated projective modules (Theorem V-6.1 or Theorem 1.5), there exist comaximal localizations such that over each localized ring, P is similar to $\mathrm{I}_{r,n}$, where the integer r a priori depends on the localization. Here, since P is of rank $n-1$, we have $r = n-1$ or $1 = 0$. Therefore $P + \widetilde{P} = \mathrm{I}_n$ over each localized ring, and the equality is also globally true by the basic local-global principle.

2. Let us see the proof by comaximal localizations. Over the localized ring $\mathbf{A}_s$, the projector P is similar to $Q_s = \mathrm{I}_{r,n}$, where r depends on s. We have $Q_s + \widetilde{Q_s} = \mathrm{I}_n$. If $r < n-1$, then $Q_s + \widetilde{Q_s} = \mathrm{I}_{r,n}$. If $r = n$, then $Q_s + \widetilde{Q_s} = 2\,\mathrm{I}_n$.
Recap: if $r \neq n-1$, then $1 = 0$ and the rank is also equal to $n-1$. Consequently over all the localized rings $\mathbf{A}_s$, the projector P is of rank $n-1$, and therefore also globally.

3. It suffices to multiply $P + \widetilde{P} = \mathrm{I}_n$ by P to obtain $P^2 = P$.

Exercise 11. There exists a $B \in \mathbb{M}_n(\mathbf{A})$ such that $ABA = A$, in order for AB to be a projector with the same image as A, so of rank $n-1$, and for BA to be a projector with the same kernel as A, therefore also of rank $n-1$. We define P and $Q \in \mathbb{M}_n(\mathbf{A})$ by $AB = \mathrm{I}_n - P$, and $BA = \mathrm{I}_n - Q$.
Thus P, $Q \in \mathbb{AG}_{1,n}(\mathbf{A})$, with $A = (\mathrm{I}_n - P)A = A(\mathrm{I}_n - Q)$.

1. We have $\det A = 0$, i.e. $\widetilde{A}A = A\widetilde{A} = 0$, so $\mathrm{Im}\, A \subseteq \mathrm{Ker}\, \widetilde{A}$.
Next $\widetilde{AB} = \widetilde{\mathrm{I}_n - P} = P$ (because $P \in \mathbb{AG}_{1,n}(\mathbf{A})$), and the equality $\widetilde{B}\widetilde{A} = P$ proves that

$$\mathrm{Ker}\, \widetilde{A} \subseteq \mathrm{Ker}\, P = \mathrm{Im}(\mathrm{I}_n - P) = \mathrm{Im}\, A.$$

Conclusion: $\mathrm{Ker}\, \widetilde{A} = \mathrm{Im}\, A = \mathrm{Im}(\mathrm{I}_n - P)$.

2. By reasoning as in item *1*, we obtain $\mathrm{Im}\, \widetilde{A} \subseteq \mathrm{Ker}\, A = \mathrm{Ker}(BA) = \mathrm{Im}\, Q$, then $\widetilde{A}\widetilde{B} = \widetilde{BA} = \widetilde{\mathrm{I}_n - Q} = Q$, and $\mathrm{Ker}\, A = \mathrm{Im}\, \widetilde{A} = \mathrm{Im}\, Q$.

3. We apply item *1* to ${}^{\mathrm{t}}\!A$, so $\mathrm{Im}\ {}^{\mathrm{t}}\!A = \mathrm{Ker}\ {}^{\mathrm{t}}\widetilde{A}$. Then, we explicate the "left" projector (of rank 1) associated with ${}^{\mathrm{t}}\!A$. We have

$$ {}^{\mathrm{t}}\!A\,{}^{\mathrm{t}}\!B\,{}^{\mathrm{t}}\!A = {}^{\mathrm{t}}\!A, \quad \text{which we write} \quad {}^{\mathrm{t}}(BA)\,{}^{\mathrm{t}}\!A = {}^{\mathrm{t}}\!A \quad \text{with} \quad {}^{\mathrm{t}}(BA) = \mathrm{I}_n - {}^{\mathrm{t}}Q. $$

This left-projector is therefore ${}^{\mathrm{t}}Q$.

4. Similarly, item *2* gives $\mathrm{Im}\ {}^{\mathrm{t}}\widetilde{A} = \mathrm{Ker}\ {}^{\mathrm{t}}\!A$. We explicate the "right-projector" (of rank 1) associated with ${}^{\mathrm{t}}\!A$, we obtain ${}^{\mathrm{t}}P$, whence the stated result.

5. Finally

$$ \mathbf{A}^n/\,\mathrm{Im}\,A = \mathbf{A}^n/\,\mathrm{Im}(\mathrm{I}_n - P) \simeq \mathrm{Im}\,P, \qquad \mathrm{Ker}\ {}^{\mathrm{t}}\!A = \mathrm{Im}\ {}^{\mathrm{t}}P, $$

so the two modules (projective of rank 1) are indeed duals of one another.
Remark: we can also use

$$ \mathbf{A}^n/\,\mathrm{Im}\ {}^{\mathrm{t}}\!A = \mathbf{A}^n/\,\mathrm{Im}(\mathrm{I}_n - {}^{\mathrm{t}}Q) \simeq \mathrm{Im}\ {}^{\mathrm{t}}Q, \qquad \mathrm{Ker}\,A = \mathrm{Im}\,Q, $$

to see that the two modules (projective of rank 1) $\mathbf{A}^n/\,\mathrm{Im}\ {}^{\mathrm{t}}\!A$ and $\mathrm{Ker}\,A$ are indeed duals.

Exercise 12. *(Intersection of two affine schemes over* $\mathbf{k}$*)*
First of all we notice that surjective arrows $\mathbf{k}[\underline{X}] \xrightarrow{\pi_1} \mathbf{A}$ and $\mathbf{k}[\underline{X}] \xrightarrow{\pi_2} \mathbf{B}$ in the category of finitely presented $\mathbf{k}$-algebras are seen, from the point of view of the schemes, as "inclusions" $A \xrightarrow{\iota_1} \mathbf{k}^n$ and $B \xrightarrow{\iota_2} \mathbf{k}^n$, where $\mathbf{k}^n$ is interpreted as the affine scheme corresponding to $\mathbf{k}[\underline{X}]$. The definition of the intersection by tensor product is therefore in fact a definition as the push out of the two arrows π_1 and π_2 in the category of finitely presented $\mathbf{k}$-algebras, or as the pull back of the two arrows ι_1 and ι_2 in the category of affine schemes over $\mathbf{k}$.

The center of the ellipse, the center of the circle and the double point of intersection have for respective coordinates $(0, 0)$, $(c, 0)$ and $(a, 0)$. The computation of other points of intersection gives

$$ x = a(2ac + 1 - a^2)/(a^2 - 1) \text{ and } y^2 = 4ac(a^2 - ac - 1)/(a^2 - 1)^2. $$

From the point of view of quotient algebras we obtain

$$ \mathbf{A} = \mathbf{k}[X, Y]/\langle f\rangle\,, \quad \mathbf{B} = \mathbf{k}[X, Y]/\langle g\rangle\,, \quad \mathbf{C} = \mathbf{k}[X, Y]/\langle f, g\rangle\,. $$

Which gives the morphisms

$$\begin{tikzcd}
 & \mathbf{K} = \mathbf{k}[X, Y] \arrow[ld, "\pi_1"'] \arrow[rd, "\pi_2"] \arrow[d] & \\
\mathbf{A} \arrow[rd] & & \mathbf{B} \arrow[ld] \\
 & \mathbf{C} = \mathbf{A} \otimes_{\mathbf{K}} \mathbf{B} &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & \mathbf{k}^2 & \\
\{f = 0\} \arrow[ru, "\iota_1"] & & \{g = 0\} \arrow[lu, "\iota_2"'] \\
 & \{f = 0\} \cap \{g = 0\} \arrow[lu] \arrow[ru] \arrow[uu] &
\end{tikzcd}$$

If $\mathbf{k}$ is a discrete field and if $4ac(a^2 - ac - 1)(a^2 - 1) \in \mathbf{k}^{\times}$, the $\mathbf{k}$-algebras $\mathbf{A}$ and $\mathbf{B}$ are integral, but not $\mathbf{C}$: we have an isomorphism

$$ \mathbf{C} \xrightarrow{\sim} \mathbf{k}[\zeta] \times \mathbf{k}[\varepsilon], \;\; \text{where } \varepsilon^2 = 0 \;\text{ and }\; \zeta^2 = 4ac(a^2 - ac - 1)/(a^2 - 1)^2. $$

The algebra $\mathbf{C}$ is a $\mathbf{k}$-vector space of dimension 4, corresponding to the affine scheme formed by two points of multiplicity 1 (defined over $\mathbf{k}$ or over a quadratic extension of $\mathbf{k}$) and a point of multiplicity 2 (defined over $\mathbf{k}$).

Exercise 13. *(Pseudomonic polynomials)*
Recall that for an idempotent e, we have $\langle a, e\rangle = \langle (1-e)a + e\rangle$; if e' is another idempotent orthogonal to e, we have $\langle \overline{a}\rangle = \left\langle \overline{e'}\right\rangle$ in $\mathbf{A}/\langle e\rangle$ if and only if $\langle (1-e)a\rangle = \langle e'\rangle$ in $\mathbf{A}$.

1. For $k > r$, we have $a_k = 0$ in each component, so in $\mathbf{A}$. The element a_r is null in $\mathbf{A}/\langle e_r\rangle$, invertible in $\mathbf{A}/\langle 1-e_r\rangle$ therefore $\langle a_r\rangle = \langle e_r\rangle$.
Similarly in $\mathbf{A}/\langle e_r\rangle$, we have $\langle \overline{a_{r-1}}\rangle = \langle \overline{e_{r-1}}\rangle$ thus $\langle (1-e_r)a_{r-1}\rangle = \langle e_{r-1}\rangle$, and so on.

2. Localize at each of the e_i's.

Exercise 14. *(Locally monic polynomials)*
1. As $f(t) = 0$, we have $f \in \mathfrak{a}$, hence a surjective $\mathbf{A}$-linear map $\mathbf{A}[T]/\langle f\rangle \twoheadrightarrow \mathbf{A}[T]/\mathfrak{a}$ between two free $\mathbf{A}$-modules of the same rank n: it is an isomorphism (Proposition II-5.2), so $\mathfrak{a} = \langle f\rangle$.

2. The characteristic polynomial f of t is monic of degree n because $\mathbf{A}[t]$ is of constant rank n. As $f(t) = 0$, we have $f \in \mathfrak{a}$, hence a surjective $\mathbf{A}$-linear map $\mathbf{A}[T]/\langle f\rangle \twoheadrightarrow \mathbf{A}[T]/\mathfrak{a}$, of a free $\mathbf{A}$-module of rank n over an $\mathbf{A}$-projective module of constant rank n; it is therefore an isomorphism (Proposition 3.4), so $\mathfrak{a} = \langle f\rangle$.

3. Let $f = \sum_{i=0}^{r} a_i T^i = \sum_{i=0}^{r} f_r$ be a locally monic polynomial of formal degree r, with the fundamental system of orthogonal idempotents $(e_0, \dots, e_r)$, and $fe_d = f_d$ monic of degree d modulo $\langle 1-e_d\rangle$ for each $d \in [\![0..r]\!]$.
Then $a_r = e_r$ is idempotent. Then $f - f_r = (1-e_r)f$ is locally monic of formal degree $r-1$ and we can end by descending induction on r to compute the e_d's from f. If the ring is discrete we obtain a test to decide if a given polynomial is locally monic: each of the successively computed e_d's must be idempotent and the sum of the e_d's must be equal to 1.

Exercise 15. *(Invertible modules and projective modules of constant rank* 1*)*
1. There exists an $\mathbf{A}$-submodule N of $\mathbf{B}$ such that $M.N = \mathbf{A}$.
We have $(x_1, \dots, x_n)$ in M and $(y_1, \dots, y_n)$ in N such that $1 = \sum_i x_i y_i$ and $x_i y_j \in \mathbf{A}$. We verify that $M = \sum_i \mathbf{A}x_i$ and $N = \sum_i \mathbf{A}y_i$. Let $\sum_k z_k \otimes z'_k$ in $M \otimes_{\mathbf{A}} M'$. We have, by noticing that $y_i z_k \in N.M = \mathbf{A}$

$$\begin{aligned} \textstyle\sum_k z_k \otimes z'_k &= \textstyle\sum_{k,i} x_i y_i z_k \otimes z'_k &&= \textstyle\sum_{k,i} x_i\,(y_i z_k) \otimes z'_k \\ &= \textstyle\sum_{k,i} x_i \otimes (y_i z_k)\, z'_k &&= \textstyle\sum_i x_i \otimes \left(y_i \sum_k z_k z'_k\right), \end{aligned}$$

therefore the canonical surjection $M \otimes_{\mathbf{A}} M' \to M.M'$ is injective.

2. It must be shown that $\mathfrak{a}$ contains a regular element (Lemma V-7.7 *5*), which is immediate.

Exercise 16. *(The exact sequence with* $\mathsf{Pic}\,\mathbf{A}$ *and* $\mathsf{Pic}\,\mathbf{K}$*, where* $\mathbf{K} = \mathrm{Frac}\,\mathbf{A}$*)*
Defining the sequence is obvious; thus, the map $\mathbf{K}^\times \to \mathrm{Gfr}(\mathbf{A})$ is that which to $x \in \mathbf{K}^\times$ associates the principal fractional ideal $\mathbf{A}x$. No issues either to verify that the composition of two consecutive morphisms is trivial.
Exactness in $\mathbf{K}^\times$*:* if $x \in \mathbf{K}^\times$ is such that $\mathbf{A}x = \mathbf{A}$, then $x \in \mathbf{A}^\times$.
Exactness in $\mathrm{Gfr}(\mathbf{A})$*:* if $\mathfrak{a} \in \mathrm{Gfr}(\mathbf{A})$ is free, it means that it is principal i.e. of the form $\mathbf{A}x$ with $x \in \mathbf{K}^\times$.

Only the exactness in $\mathsf{Pic}\,\mathbf{A}$ is more delicate. Generally, if P is a finitely generated projective $\mathbf{A}$-module, then the canonical map $P \to \mathbf{K} \otimes_{\mathbf{A}} P$ is injective because P is contained in a free $\mathbf{A}$-module. Thus let P be an $\mathbf{A}$-projective module of constant rank 1 such that $\mathbf{K} \otimes_{\mathbf{A}} P \simeq \mathbf{K}$. Then P is injected into $\mathbf{K}$, then into $\mathbf{A}$ (multiply by a denominator), i.e. P is isomorphic to an integral ideal $\mathfrak{a}$ of $\mathbf{A}$. Similarly, the dual $P^\star$ is isomorphic to an integral ideal $\mathfrak{b}$ of $\mathbf{A}$.

We have $\mathbf{A} \simeq P \otimes_{\mathbf{A}} P^\star \simeq \mathfrak{a} \otimes_{\mathbf{A}} \mathfrak{b} \simeq \mathfrak{a}\mathfrak{b}$, so $\mathfrak{a}\mathfrak{b}$ is generated by a regular element $x \in \mathbf{A}$. We have $x \in \mathfrak{a}$ so $\mathfrak{a}$ is an invertible ideal: we have found an invertible ideal $\mathfrak{a}$ of $\mathbf{A}$ such that $\mathfrak{a} \simeq P$.

Exercise 24. *1* and *2.* Immediate.

3. Consider the short sequence $\mathbf{A}^N \xrightarrow{A'} \mathbf{A}^m \xrightarrow{A} \mathbf{A}^n$; it is locally exact, so it is globally exact.

4. Every stably free module of rank 1 can be given in the form $\operatorname{Ker} A$ where $A \in \mathbf{A}^{n\times(n+1)}$ is a surjective matrix $\mathbf{A}^{n+1} \xrightarrow{A} \mathbf{A}^n$. Since $1 \in \mathcal{D}_n(A)$, we apply question *3* with $m = n+1$. We obtain $A' \in \mathbf{A}^{(n+1)\times 1}$ of rank 1 with $\operatorname{Im} A' = \operatorname{Ker} A$; so the column A' is a basis of $\operatorname{Ker} A$.

Exercise 25. *(Homogeneous polynomials and* $\mathbb{P}^n(\mathbf{k})$*)*

Let $f \in \mathbf{k}[X_0, \dots, X_n]$ be a homogeneous polynomial of degree m and (to simplify) $P = \langle \underline{a}, \underline{b}, \underline{c} \rangle \subseteq \mathbf{k}^{n+1}$ be a direct summand of rank 1. Suppose that $f(\underline{a}) = f(\underline{b}) = f(\underline{c}) = 0$ and that we want to show that $f(\underline{x}) = 0$ if $\underline{x} = \alpha\underline{a}+\beta\underline{b}+\gamma\underline{c}$. The matrix of $(\underline{a}, \underline{b}, \underline{c})$ is of rank 1, therefore the a_i's, b_j's, c_k's are comaximal. It therefore suffices to prove the equality after localization at one of these coordinates. For example over $\mathbf{k}[1/a_0]$ we have $\underline{x} = (\alpha + \frac{b_0}{a_0}\beta + \frac{c_0}{a_0}\gamma)\underline{a} = \lambda\underline{a}$, and so $f(\underline{x}) = \lambda^m f(\underline{a}) = 0$.

Exercise 26. *(Tangent space to* $\mathbb{GL}_n$*)*

Consider the $\mathbf{k}$-algebra $\mathbf{k}[\varepsilon] = \mathbf{k}[T]\big/\big\langle T^2 \big\rangle$.

Let $A \in \mathbb{GL}_n(\mathbf{k})$ and $H \in \mathbb{M}_n(\mathbf{k})$. We have $A + \varepsilon H = A(\mathrm{I}_n + \varepsilon A^{-1}H)$, and $\mathrm{I}_n + \varepsilon M$ is invertible, with inverse $\mathrm{I}_n - \varepsilon M$, for every $M \in \mathbb{M}_n(\mathbf{k})$. Therefore $A + \varepsilon H \in \mathbb{GL}_n(\mathbf{k})$ for any H. Thus, the tangent space $\mathrm{T}_A(\mathbb{GL}_n)$ is isomorphic to $\mathbb{M}_n(\mathbf{k})$.

NB: $(A + \varepsilon H)^{-1} = A^{-1} - \varepsilon A^{-1}HA^{-1}$.

Exercise 27. *(Tangent space to* $\mathbb{SL}_n$*)*

We use the $\mathbf{k}$-algebra $\mathbf{k}[\varepsilon]$ of Exercise 26. For A, $H \in \mathbb{M}_n(\mathbf{k})$, we have $\det(A + \varepsilon H) = \det(A) + \varepsilon \operatorname{Tr}(\widetilde{A}H)$. We deduce

$$\det(A + \varepsilon H) = 1 \iff (\det(A) = 1 \text{ and } \operatorname{Tr}(\widetilde{A}H) = 0).$$

We therefore have, for $A \in \mathbb{SL}_n(\mathbf{k})$, $\mathrm{T}_A(\mathbb{SL}_n) = \big\{\, H \in \mathbb{M}_n(\mathbf{k}) \;\big|\; \operatorname{Tr}(\widetilde{A}H) = 0 \,\big\}$.

Let us show that $\mathrm{T}_A(\mathbb{SL}_n)$ is a free $\mathbf{k}$-module of rank $n^2 - 1$.

Indeed, the $\mathbf{k}$-linear automorphism $H \mapsto AH$ of $\mathbb{M}_n(\mathbf{k})$ transforms I_n into A and bijectively applies $\mathrm{T}_{\mathrm{I}_n}(\mathbb{SL}_n)$ over $\mathrm{T}_A(\mathbb{SL}_n)$, since we can verify it by writing $\operatorname{Tr}(H) = \operatorname{Tr}(\widetilde{A}\,AH)$. Finally, $\mathrm{T}_{\mathrm{I}_n}(\mathbb{SL}_n)$ is the $\mathbf{k}$-submodule of $\mathbb{M}_n(\mathbf{k})$ made of the matrices of null trace (which is indeed free of rank $n^2 - 1$).

NB: $H \mapsto HA$ was also possible, because $\operatorname{Tr}(AH\,\widetilde{A}) = \operatorname{Tr}(\widetilde{A}\,AH) = \operatorname{Tr}(H)$.

Exercise 28. *(Tangent space at J_0 to the nilpotent cone)*
1. We easily see that $\varphi(H)J_0 = J_0\varphi(H)$. If $\mathbf{k}$ was a field, we could deduce that $\varphi(H)$ is a polynomial in J_0. The direct computation gives

$$\varphi(e_{ij}) = \begin{cases} 0 & \text{if } i < j \\ J_0^{n-1-(i-j)} & \text{otherwise.} \end{cases}$$

In particular, $\varphi(e_{i1}) = J_0^{n-i}$. We therefore have $\operatorname{Im}\varphi = \bigoplus_{k=0}^{n-1} \mathbf{k}J_0^k$.

2. For $k \in [\![0..n-1]\!]$, the matrix J_0^k has null coefficients, except for those that are on the k^{th} up-diagonal, all equal to 1. We can therefore take as direct complement of $\operatorname{Im}\varphi$ the submodule generated by the e_{ij}'s, with $j < n$ (we therefore omit the e_{in}'s which corresponds to the last position of the up-diagonals of the J_0^k's). We then define ψ by

$$\psi(e_{ij}) = \begin{cases} 0 & \text{if } j < n \\ e_{i1} & \text{if } j = n \end{cases} \quad \text{or} \quad \psi(H) = H\,{}^{\text{t}}J_0^{n-1}.$$

We easily verify that $\psi(J_0^{n-i}) = e_{i1}$ for $i \in [\![1..n]\!]$, then $(\varphi\circ\psi)(A) = A$ if $A \in \operatorname{Im}\varphi$, and finally $\varphi\circ\psi\circ\varphi = \varphi$. By miracle, we also have $\psi\circ\varphi\circ\psi = \psi$.
We have $e_{ij} - e_{i'j'} \in \operatorname{Ker}\varphi$ as soon as $i'-j' = i-j$ ($i' \geqslant j'$, $i \geqslant j$) and we obtain a basis of $\operatorname{Ker}\varphi$ by considering the $\frac{n(n-1)}{2}$ matrices e_{ij} with $i < j$ and the $\frac{n(n-1)}{2}$ matrices $e_{i1} - e_{i+r,1+r}$, $r \in [\![1..n-i]\!]$, $i \in [\![1..n-1]\!]$.

3. We use the $\mathbf{k}$-algebra $\mathbf{k}[\varepsilon] \simeq \mathbf{k}[T]\big/\big\langle T^2\big\rangle$. For $A, H \in \mathbb{M}_n(\mathbf{k})$, we have

$$(A+\varepsilon H)^n = A^n + \varepsilon \textstyle\sum_{i+j=n-1} A^i H A^j.$$

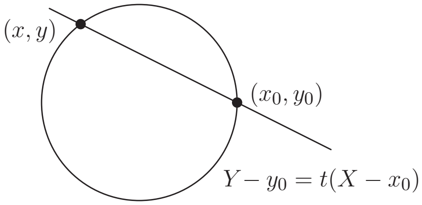
For $A = J_0$, we find that the tangent space "to the nilpotent cone" is $\operatorname{Ker}\varphi$ which is a free module of rank $n^2 - n$ (it is the dimension of the nilpotent cone).

Problem 1. *(The ring of the circle)*
1. Naively: let $f = f(x,y) \in \mathbf{k}[x,y]$ be a conic, i.e. a polynomial of degree 2, and (x_0,y_0) be a $\mathbf{k}$-point of $\{f(x,y)=0\}$.

The classical trick of parameterization consists in defining t by $y - y_0 = t(x - x_0)$ and, in the equation

$$f(x,y) = f\big(x, t_0 + t(x-x_0)\big) = 0,$$

in looking for x in terms of t. This equation admits $x = x_0$ as a solution, hence the other solution in the rational form.



Algebraically speaking, we suppose that f is irreducible. Let $\mathbf{k}[x,y] = \mathbf{k}[X,Y]/\langle f\rangle$. We obtain $\mathbf{k}(x,y) = \mathbf{k}(t)$ with $t = (y-y_0)/(x-x_0)$. Here, the reader will compute the expressions of x, y in terms of t: $x = \frac{t^2-1}{t^2+1}$, $y = \frac{-2t}{t^2+1}$.
Geometrically, the elements of $\mathbf{k}[x,y]$ are precisely the rational fractions defined everywhere on the projective line $\mathbb{P}^1(\mathbf{k})$ (parameterized by t) except maybe at the "point" $t = \pm i$.

2. We have $x = 1 - 2u$, $y = -2v$, so $\mathbf{k}[x,y] = \mathbf{k}[u,v]$. The equality $\mathbf{k}[x,y] = \mathbf{k}[u,v]$ is not difficult and is left to the reader. What is more difficult, is to show that $\mathbf{k}[u,v]$ is the integral closure of $\mathbf{k}[u]$ in $\mathbf{k}(t)$. We refer the reader to Exercise XII-8.

Geometrically, the poles of x and y are $t = \pm i$, which confirms that x, y are integral over $\mathbf{k}[(1+t^2)^{-1}] = \mathbf{k}[u]$. Algebraically, we have $x = 1 - u$, $y^2 = -1 - x^2 \in \mathbf{k}[u]$, and x, y are indeed integral over $\mathbf{k}[u]$.

3. If $i^2 = -1$, we have $(x+iy)(x-iy) = 1$.

By letting $w = x + iy$, we have $\mathbf{k}[x,y] = \mathbf{k}[w, w^{-1}]$.

4. We apply the standard method at a smooth point of a planar curve. We write

$$f(X,Y) - f(x_0,y_0) = (X - x_0)u(X,Y) + (Y - y_0)v(X,Y)$$

with here $u = X + x_0$, $v = Y + y_0$; the matrix $A = \begin{bmatrix} y - y_0 & x + x_0 \\ x_0 - x & y + y_0 \end{bmatrix}$ is therefore a presentation matrix of $(x - x_0, y - y_0)$ with $1 \in \mathcal{D}_1(A)$. Let us explicate the membership $1 \in \mathcal{D}_1(A)$:

$$(-y_0)(y - y_0) + x_0(x + x_0) + x_0(x_0 - x) + y_0(y + y_0) = 2.$$

This leads to the matrix $B = \frac{1}{2}\begin{bmatrix} -y_0 & x_0 \\ x_0 & y_0 \end{bmatrix}$; this one satisfies $ABA = A$ and the desired matrix P is $P = \mathrm{I}_2 - AB = \widetilde{AB}$

$$AB = \frac{1}{2}\begin{bmatrix} y - y_0 & x + x_0 \\ x_0 - x & y + y_0 \end{bmatrix}\begin{bmatrix} -y_0 & x_0 \\ x_0 & y_0 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} x_0x - y_0y + 1 & y_0x + x_0y \\ y_0x + x_0y & -x_0x + y_0y + 1 \end{bmatrix}.$$

Hence the general expression of P, $P = \frac{1}{2}\begin{bmatrix} -x_0x + y_0y + 1 & -(y_0x + x_0y) \\ -(y_0x + x_0y) & x_0x - y_0y + 1 \end{bmatrix}$,

for $x_0 = 1$, $y_0 = 0$: $\frac{1}{2}\begin{bmatrix} 1 - x & -y \\ -y & 1 + x \end{bmatrix}$. Thus, P is a projector of rank 1, presentation matrix of $(x - x_0, y - y_0)$. As P is symmetric, Equality (5) of Proposition V-7.4 has as consequence that $(x - x_0)^2 + (y - y_0)^2$ is a generator of $\langle x - x_0, y - y_0\rangle$ with $(x - x_0)^2 + (y - y_0)^2 = -2(x_0x + y_0y - 1)$.

Geometrically, $xx_0 + yy_0 - 1 = 0$ is the tangent line to the circle $x^2 + y^2 = 1$ at the point $P_0 = (x_0, y_0)$. For those who know the divisors: the divisor of the zeros-poles of this tangent is the principal divisor $2P_0 - 2P_{t=\pm i}$, which corresponds to the fact that the square of the ideal $\langle x - x_0, y - y_0\rangle$ is principal.

Variant I: we directly treat the case of the point $(x,y) = (1,0)$ (see the following question) then we use the fact that the circle is a group to pass from the point $(1,0)$ to an arbitrary point $P_0 = (x_0,y_0)$. Thus, we dispose of the "rotation" automorphism

$$\begin{bmatrix} x \\ y \end{bmatrix} \mapsto \begin{bmatrix} x_0 & -y_0 \\ y_0 & x_0 \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix} \text{ which realises } \begin{bmatrix} x_0 & -y_0 \\ y_0 & x_0 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} x_0 \\ y_0 \end{bmatrix}.$$

We consider its inverse R

$$R = \begin{bmatrix} x_0 & y_0 \\ -y_0 & x_0 \end{bmatrix},\ R\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x' \\ y' \end{bmatrix},\ R\begin{bmatrix} x_0 \\ y_0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix},$$

so that

$$R\begin{bmatrix} x - x_0 \\ y - y_0 \end{bmatrix} = \begin{bmatrix} x' - 1 \\ y' \end{bmatrix}, \quad \text{hence} \quad \left\langle x' - 1, y' \right\rangle = \langle x - x_0, y - y_0\rangle.$$

As $\langle x'-1,y'\rangle^2=\langle x'-1\rangle$, we obtain $\langle x-x_0,y-y_0\rangle^2=\langle x_0x+y_0y-1\rangle$.

Variant II: we provide another justification of the invertibility of $\langle x-x_0,y-y_0\rangle$ which does not directly use the fact that the circle is smooth. We consider $\mathbf{k}[x,y]$ as an extension of degree 2 of $\mathbf{k}[x]$, by using $(1,y)$ as the basis. We dispose of a $\mathbf{k}[x]$-automorphism σ which transforms y into $-y$.

We consider the norm N of $\mathbf{k}[x,y]$ over $\mathbf{k}[x]$. For $z=a(x)+b(x)y$, we have

$$\mathrm{N}(z)=z\sigma(z)=(a+by)(a-by)=a^2-(1-x^2)b^2=a^2+(x^2-1)b^2.$$

The idea to invert $\langle x-x_0,y-y_0\rangle$ is to multiply it by its $\mathbf{k}[x]$-conjugate. Let us show the following equality, certificate of the invertibility of the ideal $\langle x-x_0,y-y_0\rangle$,

$$\langle x-x_0,y-y_0\rangle\ \langle x-x_0,y+y_0\rangle=\langle x-x_0\rangle\,.$$

Indeed, the generators of the left-product are

$$(x-x_0)^2,\quad (x-x_0)(y+y_0),\quad (x-x_0)(y-y_0),\quad y^2-y_0^2=x_0^2-x^2.$$

Hence $\langle x-x_0,y-y_0\rangle\ \langle x-x_0,y+y_0\rangle=(x-x_0)\,\langle g_1,g_2,g_3,g_4\rangle$ with

$$g_1=x-x_0,\quad g_2=y+y_0,\quad g_3=y-y_0,\quad g_4=x+x_0.$$

But $\langle g_1,g_2,g_3,g_4\rangle$ contains $\frac{g_4-g_1}{2}=x_0$ and $\frac{g_2-g_3}{2}=y_0$ therefore it contains $1=x_0^2+y_0^2$.

5. By brute force, by using only using $1\in\langle x-1,x+1\rangle$ on the right-hand side,

$$\langle x-1,y\rangle\ \langle x-1,y\rangle=\left\langle (x-1)^2,(x-1)y,y^2\right\rangle=(x-1)\ \langle x-1,y,-(x+1)\rangle=\langle x-1\rangle\,.$$

We divide this equality by $x-1$: $\langle x-1,y\rangle\ \left\langle 1,\frac{y}{x-1}\right\rangle=\langle 1\rangle$ and let

$$x_1=x-1,\quad x_2=y,\ y_1=1,\ y_2=\tfrac{y}{x-1},\ \text{ such that } x_1y_1+x_2y_2=-2,$$

which leads to the projection matrix P of rank 1

$$P=\frac{-1}{2}\begin{bmatrix}y_1\\ y_2\end{bmatrix}[x_1,x_2]=\frac{-1}{2}\begin{bmatrix}x_1y_1 & x_2y_1\\ x_1y_2 & x_2y_2\end{bmatrix}=\frac{1}{2}\begin{bmatrix}1-x & -y\\ -y & 1+x\end{bmatrix}$$

6. Let $\mathrm{N}=\mathrm{N}_{\mathbf{k}[x,y]/\mathbf{k}}$. For $a,b\in\mathbf{k}[x]$, $\mathrm{N}(a+by)=a^2+(x^2-1)b^2$. The equality to prove on the degrees is obvious if a or b is null. Otherwise, we write, with $n=\deg a$ and $m=1+\deg b$, $a^2=\alpha^2x^{2n}+\dots$, $(x^2-1)b^2=\beta^2x^{2m}+\dots$ $(\alpha,\beta\in\mathbf{k}^\star)$. The case where $2n\neq 2m$ is easy. If $2n=2m$, then $\alpha^2+\beta^2\neq 0$ (because -1 is not a square in $\mathbf{k}$), and so the polynomial $a^2+(x^2-1)b^2$ is of degree $2n=2m$.

If $a+by$ is invertible in $\mathbf{A}$, $\mathrm{N}(a+by)\in\mathbf{k}[x]^\times=\mathbf{k}^\star$; hence $b=0$ then a is constant. Recap: $\mathbf{k}[x,y]^\times=\mathbf{k}^\star$. This is specific to the fact that -1 is not a square in $\mathbf{k}$ because if $i^2=-1$, the equality $(x+iy)(x-iy)=1$ shows the existence of invertibles other than the constants.

Let us show that y is irreducible.

If $y=zz'$, then $\mathrm{N}(y)=\mathrm{N}(z)\mathrm{N}(z')$, i.e. $x^2-1=(x-1)(x+1)=\mathrm{N}(z)\mathrm{N}(z')$. But in $\mathbf{k}[x]$, $x\pm 1$ are not associated with a norm (a nonzero norm is of even degree). Therefore $\mathrm{N}(z)$ or $\mathrm{N}(z')$ is a constant, i.e. z or z' is invertible. Similarly, $1\pm x$ are irreducible.

We will use the equality

$$y^2=(1-x)(1+x),\ \text{ analogous to }\ 2\cdot 3=(1+\sqrt{-5})(1-\sqrt{-5})\text{ in }\mathbb{Z}[\sqrt{-5}],$$

to see that $\langle x-1,y\rangle$ is not a principal ideal : an equality $\langle x-1,y\rangle=\langle d\rangle$ would entail $d\mid x-1$, $d\mid y$, i.e. d invertible, and thus $1\in\langle x-1,y\rangle$, which is not the case.

Problem 2. *(The operations λ_t and γ_t over $\mathsf{K}_0(\mathbf{A})$)*
1. We have $\lambda_t(\mathbf{A}) = \lambda_t(1) = 1+t$ and $\gamma_t(1) = 1/(1-t)$, so $\lambda_t(p) = (1+t)^p$ and $\gamma_t(p) = 1/(1-t)^p$ for $p \in \mathbb{N}^*$.
We write x in the form $[P]-[\mathbf{A}^p] = P-p$ for a certain $p \in \mathbb{N}^*$, with P of constant rank p. By definition $\gamma_t([P]) = \sum_{n=0}^{p} \lambda^n(P)t^n/(1-t)^n$, we have

$$\gamma_t(x) = \frac{\gamma_t([P])}{\gamma_t(p)} = \textstyle\sum_{n=0}^{p} \lambda^n(P)t^n(1-t)^{p-n}.$$

Thus $\gamma_t(x)$ is a polynomial of degree $\leqslant p$ in t.
Note: $\gamma^p(x) = \sum_{n=0}^{p} \lambda^n(P)(-1)^{p-n} = (-1)^p \sum_{n=0}^{p} \lambda^n(P)(-1)^n = (-1)^p\lambda_{-1}(P)$.
We have $\gamma_t(x)\gamma_t(-x) = 1$ and as they are polynomials of $\mathsf{K}_0(\mathbf{A})[t]$, their coefficients of degree > 0 are nilpotent (Lemma II-2.6 and Exercise VII-8). In particular the element x, which is the coefficient of degree 1 of $\gamma_t(x)$, is nilpotent.

2. Let $x \in \mathsf{K}_0(\mathbf{A})$ be nilpotent, then $\operatorname{rk} x$ is a nilpotent element of $\mathsf{H}_0(\mathbf{A})$. But this last ring is reduced (actually, pp-ring); thus $\operatorname{rk} x = 0$.

3. Suppose $\operatorname{rk} x = [e]$ for some idempotent e.
We have $\bigwedge^n(e\mathbf{A}) = 0$ for $n \geqslant 2$, therefore $\lambda_t([e]) = 1+[e]t$. By definition of a^r for $a \in \mathbf{B}$ and $r \in \mathsf{H}_0\,\mathbf{B}$, we obtain $(1+t)^{[e]} = (1-e)+e(1+t) = 1+et$.
By direct computation we also obtain $\mathrm{R}_{e\mathbf{A}}(t) = (1-e)+te$.
Finally, we have by convention $\mathbb{B}(\mathbf{A}) \subseteq \mathsf{H}_0\,\mathbf{A}$ with the identification $e = [e]$.
We then obtain the general equality for $x = [P]$ by using the fundamental system of orthogonal idempotents formed by the coefficients of R_P and by noting that the two members are morphisms from $\mathsf{K}_0(\mathbf{A})$ to $1 + t\,\mathsf{K}_0(\mathbf{A})[[t]]$.
Let us also note that $\lambda_t(p) = (1+t)^p$ for $p \in \mathbb{N}^*$ is the desired equality when $\operatorname{rk} x \in \mathbb{N}^*$.

4. Is obtain from item *1* by replacing t by $t/(1-t)$.

5. Some $x \in \mathsf{K}_0(\mathbf{A})$ is of the form $y+r$ with $r = \operatorname{rk} x \in \mathsf{H}_0\,\mathbf{A}$ and $y \in \widetilde{\mathsf{K}}_0\,\mathbf{A}$. Then $\gamma_t(x) = \gamma_t(y)(1-t)^{-r}$.

6. Recall the two following formulas, for $d \geqslant 1$,

$$\tfrac{1}{(1-t)^d} = \textstyle\sum_{k\geqslant 0} \binom{k+d-1}{d-1} t^k, \qquad (1-t)^{-d} = \sum_{k\geqslant 0} \binom{-d}{k}(-t)^k.$$

They are related by the equality

$$\tbinom{k+d-1}{d-1} = \tbinom{k+d-1}{k} = \tbinom{-d}{k}(-1)^k.$$

By definition,

$$\gamma_t(x) = 1 + \textstyle\sum_{d\geqslant 1} \frac{\lambda^d(x)t^d}{(1-t)^d} = 1 + \sum_{d\geqslant 1, k\geqslant 0} \lambda^d(x)t^d\binom{k+d-1}{d-1}t^k.$$

For $n \geqslant 1$, the coefficient $\gamma^n(x)$ of t^n is

$$\textstyle\sum_{k+d=n} \lambda^d(x)\binom{k+d-1}{d-1} \quad \text{i.e. with } p = d-1 \quad \sum_{p=0}^{n-1} \lambda^{p+1}(x)\binom{n-1}{p}.$$

The other equality is deduced via the equivalence $\gamma_t = \lambda_{t/(1-t)} \iff \lambda_t = \gamma_{t/(1+t)}$.

Problem 3. *(The projective map of Noether and the projective modules of constant rank* 1 *direct summands in* $\mathbf{k}^2$*)*
1. Uniqueness of the factorization up to order of the factors and up to invertible elements .

2. The product of primitive polynomials is a primitive polynomial, cf. Lemma II-2.6 (Poor man's Gauss-Joyal). We have the more precise result which consists of the inclusion of ideals

$$\langle x_1, y_1\rangle \cdots \langle x_n, y_n\rangle \subseteq \mathrm{D}_{\mathbf{k}}(\langle z_0, \dots, z_n\rangle).$$

We can deduce it from the following fact: if f, g are two polynomials with an indeterminate, the product of a coefficient of f and of a coefficient of g is integral over the ideal generated by the coefficients of the product fg (see Lemma XII-2.7), and in particular it is in the radical of this ideal.

We can also use the following approach: for $I \subseteq [\![1..n]\!]$, let I' be its complement, $x_I = \prod_{i\in I} x_i$, $y_I = \prod_{i\in I} y_i$. For $d = \#I$ and $N = \binom{n}{d}$, we will show an equality

$$(\star') \qquad \prod\nolimits_{\#I=d}(T - x_I y_{I'}) = T^N + \sum\nolimits_{j=1}^{N} a_j T^{N-j}, \quad a_j \in \langle z_0, \dots, z_n\rangle\,.$$

By making $T = x_I y_{I'}$, we will have $(x_I y_{I'})^N \in \langle z_0, \dots, z_n\rangle$, therefore showing the stated inclusion of ideals. To prove $(\star')$, we first examine the case where all the y_i's are equal to 1. We write, by letting $S_1(x), \dots, S_n(x)$ be the elementary symmetric functions of $(x_1, \dots, x_n)$

$$\prod\nolimits_{\#I=d}(T - x_I) = T^N + \sum\nolimits_{j=1}^{N} b_j T^{N-j}, \qquad b_j = f_j\big(S_1(x), \dots, S_n(x)\big).$$

A careful examination shows that f_j is a polynomial of degree $\leqslant j$ in $(S_1, \dots, S_n)$. Let us replace in this last equality x_i by x_i/y_i and multiply by $(y_1 \cdots y_n)^N$; we obtain, with $U = y_1 \cdots y_n T$ and $s_i = S_i(x_1/y_1, \dots, x_n/y_n)$

$$\prod\nolimits_{\#I=d}(U - x_I y_{I'}) = U^N + \sum\nolimits_{j=1}^{N} (y_1 \cdots y_n)^j f_j(s_1, \dots, s_n) U^{N-j}.$$

Let $s_1^{\alpha_1} \cdots s_n^{\alpha_n}$ be a monomial of $f_j(s_1, \dots, s_n)$; since $\sum_i \alpha_i \leqslant \deg f_j \leqslant j$, we obtain, by remembering that $z_n = y_1 \cdots y_n$, an equality

$z_n^j s_1^{\alpha_1} \cdots s_n^{\alpha_n} = z_n^{\alpha_0}(z_n s_1)^{\alpha_1} \cdots (z_n s_n)^{\alpha_n} = z_n^{\alpha_0} z_{n-1}^{\alpha_1} \cdots z_0^{\alpha_n}$ with $\alpha_0 = j - \sum_i \alpha_i$.

Since $j \geqslant 1$, one of the exponents α_i above is not null and we indeed have the membership to $\langle z_0, \dots, z_n\rangle$, then the equality $(\star')$.

3. Let $E = P_1 \otimes_{\mathbf{k}} \cdots \otimes_{\mathbf{k}} P_n \subset L^{n\otimes}$; it is a projective module of constant rank 1. Let us show that the restriction of π to E is injective and that $\pi(E)$ is a direct summand in $S_n(L)$. This will indeed prove that $\pi(E)$ is a $\mathbf{k}$-point of $\mathbb{P}^n$. Thanks to a finite number of comaximal localizations, we are brought back to the case where each P_i is free with basis $x_i X + y_i Y$. Then each (x_i, y_i) is unimodular and $\sum_{i=0}^{n} z_i X^{n-i} Y^i$ is a unimodular basis of $\pi(E)$. This proves on the one hand that $\pi|_E$ is injective (since it transforms a basis of E into a unimodular vector of $S_n(L)$) and that $\pi(E)$ is a direct summand in $S_n(L)$.

4. It seems that φ is injective, i.e. $(z_0, \dots, z_n)$ are algebraically independent over $\mathbf{k}$. The image by φ is the graded subring $\mathbf{A} = \mathbf{k}[z_0, \dots, z_n] \subset \mathbf{k}[\underline{X}, \underline{Y}]$ (the homogeneous component of an element of $\mathbf{A}$ is in $\mathbf{A}$); if $f \in \mathbf{A}$ is homogeneous of degree m, we have $m \equiv 0 \bmod n$, and for arbitrary $t_1, \dots, t_n$

$$f(t_1 X_1, t_1 Y_1, \dots, t_n X_n, t_n Y_n) = (t_1 \dots t_n)^{m/n} f(X_1, Y_1, \dots, X_n, Y_n).$$

Finally, $\mathbf{A}$ is invariant under the action of the symmetric group S_n which acts on $\mathbf{k}[\underline{X}, \underline{Y}]$ by

$$\sigma \cdot f(X_1, Y_1, \dots, X_n, Y_n) = f(X_{\sigma(1)}, Y_{\sigma(1)}, \dots, X_{\sigma(n)}, Y_{\sigma(n)}).$$

These last two properties probably characterize $\mathbf{A}$.

Problem 4. *(Hilbert's theorem 90, multiplicative form)*
We fix once and for all an element $b_0 \in \mathbf{B}$ of trace 1.

1 and *2.* No difficulty. The fact that θ_c is multiplicative exactly translates the fact that c is a 1-cocycle.

3. The action of G over $\mathbf{B}$ twisted by the 1-cocycle c is $\sigma \cdot_c b = c_\sigma \sigma(b)$; the fact that this is an action is exactly the condition of 1-cocyclicity of c. Indeed

$$\tau \cdot_c (\sigma \cdot_c b) = \tau \cdot_c c_\sigma \sigma(b) = c_\tau \tau\big(c_\sigma \sigma(b)\big) = c_\tau \tau(c_\sigma)\,(\tau\sigma)(b) = c_{\tau\sigma}\,(\tau\sigma)(b) = (\tau\sigma) \cdot_c b.$$

We will notice that $\pi_c = \sum_\sigma c_\sigma\, \sigma$ is some sort of G-trace relatively to the action of G twisted by c.

We therefore have $\mathbf{B}_c^G = \{\, b \in \mathbf{B} \mid c_\sigma \sigma(b) = b \,\}$. By using the fact that c is a 1-cocycle, we find that $\tau \circ \pi_c = c_\tau^{-1}\, \pi_c$; we deduce that $c_\tau \tau(z) = z$ for every $z \in \operatorname{Im} \pi_c$, i.e. $\operatorname{Im} \pi_c \subseteq \mathbf{B}_c^G$. We define $s : \mathbf{B}_c^G \to \mathbf{B}$ by $s(b) = bb_0$. Then $\pi_c \circ s = \mathrm{Id}_{\mathbf{B}_c^G}$; indeed, for $b \in \mathbf{B}_c^G$,

$$\pi_c(b_0 b) = \textstyle\sum_\sigma c_\sigma \sigma(bb_0) = \sum_\sigma c_\sigma \sigma(b)\sigma(b_0) = \sum_\sigma b\sigma(b_0) = b\,\mathrm{Tr}_{\mathbf{B}/\mathbf{A}}(b_0) = b.$$

From the equality $\pi_c \circ s = \mathrm{Id}_{\mathbf{B}_c^G}$, we deduce that π_c is a surjection from $\mathbf{B}$ to $\mathbf{B}_c^G$, that s is injective and that $\mathbf{B} = s(\mathbf{B}_c^G) \oplus \operatorname{Ker} \pi_c \simeq \mathbf{B}_c^G \oplus \operatorname{Ker} \pi_c$. In particular, $\mathbf{B}_c^G$ is a finitely generated projective $\mathbf{A}$-module.

Remark. Let us consider $s : b \mapsto b_0 b$ in $\mathrm{End}_{\mathbf{A}}(\mathbf{B})$, then $(\pi_c \circ s)\big(\pi_c(z)\big) = \pi_c(z)$ for all $z \in \mathbf{B}$, i.e. $\pi_c \circ s \circ \pi_c = \pi_c$. Consequently $\pi_c' \overset{\mathrm{def}}{=} \pi_c \circ s = \sum_\sigma c_\sigma \sigma(b_0 \bullet)$ is a projector; we could certainly compute its trace and find 1, which would prove that π_c' is a projector of rank 1.

4. Let c, d be two 1-cocycles, $x \in \mathbf{B}_c^G$, $y \in \mathbf{B}_d^G$, so $c_\sigma \sigma(x) = x$, $d_\sigma \sigma(y) = y$; we easily verify that $xy \in \mathbf{B}_{cd}^G$.
Hence an $\mathbf{A}$-linear map $\mathbf{B}_c^G \otimes_{\mathbf{A}} \mathbf{B}_d^G \to \mathbf{B}_{cd}^G$, $x \otimes y \mapsto xy$, denoted by $\mu_{c,d}$.
Let (x_i), (y_i) be two systems of elements of $\mathbf{B}$ like in Lemma VI-7.10 and let $\varepsilon = \sum_i x_i \otimes y_i = \sum_i y_i \otimes x_i$ (separability idempotent). Recall that $\varepsilon \in \mathrm{Ann}(\mathrm{J})$, which translates to

$$\forall\, b \in \mathbf{B} \quad \textstyle\sum_i bx_i \otimes y_i = \sum x_i \otimes by_i \quad \text{in} \quad \mathbf{B}_{\mathbf{A}}^{\mathrm{e}} \overset{\mathrm{def}}{=} \mathbf{B} \otimes_{\mathbf{A}} \mathbf{B}.$$

We also have, for b, $b' \in \mathbf{B}$

$$\mathrm{Tr}_{\mathbf{B}/\mathbf{A}}(bb') = \textstyle\sum_i \mathrm{Tr}_{\mathbf{B}/\mathbf{A}}(bx_i)\,\mathrm{Tr}_{\mathbf{B}/\mathbf{A}}(b'y_i).$$

We will show that $z \mapsto (\pi_c \otimes \pi_d)(b_0 z \varepsilon)$, $\mathbf{B}_{cd}^G \mapsto \mathbf{B}_c^G \otimes_{\mathbf{A}} \mathbf{B}_d^G$ and $\mu_{c,d}$ are reciprocals of one another. In one direction,

$$(\pi_c \otimes \pi_d)(b_0 z \varepsilon) = \textstyle\sum_i a_i \otimes b_i, \quad \text{with} \quad a_i = \sum_\sigma c_\sigma \sigma(b_0 z x_i), \quad b_i = \sum_\tau c_\tau \tau(y_i),$$

and we have

$$\textstyle\sum_i a_i b_i = \sum_{\sigma,\tau} \sigma(b_0 z) c_\sigma d_\tau \sum_i \sigma(x_i)\tau(y_i),$$

and since the internal sum (over i) evaluates to 1 or 0, there remains, for $z \in \mathbf{B}_{cd}^G$

$$\sum_i a_i b_i = \sum_\sigma \sigma(b_0 z) c_\sigma d_\sigma = \sum_\sigma \sigma(b_0)\sigma(z)(cd)_\sigma = \sum_\sigma \sigma(b_0) z = z\,\mathrm{Tr}_{\mathbf{B}/\mathbf{A}}(b_0) = z.$$

In the other direction, let $x \in \mathbf{B}_c^G$ and $y \in \mathbf{B}_d^G$. Then, since $\varepsilon \in \mathrm{Ann}(\mathrm{J})$, we can write

$$(\pi_c \otimes \pi_d)(b_0 xy\varepsilon) = \textstyle\sum_i a_i \otimes b_i, \text{ with } a_i = \sum_\sigma c_\sigma \sigma(b_0 x x_i),\ b_i = \sum_\tau d_\tau \tau(y y_i).$$

By using

$$c_\sigma\sigma(b_0 x x_i) = c_\sigma\sigma(x)\sigma(b_0 x_i) = x\sigma(b_0 x_i) \text{ and } d_\tau\tau(y y_i) = d_\tau\tau(y)\tau(y_i) = y\tau(y_i),$$

we get

$$\sum\nolimits_i a_i \otimes b_i = \sum\nolimits_i x \,\mathrm{Tr}_{\mathbf{B}/\mathbf{A}}(b_0 x_i) \otimes y \,\mathrm{Tr}_{\mathbf{B}/\mathbf{A}}(y_i) =$$
$$(x\otimes y)\cdot\Big(\sum\nolimits_i \mathrm{Tr}_{\mathbf{B}/\mathbf{A}}(b_0 x_i)\,\mathrm{Tr}_{\mathbf{B}/\mathbf{A}}(y_i)\otimes 1\Big) = (x\otimes y)\cdot\Big(\mathrm{Tr}_{\mathbf{B}/\mathbf{A}}(b_0)\otimes 1\Big) = x\otimes y.$$

Item a is proved.
For item b, let there be a 1-cocycle, coboundary of $b_1 \in \mathbf{B}^\times$, $c_\sigma = \sigma(b_1)b_1^{-1}$.
Then $b \in \mathbf{B}_c^G$ if and only if for every σ, $c_\sigma\sigma(b) = b$, i.e. $\sigma(b_1 b) = b_1 b$ i.e. $b_1 b \in \mathbf{A}$; so $\mathbf{B}_c^G = b_1^{-1}\mathbf{A}$. We deduce that $\mathbf{B}_c^G \otimes \mathbf{B}_{c^{-1}}^G \simeq \mathbf{A}$, so $\mathbf{B}_c^G$ is an projective $\mathbf{A}$-module of constant rank 1.
Moreover $c \mapsto \mathbf{B}_c^G$ induces a morphism $Z^1(G,\mathbf{B}^\times) \to \mathsf{Pic}(\mathbf{A})$.

It remains to show that if $\mathbf{B}_c^G$ is free, i.e. $\mathbf{B}_c^G = \mathbf{A}b_1$ with $b_1 \in \mathbf{B}$ and $\mathrm{Ann}_{\mathbf{A}}(b_1) = 0$, then c is a coboundary. But $\mathbf{B}_{c^{-1}}^G$, being the inverse of $\mathbf{B}_c^G$ is also free, $\mathbf{B}_{c^{-1}}^G = \mathbf{A}b_2$, and $\mathbf{B}_c^G\mathbf{B}_{c^{-1}}^G = \mathbf{B}_1^G = \mathbf{A}$. We therefore have $\mathbf{A}b_1b_2 = \mathbf{A}$, then b_1, b_2 are invertible in $\mathbf{B}$ (and $\mathbf{A}b_2 = \mathbf{A}b_1^{-1}$). Then $c_\sigma^{-1}\sigma(b_2) = b_2$, i.e. c is the coboundary of b_2.

5. Since $\mathbf{A}$ is a zero-dimensional ring, $\mathsf{Pic}(\mathbf{A}) = 0$ so $H^1(G,\mathbf{B}^\times) = 0$.

6. Let $c_\tau = x\sigma(x)\cdots\sigma^{i-1}(x)$ with $i \in [\![1..n]\!]$ and $\tau = \sigma^i$.
Thus, $c_{\mathrm{Id}} = \mathrm{N}_{\mathbf{B}/\mathbf{A}}(x) = 1$, $c_\sigma = x$, $c_{\sigma^2} = x\sigma(x)$.
It is a 1-cocycle: $c_\sigma\sigma(c_{\sigma^i}) = c_{\sigma^{i+1}}$, i.e. $c_\sigma\sigma(c_\tau) = c_{\sigma\tau}$, then $c_{\sigma^j}\sigma^j(c_\tau) = c_{\sigma^j\tau}$.

Problem 5. *(The Segre morphism in a special case)*
It is clear that $\mathfrak{a} \subseteq \mathrm{Ker}\,\varphi$.

1. Let $m = X_{i_1}\cdots X_{i_r}Y_{j_1}\cdots Y_{j_s}$, $m' = X_{i'_1}\cdots X_{i'_{r'}}Y_{j'_1}\cdots Y_{j'_{s'}}$ with

$$1 \leqslant i_1 \leqslant \cdots \leqslant i_r \leqslant j_1 \leqslant \cdots \leqslant j_s \leqslant n,\ 1 \leqslant i'_1 \leqslant \cdots \leqslant i'_{r'} \leqslant j'_1 \leqslant \cdots \leqslant j'_{s'} \leqslant n.$$

The equality $\varphi(m) = \varphi(m')$ provides

$$T^rU^sZ_{i_1}\dots Z_{i_r}Z_{j_1}\dots Z_{j_s} = T^{r'}U^{s'}Z_{i'_1}\dots Z_{i'_{r'}}Z_{j'_1}\dots Z_{j'_{s'}}.$$

Therefore $r = r'$, $s = s'$ then $i_k = i'_k$ and $j_\ell = j'_\ell$. Ultimately $m = m'$.
Let $s = \sum_\alpha a_\alpha m_\alpha$ be an $\mathbf{A}$-linear combination of normalized monomials such that $\varphi(s) = 0$. As the monomials $\varphi(m_\alpha)$ are pairwise distinct, we have $a_\alpha = 0$, i.e. $s = 0$.

2. Since $X_iY_j \equiv X_jY_i \bmod \mathfrak{a}$, we see that every monomial is equivalent modulo $\mathfrak{a}$ to a normalized monomial. We therefore get $\mathbf{A}[\underline{X},\underline{Y}] = \mathfrak{a} + \mathfrak{a}_{\mathrm{nor}}$. As $\mathfrak{a} \subseteq \mathrm{Ker}\,\varphi$, the sum is direct by the previous question.

3. Let $h \in \mathrm{Ker}\,\varphi$ which we decompose into $h = f + g$ with $f \in \mathfrak{a}$, $g \in \mathfrak{a}_{\mathrm{nor}}$.
Since $\mathfrak{a} \subseteq \mathrm{Ker}\,\varphi$, we have $g \in \mathrm{Ker}\,\varphi$, so $g = 0$. Conclusion: $h = f \in \mathfrak{a}$, which proves $\mathrm{Ker}\,\varphi \subseteq \mathfrak{a}$, then $\mathrm{Ker}\,\varphi = \mathfrak{a}$.

Problem 6. *(The Veronese morphism in a special case)*
It is clear that $\mathfrak{b} \subseteq \mathfrak{a} \subseteq \mathrm{Ker}\,\varphi$.

1. Let f be in the intersection; f is of the form $f = f_0 + \sum_{i=1}^{d-1} f_iX_i$ with $f_i \in \mathbf{A}[X_0, X_d]$; We write that $\varphi(f) = 0$

$$f_0(U^d,V^d) + f_1(U^d,V^d)U^{d-1}V + \cdots + f_{d-1}(U^d,V^d)UV^{d-1} = 0.$$

This is of the form, in $\mathbf{A}[U][V]$, $h_0(V^d)+h_1(V^d)V+\cdots+h_{d-1}(V^d)V^{d-1}=0$; by examining in this equality the exponents of V modulo d, we obtain $h_0=h_1=\cdots=h_{d-1}=0$. Recap: $f_i=0$ then $f=0$.

2. We work modulo $\mathfrak{b}$ by letting

$$\mathbf{A}[\underline{x}]=\mathbf{A}[\underline{X}]/\mathfrak{b},\ \mathbf{B}=\mathbf{A}[x_0,x_d]+\mathbf{A}[x_0,x_d]x_1+\cdots+\mathbf{A}[x_0,x_d]x_{d-1}\subseteq\mathbf{A}[\underline{x}].$$

We will show that $\mathbf{B}$ is an $\mathbf{A}$-subalgebra; as it contains the x_i's, it is all of the $\mathbf{A}[\underline{x}]$. It suffices to prove that $x_ix_j\in\mathbf{B}$ for $i\leqslant j\in[\![1..d-1]\!]$, because the other products are in $\mathbf{B}$ by definition of $\mathbf{B}$. We use the syzygies $x_ix_j=x_{i-1}x_{j+1}$ for $i\leqslant j\in[\![1..d-1]\!]$. We have $x_0x_k\in\mathbf{B}$ for every k; we deduce $x_1x_j\in\mathbf{B}$ for all $j\in[\![1..d-1]\!]$ and it is still true for $j=d$ and 0 by definition of $\mathbf{B}$. We then deduce that $x_2x_j\in\mathbf{B}$ for $j\in[\![2..d-1]\!]$, and so on.
The obtained equality $\mathbf{B}=\mathbf{A}[\underline{x}]$ is written as

$$\mathbf{A}[\underline{X}]=\mathfrak{b}+\big(\mathbf{A}[X_0,X_d]\oplus\mathbf{A}[X_0,X_d]X_1\oplus\cdots\oplus\mathbf{A}[X_0,X_d]X_{d-1}\big),$$

and the $+$ represents a direct sum by item *1* (since $\mathfrak{b}\subseteq\operatorname{Ker}\varphi$).

3. Let $h\in\operatorname{Ker}\varphi$ which we decompose into $h=f+g$ as above.
Since $f\in\mathfrak{b}\subseteq\operatorname{Ker}\varphi$, we have $g\in\operatorname{Ker}\varphi$, so $g=0$. Conclusion: $h=f\in\mathfrak{b}$, which proves $\operatorname{Ker}\varphi\subseteq\mathfrak{b}$, then $\operatorname{Ker}\varphi=\mathfrak{b}=\mathfrak{a}$.

Problem 7. *(Veronese matrices)*
2. It is clear that $V_d(P)$ is a projector if P is also a projector, and the diagram is commutative for functorial reasons.
We can add the following precision: if P, $Q\in\mathbb{M}_n(\mathbf{k})$ are two projectors such that $\operatorname{Im}P\subseteq\operatorname{Im}Q$, then $\operatorname{Im}V_d(P)\subseteq\operatorname{Im}V_d(Q)$. Indeed, we have $\operatorname{Im}P\subseteq\operatorname{Im}Q$ if and only if $QP=P$, and we deduce that $V_d(Q)V_d(P)=V_d(P)$, i.e. $\operatorname{Im}V_d(P)\subseteq\operatorname{Im}V_d(Q)$.

3. It suffices to do this locally, i.e. to compute $V_d(A)$ when A is a standard projector $\mathrm{I}_{r,n}$. If $A=\operatorname{Diag}(a_1,\dots,a_n)$, then $V_d(A)$ is diagonal, with diagonal the n' monomials a^α with $|\alpha|=d$. In particular, for $A=\mathrm{I}_{r,n}$, we see that $V_d(A)$ is a standard projection, of rank the number of α such that $\alpha_1+\cdots+\alpha_r=d$, i.e. $\binom{d+1-r}{r-1}$, and $V_d(\mathrm{I}_{1,n})=\mathrm{I}_{1,n'}$.

Problem 8. *(Some examples of finite projective resolutions)*
1. The computation of $F_k^2-F_k$ is done by induction and poses no problem. For the conjugation ($n\geqslant 1$), we use

$$\begin{bmatrix}0&-\mathrm{I}\\ \mathrm{I}&0\end{bmatrix}\begin{bmatrix}A&B\\ C&D\end{bmatrix}\begin{bmatrix}0&\mathrm{I}\\ -\mathrm{I}&0\end{bmatrix}=\begin{bmatrix}D&-C\\ -B&A\end{bmatrix}.$$

For $\begin{bmatrix}A&B\\ C&D\end{bmatrix}=F_n$, this provides a conjugation between F_n and $\mathrm{I}_{2^n}-{}^{\mathrm{t}}F_n$.
When $z(z-1)+\sum_{i=1}^n x_iy_i=0$, the projectors F_n and $\mathrm{I}_{2^n}-F_n$ have for image finitely generated projective modules P and Q with $P\oplus Q\simeq\mathbf{A}^{2^n}$ and $P\simeq Q^\star$. Therefore $2\operatorname{rk}(P)=2^n$, and since $mx=0\Rightarrow x=0$ for $m\in\mathbb{N}^*$ and $x\in\mathsf{H}_0\,\mathbf{A}$, we obtain $\operatorname{rk}(P)=2^{n-1}$.

2. The computation of U_kV_k and V_kU_k is done by induction. The fact that F_n and G_n are conjugated by a permutation matrix is left to the sagacity of the reader.

For example, $G_2 = P_\tau F_2 P_\tau^{-1}$ for $\tau = (2,4,3) = (3,4)(2,3)$, and $G_3 = P_\tau F_3 P_\tau^{-1}$ for $\tau = (2,4,7,5)(3,6) = (3,6)(2,4)(4,7)(5,7)$.
Regarding the constant rank 2^{n-1} we can invoke item *1*, or make the direct computation after localization at z and at $\overline{z} = 1 - z$.

3a. Direct use of the referenced exercise.

3b. Let S be the monoid $a^{\mathbb{N}}$. We can localize a finite projective resolution of M over $\mathbf{A}$ to obtain one over $S^{-1}\mathbf{A}$

$$0 \to S^{-1}P_n \to \cdots \to S^{-1}P_1 \to S^{-1}P_0 \twoheadrightarrow S^{-1}M \to 0.$$

As $aM = 0$, we have $S^{-1}M = 0$, therefore $\sum_{i=0}^{n}(-1)^i \operatorname{rk}(S^{-1}P_i) = 0$. But the natural morphism $\mathsf{H}_0(\mathbf{A}) \to \mathsf{H}_0(S^{-1}\mathbf{A})$ is injective.
Therefore $\sum_{i=0}^{n}(-1)^i \operatorname{rk} P_i = 0$.

4. The localized ring $(\mathbf{B}_n)_z$ contains all the $y'_i = y_i/z$, and since $z(1-z) = \sum_i x_i y_i$, we have $1 - z = \sum_i x_i y'_i$. Therefore $z \in \mathbf{k}[x_1,\dots,x_n,y'_1,\dots,y'_n]$ and $1 - \sum_i x_i y'_i \in (\mathbf{B}_n)_z^{\times}$. We then verify that

$$(\mathbf{B}_n)_z = \mathbf{k}[x_1,\dots,x_n,y'_1,\dots,y'_n]_s \quad \text{with} \quad s = 1 - \sum x_i y'_i.$$

Similarly, $(\mathbf{B}_n)_{1-z} = \mathbf{k}[x'_1,\dots,x'_n,y_1,\dots,y_n]_{1-\sum x'_i y_i}$ with $x'_i = x_i/(1-z)$.

5. For $n \geqslant 1$, every element $a \in \{z, x_1, \dots, x_n\}$ is regular and $a(\mathbf{B}_n/\mathfrak{b}_n) = 0$. As $F_1 = \begin{bmatrix} z & x_1 \\ y_1 & \overline{z} \end{bmatrix}$ is a projector, we have $[z, x_1]F_1 = [z, x_1]$. The reader will check that $\operatorname{Ker}[z, x_1] = \operatorname{Ker} F_1 = \operatorname{Im}(\mathrm{I}_2 - F_1)$; hence the exact sequence

$$0 \to \operatorname{Im}(\mathrm{I}_2 - F_1) \to \mathbf{B}_1^2 \xrightarrow{[z,x_1]} \mathbf{B}_1 \twoheadrightarrow \mathbf{B}_1/\mathfrak{b}_1 \to 0.$$

We indeed have $\operatorname{rk}(\mathbf{B}_1/\mathfrak{b}_1) = 1 - 2 + 1 = 0$.

6. Let A be the matrix constituted of the first 3 rows of $\mathrm{I}_4 - F_2$

$$A = \begin{bmatrix} 1-z & -x_1 & -x_2 & 0 \\ -y_1 & z & 0 & -x_2 \\ -y_2 & 0 & z & x_1 \end{bmatrix}.$$

It is clear that $AF_2 = 0$ and $[z, x_1, x_2]A = 0$. The reader will check that the sequence below is exact

$$0 \to \operatorname{Im} F_2 \to \mathbf{B}_2^4 \xrightarrow{A} \mathbf{B}_2^3 \xrightarrow{[z,x_1,x_2]} \mathbf{B}_2 \twoheadrightarrow \mathbf{B}_2/\mathfrak{b}_2 \to 0.$$

We indeed have $\operatorname{rk}(\mathbf{B}_2/\mathfrak{b}_2) = 1 - 3 + 4 - 2 = 0$.

7. Immediate given the definition of F_n.

8. Consider the upper half of the matrix $\mathrm{I}_8 - F'_3$ and delete its last (zero) column to obtain a matrix A of format 4×7. Let B be the matrix of format 7×8 obtained by deleting the last row of F'_3. Then the brave reader will check the exactness of

$$0 \to \operatorname{Im}(\mathrm{I}_8 - F'_3) \to \mathbf{B}_3^8 \xrightarrow{B} \mathbf{B}_3^7 \xrightarrow{A} \mathbf{B}_3^4 \xrightarrow{[z,x_1,x_2,x_3]} \mathbf{B}_3 \twoheadrightarrow \mathbf{B}_3/\mathfrak{b}_3 \to 0.$$

We have $\operatorname{rk}(\mathbf{B}_3/\mathfrak{b}_3) = 1 - 4 + 7 - 8 + 4 = 0$.

9. There is an exact sequence (let $\mathbf{B} = \mathbf{B}_n$, $\mathfrak{b} = \mathfrak{b}_n$):

$$L_{n+1} \xrightarrow{A_{n+1}} L_n \xrightarrow{A_n} L_{n-1} \xrightarrow{A_{n-1}} \cdots \longrightarrow L_2 \xrightarrow{A_2} L_1 \xrightarrow{A_1} L_0 = \mathbf{B} \twoheadrightarrow \mathbf{B}/\mathfrak{b}\ .$$

where L_r is a free module of rank $\sum_{i \in I_r} \binom{n+1}{i}$ with $I_r = \{\, i \in \llbracket 0..r \rrbracket \mid i \equiv r \bmod 2 \,\}$.
In particular, $L_1 = \mathbf{B}^{n+1}$ and $L_n = L_{n+1} = \mathbf{B}^{2^n}$.

As for the matrices A_r, we have $A_1 = [z, x_1, \dots, x_n]$, and the matrix A_r is extracted from F_n if r is odd, and extracted from $\mathrm{I} - F_n$ otherwise. We have $A_{n+1} = F_n$ for even n, and $A_{n+1} = \mathrm{I} - F_n$ for odd n.
By letting $P_{n+1} = \mathrm{Im}\, A_{n+1}$, the $\mathbf{B}$-module $\mathbf{B}/\mathfrak{b}$ admits a projective resolution of length $n+1$ of the following type

$$0 \to P_{n+1} \to L_n = \mathbf{B}^{2^n} \xrightarrow{A_n} L_{n-1} \xrightarrow{A_{n-1}} \cdots \to L_2 \xrightarrow{A_2} L_1 \xrightarrow{A_1} L_0 = \mathbf{B} \twoheadrightarrow \mathbf{B}/\mathfrak{b}\ .$$

(P_{n+1} of constant rank 2^{n-1}).
The explicit expression of the rank of L_i confirms that $[\mathbf{B}/\mathfrak{b}\,] \in \widetilde{\mathsf{K}}_0(\mathbf{B})$.
We have $\mathrm{rk}\, L_{n-1} + \mathrm{rk}\, L_0 = \mathrm{rk}\, L_{n-2} + \mathrm{rk}\, L_1 = \cdots = 2^n$ (in particular, if $n = 2m+1$, then $\mathrm{rk}\, L_m = 2^{n-1}$).

Note: If $\mathbf{k}$ is a discrete field, we can show that $\widetilde{\mathsf{K}}_0(\mathbf{B}_n) \simeq \mathbb{Z}$ with as a generator $[\mathbf{B}_n/\mathfrak{b}_n\,]$. We deduce that the ideal $\widetilde{\mathsf{K}}_0(\mathbf{B}_n)$ has a null square; generally, let $\mathbf{A}$ be a ring satisfying $\widetilde{\mathsf{K}}_0(\mathbf{A}) = \mathbb{Z}x \simeq \mathbb{Z}$, then $x^2 = mx$ with $m \in \mathbb{Z}$, so $x^{k+1} = m^k x$ for $k \geqslant 1$, since x is nilpotent (see Problem 2), there is some $k \geqslant 1$ such that $m^k x = 0$, so $m^k = 0$, then $m = 0$ and $x^2 = 0$.

Bibliographic comments

Theorem 1.4 specifies Theorem 2 in [Bourbaki] Chap. II §5.

Section 6 is based on the articles [31, 32, Chervov&Talalaev] which examine the “Hitchin systems” over the singular curves.

Problem 2 is inspired from a non-published article of R. G. Swan: *On a theorem of Mohan, Kumar and Nori.*

Problem 4 comes from an exercise of Chapter 4 of [Jensen, Ledet & Yui].

In Problem 8, the matrix F_k occurs in the article: *Vector bundles over Spheres are Algebraic*, R. Fossum, Inventiones Math. **8**, 222–225 (1969). The ring $\mathbf{B}_n$ is a classic in algebraic K-theory.

Chapter XI

Distributive lattices Lattice-groups

Contents

Introduction

This chapter begins with an introductory section which fixes the formal algebraic framework of distributive lattices and of Boolean algebras.

The distributive lattices are important in commutative algebra for several reasons.

On the one hand the theory of divisibility has as its "ideal model" the theory of divisibility of natural integers. If we take as the order relation $a \preccurlyeq b$, the relation "a is a multiple of b," we obtain that $\mathbb{N}$ is a distributive lattice with: minimum element 0, maximum element 1, the supremum $a \vee b$ equal to the gcd and the infimum $a \wedge b$ equal to the lcm. A few beautiful properties of divisibility in $\mathbb{N}$ are expressed in modern terms by saying that the ring $\mathbb{Z}$ is a Bézout ring (see Sections III-8 and IV-7). The ideal numbers in number theory have been created by Kummer to fill the gap between the theory of divisibility in the ring of integers of a number field and that in $\mathbb{N}$. The ring of integers of a number field is not a Bézout ring in general, but its finitely generated ideals[1] form a distributive lattice, and their nonzero finitely generated ideals form the non-negative submonoid of an l-group (see Section 2) which re-establishes the well-ordering of things. The rings whose finitely generated ideals form a distributive lattice are called arithmetic rings (treated elsewhere in Sections VIII-4 and XII-1). Their invertible ideals also form the non-negative submonoid of an l-group. The theory of GCD-domains (Section 3) also finds its natural framework in the context of l-groups.

On the other hand the distributive lattices intervene as the constructive counterpart of diverse and various spectral spaces which are imposed as

[1] What for Kummer was "the ideal gcd of several numbers" has been replaced in modern language by the corresponding finitely generated ideal. This tour de force, due to Dedekind, was one of the first intrusions of the "actual" infinite in mathematics.

powerful tools of the abstract algebra. The discussion on this subject is particularly enlightening when we consider the Zariski lattice of a commutative ring, relatively unknown, which serves as a constructive counterpart to the very famous Zariski spectrum: spectral space that we could believe indispensable to the Krull dimension theory and to the Grothendieck scheme theory. A systematic study of the Zariski lattice will be given in Chapter XIII regarding the Krull dimension, with a heuristic introduction in Section XIII-1. In Section 4 we define the Zariski lattice of a commutative ring $\mathbf{A}$ essentially with respect to the construction of the reduced zero-dimensional closure $\mathbf{A}^\bullet$ (page 651) of the ring. This construction can be regarded as a construction parallel to that of the Boolean algebra generated by a distributive lattice (see Theorem 4.26). The global object $\mathbf{A}^\bullet$ constructed thus essentially contains the same information as the product of rings $\mathrm{Frac}(\mathbf{A}/\mathfrak{p})$ for all the prime ideals $\mathfrak{p}$ of $\mathbf{A}$. We get this even though in the general situation we do not constructively have access to the prime ideals of a ring individually.

Another reason to be interested in distributive lattices is the constructive (or intuitionist) logic in which the set of truth values of classical logic, that is $\{\mathsf{True}, \mathsf{False}\}$, which is a Boolean algebra with two elements, is replaced with a more mysterious distributive lattice.[2] The constructive logic will be addressed in the Appendix (see page 959), particularly in Sections 2 and 3. In Section 5 of the previous chapter we implement the tools that serve as the framework for a formal algebraic study of this logic: the entailment relations and the Heyting algebras. It is remarkable that Heyting defined those algebras in the first attempt to describe the intuitionist logic formally, and that there has not been a comma to add since. Moreover, entailment relations and Heyting algebras are also useful in the general study of distributive lattices. For example it is sometimes important to be able to say that the Zariski lattice of a ring is a Heyting algebra.

1. Distributive lattices and Boolean algebras

In an ordered set X we let, for some $a \in X$,

$$\downarrow a = \{\, x \in X \mid x \leqslant a \,\}, \quad \uparrow a = \{\, x \in X \mid x \geqslant a \,\}. \tag{1}$$

We call a finite non-decreasingly ordered list $(a_0, \dots, a_n)$ of elements of X a *non-decreasing chain.* The number n is called the *length* of the chain. By convention the empty list is a chain of length -1.

[2] Actually the truth values of constructive mathematics do not strictly speaking form a set, but a class. Nevertheless the constructive logical connectives act on those truth values with the same algebraic properties as the $\land$, the $\lor$ and the $\to$ of Heyting algebras. See the discussion on page 964.

1.1. Definition.

1. A *lattice* is a set $\mathbf{T}$ equipped with an order relation $\leqslant$ for which every finite family admits an upper bound and a lower bound. Let $0_{\mathbf{T}}$ be the minimum of $\mathbf{T}$ (the upper bound of the empty family) and $1_{\mathbf{T}}$ be the maximum of $\mathbf{T}$. Let $a \vee b$ be the upper bound of (a,b) and $a \wedge b$ be its lower bound.
2. A map from one lattice to another is called a *lattice homomorphism* if it respects the laws $\vee$ and $\wedge$ and the constants 0 and 1.
3. The lattice is called a *distributive lattice* when each of the two laws $\vee$ and $\wedge$ is distributive with respect to the other.

The axioms of lattices can be formulated with universal equalities uniquely regarding the two laws $\wedge$ and $\vee$ and the two constants $0_{\mathbf{T}}$ and $1_{\mathbf{T}}$. The order relation is then defined by $a \leqslant_{\mathbf{T}} b \overset{\text{def}}{\iff} a \wedge b = a$. Here are those axioms.

$$\begin{array}{rclcrcl}
a \vee a &=& a & \qquad & a \wedge a &=& a \\
a \vee b &=& b \vee a & & a \wedge b &=& b \wedge a \\
(a \vee b) \vee c &=& a \vee (b \vee c) & & (a \wedge b) \wedge c &=& a \wedge (b \wedge c) \\
(a \vee b) \wedge a &=& a & & (a \wedge b) \vee a &=& a \\
a \vee 0_{\mathbf{T}} &=& a & & a \wedge 1_{\mathbf{T}} &=& a
\end{array}$$

We thus obtain a purely equational theory, with all the related facilities. For example we can define a lattice by generators and relations. Similarly for the distributive lattices.

In a lattice, one distributivity implies the other. Suppose for instance that $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$, for all a, b, c. Then the other distributivity results from the following computation

$$(a \vee b) \wedge (a \vee c) = \big((a \vee b) \wedge a\big) \vee \big((a \vee b) \wedge c\big) = a \vee \big((a \vee b) \wedge c\big) =$$
$$a \vee \big((a \wedge c) \vee (b \wedge c)\big) = \big(a \vee (a \wedge c)\big) \vee (b \wedge c) = a \vee (b \wedge c).$$

In a discrete lattice we have a test for $a \leqslant b$, since this relation is equivalent to $a \wedge b = a$.

The subgroups of a group (or the ideals of a commutative ring) form a lattice with repect to the inclusion, but it is not a distributive lattice in general.

A totally ordered set[3] is a distributive lattice if it possesses a maximum element and a minimum element. Let $\mathbf{n}$ be the totally ordered set with n elements. A map between two totally ordered lattices $\mathbf{T}$ and $\mathbf{S}$ is a homomorphism if and only if it is non-decreasing and $0_{\mathbf{T}}$ and $1_{\mathbf{T}}$ have as their images $0_{\mathbf{S}}$ and $1_{\mathbf{S}}$.

[3] Recall that this is a set E equipped with an order relation $\leqslant$ for which we have, for all x and $y \in E$, $x \leqslant y$ or $y \leqslant x$. This does not imply that the equality is decidable.

If $\mathbf{T}$ and $\mathbf{T}'$ are two distributive lattices, the set $\mathrm{Hom}(\mathbf{T},\mathbf{T}')$ of homomorphisms from $\mathbf{T}$ to $\mathbf{T}'$ is equipped with a natural order structure given by

$$\varphi \leqslant \psi \overset{\mathrm{def}}{\iff} \forall x \in \mathbf{T}\ \ \varphi(x) \leqslant \psi(x)$$

A cartesian product of distributive lattices is a distributive lattice (for the product laws $\wedge$ and $\vee$, which gives the product partial order relation).

For every distributive lattice $\mathbf{T}$, if we replace the order relation $x \leqslant_{\mathbf{T}} y$ by the symmetric relation $y \leqslant_{\mathbf{T}} x$ we obtain the *opposite lattice* $\mathbf{T}^{\circ}$ with an exchange of $\wedge$ and $\vee$ (we sometimes say *dual lattice*).

If $A \in \mathrm{P}_{\mathrm{fe}}(\mathbf{T})$ with a distributive lattice $\mathbf{T}$ we will let

$$\bigvee A := \bigvee\nolimits_{x\in A} x \qquad \text{and} \qquad \bigwedge A := \bigwedge\nolimits_{x\in A} x.$$

Quotient lattices, ideals, filters

If an algebraic structure is defined by laws of composition of different arities and by axioms that are universal equalities (such as groups, rings and distributive lattices), a quotient structure is obtained when we have an equivalence relation and when the laws of composition “pass to the quotient.” If we look at the structure as defined by generators and relations (which is always possible), we obtain a quotient structure by adding relations.

A *quotient lattice* $\mathbf{T}'$ *of a lattice* $\mathbf{T}$ can also be given by a binary relation $\preccurlyeq$ over $\mathbf{T}$ satisfying the following properties

$$\left.\begin{array}{rcl} a \leqslant b & \Longrightarrow & a \preccurlyeq b \\ a \preccurlyeq b,\, b \preccurlyeq c & \Longrightarrow & a \preccurlyeq c \\ a \preccurlyeq b,\, a \preccurlyeq c & \Longrightarrow & a \preccurlyeq b \wedge c \\ b \preccurlyeq a,\, c \preccurlyeq a & \Longrightarrow & b \vee c \preccurlyeq a \end{array}\right\} \tag{2}$$

The relation $\preccurlyeq$ then induces a lattice structure over the quotient set $\mathbf{T}'$ obtained with the new equality[4]

$$(a, b \in \mathbf{T}) \quad : \qquad a =_{\mathbf{T}'} b \overset{\mathrm{def}}{\iff} (a \preccurlyeq b \text{ and } b \preccurlyeq a)$$

Naturally if $\mathbf{T}$ is distributive, the same goes for $\mathbf{T}'$.

If $\varphi : \mathbf{T} \to \mathbf{T}'$ is a distributive lattice homomorphism, $\varphi^{-1}(0)$ is called an *ideal of* $\mathbf{T}$. An ideal $\mathfrak{b}$ of $\mathbf{T}$ is a subset of $\mathbf{T}$ subjected to the following

[4] The fact that, when passing to the quotient, we change only the equality relation and not the objects is simpler than the classical approach, and is more consistent with the (Gaussian) tradition and with machine implementation. No doubt the popular success of equivalence classes as objects of the quotient set is largely due to the fortunate fact that in the case of a quotient group G/H, in additive notation for example, we have $(x+H)+(y+H) = (x+y)+H$ where the symbol $+$ has three different meanings. However, things are less fortunate in the case of quotient rings. For example, $(3 + 7\mathbb{Z})(2 + 7\mathbb{Z})$ is contained within, but is not equal to $6 + 7\mathbb{Z}$.

constraints

$$\left.\begin{array}{rcl} & & 0 \in \mathfrak{b} \\ x, y \in \mathfrak{b} & \Longrightarrow & x \vee y \in \mathfrak{b} \\ x \in \mathfrak{b},\ z \in \mathbf{T} & \Longrightarrow & x \wedge z \in \mathfrak{b} \end{array}\right\} \tag{3}$$

(the last is rewritten as $(x \in \mathfrak{b},\ y \leqslant x) \Rightarrow y \in \mathfrak{b}$). A *principal ideal* is an ideal generated by a single element a, it is equal to $\downarrow a$.

The ideal $\downarrow a$, equipped with the laws $\wedge$ and $\vee$ of $\mathbf{T}$, is a distributive lattice in which the maximum element is a. The canonical injection $\downarrow a \to \mathbf{T}$ is not a morphism of distributive lattices because the image of a is not equal to $1_{\mathbf{T}}$. However, the map $\mathbf{T} \to \downarrow a,\ x \mapsto x \wedge a$ is a surjective morphism, which therefore defines $\downarrow a$ as a quotient structure.

The notion opposite to that of an ideal is the notion of a *filter*. The principal filter generated by a is equal to $\uparrow a$.

The *ideal generated* by a subset J of $\mathbf{T}$ is equal to

$$\mathcal{I}_{\mathbf{T}}(J) = \left\{x \in \mathbf{T} \;\middle|\; \exists J_0 \in \mathrm{P_{fe}}(J),\ x \leqslant \bigvee J_0\right\}.$$

Consequently *every finitely generated ideal is principal.*

If A and B are two subsets of $\mathbf{T}$ let

$$A \vee B = \left\{a \vee b \mid a \in A,\ b \in B\right\} \text{ and } A \wedge B = \left\{a \wedge b \mid a \in A,\ b \in B\right\}. \tag{4}$$

Then the ideal generated by two ideals $\mathfrak{a}$ and $\mathfrak{b}$ is equal to

$$\mathcal{I}_{\mathbf{T}}(\mathfrak{a} \cup \mathfrak{b}) = \mathfrak{a} \vee \mathfrak{b}. \tag{5}$$

The set of ideals of $\mathbf{T}$ itself forms a distributive lattice[5] with repect to the inclusion, with, for lower bound of $\mathfrak{a}$ and $\mathfrak{b}$, the ideal

$$\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a} \wedge \mathfrak{b}. \tag{6}$$

Thus the operations $\vee$ and $\wedge$ defined in (4) correspond to the supremum and the infimum in the lattice of ideals.

We will denote by $\mathcal{F}_{\mathbf{T}}(S) = \{\, x \in \mathbf{T} \mid \exists S_0 \in \mathrm{P_{fe}}(S),\ x \geqslant \bigwedge S_0 \,\}$ the filter of $\mathbf{T}$ generated by the subset S.

When we consider the lattice of filters, we must pay attention as to what the reversing of the order relation produces: $\mathfrak{f} \cap \mathfrak{g} = \mathfrak{f} \vee \mathfrak{g}$ is the infimum of the filters $\mathfrak{f}$ and $\mathfrak{g}$, whereas their supremum is equal to $\mathcal{F}_{\mathbf{T}}(\mathfrak{f} \cup \mathfrak{g}) = \mathfrak{f} \wedge \mathfrak{g}$.

The *quotient lattice of* $\mathbf{T}$ *by the ideal* $\mathfrak{a}$, denoted by $\mathbf{T}/(\mathfrak{a} = 0)$, is defined as the distributive lattice generated by the elements of $\mathbf{T}$ with as its relations

[5] Actually we need to introduce a restriction to truly obtain a set, in order to have a well-defined procedure to construct concerned ideals. For example we can consider the set of ideals obtained from principal ideals via certain predefined operations, such as countable unions and intersections. This is the same problem as the one indicated in footnote 2.

the true relations in $\mathbf{T}$ on the one hand, and the relations $x = 0$ for the $x \in \mathfrak{a}$ on the other. It can also be defined by the following preorder relation

$$a \leqslant_{\mathbf{T}/(\mathfrak{a}=0)} b \quad \overset{\text{def}}{\iff} \quad \exists x \in \mathfrak{a} \;\; a \leqslant x \vee b.$$

This gives

$$a \equiv b \mod (\mathfrak{a} = 0) \quad \iff \quad \exists x \in \mathfrak{a} \quad a \vee x = b \vee x.$$

In particular, the homomorphism of passage to the quotient

$$\varphi : \mathbf{T} \to \mathbf{T}' = \mathbf{T}/(\mathfrak{a} = 0)$$

satisfies $\varphi^{-1}(0_{\mathbf{T}'}) = \mathfrak{a}$. In the case of the quotient by a principal ideal $\downarrow a$ we obtain $\mathbf{T}/(\downarrow a = 0) \simeq \uparrow a$ with the morphism $y \mapsto y \vee a$ from $\mathbf{T}$ to $\uparrow a$.

1.2. Proposition. *Let $\mathbf{T}$ be a distributive lattice and (J, U) be a pair of subsets of $\mathbf{T}$. Consider the quotient $\mathbf{T}'$ of $\mathbf{T}$ defined by the relations $x = 0$ for each $x \in J$, and $y = 1$ for each $y \in U$. Then the inequality $a \leqslant_{\mathbf{T}'} b$ is satisfied if and only if there exist $J_0 \in \mathrm{P}_{\mathrm{fe}}(J)$ and $U_0 \in \mathrm{P}_{\mathrm{fe}}(U)$ such that*

$$a \wedge \bigwedge U_0 \;\leqslant_{\mathbf{T}}\; b \vee \bigvee J_0. \tag{7}$$

We will denote by $\mathbf{T}/(J = 0, U = 1)$ this quotient lattice $\mathbf{T}'$.

We see in the example of totally ordered sets that a quotient structure of a distributive lattice is not generally characterized by the equivalence classes of 0 and 1.

Let $\mathfrak{a}$ be an ideal and $\mathfrak{f}$ be a filter of $\mathbf{T}$. We say that $\mathfrak{a}$ is $\mathfrak{f}$-*saturated* if we have

$$(g \in \mathfrak{f},\; x \wedge g \in \mathfrak{a}) \Longrightarrow x \in \mathfrak{a},$$

we say that $\mathfrak{f}$ is $\mathfrak{a}$-*saturated* if we have

$$(a \in \mathfrak{a},\; x \vee a \in \mathfrak{f}) \Longrightarrow x \in \mathfrak{f}.$$

If $\mathfrak{a}$ is $\mathfrak{f}$-saturated and $\mathfrak{f}$ is $\mathfrak{a}$-saturated we say that $(\mathfrak{a}, \mathfrak{f})$ is a *saturated pair* in $\mathbf{T}$. When $(\mathfrak{a}, \mathfrak{f})$ is a saturated pair, we have the equivalences

$$1 \in \mathfrak{a} \iff 0 \in \mathfrak{f} \iff (\mathfrak{a}, \mathfrak{f}) = (\mathbf{T}, \mathbf{T}).$$

1.3. Fact. *Let $\varphi : \mathbf{T} \to \mathbf{T}_1$ be a distributive lattice homomorphism. The ideal $\mathfrak{a} = \varphi^{-1}(0)$ and the filter $\mathfrak{f} = \varphi^{-1}(1)$ form a saturated pair. Conversely, if $(\mathfrak{a}, \mathfrak{f})$ is a saturated pair of $\mathbf{T}$, the homomorphism of passage to the quotient $\pi : \mathbf{T} \to \mathbf{T}/(\mathfrak{a} = 0, \mathfrak{f} = 1)$ satisfies $\pi^{-1}(0) = \mathfrak{a}$ and $\pi^{-1}(1) = \mathfrak{f}$.*

Boolean algebras

In a distributive lattice an element x' is called a *complement* of x if we have $x \wedge x' = 0$ and $x \vee x' = 1$. If it exists the complement of x is unique. It is then often denoted by $\neg x$.

Recall that by definition a ring $\mathbf{B}$ is a Boolean algebra if and only if every element is idempotent. We then define an order relation $x \preccurlyeq y$ by: x is a

multiple of y, i.e. $\langle x\rangle \subseteq \langle y\rangle$.
We thus obtain a distributive lattice in which every element x admits as its complement $x' = 1 + x$ (cf. Proposition VII-3.1).

We have the following converse.

1.4. Proposition. (Boolean algebras)

1. *On a distributive lattice in which every element x admits a complement, denoted by $\neg x$, we can define a Boolean algebra structure by letting*
$$xy = x \wedge y \quad \textit{and} \quad x \oplus y = (x \wedge \neg y) \vee (y \wedge \neg x).$$
We once again find $x \vee y = x \oplus y \oplus xy$ and $\neg x = 1 \oplus x$.
2. *Every homomorphism of distributive lattices between two Boolean algebras is a homomorphism of Boolean algebras, and it respects the passage to the complement.*

Boolean algebra generated by a distributive lattice

Let us begin with a few remarks on the elements that have a complement in a distributive lattice. If a admits a complement a', since $b = (b \wedge a) \vee (b \wedge a')$ for every $b \in \mathbf{T}$, the canonical homomorphism

$$\mathbf{T} \to \mathbf{T}/(a = 1) \times \mathbf{T}/(a' = 1)$$

is injective. Moreover this morphism is onto because for $x, y \in \mathbf{T}$, defining $z = (x \wedge a) \vee (y \wedge a')$, we get $z \wedge a = x \wedge a$, i.e. $z \equiv x \bmod (a = 1)$, and in the same way $z \equiv y \bmod (a' = 1)$. Conversely, we have the following result which shows the similarity between an idempotent in a commutative ring and an element having a complement in a distributive lattice (see Fact II-4.1).

1.5. Lemma. *For every isomorphism $\lambda : \mathbf{T} \to \mathbf{T}_1 \times \mathbf{T}_2$, there exists a (unique) element $a \in \mathbf{T}$ such that*

1. *a has a complement $\neg a$,*
2. *the composed homomorphism $\mathbf{T} \to \mathbf{T}_1$ identifies $\mathbf{T}_1$ with $\mathbf{T}/(a = 0)$ and with $\mathbf{T}/(\neg a = 1)$,*
3. *the composed homomorphism $\mathbf{T} \to \mathbf{T}_2$ identifies $\mathbf{T}_2$ with $\mathbf{T}/(a = 1)$ and with $\mathbf{T}/(\neg a = 0)$.*

D The element a is given by $\lambda(a) = (0_{\mathbf{T}_1}, 1_{\mathbf{T}_2})$. □

When two elements a and b have complements $\neg a$ and $\neg b$, the *De Morgan's laws* are satisfied

$$\neg(a \wedge b) = \neg a \vee \neg b \quad \text{and} \quad \neg(a \vee b) = \neg a \wedge \neg b. \tag{8}$$

By definition, the *Boolean algebra freely generated by the distributive lattice* $\mathbf{T}$ is given by a pair $(\mathbb{B}\mathrm{o}(\mathbf{T}), \lambda)$, where $\mathbb{B}\mathrm{o}(\mathbf{T})$ is a Boolean algebra, and

where $\lambda : \mathbf{T} \to \mathbb{B}\mathrm{o}(\mathbf{T})$ is a distributive lattice homomorphism satisfying the following universal property.
Every distributive lattice homomorphism ψ from $\mathbf{T}$ to a Boolean algebra $\mathbf{B}$ is uniquely factored in the form $\varphi \circ \lambda$.

$$\begin{tikzcd}
\mathbf{T} \arrow[d, "\lambda"'] \arrow[dr, "\psi"] & & \text{distributive lattices} \\
\mathbb{B}\mathrm{o}(\mathbf{T}) \arrow[r, dashed, "\varphi\,!"'] & \mathbf{B} & \text{Boolean algebras}
\end{tikzcd}$$

Since we are in the context of purely equational algebraic structures, this Boolean algebra can be constructed from $\mathbf{T}$ by forcefully adding a unary law $a \mapsto \neg a$ and by imposing the axioms $a \wedge \neg a = 0$, $a \vee \neg a = 1$.

In other words $\mathbb{B}\mathrm{o}(\mathbf{T})$ can be defined as a Boolean algebra obtained by generators and relations. The generators are the elements of $\mathbf{T}$ and the relations are those that are true in $\mathbf{T}$: of the form $a \wedge b = c$ or $a \vee b = d$, not to mention $0_{\mathbb{B}\mathrm{o}(\mathbf{T})} = 0_{\mathbf{T}}$ and $1_{\mathbb{B}\mathrm{o}(\mathbf{T})} = 1_{\mathbf{T}}$.

This description is however somewhat vague so we will construct $\mathbb{B}\mathrm{o}(\mathbf{T})$ at turtle speed to see things more clearly.

1.6. Lemma. *Let $\mathbf{T}$ be a distributive lattice and $a \in \mathbf{T}$. Consider the distributive lattice*

$$\mathbf{T}[a^\bullet] \overset{\text{def}}{=} \mathbf{T}/(a = 0) \times \mathbf{T}/(a = 1)$$

and $\lambda_a : \mathbf{T} \to \mathbf{T}[a^\bullet]$ be the canonical homomorphism.

1. *The homomorphism λ_a is injective and $\lambda_a(a) = (0, 1)$ admits $(1, 0)$ as its complement.*
2. *For every homomorphism $\psi : \mathbf{T} \to \mathbf{T}'$ such that $\psi(a)$ admits a complement, there exists a unique homomorphism $\varphi : \mathbf{T}[a^\bullet] \to \mathbf{T}'$ such that $\varphi \circ \lambda_a = \psi$.*

$$\begin{tikzcd}
\mathbf{T} \arrow[d, "\lambda_a"'] \arrow[dr, "\psi"] & & \\
\mathbf{T}[a^\bullet] \arrow[r, dashed, "\varphi\,!"'] & \mathbf{T}' & \psi(a) \textit{ admits a complement}
\end{tikzcd}$$

D Lemma 1.5 gives $\mathbf{T}' \simeq \mathbf{T}'/(\psi(a) = 0) \times \mathbf{T}'/(\psi(a) = 1)$, hence the homomorphism φ and the uniqueness. The injectivity of λ_a is not obvious but it is a grand classic: if $x \wedge a = y \wedge a$ and $x \vee a = y \vee a$, then

$$x = (x \vee a) \wedge x = (y \vee a) \wedge x = (y \wedge x) \vee (a \wedge x).$$

Symmetrically $y = (y \wedge x) \vee (a \wedge y)$, so $x = y$ since $a \wedge x = a \wedge y$. □

1.7. Corollary. *Let $a_1, \ldots, a_n \in \mathbf{T}$.*

1. *The lattice $\mathbf{T}[a_1^\bullet][a_2^\bullet]\cdots[a_n^\bullet]$ is independent, up to isomorphism, in the order of the a_i's. It will be denoted by $\mathbf{T}[a_1^\bullet, a_2^\bullet, \ldots, a_n^\bullet]$.*
2. *A possible description is the following*
$$\mathbf{T}[a_1^\bullet, a_2^\bullet, \ldots, a_n^\bullet] \simeq \prod\nolimits_{I\in\mathcal{P}_n} \mathbf{T}/\big((a_i = 0)_{i\in I}, (a_j = 1)_{j\in[\![1..n]\!]\setminus I}\big).$$
3. *The natural homomorphism $\mathbf{T} \to \mathbf{T}[a_1^\bullet, a_2^\bullet, \ldots, a_n^\bullet]$ is injective. It uniquely factors every homomorphism ψ from $\mathbf{T}$ to a distributive lattice $\mathbf{T}'$ such that the $\psi(a_i)$'s admit a complement.*

1.8. Theorem. (Boolean algebra freely generated by a distributive lattice) *For every distributive lattice $\mathbf{T}$ there exists a Boolean algebra, denoted by $\mathbb{B}\mathrm{o}(\mathbf{T})$, with a homomorphism $\lambda : \mathbf{T} \to \mathbb{B}\mathrm{o}(\mathbf{T})$, which uniquely factorizes every homomorphism $\psi : \mathbf{T} \to \mathbf{B}$ to a Boolean algebra. This pair $(\mathbb{B}\mathrm{o}(\mathbf{T}), \lambda)$ is unique up to isomorphism. We have in addition the following properties.*

- *The homomorphism λ is injective.*
- *We have $\mathbb{B}\mathrm{o}(\mathbf{T}) = \mathbf{T}[(a^\bullet)_{a\in\mathbf{T}}]$.*

D It remains to see that the (filtering) colimit of $\mathbf{T}[a_1^\bullet, a_2^\bullet, \ldots, a_n^\bullet]$ is indeed a Boolean algebra. This results from De Morgan's laws. □

Example. Suppose that $\mathbf{T}$ is a lattice of detachable subsets of a set E, in the sense that if A and B are elements of $\mathbf{T}$, then so are $A \cup B$ and $A \cap B$ (with in addition $\emptyset$ and E as elements of $\mathbf{T}$). Then $\mathbb{B}\mathrm{o}(\mathbf{T})$ identifies with the set of finite Boolean combinations of elements of $\mathbf{T}$ and it is a Boolean algebra of subsets of E. ■

Comment. In classical mathematics, every distributive lattice is isomorphic to a lattice of subsets of a set. This provides an alternative "construction" of the Boolean algebra $\mathbb{B}\mathrm{o}(\mathbf{T})$. ■

2. Lattice-groups

First steps

In this book we limit ourselves, for the ordered groups, to the case of commutative groups.

2.1. Definition. We call an *ordered group* an Abelian group G equipped with a partial order relation *compatible* with the group law, i.e. in additive notation,
$$\forall a, x, y \in G \qquad x \leqslant y \implies a + x \leqslant a + y.$$

An ordered group is called a *lattice-group* when two arbitrary elements admit a lower bound, which we will denote by $x \wedge y$. If necessary, we specify the structure by writing $(G, 0, +, -, \wedge)$. A *morphism of l-groups* is a group homomorphism which respects the law $\wedge$.

An Abelian group equipped with a compatible total order (we say a *totally ordered group*) is an l-group. The totally ordered group morphisms are then the non-decreasing group homomorphisms.

An *l-subgroup* of an l-group G is by definition a stable subgroup for the lattice law $\wedge$. For that it is not sufficient for the induced order relation on the subgroup to make a lattice of it.

A guiding idea in the theory of l-groups is that *an l-group behaves in computations as a product of totally ordered groups.* This will be constructively translated by the closed covering principle 2.10.

Examples. 1) (Careful, multiplicative notation!) The set $\mathbb{Q}^{>0}$ of strictly positive rationals is an l-group with as its positive subset the monoid $(\mathbb{N}^{>0}, 1, \times)$. The example of this multiplicative structure is paradigmatic. We have an isomorphism of l-groups $\mathbb{Q}^{>0} \simeq \mathbb{Z}^{(P)}$, where P is the set of prime numbers, $\mathbb{Z}^{(P)} = \bigoplus_{p\in P} \mathbb{Z}$ and the order is induced by the product order. This is just another way to express the fundamental theorem of arithmetic "every natural number is uniquely expressible as a product of powers of prime numbers." It is by wanting to make multiplication for integers of number fields look like multiplication in $\mathbb{N}^{>0}$ at all costs that mathematicians have been brought to invent the "ideal gcd numbers."

2) If $(G_i)_{i\in I}$ is a family of l-groups with a discrete indexing set I, we define the *orthogonal direct sum* of the family, denoted by $\boxplus_{i\in I} G_i$, which is an l-group with as subjacent group the group $\bigoplus_{i\in I} G_i$, the law $\wedge$ being defined coordinatewise. If $I = [\![1..3]\!]$ we will let $G_1 \boxplus G_2 \boxplus G_3$.
For example $\mathbb{Z}^{(P)} = \boxplus_{p\in P} \mathbb{Z}$.
We also define the product $\prod_{i\in I} G_i$ in the usual way, and it is the product in the category of l-groups. When I is a finite set, the l-groups $\boxplus_{i\in I} G_i$ and $\prod_{i\in I} G_i$ are naturally isomorphic.

3) If $(G_i)_{i\in I}$ is a family of totally ordered discrete groups with for I a totally ordered discrete set we define the lexicographic sum of this family, it is the totally ordered discrete group G whose subjacent group is $\bigoplus_{i\in I} G_i$ and the order relation is the lexicographical order: $(x_i)_{i\in I} < (y_i)_{i\in I}$ if and only if $x_{i_0} < y_{i_0}$ for the smallest index i_0 such that $x_{i_0} \neq y_{i_0}$. ■

In an l-group the translations are automorphisms of the order structure, hence the distributivity rule

$$x + (a \wedge b) \;=\; (x + a) \wedge (x + b). \tag{9}$$

We also see that the bijection $x \mapsto -x$ reverses the order, and thus that two arbitrary elements x, y also admits an upper bound

$$x \vee y = -\big((-x) \wedge (-y)\big),$$

with $x+y-(x\vee y)=(x+y)+\big((-x)\wedge(-y)\big)=(x+y-x)\wedge(x+y-y)$, so

$$x+y=(x\wedge y)+(x\vee y), \tag{10}$$

$$x+(a\vee b)=(x+a)\vee(x+b). \tag{11}$$

However, a minimum element and a maximum element are missing to obtain a lattice.

Remarkable identities in the *l*-groups

In this subsection G is an l-group and G^+ is the submonoid of G formed from the non-negative elements.

Let $x^+=x\vee 0$, $x^-=(-x)\vee 0$ and $|x|=x\vee(-x)$. We respectively call them the *positive part*, the *negative part* and the *absolute value* of x.

2.2. Theorem. (Distributivity in the l-groups)
In an l-group the laws $\wedge$ and $\vee$ are distributive with respect to one another.

D It suffices to show $x\vee(y_1\wedge y_2)=(x\vee y_1)\wedge(x\vee y_2)$. By translating by $-x$, we are reduced to $x=0$, i.e. to $(y_1\wedge y_2)^+=y_1^+\wedge y_2^+$.
The inequality $(y_1\wedge y_2)^+\leqslant y_1^+\wedge y_2^+$ is immediate.
Let $y=y_1\wedge y_2$. The element y_i+y^+-y is $\geqslant y_i$ and $\geqslant 0$, so $\geqslant y_i^+$.
Hence $y_i^++y\leqslant y_i+y^+$. Then $(y_1^++y)\wedge(y_2^++y)\leqslant(y_1+y^+)\wedge(y_2+y^+)$, i.e. $(y_1^+\wedge y_2^+)+y\leqslant(y_1\wedge y_2)+y^+$, i.e. $y_1^+\wedge y_2^+\leqslant y^+$. □

Two elements x, y are said to be *disjoint* or *orthogonal* if $|x|\wedge|y|=0$.

2.3. Lemma. *Let $x,\ y\in G$.*

$$x=x^+-x^-,\quad x^+\perp x^-,\quad |x|=x^++x^-=x^+\vee x^-\in G^+ \tag{12}$$

$$x\leqslant y\iff x^+\leqslant y^+\ \ \textit{and}\ \ y^-\leqslant x^-,\quad x=0\iff |x|=0 \tag{13}$$

D (12). First of all $x^+-x=(x\vee 0)-x=(x-x)\vee\big(0+(-x)\big)=x^-$.
Still by distributivity we obtain
$x^++x^-=(x\vee 0)+((-x)\vee 0)=(x-x)\vee(x+0)\vee\big(0+(-x)\big)\vee(0+0)=x^+\vee x^-$.
Finally, since $x^++x^-=(x^+\vee x^-)+(x^+\wedge x^-)$, this gives $x^+\wedge x^-=0$.
(13). Left to the reader. □

2.4. Lemma. (Gauss' lemma) *Let $x,\ y,\ z\in G^+$.*

$$(x\perp y\ \ \textit{and}\ \ x\leqslant y+z)\implies x\leqslant z \tag{14}$$

$$x\perp y\implies x\wedge(y+z)=x\wedge z \tag{15}$$

$$(x\perp y\ \ \textit{and}\ \ x\perp z)\implies x\perp(y+z) \tag{16}$$

$$(x\perp y\ \ \textit{and}\ \ x\leqslant z\ \ \textit{and}\ \ y\leqslant z)\implies x+y\leqslant z \tag{17}$$

D (14). We have $x\leqslant z+x$ because $z\geqslant 0$ and $x\leqslant z+y$ by hypothesis, therefore $x\leqslant(z+x)\wedge(z+y)=z+(x\wedge y)=z$.

(15). Let $x' = x \wedge (y + z)$. It suffices to see that $x' \leqslant x \wedge z$. We have $x' \geqslant 0$, $x' \leqslant x$ so $x' \perp y$. We can apply the previous item to the inequality $x' \leqslant y + z$: it provides $x' \leqslant z$, as desired.

(16). Direct consequence of the previous item.

(17). Because $x + y = x \vee y$ and $x \vee y \leqslant z$. □

2.5. Corollary. *Let x, y, $z \in G$, $n \in \mathbb{N}^*$.*

$$(x = y - z,\ y \geqslant 0,\ z \geqslant 0,\ \textit{and}\ y \perp z) \iff (y = x^+\ \textit{and}\ z = x^-) \tag{18}$$

$$(x \geqslant 0,\ y \geqslant 0,\ \textit{and}\ x \perp y) \implies x \perp ny \tag{19}$$

$$(nx)^+ = nx^+,\ (nx)^- = nx^-,\ |nx| = n\,|x| \tag{20}$$

$$nx = 0 \implies x = 0 \tag{21}$$

$$n(x \wedge y) = nx \wedge ny, \quad n(x \vee y) = nx \vee ny \tag{22}$$

D (18). It remains to show $\implies$. We have $x^+ + z = x^- + y$. By applying Gauss' lemma, we obtain $y \leqslant x^+$ (because $y \perp z$) and $x^+ \leqslant y$ (because $x^+ \perp x^-$).

(19). Results from (21).

(20). By (18) and (19) since $nx = nx^+ - nx^-$ and $nx^+ \perp nx^-$.

(21). By (20) since the implication is true for $x \geqslant 0$.

(22). The elements $b = x \vee y$, $a = x \wedge y$, $x_1 = x - a$ and $y_1 = y - a$ are characterized by the following relations

$$x_1 \geqslant 0,\ y_1 \geqslant 0,\ x = x_1 + a,\ y = y_1 + a,\ x_1 \perp y_1,\ a + b = x + y.$$

We multiply everything by n. □

Simultaneous congruences, covering principle by quotients

2.6. Definition. If $a \in G$, we define *congruence modulo* a as follows

$$x \equiv y \mod a \overset{\text{def}}{\iff} \exists n \in \mathbb{N}^*,\ |x - y| \leqslant n\ |a|\,.$$

We denote by $\mathcal{C}(a)$ the set of x's congruent to 0 modulo a.

2.7. Fact. *The set $\mathcal{C}(a)$ is an l-subgroup of G and the lattice laws pass to the quotient in $G/\mathcal{C}(a)$.*
Thus, the canonical map $\pi_a : G \to G/\mathcal{C}(a)$ is a morphism of l-groups, and every l-group morphism $G \to G'$ which annihilates a is factorized by π_a.

The meaning of the congruence $x \equiv 0 \bmod a$ is therefore that every l-group morphism $G \xrightarrow{\varphi} G'$ that annihilates a annihilates x.[6]

[6] In fact, by direct computation, if $\varphi(a) = 0$, then $\varphi(|a|) = |\varphi(a)| = 0$, and $|\varphi(x)| = \varphi(|x|) \leqslant \varphi(n\,|a|) = n\varphi(|a|) = 0$, so $\varphi(x) = 0$.

The following lemma has an arithmetic Chinese remainder theorem flavor (see Theorem XII-1.6 item *5*) for the l-groups, but only a flavor. It is distinctly simpler.

2.8. Lemma. (Lemma of simultaneous congruences)
Let $(x_1, \dots, x_n)$ in G^+ and $(a_1, \dots, a_n)$ in G.

1. *If the inequalities $|a_i - a_j| \leqslant x_i + x_j$, $i, j \in [\![1..n]\!]$, are satisfied there exists some $a \in G$ such that $|a - a_i| \leqslant x_i$, $i \in [\![1..n]\!]$. Moreover*
   - *If the a_i's are in G^+ we have a solution a in G^+.*
   - *If $\bigwedge_i x_i = 0$, the solution a is unique.*
2. *Similarly, if $a_i \equiv a_j \bmod x_i + x_j$ for i, $j \in [\![1..n]\!]$, there exists an $a \in G$ such that $a \equiv a_i \bmod x_i$, $i \in [\![1..n]\!]$. Moreover*
   - *If the a_i's are in G^+ we have a solution a in G^+.*
   - *If $\bigwedge_i x_i = 0$, the solution a is unique.*

D It suffices to prove item *1*. Let us first take a look at uniqueness. If we have two solutions a and a' we will have $|a - a'| \leqslant 2x_i$ for each i, so $|a - a'| \leqslant 2 \bigwedge_i x_i$.
Let us move on to existence. We treat the case where the a_i's are in G^+. This is actually a matter of showing that the hypotheses imply the inequality $\bigvee_i (a_i - x_i)^+ \leqslant \bigwedge_i (a_i + x_i)$. It suffices to verify that for each i, j, we have $(a_i - x_i) \vee 0 \leqslant a_j + x_j$. However, $0 \leqslant a_j + x_j$, and $a_i - x_i \leqslant a_j + x_j$ by hypothesis. □

2.9. Lemma. *Given a finite family $(a_j)_{j \in J}$ in an l-group G and a finite subset P of $J \times J$, there exists a finite family $(x_i)_{i \in I}$ in G such that*

1. *$\bigwedge_{i \in I} x_i = 0$.*
2. *Modulo each of the x_i's, for each $(j, k) \in P$, we have $a_j \leqslant a_k$ or $a_k \leqslant a_j$.*

D Let $y_{j,k} = a_j - (a_j \wedge a_k)$ and $z_{j,k} = a_k - (a_j \wedge a_k)$. We have $y_{j,k} \wedge z_{j,k} = 0$. Modulo $y_{j,k}$, we have $a_j = a_j \wedge a_k$, i.e. $a_j \leqslant a_k$, and modulo $z_{j,k}$, we have $a_k \leqslant a_j$.
By expanding by distributivity the sum $0 = \sum_{(j,k) \in P} (y_{j,k} \wedge z_{j,k})$ we obtain some $\bigwedge_{i \in I} x_i$, where each x_i is a sum $\sum_{j,k} t_{j,k}$, with one of the two elements $y_{j,k}$ or $z_{j,k}$ as $t_{j,k}$. Modulo such a x_i each of the $t_{j,k}$'s is null (because they are $\geqslant 0$ and their sum is null). We are therefore indeed in the stated situation. □

The next principle is a kind of analogue, for l-groups, of the basic local-global principle for commutative rings.

Actually this is a simple special case of item *2* of Lemma 2.8 when the a_i's are all zeros: we apply uniqueness.

2.10. Covering principle by quotients. (For l-groups)
Let a, $b \in G$, $x_1, \ldots, x_n \in G^+$ with $\bigwedge_i x_i = 0$. Then $a \equiv b \bmod x_i$ for each i if and only if $a = b$.
Consequently, given Lemma 2.9, to demonstrate an equality $a = b$ we can always suppose that the (finite number of) elements which occur in a computation for a proof of the equality are comparable, if we need it to do the proof. The principle applies just as well for inequalities as for equalities since $a \leqslant b$ is equivalent to $a \wedge b = a$.

Remark. In slightly more abstract terms, we could have said that the canonical l-group morphism $G \to \prod_i G/\mathcal{C}(x_i)$ is injective, and the comment that concludes the covering principle by quotients can be paraphrased as follows: in computations, an l-group always behaves like a product of totally ordered groups. ■

In the Riesz theorem that follows we will note that the "there exists" are abbreviations for explicit formulas which result from the proof. Thus the theorem can be seen as a family of algebraic identities in G, under certain sign conditions (which are in the hypothesis). It is also possible to regard this theorem as a family of "pure" algebraic identities in G^+, i.e. without any sign condition. In this case G^+ must be considered as an algebraic structure for which we add the operation $x \dot{-} y \overset{\text{def}}{=} x - (x \wedge y)$ (well-defined over G^+ despite the fact that it calls upon the $-$ operation of G).

2.11. Theorem. (Riesz theorem)
Let G be an l-group and u, $x_1, \ldots, x_n$, $y_1, \ldots, y_m$ in G^+.

1. *If $u \leqslant \sum_j y_j$, there exist $u_1, \ldots, u_m \in G^+$ such that $u_j \leqslant y_j$ for $j \in [\![1..m]\!]$ and $u = \sum_j u_j$.*
2. *If $\sum_i x_i = \sum_j y_j$, there exists $(z_{i,j})_{i \in [\![1..n]\!], j \in [\![1..m]\!]}$ in G^+ such that for all i, j we have $\sum_{k=1}^{m} z_{i,k} = x_i$ and $\sum_{\ell=1}^{n} z_{\ell,j} = y_j$.*

Direct proof, but clever.
1. It suffices to prove it for $m = 2$ (easy induction on m). If $u \leqslant y_1 + y_2$, let $u_1 = u \wedge y_1$ and $u_2 = u - u_1$. We need to prove $0 \leqslant u_2 \leqslant y_2$. However, $u_2 = u - (u \wedge y_1) = u + \big((-u) \vee (-y_1)\big) = (u - u) \vee (u - y_1) \leqslant y_2$.
2. For $n = 1$ or $m = 1$ there is nothing to do. For $n = 2$, it is given by item *1.* Therefore let us suppose $n \geqslant 3$. Let $z_{1,1} = x_1 \wedge y_1$, $x_1' = x_1 - z_{1,1}$ and $y_1' = y_1 - z_{1,1}$. We have $x_1' + x_2 + \cdots + x_n = y_1' + y_2 + \cdots + y_m$.
Since $x_1' \wedge y_1' = 0$, Gauss' lemma gives $x_1' \leqslant y_2 + \cdots + y_m$.
By item *1* we can write $x_1' = z_{1,2} + \cdots + z_{1,m}$ with each $z_{1,j} \leqslant y_j$, i.e. $y_j = z_{1,j} + y_j'$ and $y_j' \in G^+$. Therefore $x_2 + \cdots + x_n = y_1' + y_2' + \cdots + y_m'$.
This therefore allows us to perform an induction on n.

Proof by the covering principle by quotients.
It suffices to prove item *2.* By applying the principle 2.10, we can assume

that the group is totally ordered. Suppose for example $x_1 \leqslant y_1$. Let $z_{1,1} = x_1$, $z_{1,k} = 0$ for $k \geqslant 2$. We replace y_1 with $y_1 - x_1 = y_1'$. We are reduced to solving the problem for $x_2, \ldots, x_n$ and $y_1', y_2, \ldots, y_m$. Gradually, we thus decrease $n + m$ until $n = 1$ or $m = 1$, in which case everything is clear. □

2.12. Fact. (Other identities in the l-groups)
Let x, y, x', y', z, $t \in G$, $n \in \mathbb{N}$, $x_1, \ldots, x_n \in G$.

1. $x + y = |x - y| + 2(x \wedge y)$.

2. $(x \wedge y)^+ = x^+ \wedge y^+$, $(x \wedge y)^- = x^- \vee y^-$,
$(x \vee y)^+ = x^+ \vee y^+$, $(x \vee y)^- = x^- \wedge y^-$.

3. $2(x \wedge y)^+ \leqslant (x + y)^+ \leqslant x^+ + y^+$.

4. $|x + y| \leqslant |x| + |y| \ : \ |x| + |y| = |x + y| + 2(x^+ \wedge y^-) + 2(x^- \wedge y^+)$.

5. $|x - y| \leqslant |x| + |y| \ : \ |x| + |y| = |x - y| + 2(x^+ \wedge y^+) + 2(x^- \wedge y^-)$.

6. $|x + y| \vee |x - y| = |x| + |y|$.

7. $|x + y| \wedge |x - y| = \big||x| - |y|\big|$.

8. $|x - y| = (x \vee y) - (x \wedge y)$.

9. $|(x \vee z) - (y \vee z)| + |(x \wedge z) - (y \wedge z)| = |x - y|$.

10. $|x^+ - y^+| + |x^- - y^-| = |x - y|$.

11. $x \leqslant z \implies (x \wedge y) \vee z = x \wedge (y \vee z)$.

12. $x + y = z + t \implies x + y = (x \vee z) + (y \wedge t)$.

13. $n\,x \geqslant \bigwedge_{k=1}^{n} (ky + (n-k)x) \implies x \geqslant y$.

14. $\bigvee_{i=1}^{n} x_i = \sum_{k=1}^{n} (-1)^{k-1} \big(\sum_{I \in \mathcal{P}_{k,n}} \bigwedge_{i \in I} x_i \big)$.

15. $x \perp y \iff |x + y| = |x - y| \iff |x + y| = |x| \vee |y|$.

16. $x \perp y \implies |x + y| = |x| + |y| = |x| \vee |y|$.

17. $(x \perp y,\ x' \perp y,\ x \perp y',\ x' \perp y',\ x + y = x' + y') \implies (x = x',\ y = y')$.

18. *We define* $\mathrm{Tri}(\underline{x}) = [\mathrm{Tri}_1(\underline{x}), \mathrm{Tri}_2(\underline{x}), \ldots, \mathrm{Tri}_n(\underline{x})]$, *where*
$$\mathrm{Tri}_k(x_1, \ldots, x_n) = \bigwedge_{I \in \mathcal{P}_{k,n}} \big(\bigvee_{i \in I} x_i \big) \quad (k \in [\![1..n]\!]).$$
We have the following results.

- *a.* $\mathrm{Tri}_k(x_1, \ldots, x_n) = \bigvee_{J \in \mathcal{P}_{n-k+1,n}} \big(\bigwedge_{j \in J} x_j \big)$, $(k \in [\![1..n]\!])$.
- *b.* $\mathrm{Tri}_1(\underline{x}) \leqslant \mathrm{Tri}_2(\underline{x}) \leqslant \cdots \leqslant \mathrm{Tri}_n(\underline{x})$.
- *c. If the x_i's are pairwise comparable, the list* $\mathrm{Tr}(\underline{x})$ *is the list of the x_i's non-decreasingly ordered (it is not necessary that the group be discrete).*

Suppose u, v, $w \in G^+$.

19. $u \perp v \iff u + v = |u - v|$.

20. $(u + v) \wedge w \leqslant (u \wedge w) + (v \wedge w)$.

21. $(x + y) \vee w \leqslant (x \vee w) + (y \vee w)$.

22. $v \perp w \implies (u + v) \wedge w = u \wedge w$.

23. $u \perp v \implies (u + v) \wedge w = (u \wedge w) + (v \wedge w)$.

D All of this is just about immediate in a totally ordered group, by reasoning case-by-case. The result follows by the principle 2.10. □

Remarks.

1) An implication like, for instance,

$$(u \wedge v = 0,\ u \geqslant 0,\ v \geqslant 0) \implies u + v = |u - v|$$

(see item *19*) can be seen as the result of an identity which expresses, for a certain integer n, that $n\,|u + v - |u - v||$ is equal to an expression which combines u^-, v^- and $|u \wedge v|$ by means of the laws $\vee$, $\wedge$ and $+$. Actually, the equality given in item *1* directly settles the question without a sign hypothesis on u and v: $|u + v - |u - v|| = 2\,|u \wedge v|$.

2) There is an important difference between the usual algebraic identities, which are ultimately equalities between polynomials in a free commutative ring over indeterminates, $\mathbb{Z}[X_1, \ldots, X_n]$, and the algebraic identities in the l-groups. The latter are certainly equalities between expressions that we can write in an l-group freely generated by a finite number of indeterminates, but the structure of such a free l-group is distinctly more difficult to decrypt than that of a polynomial ring, in which the objects have a normalized expression. The comparison of two expressions in $\mathbb{Z}[X_1, \ldots, X_n]$ is "easy" in so far as we bring each of them to normal form. The task is much more difficult in the free l-groups, for which there is no unique normal form (we can reduce every expression to a supremum of infima of linear combinations of indeterminates, but there is no uniqueness). ■

Partial decomposition, complete decomposition

2.13. Definition. Let $(a_i)_{i \in I}$ be a finite family of non-negative elements in a discrete l-group G.

1. We say that this family admits a *partial decomposition* if we can find a finite family $(p_j)_{j \in J}$ of pairwise orthogonal non-negative elements such that each a_i is of the form $\sum_{j \in J} r_{i,j} p_j$ with all the $r_{i,j} \in \mathbb{N}$. The family $(p_j)_{j \in J}$ is then called a *partial decomposition basis* for the family $(a_i)_{i \in I}$.
2. Such a partial decomposition is called a *complete decomposition* if the p_j's are *irreducible* (an element $q > 0$ is said to be irreducible if an equality $q = c + d$ in G^+ implies $c = 0$ or $d = 0$).
3. We say that an l-group *admits partial decompositions* if it is discrete and if every finite family of non-negative elements admits a partial decomposition.
4. We say that an l-group *admits complete decompositions* if it is discrete and if every non-negative element admits a complete decomposition.
5. We say that an l-group *admits bounded decompositions* when for all $x \geqslant 0$ there exists an integer n such that, when $x = \sum_{j=1}^{n} y_j$ with each $y_j \geqslant 0$, at least one of the y_j's is zero.

6. An l-group is said to be *Noetherian* if every non-increasing sequence of non-negative elements admits two equal consecutive terms.

Examples.
An empty family, or a family of null elements, admits the empty family as a partial decomposition basis.
The l-group $\mathbb{Z}^{(\mathbb{N})}$ admits complete decompositions.
The l-groups $\mathbb{Q}^n$ $(n \geqslant 1)$ admit partial but not complete decompositions.
The l-group $\mathbb{Q}[\sqrt{2}]$ does not admit partial decompositions (consider the finite family $(1, \sqrt{2})$).
The lexicographical product $\mathbb{Z} \times \mathbb{Z}$ does not admit partial decompositions.
More generally a totally ordered group admitting partial decompositions is isomorphic to a subgroup of $\mathbb{Q}$. ■

It is clear that an l-group admitting complete decompositions admits bounded decompositions and that an l-group admitting bounded decompositions is Noetherian.

In an l-group admitting partial decompositions, two partial decompositions for two finite families of G^+ admit a common refinement for the union of two families: here we mean that a partial decomposition basis $(q_1, \dots, q_s)$ refines another if it is a partial decomposition basis for this other.

2.14. Proposition. *In an l-group, if an element* > 0 *admits a complete decomposition, it is unique up to the order of the factors.*

D It suffices to show that if an irreducible element q is bounded above by a sum $\sum_i p_i$ of irreducible elements it is equal to one of them.
However, we then have $q = q \wedge \sum_i p_i$, and since $q \wedge p_j = 0$ or p_j, we can conclude with Gauss' lemma (equality (15)).
Note that we do not need to assume that the group is discrete. □

2.15. Proposition. *Let G be an l-group admitting complete decompositions.*

1. *The irreducible elements of* G^+ *form a detachable subset P, and G is isomorphic to the orthogonal direct sum* $\mathbb{Z}^{(P)}$.
2. *The group G admits bounded decompositions (and a fortiori is Noetherian).*

D *1.* The irreducibility test is given by the complete decomposition of the element to be tested. The isomorphism is obtained from the uniqueness of the complete decomposition (up to the order of the factors).
2. Let $x \in G^+$. Let us write $x = \sum_{j \in J} n_j p_j$ with the irreducible p_j's and $n_j \in \mathbb{N}$, and let $n = \sum_j n_j$. Then if $x = \sum_{k=1}^{n+1} x_k$ with non-negative x_k's, one x_k is necessarily zero (consider the decomposition of each x_k as a sum of irreducible elements). □

In classical mathematics, a discrete Noetherian l-group admits complete decompositions. This result cannot be obtained constructively. Nevertheless we obtain a partial decomposition.

2.16. Theorem. (Partial decomposition under Noetherian condition)
A discrete and Noetherian l-group G admits partial decompositions.

For the proof, we will use the following lemma.

2.17. Lemma. *(under the hypotheses of Theorem 2.16)*
For $a \in G^+$ and $p_1, \ldots, p_m > 0$ pairwise orthogonal, we can find pairwise orthogonal elements $a_0, a_1, \ldots, a_m$ in G^+ satisfying the following properties.

1. $a = \sum_{i=0}^{m} a_i$.
2. *For all $i \in [\![1..m]\!]$, there exists an integer $n_i \geqslant 0$ such that $a_i \leqslant n_i p_i$.*
3. *For all $i \in [\![1..m]\!]$, $a_0 \wedge p_i = 0$.*

D For each i, we consider the non-decreasing sequence $(a \wedge np_i)_{n \in \mathbb{N}}$ bounded above by a. There exists an n_i such that $a \wedge n_i p_i = a \wedge (n_i + 1)p_i$. We then take $a_i = a \wedge n_i p_i$. If $a = a_i + b_i$, we have $b_i \wedge p_i = 0$ because $a_i \leqslant a_i + (b_i \wedge p_i) \leqslant a \wedge (n_i + 1)p_i = a_i$. The a_i's are $\leqslant a$, pairwise orthogonal and $\geqslant 0$ so $a \geqslant \bigvee_i a_i = \sum_i a_i$. Thus, we write in G^+ $a = a_1 + \cdots + a_n + a_0$, with $a_i \leqslant n_i p_i$ for $i \in [\![1..m]\!]$. Finally, we have $b_i = a_0 + \sum_{j \neq i} a_j$, so $a_0 \leqslant b_i$, then $a_0 \wedge p_i \leqslant b_i \wedge p_i = 0$. As $a_i \leqslant n_i p_i$, we a fortiori have $a_0 \wedge a_i = 0$. □

Proof of Theorem 2.16.
By induction on the number m of elements of the family.
• Suppose $m = 2$, consider the elements x_1, x_2. For ease of notation, let us call them a and b. Let $L_1 = [a, b]$, $m_1 = 1$, $E_{1,a} = [1, 0]$, and $E_{1,b} = [0, 1]$. The algorithm proceeds in steps, at the beginning of step k we have a natural integer m_k and three lists of equal length: L_k, a list of non-negative elements of G, $E_{k,a}$ and $E_{k,b}$, two lists of natural integers. At the end of the step the integer m_k and the three lists are replaced with a new integer and new lists, which are used at the next step (unless the algorithm terminates). The general idea is the following: if x, y are two consecutive non-orthogonal terms of L_k, we replace in L_k the segment (x, y) with the segment $(x - (x \wedge y), x \wedge y, y - (x \wedge y))$ (by omitting the first and/or the last term if it is null). We will denote this procedure as follows:

$$R : (x, y) \mapsto \text{ the new segment (of length 1, 2 or 3).}$$

Note that $x + y > \big(x - (x \wedge y)\big) + x \wedge y + \big(y - (x \wedge y)\big)$.
We have to define a loop-invariant. More precisely the conditions satisfied by the integer m_k and the three lists are the following:

- a is equal to the linear combination of elements of L_k with coefficients given by $E_{k,a}$,

- b is equal to the linear combination of elements of L_k with coefficients given by $E_{k,b}$,
- if $L_k = [x_{k,1}, \ldots, x_{k,r_k}]$ the elements $x_{k,j}$ and $x_{k,\ell}$ are orthogonal as soon as
  - $j < m_k$ and $\ell \neq j$ or
  - $j \geqslant m_k$ and $\ell \geqslant j+2$

In short, the $x_{k,j}$'s are pairwise orthogonal, except perhaps for certain pairs $(x_{k,j}, x_{k,j+1})$ with $j \geqslant m_k$. These conditions constitute *the loop-invariant*. It is clear that they are (trivially) satisfied at the start.

The algorithm terminates at step k if the elements of L_k are pairwise orthogonal. In addition, if the algorithm does not terminate at step k, we have the inequality $\sum_{x \in L_k} x > \sum_{z \in L_{k+1}} z$, therefore the decreasing chain condition assures the termination of the algorithm.

It remains to explain the development of a step and to verify the loop-invariant. In order to not manipulate too many indices, we make a slight abuse of notation and write $L_k = [p_1, \ldots, p_n]$, $E_{k,a} = [\alpha_1, \ldots, \alpha_n]$ and $E_{k,b} = [\beta_1, \ldots, \beta_n]$.

The segment (x, y) of L_k which is treated by the procedure $R(x, y)$ is the following: we consider the smallest index j (necessarily $\geqslant m_k$) such that $p_j \wedge p_{j+1} \neq 0$ and we take $(x, y) = (p_j, p_{j+1})$. If such an index does not exist, the elements of L_k are pairwise orthogonal and the algorithm is terminated. Otherwise we apply the procedure $R(x, y)$ and we update the integer (we can take $m_{k+1} = j$) and the three lists.

For example by letting $q_j = p_j \wedge p_{j+1}$, $p'_j = p_j - q_j$ and $p'_{j+1} = p_{j+1} - q_j$, if $p'_j \neq 0 \neq p'_{j+1}$, we will have

$$\begin{aligned}
L_{k+1} &= \left[p_1, \ldots, p_{j-1}, p'_j, q_j, p'_{j+1}, p_{j+2}, \ldots, p_n\right], \\
E_{k+1,a} &= \left[\alpha_1, \ldots, \alpha_{j-1}, \alpha_j, \alpha_j + \alpha_{j+1}, \alpha_{j+1}, \alpha_{j+2}, \ldots \alpha_n\right], \\
E_{k+1,b} &= \left[\beta_1, \ldots, \beta_{j-1}, \beta_j, \beta_j + \beta_{j+1}, \beta_{j+1}, \beta_{j+2}, \ldots \beta_n\right].
\end{aligned}$$

We verify without difficulty in each of the four possible cases that the loop-invariant is preserved.

• If $m > 2$, by induction hypothesis, we have for $(x_1, \ldots, x_{m-1})$ a partial decomposition basis $(p_1, \ldots, p_n)$. By applying Lemma 2.17 with x_m and $(p_1, \ldots, p_n)$ we write $x_m = \sum_{i=0}^{n} a_i$.

The case of two elements gives us for each (a_i, p_i), $i \in [\![1..n]\!]$, a partial decomposition basis S_i. Finally, a partial decomposition basis for $(x_1, \ldots, x_m)$ is the concatenation of S_i's and of a_0. □

Remark. It is easy to convince ourselves that the partial decomposition basis computed by the algorithm is minimal: every other partial decomposition basis for $(x_1, \ldots, x_m)$ would be obtained by decomposing certain elements of the previous basis.

3. GCD-monoids, GCD-domains

Let G be an l-group. Since $a \leqslant b$ if and only if $b \in a + G^+$, the order relation is characterized by the submonoid G^+. The equality $x = x^+ - x^-$ shows that the group G can be obtained by symmetrization of the monoid G^+, and it amounts to the same thing to speak of an l-group or of a monoid satisfying certain particular properties (see Theorem 3.1).

We would therefore have had good reason to begin with the theory of "non-negative submonoids of an l-group" rather than with l-groups. We would therefore have had good reasons to start by the theory of objects of the type "non-negative submonoid of an l-group" rather than by that of l-groups. Indeed, in an l-group the order relation must be given at once in the structure, whereas in its non-negative subset, only the law of the monoid intervenes, exactly as in the multiplicative theory of non-negative integers.

It is therefore solely for reasons of comfort in proofs that we have chosen to start with l-groups.

Non-negative submonoid of an *l*-group

3.1. Theorem. *For a commutative monoid $(M, 0, +)$ to be the non-negative submonoid of an l-group, it is sufficient and necessary that conditions 1, 2 and 3 below are satisfied. In addition, we can replace condition 3 with condition 4.*

1. *The monoid is* regular*, i.e. $x + y = x + z \Rightarrow y = z$.*
2. *The preorder relation $x \in y + M$ is an order relation. In other words, we have $x + y = 0 \Rightarrow x = y = 0$.*
   We denote it by $y \leqslant_M x$, or if the context is clear, by $y \leqslant x$.
3. *Two arbitrary elements admit an upper bound, i.e.*
   $$\forall a, b\ \exists c \quad \uparrow c = (\uparrow a) \cap (\uparrow b).$$
4. *Two arbitrary elements admit a lower bound, i.e.*
   $$\forall a, b\ \exists c \quad \downarrow c = (\downarrow a) \cap (\downarrow b).$$

D A priori condition *3* for a particular pair (a, b) is stronger than condition *4* for the following reason: if a, $b \in M$, the set of elements of M less than a and b is contained in $X = \downarrow(a + b)$. On this set X, the map $x \mapsto a + b - x$ is a bijection that reverses the order and therefore exchanges supremum and infimum when they exist. However, in the other direction, the infimum in X (which is the absolute infimum) can a priori only be transformed into a supremum for the order relation restricted to the subset X, which need not be a global upper bound.

Nevertheless, when condition *4* is satisfied for all a, $b \in M$, it implies condition *3*. Indeed, let us show that $m = a + b - (a \wedge b)$ is the supremum of (a, b) in M by considering some $x \in M$ such that $x \geqslant a$ and $x \geqslant b$. We want to show that $x \geqslant m$, i.e. by letting $y = x \wedge m$, that $y \geqslant m$. However, y is an upper bound of a and b, and $y \in X$. Since m is the supremum of a and b in X, we indeed have $m \leqslant y$.

The rest of the proof is left to the reader. □

The previous theorem leads to the notion of a GCD-monoid. As this notion is always used for the multiplicative monoid of the regular elements of a commutative ring, we pass to the multiplicative notation, and we accept that the divisibility relation defined by the monoid is only a preorder relation, in order to take into account the group of units.

GCD-monoids

In multiplicative notation, a commutative monoid M is regular when, for all a, x, $y \in M$, the equality $ax = ay$ implies $x = y$.

3.2. Definition. We consider a commutative monoid, multiplicatively denoted by $(M, 1, \cdot)$. We say that *a divides b* when $b \in a \cdot M$, we also say that *b is a multiple of a*, and we write $a \mid b$. The monoid M is called a *GCD-monoid* when the two following properties are satisfied

1. M is regular.
2. Two arbitrary elements admits a gcd, i.e.
$$\forall a, b,\ \exists g,\ \forall x, \quad (x \mid a \quad \text{and} \quad x \mid b) \iff x \mid g.$$

Let U be the group of invertible elements (it is a submonoid), also called *group of units*. Two elements a and b of M are said to be *associated* if there exists an invertible element u such that $ua = b$. This is an equivalence relation (we say "the *association* relation") and the monoid structure passes to the quotient. Let M/U be the quotient monoid. It is still a regular monoid, and the divisibility relation, which was a preorder relation on M, becomes an order relation on M/U.

By Theorem 3.1, we obtain the following result.

3.3. Theorem. *With the previous notations, a regular commutative monoid M is a GCD-monoid if and only if M/U is the non-negative submonoid of an l-group.*

In multiplicative notation, the decompositions, partial or complete, are called *factorizations.* We then speak of *partial factorization basis* instead of partial decomposition basis.

Similarly we use the following terminology: a GCD-monoid M *satisfies the divisor chain condition* if the l-group M/U is Noetherian, i.e. if in every sequence of elements $(a_n)_{n \in \mathbb{N}}$ of M such that a_{k+1} divides a_k for every k, there are two associated consecutive terms.

A GCD-monoid M is said *to admit bounded factorizations* if M/U admits bounded decompositions, i.e. if for each a in M there exists an integer n such that for every factorization $a = a_1 \cdots a_n$ of a in M, one of the a_i's is a unit. It is clear that such a monoid satisfies the divisor chain condition.

GCD-rings

We call a *GCD-ring* a commutative ring for which the multiplicative monoid of regular elements is a GCD-monoid. We define in the same way *a bounded factorization ring* or *a ring which satisfies the divisor chain condition.*

A GCD-domain for which $\mathrm{Reg}(\mathbf{A})/\mathbf{A}^\times$ admits partial factorizations is called a *GCD-domain admitting partial factorizations.* Recall that in particular, the corresponding l-group must be discrete, which here means that $\mathbf{A}^\times$ must be a detachable subset of $\mathrm{Reg}(\mathbf{A})$.

An GCD-domain for which $\mathrm{Reg}(\mathbf{A})/\mathbf{A}^\times$ admits complete factorizations is called a *unique factorization domain*, or a *UFD.* In this case we speak rather of *total factorization.*

Other than the general results on the GCD-monoids (which are the translation in multiplicative language of the corresponding results in the l-groups), we establish some specific facts about GCD-rings, because the addition intervenes in the statements. They could have been extended to pp-rings without difficulty.

3.4. Fact.

1. *An GCD-domain whose group of units is detachable and which satisfies the divisor chain condition admits partial factorizations (Theorem 2.16).*
2. *A Bézout ring is a GCD-ring.*
3. *A PID is an GCD-domain which satisfies the divisor chain condition. If the group of units is detachable, the ring admits partial factorizations.*
4. *If $\mathbf{K}$ is a nontrivial discrete field, $\mathbf{K}[X]$ is a Bézout domain, admits bounded factorizations, and the group of units is detachable. In particular, the ring $\mathbf{K}[X]$ admits partial factorizations.*
5. *The rings $\mathbb{Z}$, $\mathbb{Z}[X]$ and $\mathbb{Q}[X]$ are UFD (Proposition III-8.15).*

D The proof is left to the reader. □

3.5. Theorem. *Every GCD-domain is integrally closed.*

D The proof of Lemma III-8.11 can be reused word for word. □

We leave to the reader the proof of the following facts (for 3.8, Kronecker's theorem must be used).

3.6. Fact. *Let $\mathbf{A}$ be a GCD-domain and S be a monoid. Then $\mathbf{A}_S$ is a GCD-domain, and for a, $b \in \mathbf{A}$ a gcd in $\mathbf{A}$ is a gcd in $\mathbf{A}_S$.*

We will say that a submonoid V of a monoid S is *saturated* (in S) if $xy \in V$ and x, $y \in S$ imply $x \in V$. In the literature, we also find V *is factorially closed in S*. A monoid V of a commutative ring $\mathbf{A}$ is therefore saturated if and only if it is saturated in the multiplicative monoid $\mathbf{A}$.

3.7. Fact. *A saturated submonoid V of a GCD-monoid (resp. admitting bounded factorizations) S is a GCD-monoid (resp. admitting bounded factorizations) with the same gcd and lcm as in S.*

3.8. Fact.
Let $\mathbf{A}$ be a nontrivial integrally closed ring and $\mathbf{K}$ be its quotient field.
The multiplicative monoid of the monic polynomials of $\mathbf{A}[\underline{X}] = \mathbf{A}[X_1, \dots, X_n]$ is naturally identified with a saturated submonoid of $\mathbf{K}[\underline{X}]^*/\mathbf{K}^\times$.
In particular, the multiplicative monoid of the monic polynomials of $\mathbf{A}[\underline{X}]$ is a GCD-monoid admitting bounded factorizations.

GCD-domains of dimension at most 1

3.9. Definition. A pp-ring $\mathbf{A}$ is said to be *of dimension at most* 1 if for every regular element a the quotient $\mathbf{A}/\langle a\rangle$ is zero-dimensional.

Remark. Under the hypothesis that a is regular, we therefore obtain that for all b, there exist x, $y \in \mathbf{A}$ and $n \in \mathbb{N}$ such that

$$b^n(1 + bx) + ay = 0. \qquad (*)$$

If we no longer make anymore hypotheses about a, we can consider the idempotent e that generates $\mathrm{Ann}(a)$, and we then have an equality of the type $(*)$, but by replacing a by $a + e$, which is regular. This equality gives, after a multiplication by a that makes e disappear,

$$a(b^n(1 + bx) + ay) = 0 \qquad (+).$$

We thus obtain an equality in accordance with that given in Chapter XIII where a constructive definition constructive of the sentence "$\mathbf{A}$ is a ring of Krull dimension at most r" appears, for an arbitrary ring $\mathbf{A}$ (see item *3* of Proposition XIII-2.8). ■

3.10. Lemma. (A factorization in dimension 1)

1. *Let $\mathfrak{a}$ and $\mathfrak{b}$ be two ideals in a ring $\mathbf{A}$ with $\mathbf{A}/\mathfrak{a}$ zero-dimensional and $\mathfrak{b}$ finitely generated. Then we can write*
$$\mathfrak{a} = \mathfrak{a}_1\mathfrak{a}_2 \;\; \textit{with} \;\; \mathfrak{a}_1 + \mathfrak{b} = \langle 1\rangle \; \textit{and} \; \mathfrak{b}^n \subseteq \mathfrak{a}_2$$
for a suitable integer n. This writing is unique and we have
$$\mathfrak{a}_1 + \mathfrak{a}_2 = \langle 1\rangle\,, \;\; \mathfrak{a}_2 = \mathfrak{a} + \mathfrak{b}^n = \mathfrak{a} + \mathfrak{b}^m \; \textit{for every } m \geqslant n.$$

2. *The result applies if* $\mathbf{A}$ *is a pp-ring of dimension at most* 1*,* $\mathfrak{a}$ *is invertible, and* $\mathfrak{b}$ *is finitely generated. In this case* $\mathfrak{a}_1$ *and* $\mathfrak{a}_2$ *are invertible. In particular,* $\mathfrak{a} + \mathfrak{b}^n$ *is invertible for large enough* n*.*

D It suffices to prove item *1*.

Existence and uniqueness of the factorization. Consider a triple $(\mathfrak{a}_1, \mathfrak{a}_2, n)$ susceptible of satisfying the hypotheses. Since $\mathfrak{a}_1$ and $\mathfrak{a}_2$ must contain $\mathfrak{a}$, we can reason modulo $\mathfrak{a}$, and therefore suppose $\mathbf{A}$ is zero-dimensional with the equality $\mathfrak{a}_1\mathfrak{a}_2 = \langle 0 \rangle$.

Let $\mathfrak{a}_1 + \mathfrak{b} = \langle 1 \rangle$ imply $\mathfrak{a}_1 + \mathfrak{b}^\ell = \langle 1 \rangle$ for every exponent $\ell \geqslant 1$. In particular, $\mathbf{A} = \mathfrak{a}_1 \oplus \mathfrak{a}_2 = \mathfrak{a}_1 \oplus \mathfrak{b}^m$ for every $m \geqslant n$. This forces, with e being idempotent, $\mathfrak{a}_1 = \langle 1 - e \rangle$ and $\mathfrak{a}_2 = \mathfrak{b}^m = \langle e \rangle$ for m such that $\mathfrak{b}^m = \mathfrak{b}^{m+1}$ (see Lemma II-4.4 and item *3* of Lemma IV-8.2). □

Remark. Item *2* is valid without assuming that $\mathbf{A}$ is a pp-ring. This will become clear after the general constructive definition of the Krull dimension, since for every regular element a, if $\mathbf{A}$ is of dimension at most 1, the ring $\mathbf{A}/\langle a \rangle$ is zero-dimensional. ■

3.11. Proposition. *Let* $\mathbf{A}$ *be a GCD-domain; then every locally principal ideal is principal.*

D Let $\mathfrak{a} = \langle a_1, \dots, a_n \rangle$ be locally principal and $d = \gcd(a_1, \dots, a_n)$. Let us show that $\mathfrak{a} = \langle d \rangle$. There exists a system of comaximal elements $(s_1, \dots, s_n)$ with $\langle a_1, \dots, a_n \rangle = \langle a_i \rangle$ in $\mathbf{A}_{s_i}$. It suffices to see that $\langle a_1, \dots, a_n \rangle = \langle d \rangle$ in each $\mathbf{A}_{s_i}$ because this equality, locally true, will be true globally. But $\mathbf{A}_{s_i}$ remains a GCD-domain, and the gcds do not change. Therefore, in $\mathbf{A}_{s_i}$, we obtain $\langle a_1, \dots, a_n \rangle = \langle a_i \rangle = \langle \gcd(a_1, \dots, a_n) \rangle = \langle d \rangle$. □

3.12. Theorem. *A GCD-domain of dimension at most* 1 *is a Bézout domain.*

D Since $\langle a, b \rangle = g \langle a_1, b_1 \rangle$ with $\gcd(a_1, b_1) = 1$, it suffices to show that $\gcd(a, b) = 1$ implies $\langle a, b \rangle = \langle 1 \rangle$. However, $\gcd(a, b) = 1$ implies $\gcd(a, b^n) = 1$ for every $n \geqslant 0$. Finally, after item *2* of Lemma 3.10, for large enough n, $\langle a, b^n \rangle$ is invertible therefore locally principal, and the result follows by Proposition 3.11. □

Gcd in a polynomial ring

If $\mathbf{A}$ is a GCD-domain and $f \in \mathbf{A}[X]$ we let $\mathrm{G}_X(f)$ or $\mathrm{G}(f)$ be a gcd of the coefficients of f (it is defined up to unit elements multiplicatively) and we call it the *G-content* of f. A polynomial whose G-content is equal to 1 is said to be *G-primitive.*

3.13. Lemma. *Let $\mathbf{A}$ be a GCD-domain, $\mathbf{K}$ be its quotient field and f be a nonzero element of $\mathbf{K}[X]$.*

- *We can write $f = af_1$ with $a \in \mathbf{K}$ and f_1 as G-primitive in $\mathbf{A}[X]$.*
- *This expression is unique in the following sense: for another expression of the same type $f = a'f_1'$, there exists a $u \in \mathbf{A}^\times$ such that $a' = ua$ and $f_1 = uf_1'$.*
- *$f \in \mathbf{A}[X]$ if and only if $a \in \mathbf{A}$, in this case $a = \mathrm{G}(f)$.*

D The proof is left to the reader. □

3.14. Proposition. (Gauss' lemma, another) *Let $\mathbf{A}$ be a GCD-domain and f, $g \in \mathbf{A}[X]$. Then $\mathrm{G}(fg) = \mathrm{G}(f)\mathrm{G}(g)$. In particular, the product of two G-primitive polynomials is a G-primitive polynomial.*

D Let f_i and g_j be the coefficients of f and g. It is clear that $\mathrm{G}(f)\mathrm{G}(g)$ divides $\mathrm{G}(fg)$. By distributivity the gcd of the f_ig_j's is equal to $\mathrm{G}(f)\mathrm{G}(g)$, but Proposition III-8.13 implies that $\mathrm{G}(fg)$ divides the f_ig_j's therefore their gcd. □

3.15. Corollary. *Let $\mathbf{A}$ be a GCD-domain, $\mathbf{K}$ be its quotient field and f, $g \in \mathbf{A}[X]$. Then f divides g in $\mathbf{A}[X]$ if and only if f divides g in $\mathbf{K}[X]$ and $\mathrm{G}(f)$ divides $\mathrm{G}(g)$ in $\mathbf{A}$.*

D The "only if" results from Gauss' lemma. For the "if" we can suppose that f is G-primitive. If $g = hf$ in $\mathbf{K}[X]$, we can write $h = ah_1$ where $h_1 \in \mathbf{A}[X]$ is G-primitive and $a \in \mathbf{K}$. By Gauss' lemma, we have fh_1 G-primitive. By applying Lemma 3.13 to the equality $g = a(h_1f)$, we obtain $a \in \mathbf{A}$, then $h \in \mathbf{A}[X]$. □

Recall that if $\mathbf{A}$ is a reduces ring, $\mathbf{A}[X]^\times = \mathbf{A}^\times$ (Lemma II-2.6 *4*). In particular, if $\mathbf{A}$ is a nontrivial domain and if the group of units of $\mathbf{A}$ is detachable, the same goes for $\mathbf{A}[X]$.

3.16. Theorem. *Let $\mathbf{A}$ be a GCD-domain and $\mathbf{K}$ be its quotient field.*

1. *$\mathbf{A}[X_1, \ldots, X_n]$ is a GCD-domain.*
2. *If $\mathbf{A}$ admits partial factorizations, the same goes for $\mathbf{A}[X]$.*
3. *If $\mathbf{A}$ satisfies the divisor chain condition, the same goes for $\mathbf{A}[X]$.*
4. *If $\mathbf{A}$ admits bounded factorizations, the same goes for $\mathbf{A}[X]$.*
5. *If $\mathbf{A}[X]$ is a UFD, the same goes for $\mathbf{A}[X_1, \ldots, X_n]$* (Kronecker)*.*

D *1.* It suffices to treat the case $n = 1$. Let f, $g \in \mathbf{A}[X]$.
Let us express $f = af_1$, $g = bg_1$, with G-primitive f_1 and g_1. Let $c = \gcd_{\mathbf{A}}(a, b)$ and $h = \gcd_{\mathbf{K}[X]}(f_1, g_1)$. We can assume without loss of generality that h is in $\mathbf{A}[X]$ and that it is G-primitive. Then, by using Corollary 3.15, we verify that ch is a gcd of f and g in $\mathbf{A}[X]$.
Items *2*, *3* and *4* are left to the reader.

5. It suffices to treat the case $n = 2$ and to know how to detect if a polynomial admits a strict factor. We use the Kronecker trick. To test the polynomial $f(X, Y) \in \mathbf{A}[X, Y]$, assumed of degree $< d$ in X, we consider the polynomial $g(X) = f(X, X^d)$. A complete decomposition of $g(X)$ allows us to know if there exists a strict factor of g of the form $h(X, X^d)$ (by considering all the strict factors of g, up to association), which corresponds to a strict factor of f. For some precisions see Exercise 6. □

3.17. Corollary. *If* $\mathbf{K}$ *is a nontrivial discrete field,* $\mathbf{K}[X_1, \ldots, X_n]$ *is a GCD-domain, admitting bounded factorizations and partial factorizations. The group of units is* $\mathbf{K}^\times$*. Finally,* $\mathbf{K}[X_1, \ldots, X_n]$ *(*$n \geqslant 2$*) is a UFD if and only if* $\mathbf{K}[X]$ *is a UFD.*

4. Zariski lattice of a commutative ring

Generalities

Recall the notation $\mathrm{D}_{\mathbf{A}}(\mathfrak{a})$ with some precisions.

4.1. Notation. If $\mathfrak{a}$ is an ideal of $\mathbf{A}$, let $\mathrm{D}_{\mathbf{A}}(\mathfrak{a}) = \sqrt{\mathfrak{a}}$ be the nilradical of $\mathfrak{a}$. If $\mathfrak{a} = \langle x_1, \ldots, x_n \rangle$ let $\mathrm{D}_{\mathbf{A}}(x_1, \ldots, x_n)$ for $\mathrm{D}_{\mathbf{A}}(\mathfrak{a})$. Let $\mathsf{Zar}\,\mathbf{A}$ be the set of $\mathrm{D}_{\mathbf{A}}(x_1, \ldots, x_n)$ (for $n \in \mathbb{N}$ and $x_1, \ldots, x_n \in \mathbf{A}$).

We therefore have $x \in \mathrm{D}_{\mathbf{A}}(x_1, \ldots, x_n)$ if and only if a power of x is a member of $\langle x_1, \ldots, x_n \rangle$.

The set $\mathsf{Zar}\,\mathbf{A}$ is ordered by the inclusion relation.

4.2. Fact. $\mathsf{Zar}\,\mathbf{A}$ *is a distributive lattice with*

$$\begin{aligned} \mathrm{D}_{\mathbf{A}}(0) &= 0_{\mathsf{Zar}\,\mathbf{A}}, & \mathrm{D}_{\mathbf{A}}(\mathfrak{a}_1) \vee \mathrm{D}_{\mathbf{A}}(\mathfrak{a}_2) &= \mathrm{D}_{\mathbf{A}}(\mathfrak{a}_1 + \mathfrak{a}_2), \\ \mathrm{D}_{\mathbf{A}}(1) &= 1_{\mathsf{Zar}\,\mathbf{A}}, & \mathrm{D}_{\mathbf{A}}(\mathfrak{a}_1) \wedge \mathrm{D}_{\mathbf{A}}(\mathfrak{a}_2) &= \mathrm{D}_{\mathbf{A}}(\mathfrak{a}_1\,\mathfrak{a}_2). \end{aligned}$$

We call it the Zariski lattice of the ring $\mathbf{A}$*.*

In classical mathematics $\mathrm{D}_{\mathbf{A}}(x_1, \ldots, x_n)$ can be seen as a compact-open subspace of $\mathsf{Spec}\,\mathbf{A}$: the set of prime ideals $\mathfrak{p}$ of $\mathbf{A}$ such that at least one of the x_i's does not belong to $\mathfrak{p}$, and $\mathsf{Zar}\,\mathbf{A}$ is identified with the lattice of the compact-open subspaces of $\mathsf{Spec}\,\mathbf{A}$. For more details on the subject see Section XIII-1.

4.3. Fact.

1. *For every morphism* $\varphi : \mathbf{A} \to \mathbf{B}$*, we have a natural morphism* $\mathsf{Zar}\,\varphi$ *from* $\mathsf{Zar}\,\mathbf{A}$ *to* $\mathsf{Zar}\,\mathbf{B}$*, and we thus obtain a functor from the category of commutative rings to that of distributive lattices.*
2. *For every ring* $\mathbf{A}$ *the natural homomorphism* $\mathsf{Zar}\,\mathbf{A} \to \mathsf{Zar}\,\mathbf{A}_{\mathrm{red}}$ *is an isomorphism, so that we can identify the two lattices.*

3. *The natural homomorphism* $\mathsf{Zar}(\mathbf{A}_1 \times \mathbf{A}_2) \to \mathsf{Zar}\,\mathbf{A}_1 \times \mathsf{Zar}\,\mathbf{A}_2$ *is an isomorphism.*
4. *For a Boolean algebra* $\mathbf{B}$*, the map* $x \mapsto \mathrm{D}_{\mathbf{B}}(x)$ *is an isomorphism from* $\mathbf{B}$ *to* $\mathsf{Zar}\,\mathbf{B}$.

4.4. Fact. *The following properties are equivalent.*

1. $\mathsf{Zar}\,\mathbf{A}$ *is a Boolean algebra.*
2. $\mathbf{A}$ *is zero-dimensional.*

D Recall that a distributive lattice "is" a Boolean algebra if and only if every element admits a complement (Proposition 1.4).
Suppose *2.* Then for every finitely generated ideal $\mathfrak{a}$, there exist an idempotent e and an integer n such that $\mathfrak{a}^n = \langle e\rangle$. Therefore $\mathrm{D}_{\mathbf{A}}(\mathfrak{a}) = \mathrm{D}_{\mathbf{A}}(e)$. Moreover, it is clear that $\mathrm{D}_{\mathbf{A}}(e)$ and $\mathrm{D}_{\mathbf{A}}(1-e)$ are complements in $\mathsf{Zar}\,\mathbf{A}$.
Suppose *1.* Let $x \in \mathbf{A}$ and $\mathfrak{a}$ be a finitely generated ideal of $\mathbf{A}$ such that $\mathrm{D}_{\mathbf{A}}(\mathfrak{a})$ is the complement of $\mathrm{D}_{\mathbf{A}}(x)$ in $\mathsf{Zar}\,\mathbf{A}$. Then there exist $b \in \mathbf{A}$ and $a \in \mathfrak{a}$ such that $bx + a = 1$. As $xa = x(1-bx)$ is nilpotent we obtain an equality $x^n(1+cx) = 0$. □

4.5. Fact. *Let* $a \in \mathbf{A}$ *and* $\mathfrak{a} \in \mathsf{Zar}\,\mathbf{A}$.

1. *The homomorphism* $\mathsf{Zar}\,\pi : \mathsf{Zar}\,\mathbf{A} \to \mathsf{Zar}(\mathbf{A}/\langle a\rangle)$*, where* $\pi : \mathbf{A} \to \mathbf{A}/\langle a\rangle$ *is the canonical projection, is surjective, and it allows us to identify* $\mathsf{Zar}(\mathbf{A}/\langle a\rangle)$ *with the quotient lattice* $\mathsf{Zar}(\mathbf{A})/(\mathrm{D}_{\mathbf{A}}(a) = 0)$. *More generally,* $\mathsf{Zar}(\mathbf{A}/\mathfrak{a})$ *is identified with* $\mathsf{Zar}(\mathbf{A})/(\mathfrak{a} = 0)$.
2. *The homomorphism* $\mathsf{Zar}\,j : \mathsf{Zar}\,\mathbf{A} \to \mathsf{Zar}(\mathbf{A}[1/a])$*, where* $j : \mathbf{A} \to \mathbf{A}[1/a]$ *is the canonical homomorphism, is surjective and it allows us to identify* $\mathsf{Zar}(\mathbf{A}[1/a])$ *with the quotient lattice* $\mathsf{Zar}(\mathbf{A})/(\mathrm{D}_{\mathbf{A}}(a) = 1)$.
3. *For some ideal* $\mathfrak{c}$ *and some monoid* S *of* $\mathbf{A}$ *we have a natural isomorphism*
$$\mathsf{Zar}(\mathbf{A}_S/\mathfrak{c}\mathbf{A}_S) \;\simeq\; \mathsf{Zar}(\mathbf{A})/(\mathfrak{b} = 0, \mathfrak{f} = 1)\ ,$$
where $\mathfrak{b}$ *is the ideal of* $\mathsf{Zar}\,\mathbf{A}$ *generated by the* $\mathrm{D}_{\mathbf{A}}(c)$*'s for* $c \in \mathfrak{c}$*, and* $\mathfrak{f}$ *is the filter of* $\mathsf{Zar}\,\mathbf{A}$ *generated by the* $\mathrm{D}_{\mathbf{A}}(s)$*'s for* $s \in S$.

Duality in the commutative rings

Annihilating and inverting simultaneously

In the distributive lattices we exchange the roles of ∧ and ∨ by passing to the opposite lattice, i.e. by reversing the order relation.

In the commutative rings, a fecund duality also exists between the addition and the multiplication, more mysterious when we try to exchange their roles.

Recall that a saturated monoid is called a *filter*. The notion of filter is a dual notion to that of ideal, just as important.

The ideals are the inverse images of 0 under the homomorphisms. They serve to pass to the quotient, i.e. to annihilate elements by force. The filters are the inverse images of the group of units under the homomorphisms. They serve to localize, i.e. to render elements invertible by force.

Given an ideal $\mathfrak{a}$ and a monoid S of the ring $\mathbf{A}$ we may want to annhilate the elements of $\mathfrak{a}$ and invert the elements of S. The solution of this problem is given by consideration of the following ring.

4.6. Definition and notation. Let (by abuse) $\mathbf{A}_S/\mathfrak{a}$ or $S^{-1}\mathbf{A}/\mathfrak{a}$ be the ring whose elements are given by the pairs $(a, s) \in \mathbf{A} \times S$, with the equality $(a, s) = (a', s')$ in $\mathbf{A}_S/\mathfrak{a}$ if and only if there exists an $s'' \in S$ such that $s''(as' - a's) \in \mathfrak{a}$ (we will write a/s for the pair (a, s)).

The fact that $\mathbf{A}_S/\mathfrak{a}$ defined thus answers the posed problem signifies that the following factorization theorem is true (see the analogous Facts II-1.1 and II-1.2).

4.7. Fact. (Factorization theorem)
With the above notations, let $\psi : \mathbf{A} \to \mathbf{B}$ be a homomorphism. Then ψ is factorized by $\mathbf{A}_S/\mathfrak{a}$ if and only if $\psi(\mathfrak{a}) \subseteq \{0\}$ and $\psi(S) \subseteq \mathbf{B}^\times$. In this case, the factorization is unique.

$$\begin{tikzcd}
\mathbf{A} \arrow[d, "\lambda"'] \arrow[dr, "\psi"] & \\
\mathbf{A}_S/\mathfrak{a} \arrow[r, dashed, "\theta\,!"'] & \mathbf{B}
\end{tikzcd}$$

$\psi(\mathfrak{a}) \subseteq \{0\}$ and $\psi(S) \subseteq \mathbf{B}^\times$

Naturally we can also solve the problem by first annihilating $\mathfrak{a}$ then by inverting (the image of) S, or by first inverting S then by annihilating (the image of) $\mathfrak{a}$. We thus obtain canonical isomorphisms

$$\mathbf{A}_S/\mathfrak{a} \;\simeq\; \big(\pi_{\mathbf{A},\mathfrak{a}}(S)\big)^{-1}(\mathbf{A}/\mathfrak{a}) \;\simeq\; (\mathbf{A}_S)/(j_{\mathbf{A},S}(\mathfrak{a})\mathbf{A}_S)\;.$$

Dual definitions

The duality between ideals and filters is a form of duality between addition and multiplication.

This is easily seen from the respective axioms that are used to define the ideals (resp. prime ideals) and the filters (resp. prime filters)

$$\begin{array}{rcl@{\qquad\qquad}rcl}
\text{ideal } \mathfrak{a} & & & \text{filter } \mathfrak{f} & & \\
 & \vdash & 0 \in \mathfrak{a} & & \vdash & 1 \in \mathfrak{f} \\
x \in \mathfrak{a},\, y \in \mathfrak{a} & \vdash & x + y \in \mathfrak{a} & x \in \mathfrak{f},\, y \in \mathfrak{f} & \vdash & xy \in \mathfrak{f} \\
x \in \mathfrak{a} & \vdash & xy \in \mathfrak{a} & xy \in \mathfrak{f} & \vdash & x \in \mathfrak{f} \\
\text{prime —} & & & \text{prime —} & & \\
xy \in \mathfrak{a} & \vdash & x \in \mathfrak{a} \vee y \in \mathfrak{a} & x + y \in \mathfrak{f} & \vdash & x \in \mathfrak{f} \vee y \in \mathfrak{f}
\end{array}$$

Note that according to the above definition, $\mathfrak{a}$ is both a prime ideal and a prime filter of $\mathbf{A}$. This convention can seem strange, but it happens to be the most practical one: an ideal is prime if and only if the quotient ring is without zerodivisors, a filter is prime if and only if the localized ring is a local ring. With regard to ideals we have already commented on this on page 491.

We will adopt the following definition for a *maximal filter*: the localized ring is a zero-dimensional local ring (when the ring is reduced: a discrete field). In particular, every maximal filter is prime. We will essentially make use of this definition as a heuristic.

Now suppose the ring $\mathbf{A}$ is nontrivial. Then a detachable strict ideal (resp. a detachable strict filter) is prime if and only if its complement is a filter (resp. an ideal). We once again find in this case the familiar ground in classical mathematics.

Generally in classical mathematics the complement of a strict prime ideal is a strict prime filter and vice versa, therefore the complement of a strict maximal ideal is a minimal prime filter, and the complement of a strict maximal filter is a minimal prime ideal. The prime filters therefore seem more or less useless and have a tendency to disappear from the scene in classical mathematics.

Saturated pairs

A good way to understand the duality is to simultaneously treat ideals and filters. For this we introduce the notion of a *saturated pair*, analogous to that which we have given for distributive lattices.

4.8. Definition. Let $\mathfrak{a}$ be an ideal and $\mathfrak{f}$ be a filter of $\mathbf{A}$. We say that $\mathfrak{a}$ is $\mathfrak{f}$-*saturated* if we have

$$(as \in \mathfrak{a},\ s \in \mathfrak{f}) \implies a \in \mathfrak{a},$$

we say that $\mathfrak{f}$ is $\mathfrak{a}$-*saturated* if we have

$$(a + s \in \mathfrak{f},\ a \in \mathfrak{a}) \implies s \in \mathfrak{f}.$$

If $\mathfrak{a}$ is $\mathfrak{f}$-saturated and $\mathfrak{f}$ is $\mathfrak{a}$-saturated we say that $(\mathfrak{a}, \mathfrak{f})$ is a *saturated pair* in $\mathbf{A}$.

To recap the axioms for the saturated pairs (note that the last condition can be rewritten as $\mathfrak{a} + \mathfrak{f} = \mathfrak{f}$).

$$\begin{array}{rlrl}
 & \vdash\ 0 \in \mathfrak{a} & & \vdash\ 1 \in \mathfrak{f} \\
x \in \mathfrak{a},\ y \in \mathfrak{a} & \vdash\ x + y \in \mathfrak{a} & x \in \mathfrak{f},\ y \in \mathfrak{f} & \vdash\ xy \in \mathfrak{f} \\
x \in \mathfrak{a} & \vdash\ xy \in \mathfrak{a} & xy \in \mathfrak{f} & \vdash\ x \in \mathfrak{f} \\
xy \in \mathfrak{a},\ y \in \mathfrak{f} & \vdash\ x \in \mathfrak{a} & x + y \in \mathfrak{f},\ y \in \mathfrak{a} & \vdash\ x \in \mathfrak{f}
\end{array}$$

4.9. Fact.

1. *For every homomorphism $\varphi : \mathbf{A} \to \mathbf{B}$, the pair $\big(\operatorname{Ker}\varphi, \varphi^{-1}(\mathbf{B}^\times)\big)$ is a saturated pair.*
2. *Conversely if $(\mathfrak{a}, \mathfrak{f})$ is a saturated pair and if $\psi : \mathbf{A} \to \mathbf{A}_\mathfrak{f}/\mathfrak{a} = \mathbf{C}$ designates the canonical homomorphism, we have $\operatorname{Ker}\psi = \mathfrak{a}$ and $\psi^{-1}(\mathbf{C}^\times) = \mathfrak{f}$.*
3. *Let $\varphi : \mathbf{A} \to \mathbf{C}$ be a homomorphism and $(\mathfrak{b}, \mathfrak{g})$ be a saturated pair of $\mathbf{C}$, then $\big(\varphi^{-1}(\mathfrak{b}), \varphi^{-1}(\mathfrak{g})\big)$ is a saturated pair of $\mathbf{A}$.*

4.10. Fact. *Let $(\mathfrak{a}, \mathfrak{f})$ be a saturated pair.*

1. *$\mathbf{A}_\mathfrak{f}/\mathfrak{a}$ is local if and only if $\mathfrak{f}$ is a prime filter (i.e. if and only if $\mathbf{A}_\mathfrak{f}$ is local).*
2. *$\mathbf{A}_\mathfrak{f}/\mathfrak{a}$ is without zerodivisors if and only if $\mathfrak{a}$ is a prime ideal (i.e. if and only if $\mathbf{A}/\mathfrak{a}$ is without zerodivisors).*

4.11. Definition. If $(\mathfrak{a}, \mathfrak{f})$ and $(\mathfrak{b}, \mathfrak{g})$ are two saturated pairs of $\mathbf{A}$ we say that $(\mathfrak{b}, \mathfrak{g})$ *refines* $(\mathfrak{a}, \mathfrak{f})$ and we write it $(\mathfrak{a}, \mathfrak{f}) \leqslant (\mathfrak{b}, \mathfrak{g})$ when $\mathfrak{a} \subseteq \mathfrak{b}$ and $\mathfrak{f} \subseteq \mathfrak{g}$.

The following lemma describes the saturated pair "generated" (in the sense of the refinement relation) by a pair of subsets of $\mathbf{A}$. Actually it suffices to treat the case of a pair formed by an ideal and a monoid.

4.12. Lemma. *Let $\mathfrak{a}$ be an ideal and $\mathfrak{f}$ of $\mathbf{A}$ be a monoid.*

1. *The saturated pair $(\mathfrak{b}, \mathfrak{g})$ generated by $(\mathfrak{a}, \mathfrak{f})$ is obtained as follows* $\mathfrak{b} = \{\, x \in \mathbf{A} \,|\, \exists s \in \mathfrak{f},\ xs \in \mathfrak{a} \,\}$, *and* $\mathfrak{g} = \{\, y \in \mathbf{A} \,|\, \exists u \in \mathbf{A},\ uy \in \mathfrak{a} + \mathfrak{f} \,\}$.
2. *If $\mathfrak{f} \subseteq \mathbf{A}^\times$, then $\mathfrak{b} = \mathfrak{a}$ and $\mathfrak{g}$ is the filter obtained by saturating the monoid $1 + \mathfrak{a}$. In this case, $\mathbf{A}_\mathfrak{g}/\mathfrak{a} = \mathbf{A}/\mathfrak{a}$.*
3. *If $\mathfrak{a} = 0$, then $\mathfrak{b} = \{\, x \in \mathbf{A} \,|\, \exists s \in \mathfrak{f},\ xs = 0 \,\} = \sum_{s \in \mathfrak{f}} (0 : s)$, and $\mathfrak{g}$ is the saturation of $\mathfrak{f}$. In this case, $\mathbf{A}_\mathfrak{g}/\mathfrak{b} = \mathbf{A}_\mathfrak{f}$. If in addition $\mathfrak{f} = s^\mathbb{N}$, $\mathfrak{b} = (0 : s^\infty)$.*

An important case is that of the filter obtained by saturation of a monoid S. We introduce the notation S^{sat}, or, if necessary, $S^{\mathrm{sat}_\mathbf{A}}$ for this filter.

Incompatible ideal and filter

For any saturated pair $(\mathfrak{a}, \mathfrak{f})$ we have the following equivalences.

$$\mathfrak{a} = \mathbf{A} \iff 1 \in \mathfrak{a} \iff 0 \in \mathfrak{f} \iff \mathfrak{f} = \mathbf{A} \iff \mathbf{A}_\mathfrak{f}/\mathfrak{a} = \{0\}. \qquad (23)$$

An ideal $\mathfrak{a}$ and a filter $\mathfrak{f}$ are said to be *incompatible* when they generate the pair $(\mathbf{A}, \mathbf{A})$, i.e. when $0 \in \mathfrak{a} + \mathfrak{f}$.

An ideal $\mathfrak{a}$ and a filter $\mathfrak{f}$ are said to be *compatible* if they satsify $(0 \in \mathfrak{a} + \mathfrak{f} \Rightarrow 1 = 0)$. If the ring is nontrivial this also means $\mathfrak{a} \cap \mathfrak{f} = \emptyset$. In this case we can both annihilate the elements of $\mathfrak{a}$ and render the elements of $\mathfrak{f}$ invertible without reducing the ring to 0.

4.13. Fact. *Let $\mathfrak{a}$ be an ideal and $\mathfrak{f}$ be a compatible filter. If $\mathfrak{a}$ is prime, it is $\mathfrak{f}$-saturated, if $\mathfrak{f}$ is prime, it is $\mathfrak{a}$-saturated.*

4.14. Fact. (The lattice of saturated pairs) *The saturated pairs of $\mathbf{A}$ have a lattice structure for the refinement relation, such that*

- *The minimum element is $(\{0\}, \mathbf{A}^{\times})$ and the maximum element $(\mathbf{A}, \mathbf{A})$.*
- *$(\mathfrak{a}, \mathfrak{f}) \vee (\mathfrak{b}, \mathfrak{g})$ is the saturated pair generated by $(\mathfrak{a} + \mathfrak{b}, \mathfrak{f}\,\mathfrak{g})$.*
- *$(\mathfrak{a}, \mathfrak{f}) \wedge (\mathfrak{b}, \mathfrak{g}) = (\mathfrak{a} \cap \mathfrak{b}, \mathfrak{f} \cap \mathfrak{g})$.*

4.15. Fact. (Ideals and filters in a localized quotient ring) *Let $(\mathfrak{a}, \mathfrak{f})$ be a saturated pair of $\mathbf{A}$ and $\pi : \mathbf{A} \to \mathbf{B} = \mathbf{A}_{\mathfrak{f}}/\mathfrak{a}$ be the canonical map. Then*

1. *The map $(\mathfrak{b}, \mathfrak{g}) \mapsto \big(\pi^{-1}(\mathfrak{b}), \pi^{-1}(\mathfrak{g})\big)$ is a non-decreasing bijection (for the refinement relations) between on the one hand, the saturated pairs of $\mathbf{B}$, and on the other, the saturated pairs of $\mathbf{A}$ which refine $(\mathfrak{a}, \mathfrak{f})$.*
2. *If $(\mathfrak{b}, \mathfrak{g})$ is a saturated pair of $\mathbf{B}$ the canonical map*
$$\mathbf{A}_{\pi^{-1}(\mathfrak{g})}/\pi^{-1}(\mathfrak{b}) \longrightarrow \mathbf{B}_{\mathfrak{g}}/\mathfrak{b}$$
is an isomorphism.
3. *In this bijection*
    - *the ideal $\mathfrak{b}$ is prime if and only if $\pi^{-1}(\mathfrak{b})$ is prime,*
    - *every prime ideal of $\mathbf{A}$ compatible with $\mathfrak{f}$ and containing $\mathfrak{a}$ is obtained,*
    - *the filter $\mathfrak{g}$ is prime if and only if $\pi^{-1}(\mathfrak{g})$ is prime,*
    - *every prime filter of $\mathbf{A}$ compatible with $\mathfrak{a}$ and containing $\mathfrak{f}$ is obtained.*

We deduce the following instructive comparison on the duality between ideals and filters.

4.16. Fact. *Let $\mathfrak{a}$ be a strict ideal of $\mathbf{A}$ and $\pi : \mathbf{A} \to \mathbf{A}/\mathfrak{a}$ be the corresponding homomorphism.*

1. *The map $\mathfrak{b} \mapsto \pi^{-1}(\mathfrak{b})$ is a non-decreasing bijection between ideals of $\mathbf{A}/\mathfrak{a}$ and ideals of $\mathbf{A}$ containing $\mathfrak{a}$. In this bijection the prime ideals correspond to the prime ideals.*
2. *The map $\mathfrak{g} \mapsto \pi^{-1}(\mathfrak{g})$ is a non-decreasing bijection between filters of $\mathbf{A}/\mathfrak{a}$ and $\mathfrak{a}$-saturated filters of $\mathbf{A}$.*
3. *In this bijection the strict prime filters of $\mathbf{A}/\mathfrak{a}$ correspond exactly to the prime filters of $\mathbf{A}$ compatible with $\mathfrak{a}$.*

4.17. Fact. *Let $\mathfrak{f}$ be a strict filter of $\mathbf{A}$ and $\pi : \mathbf{A} \to \mathbf{A}_{\mathfrak{f}}$ be the corresponding homomorphism.*

1. *The map $\mathfrak{g} \mapsto \pi^{-1}(\mathfrak{g})$ is a non-decreasing bijection between filters of $\mathbf{A}_{\mathfrak{f}}$ and filters of $\mathbf{A}$ containing $\mathfrak{f}$. In this bijection the prime filters correspond to the prime filters.*
2. *The map $\mathfrak{b} \mapsto \pi^{-1}(\mathfrak{b})$ is a non-decreasing bijection between ideals of $\mathbf{A}_{\mathfrak{f}}$ and $\mathfrak{f}$-saturated ideals of $\mathbf{A}$.*
3. *In this bijection the strict prime ideals of $\mathbf{A}_{\mathfrak{f}}$ correspond exactly to the prime ideals of $\mathbf{A}$ compatible with $\mathfrak{f}$.*

Closed covering principles

The duality between ideals and filters suggests that a dual principle of the local-global principle must be able to function in commutative algebra. First of all note that the ideals of $\mathsf{Zar}\,\mathbf{A}$ bijectively correspond to the radical ideals (i.e. equal to their nilradical) of $\mathbf{A}$ via

$$\mathfrak{a}\ (\text{ideal of } \mathsf{Zar}\,\mathbf{A}) \mapsto \{\, x \in \mathbf{A} \,|\, \mathrm{D}_{\mathbf{A}}(x) \in \mathfrak{a}\,\}\,.$$

In addition, the prime ideals correspond to the prime ideals.

For filters, things are not quite so perfect, but for a filter $\mathfrak{f}$ of $\mathbf{A}$, the set $\{\,\mathrm{D}_{\mathbf{A}}(x) \,|\, x \in \mathfrak{f}\,\}$ generates a filter of $\mathsf{Zar}\,\mathbf{A}$, and this gives an injective map which is bijective for the first filters.

Let us return to the local-global principle and look at what it means in the lattice $\mathsf{Zar}\,\mathbf{A}$. When we have comaximal monoids S_1, …, S_n of $\mathbf{A}$, it corresponds to filters $\mathfrak{f}_i$ of $\mathsf{Zar}\,\mathbf{A}$ (each generated by the $\mathrm{D}_{\mathbf{A}}(s)$'s for $s \in S_i$) which are "comaximal" in the sense that $\bigcap_i \mathfrak{f}_i = \{1_{\mathsf{Zar}\,\mathbf{A}}\}$. In this case the natural homomorphisms

$$\mathbf{A} \to \textstyle\prod_i \mathbf{A}_{S_i} \quad \text{and} \quad \mathsf{Zar}\,\mathbf{A} \to \textstyle\prod_i \mathsf{Zar}\,\mathbf{A}/(\mathfrak{f}_i = 1)$$

are injective.

By duality, we will say that a system of ideals $(\mathfrak{a}_1, \ldots, \mathfrak{a}_n)$ constitutes a *closed covering* of $\mathbf{A}$ when $\bigcap_i \mathrm{D}_{\mathbf{A}}(\mathfrak{a}_i) = \{0_{\mathsf{Zar}\,\mathbf{A}}\}$, i.e. when $\prod_i \mathfrak{a}_i \subseteq \mathrm{D}_{\mathbf{A}}(0)$. In this case the natural homomorphisms

$$\mathbf{A}/\mathrm{D}_{\mathbf{A}}(0) \to \textstyle\prod_i \mathbf{A}/\mathrm{D}_{\mathbf{A}}(\mathfrak{a}_i) \quad \text{and} \quad \mathsf{Zar}\,\mathbf{A} \to \textstyle\prod_i \mathsf{Zar}\,\mathbf{A}/(\mathrm{D}_{\mathbf{A}}(\mathfrak{a}_i) = 0)$$

are injective.

We will say that a property P (regarding objects related to a ring $\mathbf{A}$) satisfies the "closed covering principle" when:
each time that ideals $\mathfrak{a}_i$ form a closed covering of $\mathbf{A}$, the property P is true for $\mathbf{A}$ if and only if it is true after passage to the quotient by each of the $\mathfrak{a}_i$'s.

For example we easily obtain (see also Lemma II-2.7).

4.18. Closed covering principle. (Nilpotent, comaximal elements)
Consider a closed covering $(\mathfrak{a}_1, \ldots, \mathfrak{a}_r)$ of the ring $\mathbf{A}$. Let x_1, …, $x_n \in \mathbf{A}$, $\mathfrak{b}$, $\mathfrak{c}$ be two ideals and S be a monoid.

1. *The monoid S contains 0 if and only if it contains 0 modulo each $\mathfrak{a}_i$.*
2. *We have $\mathfrak{b} \subseteq \sqrt{\mathfrak{c}}$ if and only if $\mathfrak{b} \subseteq \sqrt{\mathfrak{c}}$ modulo each $\mathfrak{a}_i$.*
3. *The elements x_1, …, x_n are comaximal if and only if they are comaximal modulo each $\mathfrak{a}_i$.*

D It suffices to prove item *2.* Suppose that $\mathrm{D}_{\mathbf{A}}(\mathfrak{b}) \leqslant \mathrm{D}_{\mathbf{A}}(\mathfrak{c}) \vee \mathrm{D}_{\mathbf{A}}(\mathfrak{a}_i)$, so $\mathrm{D}_{\mathbf{A}}(\mathfrak{b}) \leqslant \bigwedge_i (\mathrm{D}_{\mathbf{A}}(\mathfrak{c}) \vee \mathrm{D}_{\mathbf{A}}(\mathfrak{a}_i)) = \mathrm{D}_{\mathbf{A}}(\mathfrak{c}) \vee (\bigwedge_i \mathrm{D}_{\mathbf{A}}(\mathfrak{a}_i)) = \mathrm{D}_{\mathbf{A}}(\mathfrak{c})$. □

Remark. However, there is no closed covering principle for the solutions of systems of linear equations. Indeed, consider u, $v \in \mathbf{A}$ such that $uv = 0$. The system of linear equations (with x as the unknown)

$$ux = u,\ vx = -v,$$

admits a solution modulo u (namely $x = -1$) and a solution modulo v (namely $x = 1$). But in the case of the ring $\mathbf{A} = \mathbb{Z}[u, v] = \mathbb{Z}[U, V]/\langle UV\rangle$ the system of linear equations has no solution in $\mathbf{A}$. ■

4.19. Closed covering principle. (Finitely generated modules)
Consider a closed covering $(\mathfrak{a}_1, \dots, \mathfrak{a}_r)$ of the ring $\mathbf{A}$. Suppose that $\prod_i \mathfrak{a}_i = 0$ (this is the case if $\mathbf{A}$ is reduced). An $\mathbf{A}$-module M is finitely generated if and only if it is finitely generated modulo each $\mathfrak{a}_i$.

D Suppose without loss of generality that $r = 2$. Let $g_1, \dots, g_k$ be generators modulo $\mathfrak{a}_1$, and $g_{k+1}, \dots, g_\ell$ be generators modulo $\mathfrak{a}_2$. Let $x \in M$. We write $x = \sum_{i=1}^{k} \alpha_i g_i + \sum_{j=1}^{p} \beta_j x_j$ with $\alpha_i \in \mathbf{A}$, $\beta_j \in \mathfrak{a}_1$, $x_j \in M$.
Each x_j is written as a linear combination of $g_{k+1}, \dots, g_\ell$ modulo $\mathfrak{a}_2$. Since $\mathfrak{a}_1\mathfrak{a}_2 = 0$, we obtain x as a linear combination of $g_1, \dots, g_\ell$. □

4.20. Closed covering principle. (Finitely generated projective modules)
Consider a closed covering $(\mathfrak{a}_1, \dots, \mathfrak{a}_r)$ of the ring $\mathbf{A}$, a matrix $F \in \mathbf{A}^{m\times n}$, a finitely generated ideal $\mathfrak{a}$ and a finitely presented module M.

1. *The matrix F is of rank $\geqslant k$ if and only if it is of rank $\geqslant k$ modulo each $\mathfrak{a}_i$.*

Suppose $\bigcap_i \mathfrak{a}_i = 0$ (it is the case if $\mathbf{A}$ is reduced). Then

2. *The matrix F is of rank $\leqslant k$ if and only if it is of rank $\leqslant k$ modulo each $\mathfrak{a}_i$.*
3. *The finitely generated ideal $\mathfrak{a}$ is generated by an idempotent if and only if it is generated by an idempotent modulo each $\mathfrak{a}_i$.*
4. *The matrix F is locally simple if and only if it is locally simple modulo each $\mathfrak{a}_i$.*
5. *The module M is finitely generated projective if and only if it is finitely generated projective modulo each $\mathfrak{a}_i$.*

D Item *1* results from the closed covering principle 4.18 by considering the determinantal ideal of order k. Item *2* comes from the fact that if a determinantal ideal is null modulo each $\mathfrak{a}_i$, it is null modulo their intersection. Item *5* is a reformulation of item *4* which is a consequence of item *3*.
Let us prove item *3*. Suppose without loss of generality that $r = 2$. We use the the lemma of the ideal generated by an idempotent (Lemma II-4.5). We have

$$\mathfrak{a} + (0 : \mathfrak{a})_{\mathbf{A}/\mathfrak{a}_i} = \mathbf{A}/\mathfrak{a}_i \quad (i = 1, 2).$$

This means that $\mathfrak{a} + \mathfrak{a}_i + (\mathfrak{a}_i : \mathfrak{a}) = \mathbf{A}$, and since $\mathfrak{a}_i \subseteq (\mathfrak{a}_i : \mathfrak{a})$, we have $1 \in \mathfrak{a} + (\mathfrak{a}_i : \mathfrak{a})$. By taking the product we get $1 \in \mathfrak{a} + (\mathfrak{a}_1 : \mathfrak{a})(\mathfrak{a}_2 : \mathfrak{a})$ and since

$$(\mathfrak{a}_1 : \mathfrak{a})(\mathfrak{a}_2 : \mathfrak{a}) \subseteq (\mathfrak{a}_1 : \mathfrak{a}) \cap (\mathfrak{a}_2 : \mathfrak{a}) = ((\mathfrak{a}_1 \cap \mathfrak{a}_2) : \mathfrak{a}) = (0 : \mathfrak{a}),$$

we obtain $1 \in \mathfrak{a} + (0 : \mathfrak{a})$. □

Reduced zero-dimensional closure of a commutative ring

Let us begin with some results regarding a subring $\mathbf{A}$ of a reduced zero-dimensional ring. The reader can refer to the study of reduced zero-dimensional rings on page 210 and revisit Equalities (6) for the characterization of a quasi-inverse.

If in a ring an element c admits a quasi-inverse, we denote it by $c^\bullet$, and we denote by $e_c = c^\bullet c$ the idempotent associated with c which satisfies the equalities $\mathrm{Ann}(c) = \mathrm{Ann}(e_c) = \langle 1 - e_c \rangle$.

4.21. Lemma. (Ring generated by a quasi-inverse)

1. *Let $a \in \mathbf{A} \subseteq \mathbf{B}$. Suppose that $\mathbf{A}$ and $\mathbf{B}$ are reduced and that a admits a quasi-inverse in $\mathbf{B}$. Then*
$$\mathbf{B} \supseteq \mathbf{A}[a^\bullet] \simeq \mathbf{A}[a^\bullet]/\langle 1 - e_a \rangle \times \mathbf{A}[a^\bullet]/\langle e_a \rangle = \mathbf{A}_1 \times \mathbf{A}_2.$$
In addition
   a. *We have a well-defined natural homomorphism $\mathbf{A}[1/a] \to \mathbf{A}_1$, and it is an isomorphism. In particular, the natural homomorphism $\mathbf{A} \to \mathbf{A}_1$ has as its kernel $\mathrm{Ann}_{\mathbf{A}}(a)$.*
   b. *The natural homomorphism $\mathbf{A} \to \mathbf{A}_2$ is surjective, its kernel is the intersection $\mathfrak{a} = \mathbf{A} \cap e_a\mathbf{A}[a^\bullet]$ and satisfies the double inclusion*
$$\mathrm{Ann}_{\mathbf{A}}\big(\mathrm{Ann}_{\mathbf{A}}(a)\big) \supseteq \mathfrak{a} \supseteq \mathrm{D}_{\mathbf{A}}(a). \qquad (*)$$
In short $\mathbf{A}[a^\bullet] \simeq \mathbf{A}[1/a] \times \mathbf{A}/\mathfrak{a}$.
2. *Conversely for every ideal $\mathfrak{a}$ of $\mathbf{A}$ satisfying $(*)$, the element $(1/a, 0)$ is a quasi-inverse of (the image of) a in the ring $\mathbf{C} = \mathbf{A}[1/a] \times \mathbf{A}/\mathfrak{a}$ and the canonical homomorphism of $\mathbf{A}$ in $\mathbf{C}$ is injective.*

D The isomorphism $\mathbf{A}[a^\bullet] \simeq \mathbf{A}_1 \times \mathbf{A}_2$ only means that e_a is an idempotent in $\mathbf{A}[a^\bullet]$. Let $\pi_i : \mathbf{A}[a^\bullet] \to \mathbf{A}_i$ be the canonical homomorphisms.

1b. Let μ be the composed homomorphism $\mathbf{A} \longrightarrow \mathbf{A}[a^\bullet] \longrightarrow \mathbf{A}_2$. In $\mathbf{A}_2$, we have $a^\bullet = e_a a^\bullet = 0$, so $\mathbf{A}_2 = \mathbf{A}/(\mathbf{A} \cap e_a\mathbf{A}[a^\bullet])$. Thus $\mathfrak{a} = \mathbf{A} \cap e_a\mathbf{A}[a^\bullet]$. In $\mathbf{A}[a^\bullet]$, we have $a = e_a a$, so $\mu(a) = \pi_2(a) = \pi_2(e_a a) = 0$, and $a \in \mathfrak{a}$.
As $\mathbf{B}$ is reduced, the three rings $\mathbf{A}[a^\bullet]$, $\mathbf{A}_1$ and $\mathbf{A}_2$ are also reduced. Therefore $\langle a \rangle \subseteq \mathfrak{a}$ implies $\mathrm{D}_{\mathbf{A}}(a) \subseteq \mathfrak{a}$.
Finally, $\mathfrak{a}\,\mathrm{Ann}_{\mathbf{A}}(a) \subseteq \langle e_a \rangle\,\mathrm{Ann}_{\mathbf{A}}(a) = 0$, so $\mathfrak{a} \subseteq \mathrm{Ann}_{\mathbf{A}}\big(\mathrm{Ann}_{\mathbf{A}}(a)\big)$.

1a. Since $aa^\bullet =_{\mathbf{A}_1} 1$, we have a unique homomorphism $\lambda : \mathbf{A}[1/a] \to \mathbf{A}_1$ obtained from the composed homomorphism $\mathbf{A} \to \mathbf{A}[a^\bullet] \to \mathbf{A}_1$, and λ is clearly surjective. Consider an element x/a^n of $\mathrm{Ker}\,\lambda$. Then $\lambda(ax) = 0$, so $\pi_1(ax) = 0$. As we also have $\pi_2(ax) = 0$, we deduce that $ax = 0$, so $x =_{\mathbf{A}[1/a]} 0$. Thus λ is injective.

2. The image of a in $\mathbf{C}$ is $(a/1, 0)$, so $(1/a, 0)$ is indeed its quasi-inverse. Now let $x \in \mathbf{A}$ whose image in $\mathbf{C}$ is 0. On the one hand $x =_{\mathbf{A}[1/a]} 0$, so $ax =_{\mathbf{A}} 0$. On the other hand $x \operatorname{Ann}_{\mathbf{A}}(a) = 0$ so $x^2 =_{\mathbf{A}} 0$, and $x =_{\mathbf{A}} 0$. □

Comment. We see that the notation $\mathbf{A}[a^\bullet]$ presents a priori a possible ambiguity, at least when $\mathrm{D}_{\mathbf{A}}(a) \neq \operatorname{Ann}_{\mathbf{A}}\big(\operatorname{Ann}_{\mathbf{A}}(a)\big)$. ■

4.22. Lemma. *If $\mathbf{A} \subseteq \mathbf{C}$ with $\mathbf{C}$ reduced zero-dimensional, the smallest zero-dimensional subring of $\mathbf{C}$ containing $\mathbf{A}$ is equal to $\mathbf{A}[(a^\bullet)_{a\in\mathbf{A}}]$. More generally if $\mathbf{A} \subseteq \mathbf{B}$ with $\mathbf{B}$ reduced, and if every element of $\mathbf{A}$ admits a quasi-inverse in $\mathbf{B}$, then the subring $\mathbf{A}[(a^\bullet)_{a\in\mathbf{A}}]$ of $\mathbf{B}$ is zero-dimensional. In addition, every element of $\mathbf{A}[(a^\bullet)_{a\in\mathbf{A}}]$ is of the form*

$$\textstyle\sum_j a_j b_j^\bullet e_j, \quad \textit{with}$$

- *the e_j's are pairwise orthogonal idempotents of $\mathbf{A}[(a^\bullet)_{a\in\mathbf{A}}]$,*
- *$a_j, b_j \in \mathbf{A}$ and $b_j b_j^\bullet e_j = e_j$ for every j,*

such that $\big(\sum_j a_j b_j^\bullet e_j\big)^\bullet = \sum_j a_j^\bullet b_j e_j$.

NB: Care will be taken, however, that we do not always have $a_j a_j^\bullet e_j = e_j$. We must therefore a priori replace e_j with $e'_j = a_j a_j^\bullet e_j$ to obtain an expression of the same type as the previous one. We will also be able to note that every idempotent of $\mathbf{A}[(a^\bullet)_{a\in\mathbf{A}}]$ is expressible in the form $e_c \prod_i (1 - e_{d_i})$ for a c and some $d_i \in \mathbf{A}$.

D Among the elements of $\mathbf{B}$, those that are expressed as a sum of products $ab^\bullet$ with a, $b \in \mathbf{A}$ clearly form a subring of $\mathbf{B}$, which is therefore equal to $\mathbf{A}[(a^\bullet)_{a\in\mathbf{A}}]$. Moreover, $ab^\bullet = ab^\bullet e_b$. By considering the Boolean algebra generated by the e_b's which intervene in a finite sum of the previous type, we deduce that every element of $\mathbf{A}[(a^\bullet)_{a\in\mathbf{A}}]$ can be expressed in the form

$$\textstyle\sum_j \left(\sum_i a_{i,j} b_{i,j}^\bullet\right) e_j, \text{ such that}$$

- the e_j's are pairwise orthogonal idempotents in $\mathbf{A}[(a^\bullet)_{a\in\mathbf{A}}]$,
- $a_{i,j}, b_{i,j} \in \mathbf{A}$, and $b_{i,j} b_{i,j}^\bullet e_j = e_j$, for all i, j.

Note that $b_{i,j}^\bullet$ is the inverse of $b_{i,j}$ in $\mathbf{A}[(a^\bullet)_{a\in\mathbf{A}}][1/e_j]$, and we can perform the computation as for a usual sum of fractions $\sum_i a_{i,j}/b_{i,j}$. For example to simplify a term with a sum of three elements let us take

$$(a_1 b_1^\bullet + a_2 b_2^\bullet + a_3 b_3^\bullet)e.$$

Since $b_2 b_2^\bullet e = b_3 b_3^\bullet e = e$, we have $a_1 b_1^\bullet e = a_1 b_2 b_3 (b_1 b_2 b_3)^\bullet e$, and

$$(a_1 b_1^\bullet + a_2 b_2^\bullet + a_3 b_3^\bullet)e = (a_1 b_2 b_3 + a_2 b_1 b_3 + a_3 b_1 b_2)(b_1 b_2 b_3)^\bullet e = dc^\bullet e,$$

which admits for quasi-inverse $cd^\bullet e$. □

Recall that $\mathbf{B}_{\mathrm{red}}$ designates the quotient of a ring $\mathbf{B}$ by its nilradical.

In the following lemma we observe what happens when we forcefully add a quasi-inverse to an element of a ring. It is an operation neighboring localization, when we forcefully add an inverse of an element, but slightly more delicate.

4.23. Lemma. *Let $\mathbf{A}$ be a ring and $a \in \mathbf{A}$.*

1. *Consider the ring $\mathbf{A}[T]/\big\langle aT^2 - T, a^2T - a\big\rangle = \mathbf{A}[a^\flat]$ and the canonical homomorphism $\lambda_a : \mathbf{A} \to \mathbf{A}[a^\flat]$ ($a^\flat$ designates the image of T). Then for every homomorphism $\psi : \mathbf{A} \to \mathbf{B}$ such that $\psi(a)$ admits a quasi-inverse there exists a unique homomorphism $\varphi : \mathbf{A}[a^\flat] \to \mathbf{B}$ such that $\varphi \circ \lambda_a = \psi$.*

$$\begin{tikzcd}
\mathbf{A} \arrow[d, "\lambda_a"'] \arrow[dr, "\psi"] & \\
\mathbf{A}[a^\flat] \arrow[r, dashed, "\varphi\,!"'] & \mathbf{B}
\end{tikzcd}$$

$\psi(a)$ admits a quasi-inverse

2. *In addition, $aa^\flat$ is an idempotent and $\mathbf{A}[a^\flat] \simeq \mathbf{A}[1/a] \times \mathbf{A}/\langle a\rangle$.*
3. *If $\mathbf{B}$ is reduced we have a unique factorization via $(\mathbf{A}[a^\flat])_{\mathrm{red}}$.*

In the rest of the text we denote by $\mathbf{A}[a^\bullet]$ the ring $(\mathbf{A}[a^\flat])_{\mathrm{red}}$.

4. *We have $\mathbf{A}[a^\bullet] \simeq \mathbf{A}_{\mathrm{red}}[1/a] \times \mathbf{A}/\mathrm{D}_{\mathbf{A}}(a)$. If $\mathbf{A}$ is reduced the canonical homomorphism $\mathbf{A} \to \mathbf{A}[a^\bullet]$ is injective.*
5. *$\mathsf{Zar}(\mathbf{A}[a^\bullet]) = \mathsf{Zar}(\mathbf{A}[a^\flat])$ is identified with $(\mathsf{Zar}\,\mathbf{A})[\mathrm{D}_{\mathbf{A}}(a)^\bullet]$.*

D Left to the reader. The last item results from Lemma 1.6 and from Fact 4.5. □

4.24. Corollary. *Let $a_1, \ldots, a_n \in \mathbf{A}$.*

1. *The ring $\mathbf{A}[a_1^\bullet][a_2^\bullet]\cdots[a_n^\bullet]$ is independent, up to unique isomorphism, of the order of the a_i's. It will be denoted by $\mathbf{A}[a_1^\bullet, a_2^\bullet, \ldots, a_n^\bullet]$.*
2. *A possible description is the following*
$$\mathbf{A}[a_1^\bullet, a_2^\bullet, \ldots, a_n^\bullet] \simeq \big(\mathbf{A}[T_1, T_2, \ldots, T_n]/\mathfrak{a}\,\big)_{\mathrm{red}}$$
with $\mathfrak{a} = \big\langle (a_iT_i^2 - T_i)_{i=1}^n, (T_ia_i^2 - a_i)_{i=1}^n\big\rangle$.
3. *Another possible description is*
$$\mathbf{A}[a_1^\bullet, a_2^\bullet, \ldots, a_n^\bullet] \simeq \prod\nolimits_{I \in \mathcal{P}_n} \left(\mathbf{A}/\langle (a_i)_{i\in I}\rangle\right)_{\mathrm{red}}[1/\alpha_I]$$
with $\alpha_I = \prod_{j \in [\![1..n]\!]\setminus I} a_j$.

4.25. Theorem. (Reduced zero-dimensional closure of a commutative ring) *For every ring* $\mathbf{A}$ *there exists a reduced zero-dimensional ring* $\mathbf{A}^\bullet$ *with a homomorphism* $\lambda : \mathbf{A} \to \mathbf{A}^\bullet$*, which uniquely factorizes every homomorphism* $\psi : \mathbf{A} \to \mathbf{B}$ *to a reduced zero-dimensional ring. This pair* $(\mathbf{A}^\bullet, \lambda)$ *is unique up to unique isomorphism.*

$$\begin{tikzcd}
\mathbf{A} \arrow[d, "\lambda"'] \arrow[dr, "\psi"] & & \textit{commutative rings} \\
\mathbf{A}^\bullet \arrow[r, dashed, "\varphi\,!"'] & \mathbf{B} & \textit{reduced zero-dimensional rings}
\end{tikzcd}$$

In addition

- *The natural homomorphism* $\mathbf{A}_{\mathrm{red}} \to \mathbf{A}^\bullet$ *is injective.*
- *We have* $\mathbf{A}^\bullet = \mathbf{A}_{\mathrm{red}}[(a^\bullet)_{a\in\mathbf{A}_{\mathrm{red}}}]$.

D This is a corollary of the previous lemmas. We can suppose that $\mathbf{A}$ is reduced. The uniqueness result (Corollary 4.24) allows for a construction of a colimit (which mimics a filtering union) based on the extensions of the type $\mathbf{A}[a_1^\bullet, a_2^\bullet, \ldots, a_n^\bullet]$, and the result follows by Lemma 4.22. □

Comments. 1) A priori, since we are dealing with purely equational structures, the universal reduced zero-dimensional closure of a ring exists and we could construct it as follows: we formally add the unary operation $a \mapsto a^\bullet$ and we force $a^\bullet$ to be a quasi-inverse of a. Our proof has also allowed us to give a simplified precise description of the constructed object and to show the injectivity in the reduced case.

2) In classical mathematics, the reduced zero-dimensional closure $\mathbf{A}^\bullet$ of a ring $\mathbf{A}$ can be obtained as follows. First of all we consider the product $\mathbf{B} = \prod_{\mathfrak{p}} \mathrm{Frac}(\mathbf{A}/\mathfrak{p})$, where $\mathfrak{p}$ ranges over all the prime ideals of $\mathbf{A}$. As $\mathbf{B}$ is a product of fields, it is reduced zero-dimensional. Next we consider the smallest zero-dimensional subring of $\mathbf{B}$ containing the image of $\mathbf{A}$ in $\mathbf{B}$ under the natural diagonal homomorphism.

We then understand the importance of the earlier construction of $\mathbf{A}^\bullet$. It allows us to have explicit access to something which looks like "the set of all the" prime ideals of $\mathbf{A}$ (those of classical mathematics) without needing to construct any one of them individually. The assumption is that the classical mathematical reasoning that manipulates unspecified arbitrary prime ideals of the ring $\mathbf{A}$ (generally inaccessible objects) can be reread as arguments about the ring $\mathbf{A}^\bullet$: a mystery-free object! ■

Examples.

1) Here is a description of the reduced zero-dimensional closure of $\mathbb{Z}$.

First of all, for $n \in \mathbb{N}^*$ the ring $\mathbb{Z}[n^\bullet]$ is isomorphic to $\mathbb{Z}[1/n] \times \prod_{p|n} \mathbb{F}_p$, where p indicates "p prime," and $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Next, $\mathbb{Z}^\bullet$ is the colimit (that we can regard as a non-decreasing union) of the $\mathbb{Z}[(n!)^\bullet]$'s.

2) Here is a description of the reduced zero-dimensional closure of $\mathbb{Z}[X]$. First of all, if Q is a square-free monic polynomial, and if $n \in \mathbb{N}^*$ is a multiple of $\mathrm{disc}(Q)$, the ring $\mathbb{Z}[X][n^\bullet, Q^\bullet]$ is isomorphic to

$$\mathbb{Z}[X, 1/n, 1/Q] \times \prod_{p|n} \mathbb{F}_p[X, 1/Q] \times \prod_{P|Q} \mathbb{Z}[X, 1/n]/\langle P\rangle \times \prod_{p|n, R|Q} \mathbb{F}_p[X]/\langle R\rangle$$

with p standing for "p prime," P standing for "irreducible P in $\mathbb{Z}[X]$," and $R \mid Q$ standing for "irreducible R in $\mathbb{F}_p[X]$ divides Q in $\mathbb{F}_p[X]$."
Next, we pass to the colimit of the rings $\mathbb{Z}[X][u_n^\bullet, Q_n^\bullet]$ (here, it is a non-decreasing union), where Q_n is the squarefree part of the product of the first n elements in an enumeration of squarefree monic polynomials of $\mathbb{Z}[X]$, and where $u_n = n!\,\mathrm{disc}(Q_n)$.
Note that we thus obtain a ring by which all the natural homomorphisms $\mathbb{Z}[X] \to \mathrm{Frac}(\mathbb{Z}[X]/\mathfrak{p})$ are factorized for all the prime ideals $\mathfrak{p}$ of $\mathbb{Z}[X]$: such a $\mathrm{Frac}(\mathbb{Z}[X]/\mathfrak{p})$ is indeed either $\mathbb{Q}(X)$, or some $\mathbb{Q}[X]/\langle P\rangle$, or some $\mathbb{F}_p(X)$, or some $\mathbb{F}_p[X]/\langle R\rangle$.

3) The (constructively well-defined) ring $\mathbb{R}^\bullet$ is certainly one of the more intriguing objects in the world "without LEM" that constitutes constructive mathematics. Naturally, in classical mathematics, $\mathbb{R}$ is zero-dimensional and $\mathbb{R}^\bullet = \mathbb{R}$. ■

4.26. Theorem. *For every ring* $\mathbf{A}$ *we have natural isomorphisms*

$$\mathbb{B}\mathrm{o}(\mathsf{Zar}\,\mathbf{A}) \simeq \mathbb{B}(\mathbf{A}^\bullet) \simeq \mathsf{Zar}(\mathbf{A}^\bullet).$$

D This results from the last item of Lemma 4.23, and from the fact that the two constructions can be seen as colimits of "constructions at a step" $\mathbf{E} \rightsquigarrow \mathbf{E}[a^\bullet]$ ($\mathbf{E}$ is a ring or a distributive lattice). □

Note that if we adopted the notation $\mathbf{T}^\bullet$ for $\mathbb{B}\mathrm{o}(\mathbf{T})$ we would have the pretty formula $(\mathsf{Zar}\,\mathbf{A})^\bullet \simeq \mathsf{Zar}(\mathbf{A}^\bullet)$.

4.27. Proposition. *Let* $\mathbf{A}$ *be a ring,* $\mathfrak{a}$ *be an ideal and* S *be a monoid.*

- *The two rings* $(\mathbf{A}/\mathfrak{a})^\bullet$ *and* $\mathbf{A}^\bullet/\mathrm{D}(\mathfrak{a}\mathbf{A}^\bullet)$ *are canonically isomorphic.*
- *The two rings* $(\mathbf{A}_S)^\bullet$ *and* $(\mathbf{A}^\bullet)_S$ *are canonically isomorphic.*

D Note that $(\mathbf{A}^\bullet)_S$ is reduced zero-dimensional as a localization of a reduced zero-dimensional ring. Similarly, $\mathbf{A}^\bullet/\mathrm{D}(\mathfrak{a}\mathbf{A}^\bullet)$ is reduced zero-dimensional. Let us write the proof for the localizations. Consider the natural homomorphisms

$$\mathbf{A} \to \mathbf{A}_S \to (\mathbf{A}_S)^\bullet \quad \text{and} \quad \mathbf{A} \to \mathbf{A}^\bullet \to (\mathbf{A}^\bullet)_S.$$

The homomorphism $\mathbf{A} \to \mathbf{A}^\bullet$ uniquely "extends" to a homomorphism $\mathbf{A}_S \to (\mathbf{A}^\bullet)_S$, and by the universal property of the reduced zero-dimensional closure, provides a unique morphism $(\mathbf{A}_S)^\bullet \to (\mathbf{A}^\bullet)_S$ which renders the ad hoc commutative diagram. Similarly, the morphism $\mathbf{A} \to \mathbf{A}_S$ gives birth to a unique morphism $\mathbf{A}^\bullet \to (\mathbf{A}_S)^\bullet$ which extends to a morphism

$(\mathbf{A}^\bullet)_S \to (\mathbf{A}_S)^\bullet$. By composing these two morphisms, by uniqueness, we obtain the identity twice. □

5. Entailment relations and Heyting algebras

A new look at distributive lattices

A particularly important rule for distributive lattices, known as the *cut*, is the following

$$\big(x \wedge a \ \leqslant \ b\big) \quad \& \quad \big(a \ \leqslant \ x \vee b\big) \quad \Longrightarrow \quad a \leqslant \ b. \tag{24}$$

To prove it we write $x \wedge a \wedge b = x \wedge a$ and $a = a \wedge (x \vee b)$ so

$$a = (a \wedge x) \vee (a \wedge b) = (a \wedge x \wedge b) \vee (a \wedge b) = a \wedge b$$

5.1. Notation. For a distributive lattice $\mathbf{T}$ we denote by $A \vdash B$ or $A \vdash_{\mathbf{T}} B$ the relation defined as follows over the set $\mathrm{P}_{\mathrm{fe}}(\mathbf{T})$

$$A \vdash B \quad \overset{\mathrm{def}}{\Longleftrightarrow} \quad \bigwedge A \ \leqslant \ \bigvee B.$$

Note that the relation $A \vdash B$ is well-defined over $\mathrm{P}_{\mathrm{fe}}(\mathbf{T})$ because the laws $\wedge$ and $\vee$ are associative, commutative and idempotent. Note that $\emptyset \vdash \{x\}$ implies $x = 1$ and that $\{y\} \vdash \emptyset$ implies $y = 0$. This relation satisfies the following axioms, in which we write x for $\{x\}$ and A, B for $A \cup B$.

$$\begin{array}{rcrclc} & & a & \vdash & a & (R) \\ A \vdash B & \Longrightarrow & A, A' & \vdash & B, B' & (M) \\ (A, x \vdash B) \ \& \ (A \vdash B, x) & \Longrightarrow & A & \vdash & B & (T). \end{array}$$

We say that the relation is *reflexive*, *monotone* and *transitive*. The third rule (transitivity) can be seen as a generalization of the rule (24) and is also called the *cut* rule.

Let us also quote the following so-called *distributivity* rules:

$$\begin{array}{rcl} (A,\ x \vdash B) \ \& \ (A,\ y \vdash B) & \Longleftrightarrow & A,\ x \vee y \vdash B \\ (A \vdash B,\ x) \ \& \ (A \vdash B,\ y) & \Longleftrightarrow & A \vdash B,\ x \wedge y \end{array}$$

An interesting way to approach the question of distributive lattices defined by generators and relations is to consider the relation $A \vdash B$ defined over the set $\mathrm{P}_{\mathrm{fe}}(\mathbf{T})$ of finitely enumerated subsets of a distributive lattice $\mathbf{T}$. Indeed, if $S \subseteq \mathbf{T}$ generates $\mathbf{T}$ as a lattice, then the knowledge of the relation $\vdash$ over $\mathrm{P}_{\mathrm{fe}}(S)$ suffices to characterize without ambiguity the lattice $\mathbf{T}$, because every formula over S can be rewritten, either in "conjunctive normal form" (infimum of supremums in S) or in "disjunctive normal form" (supremum of infimums in S). Therefore if we want to compare two elements of the lattice generated by S we write the first in disjunctive normal form, the second in conjunctive normal form, and we observe that

$$\bigvee\nolimits_{i\in I}\left(\bigwedge A_i\right) \leqslant \bigwedge\nolimits_{j\in J}\left(\bigvee B_j\right) \quad\iff\quad \forall i\in I,\ \forall j\in J,\ \ A_i \vdash B_j$$

5.2. Definition. For an arbitrary set S, a relation over $\mathrm{P_{fe}}(S)$ which is reflexive, monotone and transitive is called an *entailment relation.*

The following theorem is fundamental. It says that the three properties of entailment relations are exactly what is needed for the interpretation in the form of a distributive lattice to be adequate.

5.3. Theorem. (Fundamental theorem of the entailment relations)
Let S be a set with an entailment relation $\vdash_S$ over $\mathrm{P_{fe}}(S)$. We consider the distributive lattice $\mathbf{T}$ defined by generators and relations as follows: the generators are the elements of S and the relations are the

$$A \vdash_{\mathbf{T}} B$$

each time that $A \vdash_S B$. Then, for all A, B in $\mathrm{P_{fe}}(S)$, we have

$$A \vdash_{\mathbf{T}} B \implies A \vdash_S B.$$

D We give an explicit description of the distributive lattice $\mathbf{T}$. The elements of $\mathbf{T}$ are represented by those of $\mathrm{P_{fe}}\big(\mathrm{P_{fe}}(S)\big)$, i.e. X's of the form

$$X = \{A_1, \dots, A_n\}$$

(intuitively X represents $\bigwedge_{i\in[\![1..n]\!]}\bigvee A_i$). We then inductively define the relation $A \preccurlyeq Y$ for $A \in \mathrm{P_{fe}}(S)$ and $Y \in \mathrm{P_{fe}}\big(\mathrm{P_{fe}}(S)\big)$ as follows

- If $B \in Y$ and $B \subseteq A$ then $A \preccurlyeq Y$.
- If we have $A \vdash_S y_1, \dots, y_m$ and $A, y_j \preccurlyeq Y$ for $j = 1, \dots, m$ then $A \preccurlyeq Y$.

We easily show that if $A \preccurlyeq Y$ and $A \subseteq A'$ then we have $A' \preccurlyeq Y$. We deduce that $A \preccurlyeq Z$ if $A \preccurlyeq Y$ and $B \preccurlyeq Z$ for all $B \in Y$. We can then define $X \leqslant Y$ by "$A \preccurlyeq Y$ for every $A \in X$." We finally verify that $\mathbf{T}$ is a distributive lattice[7] with respect to the operations (0-aries and binaries)

$$\left.\begin{array}{rclcrcl} 1 & = & \emptyset & \qquad & 0 & = & \{\emptyset\} \\ X \wedge Y & = & X \cup Y & \qquad & X \vee Y & = & \{\, A \cup B \,|\, A \in X,\ B \in Y \,\} \end{array}\right| \tag{25}$$

For this we show that if $C \preccurlyeq X$ and $C \preccurlyeq Y$, then we have $C \preccurlyeq X \wedge Y$ by induction on the proofs of $C \preccurlyeq X$ and $C \preccurlyeq Y$.
We notice that if $A \vdash_S y_1, \dots, y_m$ and $A, y_j \vdash_S B$ for all j, then we obtain $A \vdash_S B$ by using the cut rule m times. From this, it results that if we have $A \vdash_{\mathbf{T}} B$, that is that $A \preccurlyeq \{\{b\} \mid b \in B\}$, then we have $A \vdash_S B$. □

[7] More precisely, as $\preccurlyeq$ is only a preorder, we take for $\mathbf{T}$ the quotient of $\mathrm{P_{fe}}\big(\mathrm{P_{fe}}(S)\big)$ with respect to the equivalence relation: $X \preccurlyeq Y$ and $Y \preccurlyeq X$.

5.4. Corollary. (Finitely presented distributive lattice)

1. A distributive lattice freely generated by a finite set E is finite.

2. A finitely presented distributive lattice is finite.

D *1.* Consider the minimal entailment relation on E. It is defined by

$$A \vdash_E B \overset{\text{def}}{\iff} \exists x \in A \cap B.$$

We then consider the distributive lattice corresponding to this entailment relation via Theorem 5.3. It is isomorphic to a subset of $\mathrm{P}_{\mathrm{fe}}\big(\mathrm{P}_{\mathrm{fe}}(E)\big)$, the one which is represented by the lists $(A_1, \ldots, A_k)$ in $\mathrm{P}_{\mathrm{fe}}(E)$ such that two A_i with distinct indices are incomparable with respect to the inclusion. The laws are obtained from (25), by simplifying the obtained lists when they do not satisfy the criteria of incompatibility.

2. If we impose a finite number of relations between the elements of E, we have to pass to a quotient lattice of the free distributive lattice over E. The equivalence relation generated by these relations and compatible with the lattice laws is decidable because the structure is defined by only using a finite number of axioms. □

Remarks. 1) Another proof of item *1* could be the following. The Boolean algebra freely generated by the distributive lattice $\mathbf{T}$ freely generated by E is the Boolean algebra $\mathbf{B}$ freely generated by E. The latter can easily be described by the elements of $\mathrm{P}_{\mathrm{fe}}\big(\mathrm{P}_{\mathrm{fe}}(E)\big)$, without any passage to the quotient: the subset $\{A_1, \ldots, A_n\}$ intuitively represents $\bigvee_{i \in [\![1..n]\!]} \left(\bigwedge A_i \wedge \bigwedge A_i'\right)$, by designating by A_i' the subset of E formed by the $\neg x$'s for the $x \notin A_i$. Therefore $\mathbf{B}$ has $2^{2^{\#E}}$ elements. Finally, we have seen that $\mathbf{T}$ is identified with a distributive sublattice of $\mathbf{B}$ (Theorem 1.8).

2) The given proof of item *2* uses an altogether general argument. In the case of distributive lattices we can more precisely refer to the description of the quotients given on page 621. ■

Duality between finite distributive lattices and finite ordered sets

If $\mathbf{T}$ is a distributive lattice let $\mathsf{Spec}\,\mathbf{T} \overset{\text{def}}{=} \mathrm{Hom}(\mathbf{T}, \mathbf{2})$. It is an ordered set called the *(Zariski) spectrum of* $\mathbf{T}$. An element α of $\mathsf{Spec}\,\mathbf{T}$ is characterized by its kernel. In classical mathematics such a kernel is called a prime ideal. From the constructive point of view it must be detachable. Here we are interested in the case where $\mathbf{T}$ is finite, which implies that $\mathsf{Spec}\,\mathbf{T}$ is also finite (in the constructive sense).

If $\varphi : \mathbf{T} \to \mathbf{T}'$ is a homomorphism of distributive lattices and if $\alpha \in \mathsf{Spec}\,\mathbf{T}'$, then $\alpha \circ \varphi \in \mathsf{Spec}\,\mathbf{T}$. This defines a non-decreasing map from $\mathsf{Spec}\,\mathbf{T}'$ to $\mathsf{Spec}\,\mathbf{T}$, denoted by $\mathsf{Spec}\,\alpha$, called the "dual" of φ.

Conversely, let E be a finite ordered set. Let $E^\star$ be the set of *initial sections* of E, i.e. the set of finite subsets of E that are stable under the operation $x \mapsto {\downarrow}x$. This set, ordered by the relation $\supseteq$, is a finite distributive lattice, a sublattice of the lattice $\mathrm{P_f}(E)^\circ$ (the opposite lattice of $\mathrm{P_f}(E)$).

5.5. Fact. *The number of elements of a finite ordered set E is equal to the maximum length of a strictly increasing chain of elements of $E^\star$.*

D It is clear that a strictly monotone chain of elements of $E^\star$ (therefore of finite subsets of E) cannot have more than $1 + \#E$ elements. Its "length" is therefore $\leqslant \#E$. Regarding the reverse inequality, we verify it for $E = \emptyset$ (or for a singleton), then we perform an induction on $\#E$, by regarding an ordered set with n elements ($n \geqslant 1$) as an ordered set with $n-1$ elements that we extend by adding a maximal element. □

If $\psi : E \to E_1$ is a non-decreasing map between finite ordered sets, then for every $X \in E_1^\star$, $\psi^{-1}(X)$ is an element of $E^\star$. This defines a homomorphism $E_1^\star \to E^\star$ denoted by $\psi^\star$, called the "dual" of ψ.

5.6. Theorem. (Duality between finite distributive lattices and finite ordered sets)

1. *For every finite ordered set E let us define $\nu_E : E \to \mathsf{Spec}(E^\star)$ by*
$$\nu_E(x)(S) = 0 \;\; \textit{if} \;\; x \in S, \;\; 1 \;\; \textit{otherwise}.$$
Then, ν_E is an isomorphism of ordered sets. In addition, for every non-decreasing map $\psi : E \to E_1$, we have $\nu_{E_1} \circ \psi = \mathsf{Spec}(\psi^\star) \circ \nu_E$.

2. *For every finite distributive lattice $\mathbf{T}$ let us define $\iota_{\mathbf{T}} : \mathbf{T} \to (\mathsf{Spec}\,\mathbf{T})^\star$ by*
$$\iota_{\mathbf{T}}(x) = \{\, \alpha \in \mathsf{Spec}\,\mathbf{T} \mid \alpha(x) = 0 \,\}.$$
Then, $\iota_{\mathbf{T}}$ is an isomorphism of distributive lattices. In addition, for every morphism $\varphi : \mathbf{T} \to \mathbf{T}'$, we have $\iota_{\mathbf{T}'} \circ \varphi = (\mathsf{Spec}\,\varphi)^\star \circ \iota_{\mathbf{T}}$.

D See Exercise 13. □

In other terms, the categories of finite distributive lattices and of finite ordered sets are antiequivalent. The antiequivalence is given by the contravariant functors $\mathsf{Spec}\,\bullet$ and $\bullet^\star$, and by the natural transformations ν and ι defined above. The generalization of this antiequivalence of categories to the case of not necessarily finite distributive lattices will briefly be addressed on page 748.

Heyting algebras

A distributive lattice $\mathbf{T}$ is called an *implicative lattice* or a *Heyting algebra* when there exists a binary operation $\rightarrow$ satisfying for all a, b, c,

$$a \wedge b \leqslant c \iff a \leqslant (b \rightarrow c)\,. \tag{26}$$

This means that for all b, $c \in \mathbf{T}$, the *conductor ideal*

$$(c : b)_{\mathbf{T}} \overset{\mathrm{def}}{=} \{\, x \in \mathbf{T} \,|\, x \wedge b \leqslant c \,\}$$

is principal, its generator being denoted by $b \rightarrow c$. Therefore if it exists, the operation $\rightarrow$ is uniquely determined by the structure of the lattice. We then define the unary law $\neg x = x \rightarrow 0$. The structure of a Heyting algebra can be defined as purely equational by giving suitable axioms, described in the following fact.

5.7. Fact. *A lattice* $\mathbf{T}$ *(not assumed distributive) equipped with a law* $\rightarrow$ *is a Heyting algebra if and only if the following axioms are satisfied*

$$\begin{aligned} a \rightarrow a &= 1, \\ a \wedge (a \rightarrow b) &= a \wedge b, \\ b \wedge (a \rightarrow b) &= b, \\ a \rightarrow (b \wedge c) &= (a \rightarrow b) \wedge (a \rightarrow c). \end{aligned}$$

Let us also note the following important facts.

5.8. Fact. *In a Heyting algebra we have*

$$a \leqslant b \Leftrightarrow a \rightarrow b = 1,$$

$$\begin{aligned} a \rightarrow (b \rightarrow c) &= (a \wedge b) \rightarrow c, & a \rightarrow b &\leqslant \neg b \rightarrow \neg a, \\ (a \vee b) \rightarrow c &= (a \rightarrow c) \wedge (b \rightarrow c), & a &\leqslant \neg\neg a, \\ \neg\neg\neg a &= \neg a, & a \rightarrow b &\leqslant (b \rightarrow c) \rightarrow (a \rightarrow c), \\ \neg(a \vee b) &= \neg a \wedge \neg b, & \neg a \vee b &\leqslant a \rightarrow b. \end{aligned}$$

Every finite distributive lattice is a Heyting algebra, because every finitely generated ideal is principal. A special important case of Heyting algebra is a Boolean algebra.

A *homomorphism of Heyting algebras* is a homomorphism of distributive lattices $\varphi : \mathbf{T} \rightarrow \mathbf{T}'$ such that $\varphi(a \rightarrow b) = \varphi(a) \rightarrow \varphi(b)$ for all a, $b \in \mathbf{T}$.

The following fact is immediate.

5.9. Fact. *Let* $\varphi : \mathbf{T} \rightarrow \mathbf{T}_1$ *be a homomorphism of distributive lattices, with* $\mathbf{T}$ *and* $\mathbf{T}_1$ *being Heyting algebras. Let* $a \preccurlyeq b$ *for* $\varphi(a) \leqslant_{\mathbf{T}_1} \varphi(b)$*. Then* φ *is a homomorphism of Heyting algebras if and only if we have for all* a*,* a'*,* b*,* $b' \in \mathbf{T}$

$$a \preccurlyeq a' \implies (a' \rightarrow b) \preccurlyeq (a \rightarrow b), \quad \textit{and} \quad b \preccurlyeq b' \implies (a \rightarrow b) \preccurlyeq (a \rightarrow b').$$

5.10. Fact. *If* $\mathbf{T}$ *is a Heyting algebra every quotient* $\mathbf{T}/(y=0)$ *(i.e. every quotient by a principal ideal) is also a Heyting algebra.*

D Let $\pi : \mathbf{T} \to \mathbf{T}' = \mathbf{T}/(y=0)$ be the canonical projection. We have

$$\begin{aligned} \pi(x) \wedge \pi(a) \leqslant_{\mathbf{T}'} \pi(b) \iff \pi(x \wedge a) \leqslant_{\mathbf{T}'} \pi(b) \iff \\ x \wedge a \leqslant b \vee y \iff x \leqslant a \to (b \vee y). \end{aligned}$$

However, $y \leqslant b \vee y \leqslant a \to (b \vee y)$, therefore

$$\pi(x) \wedge \pi(a) \leqslant_{\mathbf{T}'} \pi(b) \iff x \leqslant \big(a \to (b \vee y)\big) \vee y,$$

i.e. $\pi(x) \leqslant_{\mathbf{T}'} \pi\big(a \to (b \vee y)\big)$, which shows that $\pi\big(a \to (b \vee y)\big)$ holds for $\pi(a) \to \pi(b)$ in $\mathbf{T}'$. □

Remarks. 1) The notion of a Heyting algebra is reminiscent of the notion of a coherent ring in commutative algebra. Indeed, a coherent ring can be characterized as follows: the intersection of two finitely generated ideals is a finitely generated ideal and the conductor of a finitely generated ideal into a finitely generated ideal is a finitely generated ideal. If we "reread" this for a distributive lattice by recalling that every finitely generated ideal is principal we obtain a Heyting algebra.

2) Every distributive lattice $\mathbf{T}$ generates a Heyting algebra naturally. In other words we can formally add a generator for every ideal $(b : c)$. But if we start from a distributive lattice which happens to be a Heyting algebra, the Heyting algebra which it generates is strictly greater. Let us take for example the lattice **3** which is the free distributive lattice with a single generator. The Heyting algebra that it generates is therefore the free Heyting algebra with one generator. But it is infinite (cf. [Johnstone]). A contrario the Boolean lattice generated by $\mathbf{T}$ (cf. Theorem 1.8) remains equal to $\mathbf{T}$ when it is Boolean. ■

Exercises and problems

Exercise 1. We recommend that the proofs which are not given, or are sketched, or left to the reader, etc, be done. But in particular, we will cover the following cases.

- Show that the relations (2) on page 621 are exactly what is needed to define a quotient lattice.
- Prove Proposition 1.2.
- Prove Corollary 1.7.
- Prove Facts 3.4, 3.6, 3.7 and 3.8.
- Prove Fact 4.3 and all the numbered facts between 4.5 and 4.17 (for Fact 4.2 see Exercise 7).
- Prove what is affirmed in the examples on page 654.
- Prove Facts 5.7 and 5.8.

Exercise 2. Let $\mathbf{T}$ be a distributive lattice and $x \in \mathbf{T}$. We have seen (Lemma 1.6) that

$$\lambda_x : \mathbf{T} \to \mathbf{T}[x^\bullet] \overset{\text{def}}{=} \mathbf{T}/(x = 0) \times \mathbf{T}/(x = 1)$$

is injective, which means: if $y \wedge x = z \wedge x$ and $y \vee x = z \vee x$, then $y = z$.
Show that we can deduce the cut rule (24).

Exercise 3. Let $\mathbf{A}$ be an integral ring and p, a, $b \in \operatorname{Reg}(\mathbf{A})$, with p irreducible. Suppose that $p \mid ab$, but $p \nmid a$, $p \nmid b$. Show that (pa, ab) does not have a gcd. Show that in $\mathbb{Z}[X^2, X^3]$ the elements X^2 and X^3 admit a gcd, but no lcm, and that the elements X^5 and X^6 do not have a gcd.

Exercise 4. *(Another definition of l-groups)*
Show that the axioms that must satisfy a subset G^+ of a group $(G, 0, +, -)$ to define a compatible lattice-order are

- $G = G^+ - G^+$,
- $G^+ \cap -G^+ = \{0\}$,
- $G^+ + G^+ \subseteq G^+$,
- $\forall a, b\ \exists c,\ \ c + G^+ = (a + G^+) \cap (b + G^+)$.

Exercise 5. *(Another proof of Gauss' lemma)*
In the context of Proposition 3.14, show that $\mathrm{G}(fg) = \mathrm{G}(f)\mathrm{G}(g)$ with the help of a proof based on the Dedekind-Mertens lemma III-2.1.

Exercise 6. *(Kronecker's trick)* Let d be a fixed integer $\geqslant 2$.
1. Let $\mathbf{A}[\underline{X}]_{<d} \subset \mathbf{A}[\underline{X}] = \mathbf{A}[X_1, \dots, X_n]$ be the $\mathbf{A}$-submodule constituted from polynomials P such that $\deg_{X_i} P < d$ for every $i \in [\![1..n]\!]$, and $\mathbf{A}[T]_{<d^n} \subset \mathbf{A}[T]$ be the one formed from the polynomials $f \in \mathbf{A}[T]$ of degree $< d^n$.
Show that $\varphi : P(X_1, \dots, X_n) \mapsto P(T, T^d, \dots, T^{d^{n-1}})$ induces an isomorphism of $\mathbf{A}$-modules between the $\mathbf{A}$-modules $\mathbf{A}[\underline{x}]_{<d}$ and $\mathbf{A}[T]_{<d^n}$.
2. We assume that $\mathbf{A}[X]$ is a UFD. Let $P \in \mathbf{A}[\underline{X}]_{<d}$ and $f = \varphi(P) \in \mathbf{A}[T]_{d^n}$. Show that any factorization of P in $\mathbf{A}[\underline{X}]$ can be found by a finite procedure from those of f in $\mathbf{A}[T]$.

Exercise 7. Verify Fact 4.2, i.e. $\mathsf{Zar}\,\mathbf{A}$ is a distributive lattice. Show that this distributive lattice can be defined by generators and relations as follows. The generators are the symbols $\mathrm{D}(a)$, $a \in \mathbf{A}$, with the system of relations:

$$\mathrm{D}(0) = 0, \quad \mathrm{D}(1) = 1, \quad \mathrm{D}(a + b) \leqslant \mathrm{D}(a) \vee \mathrm{D}(b), \quad \mathrm{D}(ab) = \mathrm{D}(a) \wedge \mathrm{D}(b).$$

Exercise 8. The context is that of the closed covering principle 4.19. We consider a closed covering of the ring $\mathbf{A}$ by ideals $\mathfrak{a}_1, \dots, \mathfrak{a}_r$. We do not suppose that $\prod_i \mathfrak{a}_i = 0$, but we suppose that each $\mathfrak{a}_i$ is finitely generated. Show that an $\mathbf{A}$-module M is finitely generated if and only if it is finitely generated modulo each $\mathfrak{a}_i$.

Exercise 9. *(The ring $\mathbf{A}^\bullet$)* We are in the context of classical mathematics. Let $\mathbf{A}$ be a ring and $\varphi : \mathbf{A} \to \mathbf{A}^\bullet$ be the natural homomorphism.

1. Show that the map $\mathsf{Spec}\,\varphi : \mathsf{Spec}\,\mathbf{A}^\bullet \to \mathsf{Spec}\,\mathbf{A}$ is a bijection and that for $\mathfrak{q} \in \mathsf{Spec}\,\mathbf{A}^\bullet$, the natural homomorphism $\mathrm{Frac}(\mathbf{A}\big/\varphi^{-1}(\mathfrak{q})) \to \mathbf{A}^\bullet/\mathfrak{q}$ is an isomorphism.

2. The ring $\mathbf{A}^\bullet$ is identified with the reduced zero-dimensional subring of

$$\widetilde{\mathbf{A}} \overset{\mathrm{def}}{=} \textstyle\prod_{\mathfrak{p}\in\mathsf{Spec}\,\mathbf{A}} \mathrm{Frac}(\mathbf{A}/\mathfrak{p})$$

generated by (the image of) $\mathbf{A}$.

Exercise 10. *(Minimal prime ideals)*
We are in the context of classical mathematics. A prime ideal is said to be minimal if it is minimal among the prime ideals. Let $\mathsf{Min}\,\mathbf{A}$ be the subspace of $\mathsf{Spec}\,\mathbf{A}$ formed by the minimal prime ideals. Recall that we have defined a *maximal filter* as a filter whose localized ring is a reduced zero-dimensional local ring. In item *1* of this exercise we make the link with the most usual definition.

1. Show that a strict filter $\mathfrak{f}$ is maximal among the strict filters if and only if for every $x \notin \mathfrak{f}$ there exists an $a \in \mathfrak{f}$ such that ax is nilpotent. Another possible characterization is that the localized ring $\mathfrak{f}^{-1}\mathbf{A}$ is local, zero-dimensional and nontrivial. In particular, every strict maximal filter among the strict filters is prime.

NB: reformulation of the first characteristic property for the complementary prime ideal: a prime ideal $\mathfrak{p}$ is minimal if and only if for all $x \in \mathfrak{p}$, there exists an $a \notin \mathfrak{p}$ such that ax is nilpotent.

2. The dual notion of the Jacobson radical is the intersection filter of the maximal filters (i.e. the complement of the union of the minimal prime ideals). It can be characterized as follows in classical mathematics (compare with Lemma IX-1.1 and its proof): it is the set of $a \in \mathbf{A}$ "nilregular" in the following sense

$$\forall y \in \mathbf{A} \quad ay \text{ nilpotent } \Rightarrow\ y \text{ nilpotent.} \tag{27}$$

In particular, in a reduced ring, it is the set of regular elements.

Exercise 11. *(Boolean algebra freely generated by a finite set)*
Let $E = \{x_1, \dots, x_n\}$ be a finite set.

1. Show that the Boolean algebra $\mathbf{B}$ freely generated by E identifies with the algebra

$$\mathbb{F}_2[X_1, \dots, X_n]/\mathfrak{a} = \mathbb{F}_2[x_1, \dots, x_n]$$

with $\mathfrak{a} = \big\langle (X_i^2 - X_i)_{i=1}^n \big\rangle$.

2. Define two "natural" $\mathbb{F}_2$-bases of $\mathbf{B}$, indexed by $\mathrm{P_f}(E)$, one being monomial and the other being a fundamental system of orthogonal idempotents. Express one in terms of the other.

Exercise 12. Give a precise description of distributive lattices freely generated by sets with 0, 1, 2 and 3 elements. In particular, specify the number of their elements.

Exercise 13. We detail the proof of Theorem 5.6.

1. We use (as in the course) the order relation $\supseteq$ over $E^\star$ (the set of initial sections of the finite ordered set E).
If $S_1, S_2 \in E^\star$, what are $S_1 \wedge S_2$, $S_1 \vee S_2$ equal to?

2. What is the order relation over the set of prime ideals of $\mathbf{T}$ corresponding to the order which has been defined for $\mathsf{Spec}\,\mathbf{T}$?

3. Prove item *1* of the theorem.
We will start by verifying that for $S \in E^\star$, S generates a prime ideal if and only if S is of the form $\downarrow x$ with $x \in E$; then that $\mathrm{Ker}\,\nu_E(x) = \mathcal{I}_{E^\star}(\downarrow x)$.

4. How to construct $E^\star$ from E? Treat the following example

$$E = \begin{tikzcd} & & & d \\ c & & b \arrow[ur] & \\ & a \arrow[ul] \arrow[ur] & & \end{tikzcd} \qquad a < b < d,\ a < c.$$

Study the case where E is totally ordered, and the case where E is ordered by the equality relation.

5. Prove item *2* of the theorem.

6. Consider the same questions for the opposite order over $E^\star$ and adapt the order over $\mathsf{Spec}(E^\star)$.

Exercise 14. Let a, b be nonzero in an integral ring. Suppose that the ideal $\langle a, b\rangle$ is invertible and that a and b admit a lcm m.
Show that $\langle a, b\rangle$ is a principal ideal.

Exercise 15. *(A UFD with only a finite number of irreducible elements)*
Show that a UFD with only a finite number of irreducible elements is a PID.

Exercise 16. *(An interesting intersection)*
Let $\mathbf{k}$ be a discrete field. We consider the intersection

$$\mathbf{A} = \mathbf{k}(x, y)[z] \cap \mathbf{k}(z, x + yz).$$

They are two subrings of $\mathbf{k}(x, y, z)$. The first is a PID, the second is a discrete field. Show that $\mathbf{A} = \mathbf{k}[z, x + yz]$, isomorphic to $\mathbf{k}[z, u]$. Thus the intersection is not a PID, not even a Bézout ring.

Problem 1. *(Quotient lattice-groups, solid subgroups)*
In an ordered set E, if $a \leqslant b$, we call *the segment with endpoints a and b* the subset $\{\, x \in E \mid a \leqslant x \leqslant b \,\}$. We denote it by $[a, b]_E$ or $[a, b]$. A subset F of E is said to be *convex* when the implication $a, b \in F \Rightarrow [a, b] \subseteq F$ is satisfied.
A subgroup H of an l-group is said to be *solid* if it is a convex l-subgroup. We will see that this notion is the analogue for l-groups of that of an ideal for rings.

1. A subgroup H of an ordered group G is convex if and only if the order relation over G passes to the quotient in G/H, i.e. more precisely G/H is equipped with an ordered group structure for which $(G/H)^+ = G^+ + H$. We also say *isolated subgroup* for “convex subgroup of an ordered group.”

2. The kernel H of a morphism of l-groups $G \to G'$ is a solid subgroup of G.

3. Conversely, if H is a solid subgroup of an l-group G, the law $\wedge$ passes to the quotient, it defines an l-group structure over G/H, and the canonical surjection from G to G/H is a morphism of l-groups which factorizes every morphism of source G which vanishes over H.

4. We have defined in 2.6 the l-subgroup $\mathcal{C}(x)$.
Show that $\mathcal{C}(x) \cap \mathcal{C}(y) = \mathcal{C}(|x| \wedge |y|)$, and that the solid subgroup generated by x_1, …, $x_n \in G$ is equal to $\mathcal{C}(|x_1| + \cdots + |x_n|)$. In particular, the set of solid *principal* subgroups, i.e. of the form $\mathcal{C}(a)$, is "almost" a distributive lattice (in general a maximum element is missing).

Problem 2. *(Polar subgroups, orthogonal direct summands)*
1. If A is an arbitrary subset of an l-group G let

$$A^{\perp} := \{\, x \in G \mid \forall a \in A,\ |x| \perp |a| \,\}.$$

Show that $A^{\perp}$ is always a solid subgroup.
Show that, as usual in this type of situation, we have

$$A \subseteq (A^{\perp})^{\perp},\ (A \cup B)^{\perp} = A^{\perp} \cap B^{\perp},\ A \subseteq B \Rightarrow B^{\perp} \subseteq A^{\perp} \ \text{ and }\ A^{\perp^{\perp^{\perp}}} = A^{\perp}.$$

2. A solid subgroup H of an l-group is called a *polar subgroup* when $H^{\perp^{\perp}} = H$. We also say *a polar* instead of "a polar subgroup."
A subgroup H is said to be an *orthogonal direct summand* when $G = H \oplus H^{\perp}$ (direct sum of subgroups in an Abelian group), in which case G is naturally isomorphic to $H \boxplus H^{\perp}$. We also say that G is the *internal orthogonal direct sum* of H and $H^{\perp}$ and let (by abuse) $G = H \boxplus H^{\perp}$.
Show that an orthogonal direct summand is always a polar subgroup.
Show that if $G = H \boxplus K$ (with H and K identified with subgroups of G) and if L is a solid subgroup, then $L = (L \cap H) \boxplus (L \cap K)$.

3. Generally, we say that G is the *internal orthogonal direct sum of a family of l-subgroups* $(H_i)_{i \in I}$, indexed by a discrete set I, when we have $G = \sum_{i \in I} H_i$ and when the H_i's are pairwise orthogonal. In this case, each H_i is a polar subgroup of G and we have a natural isomorphism of l-groups $\boxplus_{i \in I} H_i \simeq G$. We write (by abuse) $G = \boxplus_{i \in I} H_i$.
Suppose that an l-group is an orthogonal direct sum of a family of polar subgroups $(H_i)_{i \in I}$, as well as of another family $(K_j)_{j \in J}$. Show that these two decompositions admit a common refinement.
Deduce that if the components of a decomposition as an orthogonal direct sum are nontrivial *indecomposable* subgroups, that is, which do not admit a strict orthogonal direct summand, then the decomposition is unique, up to bijection of the set of indices.

Problem 3. *(Revisiting Gauss-Joyal)*
Let $u : \mathbf{A} \to \mathbf{T}$ ($\mathbf{A}$ is a commutative ring, $\mathbf{T}$ a distributive lattice) satisfying

$$u(ab) = u(a) \wedge u(b), \quad u(1) = 1_{\mathbf{T}}, \quad u(0) = 0_{\mathbf{T}}, \quad u(a+b) \leqslant u(a) \vee u(b).$$

For $f = \sum_i a_i X^i \in \mathbf{A}[X]$, we let

$$u(f) = u\big(\mathrm{c}(f)\big) \overset{\mathrm{def}}{=} \textstyle\bigvee_i u(a_i).$$

1. Prove that "it is well-defined," i.e. that $u(f)$ only depends on $\mathrm{c}(f)$.

We want to "directly" prove (in particular, without using Lemma II-2.6), the following version of the Gauss-Joyal lemma

$$\mathsf{LGJ}: \quad u(fg) = u(f) \wedge u(g).$$

2. Verify that if $g = \sum b_j X^j \in \mathbf{A}[X]$ the result is equivalent to $u(a_i b_j) \leqslant u(fg)$.

3. What does LGJ say if $\mathbf{T} = \{\mathsf{True}, \mathsf{False}\}$ and $u(a) = (a \neq 0)$?

4. Taking inspiration from the classical proof of the result of the previous question, prove LGJ.

5. What does LGJ say if $\mathbf{T} = \mathsf{Zar}\,\mathbf{A}$ and $u(a) = \mathrm{D}_{\mathbf{A}}(a)$?

Problem 4. *(pp-ring closure of a commutative ring)*
Taking inspiration from the reduced zero-dimensional closure, give a construction of the pp-ring closure $\mathbf{A}_{\mathrm{pp}}$ of an arbitrary commutative ring $\mathbf{A}$.
The following universal problem needs to be solved:

$$\begin{tikzcd}
\mathbf{A} \arrow[d, "\lambda"'] \arrow[dr, "\psi"] & & \text{homomorphisms of rings} \\
\mathbf{A}_{\mathrm{pp}} \arrow[r, dashed, "\varphi\,!"'] & \mathbf{B} & \text{morphisms of pp-rings}
\end{tikzcd}$$

where *the pp-ring morphisms are the ring homomorphisms which respect the law* $a \mapsto e_a$ (e_a is the idempotent satisfying $\langle 1 - e_a \rangle = \mathrm{Ann}(a)$). Hereinafter, we will speak of *pp-ring morphism.*
A pp-ring closure of a ring $\mathbf{A}$ "a priori" exists, from the simple fact that the theory of pp-rings is purely equational. Indeed, for any system of generators and of relations (a relation is an equality between two terms constructed from generators, of 0 and of 1, by using the laws $+, -, \times, a \mapsto e_a$), there exists some pp-ring "the most general as possible" corresponding to this presentation: we take over the set of terms the smallest equivalence relation which respects the axioms and which places in the same equivalence class two terms related by a given relation at the start. Under these conditions the ring $\mathbf{A}_{\mathrm{pp}}$ is simply the pp-ring generated by the elements of $\mathbf{A}$ with for relations all the equalities $a + b = c$, $a \times b = d$, $a = -a'$ true in $\mathbf{A}$.
But we want a precise description, as for the reduced zero-dimensional closure.
We will then prove the following results.

1. (pp-ring morphisms)

a. A morphism $\varphi : \mathbf{A} \to \mathbf{B}$ is a pp-ring morphism if and only if it transforms every regular element into a regular element. In this case, it uniquely extends to a morphism $\mathrm{Frac}(\varphi) : \mathrm{Frac}(\mathbf{A}) \to \mathrm{Frac}(\mathbf{B})$.

b. A pp-ring morphism is injective if and only if its restriction to $\mathbb{B}(\mathbf{A})$ is injective.

c. There exist injective homomorphisms between pp-rings that are not pp-ring morphisms.

d. Every homomorphism between reduced zero-dimensional rings is a pp-ring morphism.

- *e.* If $\mathbf{A}$ is a pp-ring, $\mathbb{B}(\mathrm{Frac}\,\mathbf{A})$ is identified with $\mathbb{B}(\mathbf{A})$ and the injection $\mathbf{A} \to \mathrm{Frac}(\mathbf{A})$ is a pp-ring morphism.

2. We have natural ring homomorphisms $\mathbf{A}_{\mathrm{red}} \to \mathbf{A}_{\mathrm{pp}} \to \mathrm{Frac}(\mathbf{A}_{\mathrm{pp}}) \to \mathbf{A}^{\bullet}$.
They are all injective and the natural homomorphism $\mathrm{Frac}(\mathbf{A}_{\mathrm{pp}}) \to \mathbf{A}^{\bullet}$ is an isomorphism.

3. If $\mathbf{A} \subseteq \mathbf{C}$ with $\mathbf{C}$ a pp-ring, the smallest pp-subring of $\mathbf{C}$ containing $\mathbf{A}$ is equal to $\mathbf{A}[(e_a)_{a\in\mathbf{A}}]$.

4. If we identify $\mathbf{A}_{\mathrm{red}}$ with its image in $\mathbf{A}^{\bullet}$, we can identify $\mathbf{A}_{\mathrm{pp}}$ with the subring of $\mathbf{A}^{\bullet}$ generated by $\mathbf{A}_{\mathrm{red}}$ and by the idempotents e_x for $x \in \mathbf{A}_{\mathrm{red}}$.

In what follows we suppose without loss of generality that $\mathbf{A}$ is reduced.

5. We refer to Corollary 4.24 for the description of the finite steps of the construction of $\mathbf{A}^{\bullet}$. Given item *4*, we get a description of the finite steps of a possible construction of $\mathbf{A}_{\mathrm{pp}}$.
For $a_1, \ldots, a_n \in \mathbf{A}$, we have an injection $\mathbf{A} \to \mathbf{A}[a_1^{\bullet}, \cdots, a_n^{\bullet}] = \mathbf{C}$.
Let e_i be the idempotent $a_i a_i^{\bullet}$, $\mathbf{B} = \mathbf{A}[e_1, \ldots, e_n] \subseteq \mathbf{C}$, and $e_I = \prod_{i\in I}(1 - e_i)\prod_{j\notin I} e_j$ for $I \in \mathcal{P}_n$. Prove the following results.

- *a.* The family $(e_I)_{I\in\mathcal{P}_n}$ is a fundamental system of orthogonal idempotents of $\mathbf{B}$ and $\langle 1 - e_I\rangle_{\mathbf{B}} = \langle (e_i)_{i\in I},\ (1 - e_j)_{j\notin I}\rangle_{\mathbf{B}}$.
- *b.* $\mathrm{Ann}_{\mathbf{B}}(a_i) = \langle 1 - e_i\rangle_{\mathbf{B}}$.
- *c.* $\mathbf{A} \cap \langle e_i, \in I\rangle_{\mathbf{B}} = \mathrm{D}_{\mathbf{A}}(a_i, i \in I)$.
- *d.* By letting $\mathfrak{a}'_I = (\mathrm{D}_{\mathbf{A}}(a_i, i \in I) : \prod_{j\notin I} a_j)$, we have $\mathbf{A} \cap \langle 1 - e_I\rangle_{\mathbf{B}} = \mathfrak{a}'_I$ and an isomorphism $\mathbf{B} \simeq \prod_{I\in\mathcal{P}_n} \mathbf{A}/\mathfrak{a}'_I$.
- *e.* The ring $\mathbf{C}$ is a localization of the ring $\mathbf{B}$: $\mathbf{C} = \mathbf{B}_s$ with regular $s \in \mathbf{B}$.

In particular, let $a \in \mathbf{A}$ and $\mathbf{A}[e_a] \subseteq \mathbf{A}[a^{\bullet}]$ with $e_a = aa^{\bullet}$.
Then, $\mathrm{Ann}_{\mathbf{A}[e_a]}(a) = \langle 1 - e_a\rangle$, $\mathbf{A}[e_a] \simeq \mathbf{A}/\mathrm{Ann}_{\mathbf{A}}(a) \times \mathbf{A}/\mathrm{D}_{\mathbf{A}}(a)$, with $e_a \leftrightarrow (1, 0)$, and $\mathbf{A}[a^{\bullet}]$ is the localized ring $\mathbf{A}[e_a]_s$ with regular $s = 1 - e_a + a$.
In what follows let $\mathbf{A}_{[a_1,\ldots,a_n]}$ for $\mathbf{A}[a_1 a_1^{\bullet}, \ldots, a_n a_n^{\bullet}]$

6. Let $\varphi : \mathbf{A} \to \mathbf{D}$ be a morphism with $\mathbf{D}$ reduced, $a \in \mathbf{A}$ and $b = \varphi(a)$. Suppose that $\mathrm{Ann}_{\mathbf{D}}(b) = \langle 1 - e_b\rangle_{\mathbf{D}}$ with idempotent e_b. Show that we can extend φ to a morphism of $\mathbf{A}_{[a]} \to \mathbf{D}$ realizing $e_a \mapsto e_b$.
However, in general, for a, $b \in \mathbf{A}$, the rings $\mathbf{A}_{[a,b]}$ and $(\mathbf{A}_{[a]})_{[b]}$ are not isomorphic.

7. Give a precise description of $\mathbb{Z}_{\mathrm{pp}}$.
Explain why the homomorphism $\mathbb{Z}_{\mathrm{pp}} \to (\mathbb{Z}_{\mathrm{pp}})_{\mathrm{pp}}$ is not an isomorphism.

8. (In classical mathematics) If $\mathbf{A}$ is pp-ring, and $\imath : \mathbf{A} \to \mathrm{Frac}\,\mathbf{A}$ is the canonical injection, then $\mathsf{Spec}\,\imath$ establishes a bijection between $\mathsf{Spec}(\mathrm{Frac}\,\mathbf{A})$ and $\mathsf{Min}\,\mathbf{A}$.

9. (In classical mathematics) For every ring $\mathbf{A}$, there is a natural bijection between $\mathsf{Min}(\mathbf{A}_{\mathrm{pp}})$ and $\mathsf{Spec}\,\mathbf{A}$.

Comment. Despite $\mathbb{Z}$ being a pp-ring, $\mathbb{Z}_{\mathrm{pp}}$ is not isomorphic to $\mathbb{Z}$. This is understood by observing that the natural projection $\mathbb{Z} \to \mathbb{Z}/15\mathbb{Z}$ is not a pp-ring morphism. This situation is different from that of the reduced zero-dimensional closure: this comes from the fact that the quasi-inverse b of an element a, when it exists, is unique and simply defined by two equations $ab^2 = b$ and $a^2b = a$, which implies that every ring homomorphism respects quasi-inverses. ∎

Some solutions, or sketches of solutions

Exercise 2. Indeed, $(a \wedge b) \wedge x = a \wedge x$ since $x \wedge a \leqslant b$.
And $(a \wedge b) \vee x = (a \vee x) \wedge (b \vee x) = a \vee x$ because $a \vee x \leqslant b \vee x$ (since $a \leqslant x \vee b$).
Therefore $a \wedge b = a$, i.e. $a \leqslant b$.

Exercise 3. We write $a \sim b$ to indicate that a and b are associated. Let us prove the following form (which is actually stronger if the divisibility in $\mathbf{A}$ is not explicit): if p is irreducible, $p \mid ab$ and (pa, ab) has a gcd d, then $p \mid a$ or $p \mid b$.
We have $p \mid pa$ and $p \mid ab$, so $p \mid d$. Furthermore $a \mid pa$, $a \mid ab$, so $a \mid d$. Let $a' = d/a \in \mathbf{A}$. As $d \,|\, pa$, we have $a' \mid p$. But p being irreducible, we either have $a' \sim 1$, or $a' \sim p$.
In the first case, $d \sim a$, and as $p \mid d$, we have $p \mid a$. In the second case, we have $d \sim ap$, thus $ap \mid ab$, i.e. $p \mid b$.
In $\mathbb{Z}[X^2, X^3]$, X^2 is irreducible, $X^2 \mid X^3 \cdot X^3$ but $X^2 \not| \, X^3$, so $X^2 \cdot X^3$ and $X^3 \cdot X^3$ do not have a gcd. A fortiori they do not have a lcm.
Finally, the gcd of X^2 and X^3 in $\mathbb{Z}[X^2, X^3]$ is 1, if they had a lcm it would therefore be X^5, but X^5 does not divide X^6.

Exercise 5. Let $\mathrm{G}(\mathfrak{a})$ be the gcd of the generators of a finitely generated ideal $\mathfrak{a}$. We easily observe that it is well-defined. Next, the distributivity $a(b \wedge c) = ab \wedge ac$ is generalized in the form $\mathrm{G}(\mathfrak{a})\mathrm{G}(\mathfrak{b}) = \mathrm{G}(\mathfrak{ab})$ for two finitely generated ideals $\mathfrak{a}$ and $\mathfrak{b}$. Finally, for two polynomials f, $g \in \mathbf{A}[X]$, Dedekind-Mertens states that

$$\mathrm{c}(f)^{p+1}\mathrm{c}(g) = \mathrm{c}(f)^p\mathrm{c}(fg) \text{ for } p \geqslant \deg g.$$

As $\mathrm{G}(f) = \mathrm{G}\big(\mathrm{c}(f)\big)$ we obtain $\mathrm{G}(f)^{p+1}\mathrm{G}(g) = \mathrm{G}(f)^p\mathrm{G}(fg)$, and since they are elements of the ring, we can simplify to obtain $\mathrm{G}(fg) = \mathrm{G}(f)\mathrm{G}(g)$.

Exercise 6. *1.* Let $\underline{X}^\alpha = X_1^{\alpha_1} \cdots X_n^{\alpha_n} \in \mathbf{A}[\underline{X}]_{<d}$, then

$$\varphi(\underline{X}^\alpha) = T^a \quad \text{with} \quad a = \alpha_1 + \alpha_2 d + \cdots + \alpha_n d^{n-1}.$$

We thus see that $a < d^n$. The numbering in base d proves that φ transforms the $\mathbf{A}$-basis of $\mathbf{A}[\underline{X}]_{<d}$ constituting of $\underline{X}^\alpha$'s with $\alpha_i < d$ into the $\mathbf{A}$-basis $(1, T, \ldots, T^{d^n-1})$ of $\mathbf{A}[T]_{<d^n}$.

2. Let us recall that $\mathbf{A}[X]^\times = \mathbf{A}^\times = \mathbf{A}[\underline{X}]^\times$. Here we assume that $\mathbf{A}[T]$ is a UFD. If $P = QR \in \mathbf{A}[\underline{X}]_{<d}$ then Q and $R \in \mathbf{A}[\underline{X}]_{<d}$, and $\varphi(Q)$ and $\varphi(R) \in \mathbf{A}[T]_{<d^n}$. Since $\varphi(QR) = \varphi(Q)\varphi(R)$, and $f = \varphi(P)$ has only finitely many factors (in $\mathbf{A}[X]^*/\mathbf{A}^\times$), it is sufficient to test for each factor $g(T)$ of $f(T)$ if $\varphi^{-1}(g)$ is a factor of P. This is possible since $\mathbf{A}$ is supposed to be with explicit divisibility.

Exercise 8. We reduce to $r = 2$. The hypothesis "M is finitely generated modulo $\mathfrak{a}_i$," provides a finitely generated submodule M_i of M such that $M = M_i + \mathfrak{a}_i M$. By substituting the value of M in the right-hand side, we obtain

$$M = M_i + \mathfrak{a}_i M_i + \mathfrak{a}_i^2 M = M_i + \mathfrak{a}_i^2 M.$$

By iterating, we obtain for $k \geqslant 1$, $M = M_i + \mathfrak{a}_i^k M$. By substituting $M = M_2 + \mathfrak{a}_2^k M$ in $M = M_1 + \mathfrak{a}_1^k M$, we obtain $M = M_1 + M_2 + (\mathfrak{a}_1\mathfrak{a}_2)^k M$. But $\mathfrak{a}_1$, $\mathfrak{a}_2$ are finitely generated and $\mathfrak{a}_1\mathfrak{a}_2 \subseteq \mathrm{D}_{\mathbf{A}}(0)$, so there exists some k such that $(\mathfrak{a}_1\mathfrak{a}_2)^k = \{0\}$, and consequently $M = M_1 + M_2$ is finitely generated.

Exercise 9. We can assume that $\mathbf{A}$ is a reduced subring of $\mathbf{A}^\bullet$.
1. Let $\mathfrak{p}$ be a prime ideal of $\mathbf{A}$; the canonical morphism $\mathbf{A} \to \mathbf{K} = \mathrm{Frac}(\mathbf{A}/\mathfrak{p})$ can be factorized through $\mathbf{A}^\bullet$:

$$\begin{tikzcd}
\mathbf{A} \arrow[d] \arrow[dr] & \\
\mathbf{A}^\bullet \arrow[r, dashed, "\pi_{\mathfrak{p}}"'] & \mathrm{Frac}(\mathbf{A}/\mathfrak{p})
\end{tikzcd}$$

The morphism $\pi_{\mathfrak{p}}$ is surjective because for $a \in \mathbf{A} \setminus \mathfrak{p}$, we have $1/a = \pi_b(a^\bullet)$ in $\mathbf{K}$. Its kernel $\mathfrak{q} = \operatorname{Ker}\pi_p$ is a maximal ideal of $\mathbf{A}^\bullet$; we then have $\mathbf{A}/\mathfrak{p} \subseteq \mathbf{K} \simeq \mathbf{A}^\bullet/\mathfrak{q}$, so the natural arrow $\mathbf{A}/\mathfrak{p} \to \mathbf{A}^\bullet/\mathfrak{q}$ being injective, $\mathfrak{p} = \mathfrak{q} \cap \mathbf{A}$. We thus dispose of two transformations

$$\mathsf{Spec}\,\mathbf{A}^\bullet \to \mathsf{Spec}\,\mathbf{A},\ \mathfrak{q} \mapsto \mathfrak{q} \cap \mathbf{A}, \text{ and } \mathsf{Spec}\,\mathbf{A} \to \mathsf{Spec}\,\mathbf{A}^\bullet,\ \mathfrak{p} \mapsto \operatorname{Ker}\pi_p,$$

which are inverses of one another. Indeed, if $\mathfrak{q} \in \mathsf{Spec}\,\mathbf{A}^\bullet$ and $\mathfrak{p} = \mathfrak{q} \cap \mathbf{A}$, then $\mathbf{K} = \mathbf{A}^\bullet/\mathfrak{q}$ (because $a^\bullet = 1/a$ for $a \in \mathbf{A} \setminus \mathfrak{p}$) so $\operatorname{Ker}\pi_{\mathfrak{p}} = \mathfrak{q}$.
2. By item *1* the homomorphism $\mathbf{A}^\bullet \to \widetilde{\mathbf{A}}$ that factorizes the natural homomorphism $\mathbf{A} \to \widetilde{\mathbf{A}}$ is injective, because its kernel is the intersection of all the prime ideals of $\mathbf{A}^\bullet$. We identify $\mathbf{A} \subseteq \mathbf{A}^\bullet \subseteq \widetilde{\mathbf{A}}$. Lemma 4.22 describes the smallest reduced zero-dimensional subring of $\widetilde{\mathbf{A}}$ containing $\mathbf{A}$. We see that this is indeed of $\mathbf{A}^\bullet$ (by the construction of $\mathbf{A}^\bullet$).
Another proof, left to the reader. Let $\mathbf{A}_1$ be the smallest reduced zero-dimensional subring of $\widetilde{\mathbf{A}}$ containing $\mathbf{A}$. We then prove that this object satisfies the desired universal property.

Exercise 10. *1.* The first characterization of strict maximal filters among the strict filters is immediate: it is the same as saying that every attempt to make $\mathfrak{f}$ grow by adding an exterior element x to it fails, because the filter generated by $\mathfrak{f}$ and x contains 0.
Let us then prove that a maximal strict filter among the strict filters is prime.
Let x, $y \in \mathbf{A}$ with $x + y \in \mathfrak{f}$. We want to show that $x \in \mathfrak{f}$ or $y \in \mathfrak{f}$. If $x \notin \mathfrak{f}$, there exist $a \in \mathfrak{f}$ and $n \in \mathbb{N}$ such that $a^n x = 0$, so $a^n(x + y) = a^n y \in \mathfrak{f}$ therefore $y \in \mathfrak{f}$.
Let us now show that the localized ring is zero-dimensional, i.e. (since the ring is local) that every noninvertible element is nilpotent. A noninvertible element in the localized ring is a multiple of $x/1$ with $x \notin \mathfrak{f}$. It suffices to see that $x/1$ is nilpotent in $\mathfrak{f}^{-1}\mathbf{A}$, but there exists an $a \in \mathfrak{f}$ such that ax is nilpotent in $\mathbf{A}$, and a is invertible in the localized ring.
Let us finally show that if $\mathfrak{f}^{-1}\mathbf{A}$ is local zero-dimensional and nontrivial, then $\mathfrak{f}$

is strict, maximal among the strict filters. Indeed, some $x \notin \mathfrak{f}$ is not invertible, therefore is nilpotent in the localized ring, which means that there exists an $a \in \mathfrak{f}$ such that ax is nilpotent in $\mathbf{A}$.

2. Let S be the subset defined by Equation (27) (page 663). If $a \in S$ and $a \notin \mathfrak{f}$ with $\mathfrak{f}$ a maximal filter, we have $0 \in a^{\mathbb{N}}\mathfrak{f}$ which means that for some $x \in \mathfrak{f}$ and $n \in \mathbb{N}$, $xa^n = 0$, so, since $a \in S$, x is nilpotent; a contradiction.
If $a \notin S$, there exists some non-nilpotent x such that xa is nilpotent. Therefore there exists a strict filter containing x. By Zorn's lemma there exists a maximal filter $\mathfrak{f}$ containing x, and a cannot be in $\mathfrak{f}$ because otherwise xa and therefore 0 would be in $\mathfrak{f}$.

Exercise 11. *1.* Clearly results from the definition of a Boolean algebra as a ring where all the elements are idempotent, provided that we verify that the constructed object is indeed a Boolean algebra, which offers no difficulty. Notice that $\mathbf{B}$ is isomorphic to

$$\mathbb{F}_2[x_1] \otimes_{\mathbb{F}_2} \cdots \otimes_{\mathbb{F}_2} \mathbb{F}_2[x_n],$$

which is the direct sum of n Boolean algebras freely generated by a single generator in the category of Boolean algebras. Indeed, the direct sum of two Boolean algebras $\mathbf{B}$, $\mathbf{B}'$ is the Boolean algebra $\mathbf{B} \otimes_{\mathbb{F}_2} \mathbf{B}'$.

2. The monomial $\mathbb{F}_2$-basis of $\mathbf{B}$ is (m_I) with $m_I = \prod_{i \in I} x_i$. It is of cardinality 2^n, so $\mathbf{B}$ is of cardinality 2^{2^n}. We define e_I by $e_I = m_I \prod_{j \notin I}(1 + x_j)$; we easily verify that (e_I) is a fundamental system of orthogonal idempotents, that $m_I e_J = e_J$ if $I \subseteq J$, and 0 otherwise.
We have the same expression $e_I = \sum_{J \mid J \supseteq I} m_J$ and $m_I = \sum_{J \mid J \supseteq I} e_J$ (which confirms that (e_I) is an $\mathbb{F}_2$-basis of $\mathbf{B}$).
With respect to the description given in this course, $x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n}$ corresponds to the following element of $\mathrm{P_f}\big(\mathrm{P_f}(E)\big)$: $\{\{\, x_i \mid \varepsilon_i = 1 \,\}\}$.

Exercise 12. The distributive lattice freely generated by $\emptyset$ is the lattice $\mathbf{2}$.
The distributive lattice freely generated by $\{a\}$ is $\{0, a, 1\}$.
The distributive lattice freely generated by $\{a, b\}$ ($a \neq b$) is: $\{0, a \wedge b, a, b, a \vee b, 1\}$.
The distributive lattice freely generated by $\{a, b, c\}$ ($a \neq b \neq c \neq a$) contains:

$$0,\ 1,\ a,\ b,\ c,\ a \vee b,\ a \vee c,\ b \vee c,\ a \vee b \vee c,\ a \wedge b,\ a \wedge c,\ b \wedge c,\ a \wedge b \wedge c,$$
$$a \wedge (b \vee c),\ b \wedge (a \vee c),\ c \wedge (a \vee b),\ (a \vee b) \wedge (a \vee c),\ (a \vee b) \wedge (b \vee c),$$
$$(a \vee c) \wedge (b \vee c),\ (a \vee b) \wedge (a \vee c) \wedge (b \vee c).$$

Exercise 13. *1.* By definition of an initial section the intersection and the union of two initial sections is another initial section.
Therefore in $E^\star$: $S_1 \wedge S_2 = S_1 \cup S_2$, $S_1 \vee S_2 = S_1 \cap S_2$, $\emptyset = 1_{E^\star}$ and $E = 0_{E^\star}$.

2. It amounts to the same to give $\alpha \in \mathsf{Spec}\,\mathbf{T}$ or the prime ideal $\operatorname{Ker}\alpha$. This leads us to order the set of prime ideals of $\mathbf{T}$ by the relation $\supseteq$.

Indeed, if α, $\beta : \mathbf{T} \to \{0,1\}$ are two morphisms, we have the equivalence

$$\alpha \leqslant \beta \iff \operatorname{Ker}\alpha \supseteq \operatorname{Ker}\beta.$$

3. We have

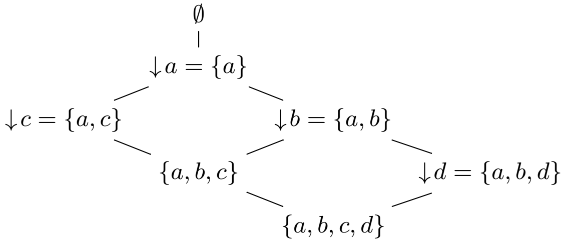
$$\operatorname{Ker}\nu_E(x) = \{\, S \in E^\star \mid x \in S \,\} = \{\, S \in E^\star \mid {\downarrow}x \subseteq S \,\} = \{\, S \in E^\star \mid S \leqslant {\downarrow}x \,\},$$

i.e. $\operatorname{Ker}\nu_E(x) = \mathcal{I}_{E^\star}({\downarrow}x)$. We indeed have the equivalences

$$x \leqslant y \iff {\downarrow}x \subseteq {\downarrow}y \iff {\downarrow}y \leqslant {\downarrow}x \iff \mathcal{I}({\downarrow}y) \subseteq \mathcal{I}({\downarrow}x) \iff \mathcal{I}({\downarrow}x) \leqslant \mathcal{I}({\downarrow}y).$$

Moreover, in $E^\star$: $S_1 \wedge S_2 \leqslant {\downarrow}x \Rightarrow (S_1 \leqslant {\downarrow}x)$ or $(S_2 \leqslant {\downarrow}x)$ (because the first inequality means ${\downarrow}x \subseteq S_1 \cup S_2$, i.e. $x \in S_1 \cup S_2$), and since ${\downarrow}x \neq 1_{E^*} = \emptyset$, ${\downarrow}x$ generates a prime ideal. Conversely, let $\mathfrak{p}$ be a prime ideal of $E^\star$. Being finite, it is principal: $\mathfrak{p} = \mathcal{I}_{E^\star}(S)$ with $S \neq 1_{E^\star}$, i.e. S is nonempty. It must be shown that S is of the form ${\downarrow}x$. If $S = \{x_1, \ldots, x_n\}$, we have $S = ({\downarrow}x_1) \cup \cdots \cup ({\downarrow}x_n)$, i.e. $({\downarrow}x_1) \wedge \cdots \wedge ({\downarrow}x_n) = S$. As S generates a prime ideal, there exists some i such that ${\downarrow}x_i \leqslant S$, i.e. $S \subseteq {\downarrow}x_i$, then $S = {\downarrow}x_i$.

4. We determine $E^\star$ by noticing that every initial section is a union of subsets ${\downarrow}x$. The picture of the lattice $E^\star$ is the following


$\emptyset$
${\downarrow}a = \{a\}$
${\downarrow}c = \{a,c\}$
${\downarrow}b = \{a,b\}$
$\{a,b,c\}$
${\downarrow}d = \{a,b,d\}$
$\{a,b,c,d\}$

If E is totally ordered, then $E^\star = \{\, {\downarrow}x \mid x \in E \,\} \cup \{\emptyset\}$ is also totally ordered and $\#E^\star = 1 + \#E$. If $\mathbf{T}$ is a finite totally ordered set, then

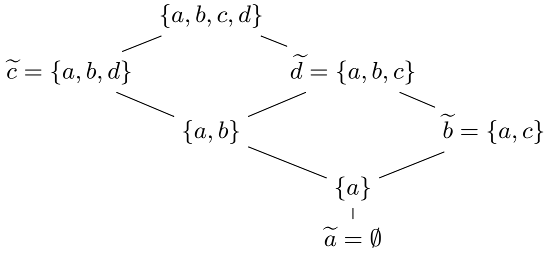
$$\mathsf{Spec}\,\mathbf{T} = \big\{\mathcal{I}_{\mathbf{T}}(a) \mid a \in \mathbf{T} \setminus \{1_{\mathbf{T}}\}\big\}, \text{ and } \#\,\mathsf{Spec}\,\mathbf{T} = \#\mathbf{T} - 1.$$

If E is ordered by the equality relation, $E^\star = \mathcal{P}(E)$ ordered by $\supseteq$. As for $\mathsf{Spec}(E^\star)$, it is the set $\mathcal{I}_{\mathcal{P}(E)}(\{x\})$ with $x \in E$ (which is indeed isomorphic to E).

5. The reader will verify that by letting, for $a \in \mathbf{T}$, $\widehat{a} = \{\, \mathfrak{p} \in \mathsf{Spec}\,\mathbf{T} \mid a \in \mathfrak{p} \,\}$, we obtain an initial section, that every initial section of $\mathsf{Spec}\,\mathbf{T}$ is of this form, and finally that $a \leqslant b \iff \widehat{a} \leqslant \widehat{b}$.

6. We now consider $E^\star$ and $\mathsf{Spec}\,\mathbf{T}$ with the order relation $\subseteq$.
Then $S_1 \wedge S_2 = S_1 \cap S_2$, $S_1 \vee S_2 = S_1 \cup S_2$, $\emptyset = 0_{E^\star}$, $E = 1_{E^\star}$. For $x \in E$, we let $\widetilde{x} = E \setminus {\uparrow}x = \{\, y \in E \mid y \not\geqslant x \,\}$: this element of $E^\star$ satisfies, for $S \in E^\star$, the equivalence $x \notin S \iff S \subseteq \widetilde{x}$. We have $\widetilde{x} \neq 1_{E^\star} = E$, and $\widetilde{x}$ generates a prime ideal of the lattice $E^\star$: $S_1 \wedge S_2 \leqslant \widetilde{x} \Rightarrow S_1 \leqslant \widetilde{x}$ or $S_2 \leqslant \widetilde{x}$ (indeed, the hypothesis is ${\uparrow}x \subseteq (E \setminus S_1) \cup (E \setminus S_2)$, therefore for example $x \notin S_1$, i.e. $S_1 \subseteq \widetilde{x}$). We have the equivalence $x \leqslant y \iff \widetilde{x} \subseteq \widetilde{y}$. We prove that every prime ideal of $E^\star$ is of the form $\widetilde{x}$, so the ordered set E is isomorphic, via $x \mapsto \mathcal{I}_{E^\star}(\widetilde{x})$, to the set of

prime ideals of $E^\star$, ordered by inclusion.


$\{a,b,c,d\}$
$\widetilde{c}=\{a,b,d\}$
$\widetilde{d}=\{a,b,c\}$
$\{a,b\}$
$\widetilde{b}=\{a,c\}$
$\{a\}$
$\widetilde{a}=\emptyset$

Exercise 14. Since $\langle a,b\rangle$ is invertible we have s, t, u, v with $sa=ub$, $tb=va$ and $s+t=1$.
Since m is the lcm of a and b we can write

$$m=ab'=ba' \text{ and } ab/m=g=b/b'=a/a'.$$

Thus $sa=mx=ab'x$ and $tb=m=ba'y$, which give $s=b'x$ and $t=a'y$.
Therefore $b'x+a'y=1$, $bx+ay=gb'x+ga'y=g$ and consequently $\langle a,b\rangle=\langle g\rangle$.

Exercise 15. *(A UFD with only a finite number of irreducible elements)*
Let $(p_i)_{i\in I}$ be the finite family of distinct irreducible elements (up to association). We must show that $\mathbf{A}$ is a Bézout ring. In order to do so, it suffices to show that if a and $b\in\mathbf{A}^*$ have as their gcd 1, then $\langle a,b\rangle=\langle 1\rangle=\mathbf{A}$. We write

$$a=\prod\nolimits_{i\in A}p_i^{\alpha_i},\ b=\prod\nolimits_{j\in B}p_i^{\beta_j}, \text{with } \alpha_i\text{'s, } \beta_j\text{'s} > 0 \text{ and } A\cap B=\emptyset.$$

Let $C=I\setminus(A\cup B)$ and $c=\prod_{k\in C}p_k$. We show that $a+bc\in\mathbf{A}^\times$.
Indeed, for $i\in A$, p_i divides a, therefore it cannot divide $a+bc$, otherwise it would divide $bc=(a+bc)-a$. Similarly, for $j\in B\cup C$, p_j cannot divide $a+bc$, otherwise it would divide $a=(a+bc)-bc$. Thus $a+bc$ is not divisible by any irreducible element.

Exercise 16. *(An interesting intersection)*
Consider the evaluation homomorphism

$$\varphi:\mathbf{k}[z,u]\to\mathbf{k}[z,x+yz],\ z\mapsto z,\ u\mapsto x+yz.$$

It is surjective by construction. It is injective because, for $f=f(z,u)$, by evaluating $\varphi(f)$ in $\mathbf{k}[x,y,z]$ we obtain $\varphi(f)(x,0,z)=f(z,x)$. It is therefore indeed an isomorphism.
In what follows we can therefore let $u=x+yz$, with $\mathbf{k}[z,x+yz]=\mathbf{k}[z,u]$ where z and u play the role of distinct indeterminates.
Moreover we notice that $\mathbf{k}[z,u][y]=\mathbf{k}[x,y,z]$. As $\mathbf{k}[z,u]$ is a GCD-domain, this implies that two elements of $\mathbf{k}[z,u]$ have gcd 1 in $\mathbf{k}[z,u]$ if and only if they have gcd 1 in $\mathbf{k}[x,y,z]$.

Now let $h\in\mathbf{A}$ be an arbitrary element that we write in the form of an irreducible fraction $f(z,u)/g(z,u)$ in $\mathbf{k}(z,u)$, and in the form of a fraction a/b ($a\in\mathbf{k}[x,y,z]$, $b\in\mathbf{k}[x,y]$) as an element of $\mathbf{k}(x,y)[z]$. This last fraction can itself be written in irreducible form, that is so that the gcd of a and b in $\mathbf{k}[x,y,z]$ is equal to 1. By uniqueness of the expression of a fraction in reduced form, we therefore have a

constant $\gamma \in \mathbf{k}^*$ such that $f(z,u) = \gamma a(x,y,z)$ and $g(z,u) = \gamma b(x,y)$.
It remains to show that the denominator $g(z, x+yz)$ is a constant. By making $z = 0$ in the equality $g(z, x+yz) = \gamma b(x,y)$ we obtain

$$g(0,x) = \gamma b(x,y) = c(x).$$

Finally, by making $(z,y) = (1,-x)$ in the equality $g(z, x+yz) = c(x)$, we obtain $c(x) = g(1,0)$.

Problem 3. The first item is left to the reader. Let $fg = \sum_k c_k X^k$.
2. We easily have $u(fg) \leqslant u(f) \wedge u(g)$.
Indeed, $c_k = \sum_{i+j=k} a_i b_j$, so $u(c_k) \leqslant \bigvee_{i+j=k} u(a_i b_j) \leqslant \bigvee_i u(a_i) = u(f)$ (we have used $u(ab) \leqslant u(a)$).
If we dispose of the Gauss-Joyal lemma, then $u(a_i b_j) \leqslant u(a_i) \wedge u(b_j) \leqslant u(f) \wedge u(g) = u(fg)$. Conversely, if we know how to prove $u(a_i b_j) \leqslant u(fg)$ for all i, j, then

$$\textstyle\bigvee_{i,j} u(a_i b_j) \leqslant u(fg), \text{ i.e. by distributivity } \big(\bigvee_i u(a_i)\big) \wedge \big(\bigvee_j u(b_j)\big) \leqslant u(fg),$$

i.e. $u(f) \wedge u(g) \leqslant u(fg)$.
3. If $\mathbf{A}$ is integral, the same goes for $\mathbf{A}[X]$.
4. Let us show by decreasing induction on $i_0 + j_0$ that $u(a_{i_0} b_{j_0}) \leqslant u(fg)$. It is true if i_0 or j_0 is large because then $a_{i_0} b_{j_0} = 0$. We write the definition of the product of two polynomials

$$a_{i_0} b_{j_0} = c_{i_0+j_0} - \sum_{\substack{i+j=i_0+j_0 \\ i>i_0}} a_i b_j - \sum_{\substack{i+j=i_0+j_0 \\ j>j_0}} a_i b_j.$$

We apply u by using on the one hand $u(\alpha + \beta + \cdots) \leqslant u(\alpha) \vee u(\beta) \vee \ldots$ and on the other hand $u(\alpha\beta) \leqslant u(\alpha)$ to obtain

$$(\star) \;:\; u(a_{i_0} b_{j_0}) \leqslant u(c_{i_0+j_0}) \vee \textstyle\bigvee_{i>i_0} u(a_i) \vee \bigvee_{j>j_0} u(b_j).$$

We thus dispose of an inequality $x \leqslant y$ which we write as $x \leqslant x \wedge y$. In other words, in $(\star)$, we reinsert $u(a_{i_0} b_{j_0})$ in the right-hand side, which gives, by distributivity

$$u(a_{i_0} b_{j_0}) \leqslant u(c_{i_0+j_0}) \vee \textstyle\bigvee_{i>i_0} \big(u(a_i) \wedge u(a_{i_0} b_{j_0})\big) \vee \bigvee_{j>j_0} \big(u(b_j) \wedge u(a_{i_0} b_{j_0})\big).$$

By using $u(a_i) \wedge u(a_{i_0} b_{j_0}) \leqslant u(a_i) \wedge u(b_{j_0})$ and $u(b_j) \wedge u(a_{i_0} b_{j_0}) \leqslant u(b_j) \wedge u(a_{i_0})$, and (by definition) $u(c_{i_0+j_0}) \leqslant u(fg)$, we bound $u(a_{i_0} b_{j_0})$ above by

$$u(fg) \vee \textstyle\bigvee_{i>i_0} u(a_i b_{j_0}) \vee \bigvee_{j>j_0} u(a_{i_0} b_j).$$

By induction on i_0, j_0, $u(a_i b_{j_0}) \leqslant u(fg)$, $u(a_{i_0} b_j) \leqslant u(fg)$.
Hence $u(a_{i_0} b_{j_0}) \leqslant u(fg)$.
5. In this case $a_i b_j \in \mathrm{D}_{\mathbf{A}}(c_k, k = 0, \ldots)$, which is the usual Gauss-Joyal lemma.

Problem 4. *(pp-ring closure of a commutative ring)*
Preliminary remark: if in a ring $\mathbf{A}$, $\mathrm{Ann}(a) = \langle e'_a \rangle$ with e'_a idempotent, then e'_a is the unique e' such that

$$e'a = 0, \quad e' + a \text{ is regular} \quad \text{and} \quad e' \text{ is idempotent.}$$

Indeed, $e' = e'e'_a$ (because $e'a = 0$) and $(e' + a)e' = (e' + a)e'_a$ $(= e')$ hence $e' = e'_a$.
1. Let $\mathbf{A}$, $\mathbf{B}$ be pp-rings and a pp-ring morphism $\varphi : \mathbf{A} \to \mathbf{B}$.
1a. If $a \in \mathbf{A}$ is regular, $e_a = 1$ so $e_{\varphi(a)} = 1$ therefore $\varphi(a)$ is regular. Conversely,

let $\psi : \mathbf{A} \to \mathbf{B}$ be a ring homomorphism which transforms every regular element into a regular element. Let $a \in \mathbf{A}$, $b = \psi(a)$ and $f = \psi(1 - e_a)$.
Then $fb = \psi\big((1 - e_a)a\big) = 0$, $f + b = \psi(1 - e_a + a)$ is regular and $f^2 = f$, and so $f = 1 - e_b$.
1b. Suppose $\varphi(x) = 0$, then $e_{\varphi(x)} = 0$, i.e. $\varphi(e_x) = 0$. Therefore if $\varphi|_{\mathbb{B}(\mathbf{A})}$ is injective, we obtain $e_x = 0$, i.e. $x = 0$.
1c. We consider the unique homomorphism $\rho : \mathbb{Z} \to \prod_{n>0} \mathbb{Z}/\langle 2^n \rangle$. Then ρ is injective but $\rho(2)$ is not regular.
1d. The homomorphism preserves the quasi-inverses, therefore also the associated idempotents because $e_a = aa^\bullet$ if $a^\bullet$ is the quasi-inverse of a.
1e. Results immediately from Fact IV-8.6.

2. Since $\mathbf{A}_{\mathrm{pp}}$ is reduced, there is a unique ring homomorphism $\mathbf{A}_{\mathrm{red}} \to \mathbf{A}_{\mathrm{pp}}$ which factorizes the two canonical homomorphisms $\mathbf{A} \to \mathbf{A}_{\mathrm{red}}$ and $\mathbf{A} \to \mathbf{A}_{\mathrm{pp}}$. Since $\mathbf{A}^\bullet$ is a pp-ring, there is a unique pp-ring morphism $\mathbf{A}_{\mathrm{pp}} \to \mathbf{A}^\bullet$ that factorizes the two canonical homomorphisms $\mathbf{A} \to \mathbf{A}_{\mathrm{pp}}$ and $\mathbf{A} \to \mathbf{A}^\bullet$. Since the morphism $\mathbf{A}_{\mathrm{pp}} \to \mathbf{A}^\bullet$ transforms a regular element into a regular element, and since a regular element in a (reduced or not) zero-dimensional ring is invertible, there exists a unique homomorphism $\mathrm{Frac}(\mathbf{A}_{\mathrm{pp}}) \to \mathbf{A}^\bullet$ which factorizes the two canonical homomorphisms $\mathbf{A}_{\mathrm{pp}} \to \mathrm{Frac}(\mathbf{A}_{\mathrm{pp}})$ and $\mathbf{A}_{\mathrm{pp}} \to \mathbf{A}^\bullet$.
Similarly, for every homomorphism $\mathbf{A} \to \mathbf{B}$ with $\mathbf{B}$ being reduced zero-dimensional, we first obtain a unique pp-ring morphism $\mathbf{A}_{\mathrm{pp}} \to \mathbf{B}$ (which factorizes what is needed), then a unique morphism $\mathrm{Frac}(\mathbf{A}_{\mathrm{pp}}) \to \mathbf{B}$ which factorizes the two homomorphisms $\mathbf{A} \to \mathrm{Frac}(\mathbf{A}_{\mathrm{pp}})$ and $\mathbf{A} \to \mathbf{B}$.
In other words, since $\mathrm{Frac}(\mathbf{A}_{\mathrm{pp}})$ is reduced zero-dimensional, it solves the universal problem of the reduced zero-dimensional closure for $\mathbf{A}$. Consequently the homomorphism $\mathrm{Frac}(\mathbf{A}_{\mathrm{pp}}) \to \mathbf{A}^\bullet$ that we have constructed is an isomorphism.

3. This item is copied from Lemma 4.22 which concerns the reduced zero-dimensional rings: the reader could also just about copy the proof.

4. First of all note that the natural homomorphism $\mathbf{A}_{\mathrm{red}} \to \mathbf{A}_{\mathrm{pp}}$ is injective because the homomorphism $\mathbf{A}_{\mathrm{red}} \to \mathbf{A}^\bullet$ is injective and there is factorization. We can therefore identify $\mathbf{A}_{\mathrm{red}}$ with a subring of $\mathbf{A}_{\mathrm{pp}}$, which is itself identified with a subring of $\mathrm{Frac}(\mathbf{A}_{\mathrm{pp}})$ that we identify with $\mathbf{A}^\bullet$. In this framework $\mathbf{A}_{\mathrm{pp}}$ necessarily contains $\mathbf{A}_{\mathrm{red}}$ while the elements $e_x = xx^\bullet$ for all $x \in \mathbf{A}_{\mathrm{red}}$ since the morphism $\mathbf{A}_{\mathrm{pp}} \to \mathbf{A}^\bullet$ is a pp-ring and is injective.
Let $\mathbf{B}$ be the subring of $\mathbf{A}^\bullet$ generated by $\mathbf{A}_{\mathrm{red}}$ and the idempotents $(e_x)_{x \in \mathbf{A}_{\mathrm{red}}}$. It remains to see that the inclusion $\mathbf{B} \subseteq \mathbf{A}_{\mathrm{pp}}$ is an equality.
It is clear that $\mathrm{Frac}(\mathbf{B}) = \mathrm{Frac}(\mathbf{A}_{\mathrm{pp}})$. On the one hand, as $\mathbf{B}$ is a pp-ring, the injection $\mathbf{A}_{\mathrm{red}} \to \mathbf{B}$ provides a (unique) pp-ring morphism $\varphi : \mathbf{A}_{\mathrm{pp}} \to \mathbf{B}$ such that $\varphi(a) = a$ for every $a \in \mathbf{A}_{\mathrm{red}}$. Since the morphism is a pp-ring morphism, we deduce that $\varphi(e_a) = e_a$ for every $a \in \mathbf{A}_{\mathrm{red}}$, then $\varphi(b) = b$ for all $b \in \mathbf{B}$. Let $x \in \mathbf{A}_{\mathrm{pp}}$; we want to show that $x \in \mathbf{B}$; as $x \in \mathrm{Frac}(\mathbf{B})$, there exists a regular $b \in \mathbf{B}$ such that $bx \in \mathbf{B}$ therefore $\varphi(bx) = bx$ i.e. $b\varphi(x) = bx$; as b is regular in $\mathbf{B}$, it is regular in $\mathrm{Frac}(\mathbf{B})$, a fortiori in $\mathbf{A}_{\mathrm{pp}}$, so $x = \varphi(x) \in \mathbf{B}$.

5a and *5b.* Easy.

5c. Since $a_j = a_je_j$, we have, for $j \in I$, $a_j \in \langle e_i, i \in I\rangle_{\mathbf{B}} = \langle e\rangle_{\mathbf{B}}$ with e the idempotent $1 - \prod_{i\in I}(1-e_i)$. But in a reduced ring, every idempotent generates a radical ideal

$$b^m \in \langle e\rangle \Rightarrow b^m(1-e) = 0 \Rightarrow b(1-e) = 0 \Rightarrow b = be \in \langle e\rangle\,.$$

Therefore $\mathrm{D}_{\mathbf{A}}(a_i, i \in I) \subseteq \langle e_i, i \in I\rangle_{\mathbf{B}}$.
Let us now show that $\mathbf{A} \cap \langle e_i, \in I\rangle_{\mathbf{C}} \subseteq \mathrm{D}_{\mathbf{A}}(a_i, i \in I)$. Let $x \in \mathbf{A} \cap \langle e_i, \in I\rangle_{\mathbf{C}}$; by returning to the initial definition of $\mathbf{C}$, we have $x \in \langle a_iT_i, i \in I\rangle_{\mathbf{A}[\underline{T}]} + \mathfrak{c}$. Let us work on the reduced ring $\mathbf{A}' = \mathbf{A}/\mathrm{D}_{\mathbf{A}}(a_i, i \in I)$; we then have

$$\overline{x} \in \mathrm{D}_{\mathbf{A}'[\underline{T}]}(a_kT_k^2 - T_k, a_k^2T_k - a_k, k \in [\![1..n]\!]).$$

Since $\mathbf{A}' \to \mathbf{A}'[\overline{a}_1^\bullet, \dots, \overline{a}_n^\bullet]$ is injective, we have $\overline{x} = 0$ i.e. $x \in \mathrm{D}_{\mathbf{A}}(a_i, i \in I)$.

5d. Let π be the product $\prod_{j\notin I} a_j$. Let $x \in \mathbf{A} \cap \langle 1 - e_I\rangle_{\mathbf{B}}$; since $\pi(1-e_j) = 0$ for $j \notin I$, we have $\pi x \in \langle e_i, i \in I\rangle_{\mathbf{B}}$, so, by *5c)*, $\pi x \in \mathrm{D}_{\mathbf{A}}(a_i, i \in I)$, i.e. $x \in \mathfrak{a}'_I = (\mathrm{D}_{\mathbf{A}}(a_i, i \in I) : \pi)$.
Conversely, let $x \in \mathfrak{a}'_I$; we write $x = \pi'x + (1-\pi')x$ with $\pi' = \prod_{j\notin I} e_j$. We have $1 - \pi' \in \langle 1 - e_j, j \notin I\rangle$. As for $\pi'x$, we notice that in $\mathbf{C}$, $\langle e_j\rangle_{\mathbf{C}} = \langle a_j\rangle_{\mathbf{C}}$, so $\pi'x \in \langle \pi x\rangle_{\mathbf{C}} \subseteq \mathrm{D}_{\mathbf{C}}(a_i, i \in I) \subseteq \langle e_i, i \in I\rangle_{\mathbf{C}}$.
Recap: $x \in \langle (e_i)_{i\in I}, (1-e_j)_{j\notin I}\rangle_{\mathbf{C}} = \langle 1 - e_I\rangle_{\mathbf{C}}$.
But $\mathbf{A} \cap \langle 1 - e_I\rangle_{\mathbf{C}} = \mathbf{A} \cap \langle 1 - e_I\rangle_{\mathbf{B}}$, so $x \in \langle 1 - e_I\rangle_{\mathbf{B}}$.
Finally, $\mathbf{B}$ is isomorphic to the product of $\mathbf{B}\big/\langle 1 - e_I\rangle_{\mathbf{B}}$ and $\mathbf{B}\big/\langle 1 - e_I\rangle_{\mathbf{B}} \simeq \mathbf{A}/\mathfrak{a}'_I$.

5e. Take $s = \sum_I e_I \prod_{j\notin I} a_j = \sum_I \prod_{i\in I}(1-e_i)\prod_{j\notin I} a_j$: s is the unique element of $\mathbf{B}$ which is equal to $\prod_{j\notin I} a_j$ over the component $e_I = 1$.

6. In the isomorphism $\mathbf{A}[e_a] \simeq \mathbf{A}/\mathrm{Ann}_{\mathbf{A}}(a) \times \mathbf{A}/\mathrm{D}_{\mathbf{A}}(a)$, we have $e_a = (1,0)$ and so $(\overline{x}, \overline{y}) = xe_a + y(1-e_a)$. We then consider the map

$$\mathbf{A} \times \mathbf{A} \to \mathbf{D},\ (x,y) \mapsto \varphi(x)e_b + \varphi(y)(1-e_b).$$

It is a ring morphism and since $\mathbf{D}$ is reduced, it passes to the quotient modulo $\mathrm{Ann}_{\mathbf{A}}(a) \times \mathrm{D}_{\mathbf{A}}(a)$.
Let us now compare $\mathbf{A}_{[a,b]}$ and $(\mathbf{A}_{[a]})_{[b]}$. We find

$$\begin{aligned} \mathbf{A}_{[a,b]} &\simeq \mathbf{A}/(0:ab) \times \mathbf{A}/(\mathrm{D}(b):a) \times \mathbf{A}/(\mathrm{D}(a):b) \times \mathbf{A}/\mathrm{D}(a,b)\ , \\ (\mathbf{A}_{[a]})_{[b]} &\simeq \mathbf{A}/(0:ab) \times \mathbf{A}\big/\mathrm{D}\big((0:a) + \langle b\rangle\,\big) \times \mathbf{A}/(\mathrm{D}(a):b) \times \mathbf{A}/\mathrm{D}(a,b)\ . \end{aligned}$$

Finally, note that $\mathrm{D}\big((0:a) + \langle b\rangle\,\big)$ is contained in $(\mathrm{D}(b):a)$ but that the inclusion can be strict. Take for example $\mathbf{A} = \mathbb{Z}$, $a = 2p$, $b = 2q$ where p and q are two distinct odd primes. We use $(x:y) = x/\gcd(x,y)$ for x, $y \in \mathbb{Z}$.
Then $\mathbb{Z}_{[a,b]} \simeq \mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, but $(\mathbb{Z}_{[a]})_{[b]} \simeq \mathbb{Z} \times \mathbb{Z}/2q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. In the first ring, $\mathrm{Ann}(a)$ is generated by $(0,0,1,1)$. In the second (the first ring is a quotient), $\mathrm{Ann}(a)$ generated by the idempotent $(0,q,1,1)$.

8. Recall (Exercise 10) that a prime ideal $\mathfrak{p}$ of a ring $\mathbf{A}$ is minimal if and only if for all $x \in \mathfrak{p}$, there exists an $s \in \mathbf{A} \setminus \mathfrak{p}$ such that $sx^n = 0$ for a certain n (if $\mathbf{A}$ is reduced, we can take $n = 1$).
First, a minimal prime ideal of $\mathbf{A}$ remains a strict prime ideal in $\mathrm{Frac}(\mathbf{A})$ (this does not use the fact that $\mathbf{A}$ is a pp-ring), i.e. $\mathfrak{p} \cap \mathrm{Reg}(\mathbf{A}) = \emptyset$: if $x \in \mathfrak{p}$, there exist $s \notin \mathfrak{p}$ and $n \in \mathbb{N}$ such that $sx^n = 0$, which proves that $x \notin \mathrm{Reg}(\mathbf{A})$.
Conversely, for $\mathfrak{q}$ a prime ideal of $\mathrm{Frac}(\mathbf{A})$, let us prove that $\mathfrak{p} = \mathfrak{q} \cap \mathbf{A}$ is a minimal

prime ideal of $\mathbf{A}$. Let $x \in \mathfrak{p}$; then $x + 1 - e_x$ is regular in $\mathbf{A}$, so invertible in $\mathrm{Frac}(\mathbf{A})$, therefore $1 - e_x \notin \mathfrak{p}$. Then $x(1 - e_x) = xe_x(1 - e_x) = 0$: we have found $s = 1 - e_x \notin \mathfrak{p}$ such that $sx = 0$.

9. By Exercise 9, the injection $\mathbf{A} \to \mathbf{A}^\bullet$ induces a bijection $\mathsf{Spec}\,\mathbf{A}^\bullet \to \mathsf{Spec}\,\mathbf{A}$; but $\mathbf{A}^\bullet = \mathrm{Frac}(\mathbf{A}_{\mathrm{pp}})$ and $\mathbf{A}_{\mathrm{pp}}$ is a pp-ring.
Therefore, by item *8* applied to $\mathbf{A}_{\mathrm{pp}}$, $\mathsf{Spec}\,\mathbf{A}^\bullet$ is identified with $\mathsf{Min}(\mathbf{A}_{\mathrm{pp}})$, hence the natural bijection between $\mathsf{Spec}\,\mathbf{A}$ and $\mathsf{Min}(\mathbf{A}_{\mathrm{pp}})$.

Bibliographic comments

Some reference books on the study of lattices are [Birkhoff], [Grätzer] and [Johnstone]. In [Johnstone] the focus is essentially on distributive lattices, which are the objects that primarily interest us. This book presents the theory of locales. The notion of a *locale* is a generalization of that of a topological space. The structure of a locale is given by the distributive lattice of its open sets, but the open sets are no longer necessarily sets of points. This is the reason why a locale is sometimes called a *pointless topological space* [114, Johnstone]. The author generally tries to give constructive proofs and explicitly signals the theorems whose proof uses the axiom of choice.

In abstract algebra, spectral spaces are omnipresent, foremost among which we include the Zariski spectrum of a commutative ring. From the constructive point of view they are very peculiar locales which "lack points." We will quickly present this notion in Section 1 of Chapter XIII devoted to the Krull dimension.

An elegant proof of Theorem 3.16 (if $\mathbf{A}$ is a GCD-domain the same goes for $\mathbf{A}[X]$) is found in [MRR, th. IV.4.7].

The origin of entailment relations is found in the Gentzen sequent calculus, which is the first to place a focus on the cut (the rule (T)). The link with distributive lattices has been highlighted in [29, 52, Coquand&al.]. The fundamental theorem of the entailment relations 5.3 (page 657) is found in [29]. In fact, its first appearance seems to date back to the article by Paul Lorenzen [135], which studies the relations between formal logic and distributive lattices.

The dynamic method is clearly presented, for the first time it seems, in the article by Lorenzen [136], which uses the equivalent of the closed covering principle 2.10. See on this subject articles [46] and [47].

We find the terminology of an *implicative lattice* in [Curry] and that of a *Heyting algebra* in [Johnstone].

A basic book for the theory of l-groups and of (not necessarily commutative) lattice-group rings is [Bigard, Keimel & Wolfenstein]. We have said that a guiding idea in the theory of *l*-groups is that an *l*-group behaves in computations like a product of totally ordered groups. This is translated in classical mathematics by the representation theorem which affirms that every (Abelian) *l*-group is isomorphic to an *l*-subgroup of a product of totally ordered groups (Theorem 4.1.8 in the cited book).

The *l*-groups that are $\mathbb{Q}$-vector spaces somewhat constitute the purely algebraic version of the theory of Riesz spaces. Every good book on Riesz spaces starts by developing the purely algebraic properties of these spaces, which are copied (with very similar, if not identical proofs) from the theory of (Abelian) *l*-groups. See for example [Zaanen].

In the exercises of Bourbaki (Commutative algebra, Diviseurs) an integral Bézout ring is called a *anneau bezoutien*, a GCD-domain is called a *anneau pseudo-bezoutien*, and a Prüfer domain is called a *anneau prüferien*.

Chapter XII

Prüfer and Dedekind rings

Contents

Introduction

The usual definitions of Dedekind ring do not lend themselves to an algorithmic treatment.

First, the notion of Noetherianity is delicate (from the algorithmic point of view). Secondly, the questions of factorization generally demand extremely strong hypotheses. For example, even if $\mathbf{K}$ is a quite explicit discrete field, there is no general method (valid over all discrete fields) for factorizing the polynomials of $\mathbf{K}[X]$.

Thus, an essential aspect of the theory of Dedekind rings, namely that the integral closure of a Dedekind ring in a finite extension of its quotient field remains a Dedekind ring, no longer works in full generality (from an algorithmic point of view) if we require the complete factorization of the ideals (see for example the treatment of this question in [MRR]).

Moreover, even if a total factorization is theoretically feasible (in the rings of integers of number fields for example), we very quickly encounter problems of a prohibitive complexity such as that of factorizing the discriminant (an impossible task in practice if it has several hundred digits). Also Lenstra and Buchmann, [25], proposed to work in the rings of integers without having a $\mathbb{Z}$-basis at our disposal. An important algorithmic fact is that it is always easy to obtain a *partial factorization* for a family of natural numbers, that is a decomposition of each of these numbers into a product of factors taken in a family of pairwise coprime numbers (see [15, Bernstein], and [16, Bernstein] for an implementation with the ideals of number fields, see also Problem II-2 (page 71)).

A goal of this chapter is to show the general validity of such a point of view and to propose tools in this framework.

A crucial and simplifying role in the theory is played by the arithmetic rings (in accordance with an intuition of Gian Carlo Rota [169]), that are the rings in which the lattice of ideals is distributive, and by the *principal localization matrices*, which are the matrices that explicate the computational machinery of the locally principal finitely generated ideals, in an essentially equivalent way to what Dedekind [57] estimated to be a fundamental property of rings of integers in the number fields (see [4, Avigad] and item *3′*. of our Proposition 1.1).

The willingness to put off implementing, for as long as possible, Noetherian hypotheses has also prompted us to develop a constructive treatment of several important points of the theory in a simpler and less rigid framework than that of Dedekind rings. This is the context of rings that have the two following properties

- the finitely generated ideals are projective (this characterizes what we call a *coherent Prüfer ring*),

- the Krull dimension is at most 1.

As the reader will observe, the proofs do not become more complicated, on the contrary, by this weakening of the hypotheses.

Similarly, we have been brought to study the partial factorization Prüfer rings (in the local case, they are the valuation domains whose group of valuation is isomorphic to a subgroup of $\mathbb{Q}$). We think that these rings constitute the natural framework suggested by Buchman and Lenstra [25].

Finally, for what concerns the Dedekind rings, we have freed ourselves of the usual hypothesis of integrity (because it is hardly preserved from an algorithmic point of view by algebraic extension) and we have left the total factorization of the finitely generated ideals in the background (for the same reason) in favor of the only Noetherian character. The Noetherianity implies the partial factorization of families of finitely generated ideals, which itself implies the dimension $\leqslant 1$ in the constructive form.

1. Arithmetic rings

Recall that an arithmetic ring is a ring whose finitely generated ideals are locally principal (see Section VIII-4). We begin with a few results regarding the locally principal ideals in an arbitrary ring.

Locally principal ideals, principal localization matrix

We take up Theorem V-7.3 again (stated for the locally cyclic finitely generated modules) in the framework of locally principal ideals.

1.1. Proposition. (Locally principal ideals)
Let $x_1, \dots, x_n \in \mathbf{A}$. The following properties are equivalent.

1. *The ideal $\mathfrak{a} = \langle x_1, \dots, x_n \rangle$ is locally principal.*
2. *There exist n comaximal elements s_i of $\mathbf{A}$ such that for each i, after localization at s_i, $\mathfrak{a}$ becomes principal, generated by x_i.*
3. *There exists a principal localization matrix for $(x_1, \dots, x_n)$, that is a matrix $A = (a_{ij}) \in \mathbb{M}_n(\mathbf{A})$ that satisfies*

$$\left\{ \begin{array}{rcll} \sum a_{ii} & = & 1 & \\ a_{\ell j} x_i & = & a_{\ell i} x_j & \quad \forall i, j, \ell \in [\![1..n]\!] \end{array} \right. \tag{1}$$

   Note: The last line is read as follows: for each row ℓ, the minors of order 2 of the matrix $\begin{bmatrix} a_{\ell 1} & \cdots & a_{\ell n} \\ x_1 & \cdots & x_n \end{bmatrix}$ *are null.*

4. $\bigwedge^2_{\mathbf{A}}(\mathfrak{a}) = 0$.
5. $\mathcal{F}_1(\mathfrak{a}) = \langle 1 \rangle$.

In the case where one of the x_k's is regular the existence of the matrix A in item 3 has the same meaning as the following item.

3′. There exist $\gamma_1, \ldots, \gamma_n$ in $\operatorname{Frac}\mathbf{A}$ *such that $\sum_i \gamma_i x_i = 1$ and each of the $\gamma_i x_j$'s is in* $\mathbf{A}$ (Dedekind formulation).

D The only new thing is the formulation *3′*. If for example $x_1 \in \operatorname{Reg}(\mathbf{A})$ and if we dispose of A, let $\gamma_i = a_{i1}/x_1$. Conversely, if we dispose of the γ_i's, let $a_{ij} = \gamma_i x_j$. □

The following proposition takes up and adds details to Proposition V-7.4. The results could be obtained more directly, by using the Dedekind formulation, when one of the x_k's is regular.

1.2. Proposition. *Let $\mathfrak{a} = \langle x_1, \ldots, x_n\rangle$ be a locally principal ideal of* $\mathbf{A}$ *and $A = (a_{ij})$ be a principal localization matrix for $(x_1, \ldots, x_n)$. We have the following results.*

1. $[\, x_1 \ \cdots \ x_n \,]\, A = [\, x_1 \ \cdots \ x_n \,]$.

2. Each x_i annihilates $\mathcal{D}_2(A)$ and $A^2 - A$.

3. Let $\mathbf{A}_i = \mathbf{A}[1/a_{ii}]$, we have $\mathfrak{a} =_{\mathbf{A}_i} \langle x_i\rangle$.

4. $\langle x_1, \ldots, x_n\rangle \langle a_{1j}, \ldots, a_{nj}\rangle = \langle x_j\rangle$.

5. More generally, if $a = \sum \alpha_i x_i$ and ${}^{\mathrm{t}}[\, y_1 \ \cdots \ y_n \,] = A \ {}^{\mathrm{t}}[\, \alpha_1 \ \cdots \ \alpha_n \,]$, then
$$\langle x_1, \ldots, x_n\rangle \langle y_1, \ldots, y_n\rangle = \langle a\rangle \,.$$
In addition, if $\operatorname{Ann}(\mathfrak{a}) = 0$, *the matrix ${}^{\mathrm{t}}\!A$ is a principal localization matrix for $(y_1, \ldots, y_n)$.*

6. In particular, if $\sum \alpha_i x_i = 0$ and ${}^{\mathrm{t}}[\, y_1 \ \cdots \ y_n \,] = A \ {}^{\mathrm{t}}[\, \alpha_1 \ \cdots \ \alpha_n \,]$, then
$$\langle x_1, \ldots, x_n\rangle \langle y_1, \ldots, y_n\rangle = 0.$$

7. Consider the linear form $\underline{x} : (\alpha_i) \mapsto \sum_i \alpha_i x_i$ associated with $(x_1, \ldots, x_n)$, let $\mathfrak{N} =$ $\operatorname{Ann} \langle x_1, \ldots, x_n\rangle$ *and $\mathfrak{N}^{(n)}$ be the cartesian product*
$$\{\, (\nu_1, \ldots, \nu_n) \,|\, \nu_i \in \mathfrak{N},\ i \in \llbracket 1..n\rrbracket \,\} \subseteq \mathbf{A}^n.$$
Then $\operatorname{Ker}\underline{x} = \operatorname{Im}(\mathrm{I}_n - A) + \mathfrak{N}^{(n)}$.

8. For $i \in \llbracket 1..n-1\rrbracket$ the intersection $\langle x_1, \ldots, x_i\rangle \cap \langle x_{i+1}, \ldots, x_n\rangle$ is the ideal generated by the n coefficients of the row vector
$$[\, x_1 \ \cdots \ x_i \, 0 \ \cdots \ 0 \,](\mathrm{I}_n - A) = -[\, 0 \ \cdots \ 0 \, x_{i+1} \ \cdots \ x_n \,](\mathrm{I}_n - A).$$

D Item *3* is clear, items *4* and *6* are special cases of the first part of item *5*. Items *1*, *2* and the first part of item *5* have been shown for the cyclic localization matrices.

5. It remains to show that, when $\operatorname{Ann}(\mathfrak{a}) = 0$, ${}^{\mathrm{t}}\!A$ is a principal localization matrix for $(y_1, \ldots, y_n)$. Indeed, on the one hand $\operatorname{Tr}({}^{\mathrm{t}}\!A) = 1$, and on the other hand, since $\mathfrak{a}\mathcal{D}_2(A) = 0$, we have $\mathcal{D}_2(A) = 0$, or $A_i \wedge A_j = 0$, A_i being the column i of A. As the vector $y := {}^{\mathrm{t}}[\, y_1 \ \cdots \ y_n \,]$ is in $\operatorname{Im} A$, we also have $y \wedge A_j = 0$, which translates that ${}^{\mathrm{t}}\!A$ is a principal localization matrix for $(y_1, \ldots, y_n)$.

7. The inclusion $\mathrm{Ker}\,\underline{x} \subseteq \mathrm{Im}(\mathrm{I}_n - A) + \mathfrak{N}^{(n)}$ results from item *6* and the reverse inclusion of item *1.*

8. Results from *7* by noticing that taking an element a of the ideal $\mathfrak{b} = \langle x_1, \ldots, x_i \rangle \cap \langle x_{i+1}, \ldots, x_n \rangle$ is the same as taking an element

$$(\alpha_1, \ldots, \alpha_n) \in \mathrm{Ker}\,\underline{x} \;:\; a = \alpha_1 x_1 + \cdots + \alpha_i x_i = -\alpha_{i+1} x_{i+1} - \cdots - \alpha_n x_n.$$

Thus, $\mathfrak{b}$ is generated by the coefficients of $[\,x_1 \;\cdots\; x_i \; 0 \;\cdots\; 0\,](\mathrm{I}_n - A)$. □

1.3. Corollary. *Let $\mathfrak{a} = \langle x_1, \ldots, x_n \rangle$ be a finitely generated ideal of $\mathbf{A}$.*

1. *If $\mathfrak{a}$ is locally principal, for every finitely generated ideal $\mathfrak{c}$ contained in $\mathfrak{a}$, there exists a finitely generated ideal $\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{b} = \mathfrak{c}$.*
2. *Conversely, if $n = 2$ and if there exists some ideal $\mathfrak{b}$ such that $\langle x_1 \rangle = \mathfrak{a}\mathfrak{b}$, then $\mathfrak{a}$ is locally principal.*
3. *The ideal $\mathfrak{a}$ is a projective module of constant rank 1 if and only if it is locally principal and faithful. In this case, if A is a principal localization matrix for $(x_1, \ldots, x_n)$, it is a projection matrix of rank 1 and $\mathfrak{a} \simeq \mathrm{Im}\,A$.*
4. *The ideal $\mathfrak{a}$ is invertible if and only if it is locally principal and contains a regular element.*

D *1*, *3*, *4.* See Lemma V-7.7, which gives slightly more general results. These items also result from the previous proposition, items *5* and *7.*
2. In $\mathfrak{b}$ we must have u_1 and u_2 such that on the one hand $u_1 x_1 + u_2 x_2 = x_1$, so $(1 - u_1)x_1 = u_2 x_2$, and on the other hand $u_1 x_2 \in \langle x_1 \rangle$. When we invert the element u_1, x_1 generates $\mathfrak{a}$, and when we invert $1 - u_1$, it is x_2 that generates $\mathfrak{a}$. □

First properties

Recall that a ring is coherent if and only if on the one hand the intersection of two finitely generated ideals is a finitely generated ideal, and on the other hand the annihilator of every element is finitely generated (Theorem II-3.4). Consequently, by using item *8* of Proposition 1.2, we obtain

1.4. Fact. *In an arithmetic ring the intersection of two finitely generated ideals is a finitely generated ideal. An arithmetic ring is coherent if and only if the annihilator of every element is finitely generated.*

Every quotient and every localized ring of an arithmetic ring is an arithmetic ring.

In a strongly discrete ring, the divisibility relation is explicit. We have the (remarkable) converse for arithmetic rings.

1.5. Proposition. *An arithmetic ring is strongly discrete if and only if the divisibility relation is explicit. More precisely, in an arbitrary ring, if an ideal $\langle b_1, \dots, b_n \rangle$ is locally principal and if $A = (a_{ij})$ is a principal localization matrix for $(b_1, \dots, b_n)$, we have the equivalence*

$$c \in \langle b_1, \dots, b_n \rangle \iff a_{jj}c \in \langle b_j \rangle \text{ for every } j.$$

In particular, we have $1 \in \langle b_1, \dots, b_n \rangle$ if and only if for all j, b_j divides a_{jj}.

D If $a_{jj}c = u_jb_j$, then $c = \sum_j u_jb_j$. Conversely, if $c \in \langle b_1, \dots, b_n \rangle$, then for each j we get

$$a_{jj}c \in \langle a_{1j}, \dots, a_{nj} \rangle \langle b_1, \dots, b_n \rangle = \langle b_j \rangle .$$

□

In the following theorem we give a few possible characterizations of arithmetic rings. The simplest characterization of arithmetic rings is no doubt the one given in item *1b*. Since an ideal $\langle x, y \rangle$ is locally principal if and only if there is a principal localization matrix for (x, y), condition *1b* means

$$\boxed{\forall x, y \in \mathbf{A} \;\; \exists u, a, b \in \mathbf{A}, \qquad ux = ay, \; (1-u)y = bx,}$$

which is also exactly what item *2c* says.

1.6. Theorem. (Characterizations of arithmetic rings)
For a ring $\mathbf{A}$ the following properties are equivalent.

1a. $\mathbf{A}$ *is arithmetic (every finitely generated ideal is locally principal).*

1b. Every ideal $\mathfrak{a} = \langle x_1, x_2 \rangle$ is locally principal.

2a. For all finitely generated ideals $\mathfrak{b} \subseteq \mathfrak{a}$, there exists some finitely generated ideal $\mathfrak{c}$ such that $\mathfrak{a}\mathfrak{c} = \mathfrak{b}$.

2b. For every ideal $\mathfrak{a} = \langle x_1, x_2 \rangle$, there exists some finitely generated ideal $\mathfrak{c}$ such that $\mathfrak{a}\mathfrak{c} = \langle x_1 \rangle$.

2c. $\forall x_1, x_2 \in \mathbf{A}$ *the following system of linear equations $BX = C$ admits a solution*

$$[\,B \mid C\,] = \left[\begin{array}{ccc|c} x_1 & x_2 & 0 & x_1 \\ x_2 & 0 & x_1 & 0 \end{array} \right] \tag{2}$$

2d. $\forall x_1, x_2 \in \mathbf{A}$ *there exists a $u \in \mathbf{A}$ such that*

$$\langle x_1 \rangle \;\cap\; \langle x_2 \rangle \;=\; \langle (1-u)x_1, ux_2 \rangle .$$

3. For all finitely generated ideals $\mathfrak{a}$ and $\mathfrak{b}$, the following short exact sequence is split

$$0 \longrightarrow \mathbf{A}/(\mathfrak{a} \cap \mathfrak{b}) \xrightarrow{\delta} \mathbf{A}/\mathfrak{a} \times \mathbf{A}/\mathfrak{b} \xrightarrow{\sigma} \mathbf{A}/(\mathfrak{a} + \mathfrak{b}) \longrightarrow 0$$

where $\delta : \overline{x}_{\mathfrak{a}\cap\mathfrak{b}} \mapsto (\overline{x}_{\mathfrak{a}}, \overline{x}_{\mathfrak{b}})$ and $\sigma : (\overline{y}_{\mathfrak{a}}, \overline{z}_{\mathfrak{b}}) \mapsto \overline{(y-z)}_{\mathfrak{a}+\mathfrak{b}}$.

4. For all finitely generated ideals $\mathfrak{a}$ and $\mathfrak{b}$, $(\mathfrak{a} : \mathfrak{b}) + (\mathfrak{b} : \mathfrak{a}) = \langle 1 \rangle$.

5. (Chinese remainder theorem, arithmetic form)
If $(\mathfrak{b}_k)_{k=1,\ldots,n}$ *is a finite family of ideals of* $\mathbf{A}$ *and* $(x_k)_{k=1,\ldots,n}$ *is a family of elements of* $\mathbf{A}$ *satisfying* $x_k \equiv x_\ell \mod \mathfrak{b}_k + \mathfrak{b}_\ell$ *for all* k, ℓ, *then there exists some* $x \in \mathbf{A}$ *such that* $x \equiv x_k \mod \mathfrak{b}_k$ *for all* k.
6. *The lattice of ideals of* $\mathbf{A}$ *is a distributive lattice.*

D *1b* ⇒ *1a.* If we have a finitely generated ideal with n generators, successive localizations (each time at comaximal elements) make it principal.
Consider item *2a.* Let $\mathfrak{a} = \langle x_1, \ldots, x_n \rangle$ and $\mathfrak{b} = \langle y_1, \ldots, y_m \rangle$. If $\mathfrak{c}$ exists, for each $j = 1, \ldots, m$ there exist elements $a_{i,j} \in \mathfrak{c}$ such that

$$\textstyle\sum_i a_{i,j} x_i = y_j.$$

Moreover, for each i, i', j we must have $a_{i,j} x_{i'} \in \mathfrak{b}$, which is expressed by the existence of elements $b_{i,i',j,j'} \in \mathbf{A}$ satisfying

$$\textstyle\sum_{j'} b_{i,i',j,j'} y_{j'} = a_{i,j} x_{i'}.$$

Conversely, if we can find some elements $a_{i,j}$ and $b_{i,i',j,j'} \in \mathbf{A}$ satisfying the linear equations above (in which the x_i's and y_j's are coefficients), then the ideal $\mathfrak{c}$ generated by the $a_{i,j}$'s indeed satisfies $\mathfrak{a}\mathfrak{c} = \mathfrak{b}$. Thus, finding $\mathfrak{c}$ comes down to solving a system of linear equations.
It follows that to prove *1a* ⇒ *2a* we can use suitable localizations: the two ideals $\mathfrak{a}$ and $\mathfrak{b}$ become principal, one being included in the other, in which case $\mathfrak{c}$ is obvious.

We easily verify that the properties *1b*, *2b*, *2c* and *2d* are equivalent (taking into account the previous remark for *1b*).

To show that *1a* implies *3*, *4*, *5* and *6*, note that each of the properties considered can be interpreted as the existence of a solution of a certain system of linear equations, and that this solution is obvious when the ideals that intervene are principal and totally ordered for the inclusion.

It remains to show the converses.

3 ⇒ *2c* and *4* ⇒ *2c*.
Consider in *3* or *4* the case where $\mathfrak{a} = \langle x_1 \rangle$ and $\mathfrak{b} = \langle x_2 \rangle$.

5 ⇒ *1b.* Let a, $b \in \mathbf{A}$. Let

$$c = a + b,\ \mathfrak{b}_1 = \langle a \rangle,\ \mathfrak{b}_2 = \langle b \rangle,\ \mathfrak{b}_3 = \langle c \rangle,\ x_1 = c,\ x_2 = a \text{ and } x_3 = b.$$

We have $\mathfrak{b}_1 + \mathfrak{b}_2 = \mathfrak{b}_1 + \mathfrak{b}_3 = \mathfrak{b}_3 + \mathfrak{b}_2 = \langle a, b \rangle$.
The congruences $x_i \equiv x_k \mod \mathfrak{b}_i + \mathfrak{b}_k$ are satisfied, so there exist u, v, w in $\mathbf{A}$ such that

$$c + ua = a + vb = b + wc,$$

hence

$$wb = (1 + u - w)a,\ (1 - w)a = (1 + w - v)b.$$

Therefore the ideal $\langle a, b \rangle$ is locally principal.

6 ⇒ *1b.* Take the property of distributivity $\mathfrak{a} + (\mathfrak{b} \cap \mathfrak{c}) = (\mathfrak{a} + \mathfrak{b}) \cap (\mathfrak{a} + \mathfrak{c})$, with $\mathfrak{a} = \langle x \rangle$, $\mathfrak{b} = \langle y \rangle$ and $\mathfrak{c} = \langle x + y \rangle$. We therefore have $y \in \langle x \rangle + (\langle y \rangle \cap \langle x + y \rangle)$, that is, there exist a, b, c such that $y = ax + by$, $by = c(x + y)$. Hence $cx = (b - c)y$ and $(1 - c)y = (a + c)x$. Thus, $\langle x, y\rangle$ is locally principal. □

The isomorphism $\mathbf{A}/\mathfrak{a} \oplus \mathbf{A}/\mathfrak{b} \simeq \mathbf{A}/(\mathfrak{a} + \mathfrak{b}) \oplus \mathbf{A}/(\mathfrak{a} \cap \mathfrak{b})$ which results from item *3* of the previous theorem admits the following generalization.

1.7. Corollary. *Let $(\mathfrak{a}_i)_{i\in[\![1..n]\!]}$ be a family of finitely generated ideals of an arithmetic ring $\mathbf{A}$. Let*

$$\mathfrak{b}_1 = \textstyle\sum_{k=1}^n \mathfrak{a}_k,\ \mathfrak{b}_2 = \sum_{1\leqslant j<k\leqslant n}(\mathfrak{a}_j \cap \mathfrak{a}_k),\ \dots$$
$$\mathfrak{b}_r = \textstyle\sum_{1\leqslant j_1<\cdots<j_r\leqslant n}(\mathfrak{a}_{j_1} \cap \cdots \cap \mathfrak{a}_{j_r}),\ \dots,\ \mathfrak{b}_n = \bigcap_{k=1}^n \mathfrak{a}_k.$$

Then we have $\mathfrak{b}_n \subseteq \cdots \subseteq \mathfrak{b}_1$ with an isomorphism

$$\bigoplus\nolimits_{k=1}^{n} \mathbf{A}/\mathfrak{a}_k \ \simeq\ \bigoplus\nolimits_{k=1}^{n} \mathbf{A}/\mathfrak{b}_k.$$

By bringing this result closer to Theorem IV-5.1 we obtain a complete classification of $\mathbf{A}$-modules of this type. We can also compare with Fact XI-2.12 *18.*

1.8. Corollary. *Let $\mathbf{B}$ be a faithfully flat $\mathbf{A}$-algebra. If $\mathbf{B}$ is an arithmetic ring (resp. a Prüfer ring, a coherent Prüfer ring), then so is $\mathbf{A}$.*

D Since $\mathbf{A} \subseteq \mathbf{B}$, if $\mathbf{B}$ is reduced, so is $\mathbf{A}$. Theorem VIII-6.7 *3* implies that if $\mathbf{B}$ is coherent, so is $\mathbf{A}$. It remains to show the result for an "arithmetic ring." Consider x, $y \in \mathbf{A}$. We must show that there exist u, a, $b \in \mathbf{A}$ such that $ux = ay$ and $(1 - u)y = bx$. This is actually a system of linear equations with coefficients in $\mathbf{A}$, with the unknowns (u, a, b). However, this system admits a solution in $\mathbf{B}$ and $\mathbf{B}$ is faithfully flat over $\mathbf{A}$, so it admits a solution in $\mathbf{A}$. □

Multiplicative structure of finitely generated ideals

Recall that we denote by $\mathrm{Ifr}\,\mathbf{A}$ the multiplicative monoid of finitely generated fractional ideals of an arbitrary ring $\mathbf{A}$ (see page 573).

A priori an inclusion $\mathfrak{a} \subseteq \mathfrak{b}$ in $\mathrm{Ifr}\,\mathbf{A}$ does not imply the existence of a fractional ideal $\mathfrak{c} \in \mathrm{Ifr}\,\mathbf{A}$ such that $\mathfrak{b}\mathfrak{c} = \mathfrak{a}$. But this is satisfied in the case of arithmetic rings.

For $\mathfrak{a}$ and $\mathfrak{b}$ in $\mathrm{Ifr}\,\mathbf{A}$, let $\boxed{\mathfrak{a} \div \mathfrak{b} = \{\, x \in \mathrm{Frac}\,\mathbf{A} \mid x\mathfrak{b} \subseteq \mathfrak{a} \,\}}$.

1.9. Lemma. *Let $\mathbf{A}$ be a* coherent ring*.*

1. $\mathrm{Ifr}\,\mathbf{A}$ *is a lattice with respect to inclusion relation, the supremum is given by the sum and the infimum by the intersection.*
2. $\mathrm{Ifr}\,\mathbf{A}$ *is a distributive lattice if and only if the ring is arithmetic.*
3. *Concerning invertible elements of* $\mathrm{Ifr}\,\mathbf{A}$*.*
   a. *If $\mathfrak{a}\,\mathfrak{a}' = \mathbf{A}$ in $\mathrm{Ifr}\,\mathbf{A}$, we have $\mathfrak{a}'\mathfrak{c} = \mathfrak{c} \div \mathfrak{a}$ and $\mathfrak{a}(\mathfrak{c} \div \mathfrak{a}) = \mathfrak{c}$ for all $\mathfrak{c} \in \mathrm{Ifr}\,\mathbf{A}$. In particular $\mathbf{A} \div \mathfrak{a}$ is the inverse of $\mathfrak{a}$.*

b. A fractional ideal $\frac{\mathfrak{a}}{a}$ (where $\mathfrak{a}$ is a finitely generated ideal of $\mathbf{A}$) is invertible in $\operatorname{Ifr}\mathbf{A}$ *if and only if $\mathfrak{a}$ is an invertible ideal.*

c. If $\mathfrak{a}(\mathbf{A} \div \mathfrak{a}) = \mathbf{A}$, $\mathfrak{a}$ is invertible in $\operatorname{Ifr}\mathbf{A}$.

Let $\mathfrak{a}$, $\mathfrak{b} \in$ $\operatorname{Ifr}\mathbf{A}$ *with $b \in \mathfrak{b} \cap$* $\operatorname{Reg}\mathbf{A}$. *Suppose that $\mathbf{A}$ is integrally closed in* $\operatorname{Frac}\mathbf{A}$.

4. We have $\mathfrak{a} \div \mathfrak{b} \in$ $\operatorname{Ifr}\mathbf{A}$.

5. If in addition $\mathfrak{a} \subseteq \mathfrak{b} \subseteq \mathbf{A}$, then we have $\mathfrak{a} \div \mathfrak{b} = \mathfrak{a} : \mathfrak{b}$.

D Every element of $\operatorname{Ifr}\mathbf{A}$ is written in the form $\frac{\mathfrak{a}}{a}$ for some finitely generated ideal $\mathfrak{a}$ of $\mathbf{A}$ and some $a \in \operatorname{Reg}\mathbf{A}$. In addition $\frac{\mathfrak{a}}{a}\frac{\mathfrak{b}}{b} = \frac{\mathfrak{a}\,\mathfrak{b}}{ab}$. Finally, the neutral element of the monoid is $\mathbf{A} = \langle 1 \rangle$. This shows items *1*, *2* and *3b*.

3a. We have $\mathfrak{a}\mathfrak{a}'\mathfrak{c} = \mathfrak{c}$ so $\mathfrak{a}'\mathfrak{c} \subseteq \mathfrak{c} \div \mathfrak{a}$ and $\mathfrak{c} = \mathfrak{a}\mathfrak{a}'\mathfrak{c} \subseteq \mathfrak{a}(\mathfrak{c} \div \mathfrak{a}) = \mathfrak{c}$.
If $x \in \mathfrak{c} \div \mathfrak{a}$, i.e. $x\mathfrak{a} \subseteq \mathfrak{c}$, then $x\mathbf{A} = x\mathfrak{a}\mathfrak{a}' \subseteq \mathfrak{a}'\mathfrak{c}$, so $x \in \mathfrak{a}'\mathfrak{c}$.

3c. With $\mathfrak{a} = \langle a_1, \ldots, a_k \rangle \subseteq \mathbf{A}$, suppose that $\mathfrak{a}(\mathbf{A} \div \mathfrak{a}) = \mathbf{A}$.
There exist $x_1, \ldots, x_k \in (\mathbf{A} \div \mathfrak{a})$ such that $\sum_i x_i a_i = 1$ and $x_i a_j \in \mathfrak{a}$ for all i, j. We can write the x_i's in the form $\frac{b_i}{c}$ with the same denominator c. We obtain $\sum_i a_i b_i = c$ and $a_i b_j \in \langle c \rangle$ for all i, j.
Thus by letting $\mathfrak{b} = \langle b_1, \ldots, b_k \rangle$ we obtain $\mathfrak{a}\,\mathfrak{b} = \langle c \rangle$.

5. The inclusion $\mathfrak{a} : \mathfrak{b} \subseteq \mathfrak{a} \div \mathfrak{b}$ is immediate. Conversely, if some $x \in \mathbf{K}$ satisfies $x\mathfrak{b} \subseteq \mathfrak{a}$, we need to show that $x \in \mathbf{A}$.
As $\mathbf{A}$ is integrally closed in $\operatorname{Frac}\mathbf{A}$, we apply item *3* of Fact III-8.2, with $M = \mathfrak{b}$ and $\mathbf{B} = \operatorname{Frac}\mathbf{A}$, because $x\mathfrak{b} \subseteq \mathfrak{a} \subseteq \mathfrak{b}$.

4. Results from item *5* because we are brought back to the case treated in item *5*, and in a coherent ring, the conductor $\mathfrak{a} : \mathfrak{b}$ is finitely generated if $\mathfrak{a}$ and $\mathfrak{b}$ is finitely generated. □

The following theorem says that the multiplicative structure of the monoid of invertible ideals of an arithmetic ring has all the desired properties.

Recall that by Lemma V-7.7, a finitely generated ideal is projective of constant rank 1 if and only if it is locally principal and faithful.

1.10. Theorem. *In an arithmetic ring the faithful finitely generated ideals form the non-negative submonoid of an l-group. The lattice laws are $\mathfrak{a} \wedge \mathfrak{b} = \mathfrak{a} + \mathfrak{b}$ and $\mathfrak{a} \vee \mathfrak{b} = \mathfrak{a} \cap \mathfrak{b}$.*
The invertible ideals (i.e. the finitely generated ideals that contain a regular element) form the non-negative submonoid of an l-subgroup of the previous l-group.

D This results from Corollary 1.3, from Theorem 1.6 and from Theorem XI-3.1. □

Actually the two groups coincide as soon as $\mathbf{A}$ is a pp-ring, or more generally when the projective modules of constant rank 1 over $\operatorname{Frac}\mathbf{A}$ are free (Theorem X-5.8, item *2*).

2. Integral elements and localization

The following definition generalizes Definition III-3.2 in two directions.

2.1. Definition. Let $\varphi : \mathbf{A} \to \mathbf{C}$ be a homomorphism between commutative rings and $\mathfrak{a}$ be an ideal of $\mathbf{A}$.

1. An element $x \in \mathbf{C}$ is said to be *integral* over $\mathfrak{a}$ if there exists an integer $k \geqslant 1$ such that
$$x^k = \varphi(a_1)x^{k-1} + \varphi(a_2)x^{k-2} + \cdots + \varphi(a_k) \qquad (*)$$
with each $a_h \in \mathfrak{a}^h$. In the case where $\mathbf{C} = \mathbf{A}$, this is equivalent to $\big(\mathfrak{a} + \langle x\rangle\big)^k = \mathfrak{a}\big(\mathfrak{a} + \langle x\rangle\big)^{k-1}$. We also say that the equality $(*)$ is *an integral dependence relation* of x over $\mathfrak{a}$.
2. An ideal $\mathfrak{a}$ of $\mathbf{A}$ is said to be *integrally closed* in $\mathbf{C}$ if every element of $\mathbf{C}$ integral over $\mathfrak{a}$ is in $\varphi(\mathfrak{a})$.
3. The ring $\mathbf{A}$ is said to be *normal* if every principal ideal of $\mathbf{A}$ is integrally closed in $\mathbf{A}$.

In all cases, a normal ring is integrally closed in its total ring of fractions. We have the following partial converse.

2.2. Fact. *A pp-ring is normal if and only if it is integrally closed in its total ring of fractions.*

D The proof is left to the reader. □

It is clear that every normal ring is reduced (because a nilpotent is integral over $\langle 0\rangle$). We even have a little better.

2.3. Lemma. *Every normal ring is a pf-ring. More precisely, we have for every ring* $\mathbf{A}$ *the implications 1 ⇒ 2 ⇒ 3.*

1. *Every principal ideal is integrally closed (i.e.* $\mathbf{A}$ *is normal).*
2. *For all* $x, y \in \mathbf{A}$, $x^2 \in \langle xy\rangle$ *implies* $x \in \langle y\rangle$.
3. *Every principal ideal is flat (i.e.* $\mathbf{A}$ *is a pf-ring).*

D Note that the ideal 0 is integrally closed if and only if the ring is reduced. We obviously have *1* ⇒ *2*, and *2* implies that the ring is reduced. Suppose *2* and let x, $y \in \mathbf{A}$ such that $xy = 0$. We have $x^2 = x(x + y)$ therefore $x \in \langle x + y\rangle$, e.g. $x = a(x + y)$. Then $(1 - a)x = ay$, $ay^2 = (1 - a)xy = 0$, and since the ring is reduced, $ay = 0$, then $(1 - a)x = 0$. □

2.4. Fact. *Let x be an element and* $\mathfrak{a}$ *be an ideal of* $\mathbf{A}$*. For the properties that follow we have 2 ⇒ 1, and 1 ⇒ 2 if* $\mathfrak{a}$ *is faithful and finitely generated.*

1. *The element x is integral over the ideal* $\mathfrak{a}$*.*
2. *There exists a finitely generated faithful* $\mathbf{A}$*-module M such that* $xM \subseteq \mathfrak{a}M$*.*

D (Compare with the proof of Fact III-8.2.)
2 ⇒ *1.* Consider a matrix A with coefficients in $\mathfrak{a}$ that represents $\mu_{M,x}$ (multiplication by x in M) over a finite generator set of M. If f is the characteristic polynomial of A, we have by the Cayley-Hamilton theorem $0 = f(\mu_{M,x}) = \mu_{M,f(x)}$, and since the module is faithful, $f(x) = 0$.

1 ⇒ *2.* If we have an integral dependence relation of degree k of x over $\mathfrak{a}$ we take $M = (\mathfrak{a} + \langle x \rangle)^{k-1}$. □

Let $\mathfrak{a}$ be an ideal of $\mathbf{A}$ and t be an indeterminate. Then the subalgebra $\mathbf{A}[\mathfrak{a}t]$ of $\mathbf{A}[t]$, i.e. precisely

$$\mathbf{A}[\mathfrak{a}t] = \mathbf{A} \oplus \mathfrak{a}t \oplus \mathfrak{a}^2t^2 \oplus \cdots$$

is called the *Rees algebra of the ideal* $\mathfrak{a}$.

The proof of the two following facts is left to the reader.

2.5. Fact. *Let $\mathfrak{a}$ be an ideal of $\mathbf{A}$.*

1. *For $x \in \mathbf{A}$, the following properties are equivalent.*
   a. *The element x is integral over the ideal $\mathfrak{a}$ of $\mathbf{A}$.*
   b. *The polynomial xt is integral over the subalgebra $\mathbf{A}[\mathfrak{a}t]$ of $\mathbf{A}[t]$.*
2. *More precisely*
   a. *If $\overline{\mathfrak{a}}$ is the set of elements of $\mathbf{A}$ integral over $\mathfrak{a}$, then the integral closure of $\mathbf{A}[\mathfrak{a}t]$ in $\mathbf{A}[t]$ is the subring $\mathbf{A}[\overline{\mathfrak{a}}t]$.*
   b. *In particular, $\overline{\mathfrak{a}}$ is an ideal of $\mathbf{A}$, called the* integral closure of the ideal $\mathfrak{a}$ in $\mathbf{A}$. *We denote it by $\mathrm{Icl}_{\mathbf{A}}(\mathfrak{a})$ or $\mathrm{Icl}(\mathfrak{a})$.*

2.6. Fact. *Let $\mathfrak{a}$ and $\mathfrak{b}$ be two ideals of $\mathbf{A}$.*

1. $\mathrm{Icl}\big(\mathrm{Icl}(\mathfrak{a})\big) = \mathrm{Icl}(\mathfrak{a})$.
2. $\mathfrak{a}\,\mathrm{Icl}(\mathfrak{b}) \subseteq \mathrm{Icl}(\mathfrak{a})\,\mathrm{Icl}(\mathfrak{b}) \subseteq \mathrm{Icl}(\mathfrak{a}\mathfrak{b})$.

We now revisit two important results which have been already established. Item *2c* of Kronecker's theorem III-3.3 gives precisely the following result.

2.7. Lemma. (Kronecker's theorem, reformulated)
Suppose that we have in $\mathbf{A}[T]$ an equality

$$f = \textstyle\sum_{i=0}^{n} f_i T^{n-i}, \ \ g = \sum_{j=0}^{m} g_j T^{m-j} \ \ \textit{and} \ \ h = fg = \sum_{r=0}^{m+n} h_r T^{m+n-r}.$$

Let $\mathbf{k}$ be the subring of $\mathbf{A}$ generated by the f_ig_j's. Then, each f_ig_j is integral over the ideal $\mathrm{c}_{\mathbf{k}}(h)$ of $\mathbf{k}$.

Note that item *2c* of Kronecker's theorem III-3.3 tells us precisely this: *there exists some homogeneous polynomial $R_{i,j} \in \mathbb{Z}[Y, H_0, \ldots, H_p]$ (all the variables have the same weight* 1*), monic in Y, such that*

$$R_{i,j}(f_ig_j, h_0, \ldots, h_p) = 0.$$

Here is a new version of the Lying Over (Lemma VI-3.12).

2.8. Lemma. (Lying Over, more precise form)
Let $\mathbf{A} \subseteq \mathbf{B}$ *with* $\mathbf{B}$ *integral over* $\mathbf{A}$ *and* $\mathfrak{a}$ *be an ideal of* $\mathbf{A}$*, then* $\mathfrak{a}\mathbf{B} \cap \mathbf{A} \subseteq \mathrm{D}_{\mathbf{A}}(\mathfrak{a})$*. More precisely, every element of* $\mathfrak{a}\mathbf{B}$ *is integral over* $\mathfrak{a}$*.*

D We textually rework the proof of Lemma VI-3.12. If $x \in \mathfrak{a}\mathbf{B}$, we have $x = \sum a_i b_i$, with $a_i \in \mathfrak{a}$, $b_i \in \mathbf{B}$. The b_i's generate an $\mathbf{A}$-subalgebra $\mathbf{B}'$ which is finite. Let G be a finite generator set (with ℓ elements) of the $\mathbf{A}$-module $\mathbf{B}'$. Let $B_i \in \mathbb{M}_\ell(\mathbf{A})$ be a matrix that expresses the multiplication by b_i over G. The multiplication by x is expressed by the matrix $\sum a_i B_i$, which is with coefficients in $\mathfrak{a}$. The characteristic polynomial of this matrix, which annihilates x (because $\mathbf{B}'$ is a faithful $\mathbf{A}$-module), therefore has its coefficient of degree $\ell - d$ in $\mathfrak{a}^d$.

We could also apply Fact 2.4 by taking $M = \mathbf{B}'$. Indeed, as $x \in \mathfrak{a}\mathbf{B}'$, we have $x\mathbf{B}' \subseteq \mathfrak{a}\mathbf{B}'$ and so x is integral over $\mathfrak{a}$. □

We now examine the relationships between properties of the type "integral over" and localizations.

2.9. Fact. *Let* $\mathfrak{a}$ *be an ideal of* $\mathbf{A}$*,* S *be a monoid of* $\mathbf{A}$ *and* $x \in \mathbf{A}$*.*

1. *The element* $x/1 \in \mathbf{A}_S$ *is integral over* $\mathfrak{a}_S$ *if and only if there exists a* $u \in S$ *such that* xu *is integral over* $\mathfrak{a}$ *in* $\mathbf{A}$*.*
2. *If* $\mathbf{A}$ *is normal, then so is* $\mathbf{A}_S$*.*

Let $\mathbf{B} \supseteq \mathbf{A}$ *be a faithfully flat algebra.*

3. *If* $\mathbf{A}'$ *is the integral closure of* $\mathbf{A}$ *in* $\mathbf{B}$*, then* $\mathbf{A}'_S$ *is the integral closure of* $\mathbf{A}_S$ *in* $\mathbf{B}_S$*.*
4. *If* $\mathbf{B}$ *is normal, then* $\mathbf{A}$ *is normal.*

D We only prove item *1.* In the proof we confuse an element of $\mathbf{A}$ and its image in $\mathbf{A}_S$ to alleviate the notation. If an equality $x^k = a_1 x^{k-1} + a_2 x^{k-2} + \cdots + a_k$ is performed in $\mathbf{A}_S$ with each $a_j \in (\mathfrak{a}\mathbf{A}_S)^j$, we obtain "by reducing all the fractions to the same denominator and by getting rid of the denominator" an equality

$$sx^k = b_1 x^{k-1} + b_2 x^{k-2} + \cdots + b_k$$

in $\mathbf{A}_S$ with $s \in S$ and each $b_j \in \mathfrak{a}^j$. This means an equality in $\mathbf{A}$ after multiplication by another element s' of S. We can also multiply by $s'^k s^{k-1}$ and we obtain with $u = ss'$ an equality

$$(xu)^k = c_1(xu)^{k-1} + c_2(xu)^{k-2} + \cdots + c_k$$

in $\mathbf{A}$ with each $c_j \in \mathfrak{a}^j$. □

The fact that a ring is normal is a local notion, in the following sense.

2.10. Concrete local-global principle. (Normal rings)
Let $S_1, \ldots, S_n$ be comaximal monoids of a ring $\mathbf{A}$, $x \in \mathbf{A}$ and $\mathfrak{a}$ be an ideal of $\mathbf{A}$.

1. *The element x is integral over $\mathfrak{a}$ if and only if it is integral over each of the $\mathfrak{a}_{S_i}$'s.*
2. *The ideal $\mathfrak{a}$ is integrally closed in $\mathbf{A}$ if and only if each of the $\mathfrak{a}_{S_i}$'s is integrally closed in $\mathbf{A}_{S_i}$.*
3. *The ring $\mathbf{A}$ is normal if and only if each of the $\mathbf{A}_{S_i}$'s is normal.*

D It suffices to prove item *1*, the passage from the local to the global. We obtain by applying Fact 2.9 for each $i \in [\![1..n]\!]$ some $s_i \in S_i$ such that $s_i x$ is integral over the ideal $\mathfrak{a}$ in $\mathbf{A}$. We can suppose that all the integral dependence relations have the same degree k. Let us write these integral dependence relations

$$(s_i x)^k \in \sum\nolimits_{h=1}^{k} \mathfrak{a}^h (s_i x)^{k-h}, \qquad i \in [\![1..n]\!].$$

A linear combination of these relations based on an equality $\sum_{i=1}^{n} b_i s_i^k = 1$ gives us an integral dependence relation of x over $\mathfrak{a}$ in $\mathbf{A}$. □

Note that since the property in item *1* is of finite character, Lemma II-2.12 says that the previous concrete local-global principle is equivalent in classical mathematics to the corresponding abstract local-global principle (in which the localization intervenes at any maximal ideal of $\mathbf{A}$).

3. Prüfer rings

Recall that a ring is said to be Prüfer when its ideals are flat, or if it is arithmetic and reduced, or if it is arithmetic and a pf-ring (Proposition VIII-4.4).

3.1. Proposition and definition. *We call a ring $\mathbf{A}$ satisfying one of the following equivalent properties a* valuation ring*.*

1. *$\mathbf{A}$ is a reduced local Bézout ring.*
2. *$\mathbf{A}$ is a local Prüfer ring.*
3. *$\mathbf{A}$ is reduced and satisfies: for all $a, b \in \mathbf{A}$, $a \mid b$ or $b \mid a$.*

If $\mathbf{K} = \operatorname{Frac} \mathbf{A}$, the quotient group $\mathbf{K}^\times/\mathbf{A}^\times$ is equipped with the total order relation $\overline{x} \mid \overline{y}$ defined by $\exists a \in \operatorname{Reg}(\mathbf{A})$, $y = ax$. This totally ordered group is called the valuation group *of $\mathbf{A}$.*

In addition, $\mathbf{A}$ is then without zerodivisors.

Example. Let $\mathbf{k}$ be a nontrivial discrete field and $(\Gamma, \cdot, 1_\Gamma)$ be a totally ordered discrete group. We construct a $\mathbf{k}$-algebra which is a valuation domain with Γ as its valuation group as follows. First of all consider the $\mathbf{k}$-algebra $\mathbf{A} = \mathbf{k}[\Gamma^+]$ described in Exercise IX-22.

For an element $a = \sum_i a_i\gamma_i$ of $\mathbf{A}^*$ we define $v(a)$ as the smallest γ_i that intervenes in the expression of a (we have taken the pairwise distinct γ_i's, and $a_i \neq 0$). We then prove that $v(ab) = v(a)v(b)$, which implies that $\mathbf{A}$ is integral. We also let $v(0) = +\infty$. Finally, our valuation ring is the subring $\mathbf{V} = \left\{ \frac{a}{b} \,|\, a \in \mathbf{A}, b \in \mathbf{A}^*, v(a) \geqslant v(b) \right\}$ of $\operatorname{Frac}\mathbf{A}$. ■

We now give a few other characteristic properties of Prüfer rings, which add to those that we can obtain from Theorem 1.6 for arithmetic rings.

3.2. Theorem. (Characterizations of Prüfer rings)
For some ring $\mathbf{A}$ the following properties are equivalent.

1a. $\mathbf{A}$ *is an arithmetic pf-ring (i.e. a Prüfer ring).*

1b. $\mathbf{A}$ *is a pf-ring and for all x, y there exist $n \in \mathbb{N}^*$ and an ideal $\mathfrak{b}$ such that $\langle x, y\rangle\, \mathfrak{b} = \langle x^n \rangle$.*

2a. Every submodule of a flat $\mathbf{A}$*-module is flat.*

2b. $\mathbf{A}$ *is a pf-ring and every torsion-free module is flat.*

3a. An arbitrary system of linear equations $BX = C$, as soon as the determinantal ideals of $[\,B \mid C\,]$ are equal to those of B, admits a solution.

3b. Likewise if we limit ourselves to $B \in \mathbf{A}^{2\times 3}$ and $C \in \mathbf{A}^{2\times 1}$.

4a. Every ideal is integrally closed.

4b. Every finitely generated ideal is integrally closed.

4c. Every ideal $\langle x, y\rangle$ is integrally closed.

4d. $\mathbf{A}$ *is normal and for all $x, y \in \mathbf{A}$, we have $xy \in \left\langle x^2, y^2 \right\rangle$.*

5a. If $\mathfrak{a}$, $\mathfrak{a}'$ and $\mathfrak{c}$ are finitely generated ideals, we have the implication
$$\mathfrak{a} + \mathfrak{a}' \subseteq \mathfrak{c},\ \ \mathfrak{a}\mathfrak{c} \subseteq \mathfrak{a}'\mathfrak{c} \implies \mathfrak{a} \subseteq \mathfrak{a}'.$$

5b. If $\mathfrak{a}$, $\mathfrak{a}'$ and $\mathfrak{c}$ are finitely generated ideals, we have the implication
$$\operatorname{Ann}(\mathfrak{a} + \mathfrak{a}') \supseteq \operatorname{Ann}(\mathfrak{c}),\ \ \mathfrak{a}\mathfrak{c} \subseteq \mathfrak{a}'\mathfrak{c} \implies \mathfrak{a} \subseteq \mathfrak{a}'.$$

D We first take care of equivalences between *1*, *2* and *3*.
The implications *1a* ⇒ *1b*, *2a* ⇒ *1a* and *3a* ⇒ *3b* are obvious.

1b ⇒ *1a.* Results from Lemma 3.3 below.

3b ⇒ *1a.* The ring is arithmetic because the system of linear equations (2) in Theorem 1.6 admits a solution. In addition, the ring is reduced: if $a^2 = 0$, the system of linear equations $\{\, ax = 0,\ 0x = a \,\}$ admits a solution because it corresponds to

$$B = \begin{bmatrix} a & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix},\ C = \begin{bmatrix} 0 \\ a \end{bmatrix} \quad \text{with } \mathcal{D}_2([\,B \,|\, C\,]) = \mathcal{D}_2(B) = 0\ !$$

1a ⇒ *3b.* First of all suppose that the ring is local. Therefore the ring is without zerodivisors and every finitely generated ideal is principal. Then, the result follows by Lemma 3.4 below. In the general case, the proof of the lemma can be reproduced after localizations at suitable comaximal monoids, and since this is a matter of solving a system of linear equations the basic local-global principle applies.

2b ⇒ 2a. A flat module is torsion-free (Lemma VIII-3.4). Every submodule of a torsion-free module is torsion-free, therefore flat.

1a ⇒ 2b. Let M be a torsion-free module over a Prüfer ring. We want to show that it is flat. Suppose first of all that the ring is local.
Let $LX = 0$ be a syzygy with $L = [\, a_1 \ \cdots \ a_m \,]$ in $\mathbf{A}$ and $X \in M^{m\times 1}$. Without loss of generality, suppose that $a_i = b_i a_1$ for $i > 1$. The syzygy is rewritten as $a_1 y = 0$ with $y = x_1 + b_2 x_2 + \cdots + b_m x_m$. The cyclic submodule $\mathbf{A}y$ is flat and the ring is local therefore $a_1 = 0$ or $y = 0$. In the first case $L = 0$. In the second case $X = HX$ and $LH = 0$ with the following triangular matrix H

$$H = \begin{bmatrix} 0 & -b_2 & -b_3 & \dots & -b_m \\ 0 & 1 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \dots & \dots & 0 & 1 \end{bmatrix}.$$

In the case of an arbitrary Prüfer ring, we repeat the previous reasoning by using the localizations (at comaximal elements) which make the ideal $\langle a_1, \dots, a_m \rangle$ generated by one of the a_i's.

We now pass to the equivalences between *1*, *4* and *5*.
The implications *4a* ⇔ *4b* ⇒ *4c* ⇒ *4d* and *5b* ⇒ *5a* are immediate.

4d ⇒ 1a. The ring $\mathbf{A}$ is a pf-ring (Lemma 2.3). It therefore suffices to show that every ideal $\mathfrak{a} = \langle x, y \rangle$ is locally principal. We have $xy = ax^2 + by^2$, and $z = ax$ satisfies $z^2 = zy - aby^2$. Therefore, since the ring is normal, $ax = a'y$ for a certain a'. Similarly, $by = b'x$ for a certain b'. Therefore, $xy(1 - a' - b') = 0$. The elements $1 - a' - b'$, a' and b' are comaximal. When we invert $1 - a' - b'$, we obtain $xy = 0$, and after two new localizations, $x = 0$ or $y = 0$, so $\mathfrak{a}$ is principal. When we invert a', we obtain $\mathfrak{a} = \langle x \rangle$ because $a'y = ax$. Likewise when we invert b'.

1a ⇒ 4b. Let $x \in \mathbf{A}$ be integral over a finitely generated ideal $\mathfrak{a}$. We have for a certain $n \in \mathbb{N}$, $\mathfrak{a}(\mathfrak{a} + \langle x \rangle)^n = (\mathfrak{a} + \langle x \rangle)^{n+1}$. Since the ring is arithmetic, we have a finitely generated ideal $\mathfrak{b}$ such that $(\mathfrak{a} + \langle x \rangle)\mathfrak{b} = \langle x \rangle$. Therefore by multiplying by $\mathfrak{b}^n$ we obtain $x^n \mathfrak{a} = x^n(\mathfrak{a} + \langle x \rangle)$ which means that there exists some $y \in \mathfrak{a}$ such that $x^{n+1} = x^n y$, i.e. $x^n(y - x) = 0$. Since the ring is a pf-ring, this implies that after comaximal localizations we have $x = 0$ or $y - x = 0$, and in each case $x \in \mathfrak{a}$.

5a ⇒ 4b. Let $x \in \mathbf{A}$ be integral over some finitely generated ideal $\mathfrak{a}$. We have for a certain $n \in \mathbb{N}$, $\mathfrak{a}(\mathfrak{a} + \langle x \rangle)^n = (\mathfrak{a} + \langle x \rangle)^{n+1}$. We apply several times the simplification property with the ideal $\mathfrak{c} = \mathfrak{a} + \langle x \rangle$ and we obtain at the end of the process $\mathfrak{a} + \langle x \rangle \subseteq \mathfrak{a}$.

4b $\Rightarrow$ *5b.* Let $\mathfrak{c}$, $\mathfrak{a}$, $\mathfrak{a}'$ be three finitely generated ideals satisfying the hypothesis in *5b*. Let x be an element of $\mathfrak{a}$ and X be a column vector column formed by a generator set of $\mathfrak{c}$. Since $x\mathfrak{c} \subseteq \mathfrak{a}'\mathfrak{c}$, there exists a matrix $G \in \mathbb{M}_n(\mathfrak{a}')$ such that $xX = GX$, i.e. $(x\mathrm{I}_n - G)X = 0$. If P is the characteristic polynomial of G, we have on the one hand $P(x)X = 0$, and on the other $P(x) \in x^n + \mathfrak{a}'$. Therefore $P(x) \in \mathrm{Ann}(\mathfrak{c}) \subseteq \mathrm{Ann}(\mathfrak{a}+\mathfrak{a}')$ and $P(x) \in \mathfrak{a}+\mathfrak{a}'$. Hence $P(x)^2 = 0$, then $P(x) = 0$. This is an integral dependence relation of x over $\mathfrak{a}'$. Therefore $x \in \mathfrak{a}'$. □

3.3. Lemma. *In a pf-ring, if we have $\langle x, y \rangle\, \mathfrak{b} = \langle x^n \rangle$ with $n \geqslant 1$, then $\langle x, y \rangle$ is locally principal.*

D It suffices to solve this problem after comaximal localizations. The pf-ring character of the ring will be used to manufacture these localizations.

We have an equality $\langle u, v \rangle \langle x, y \rangle = \langle x^n \rangle$ with $x^n = ux + vy$, $ux = u_1 x^n$, $vx = ax^n$ and $uy = bx^n$. We get

$$(u_1 y - bx)x^n = 0, \quad (u_1 x + ay - x)x^n = (ux + vy - x^n)x = 0.$$

We therefore have comaximal localizations in which $x = 0$ and the result is clear. In the latter, $u_1 y = bx$ and $u_1 x + ay = x$ i.e. $(1 - u_1)x = ay$. Thus, $\langle x, y \rangle$ is locally principal. □

3.4. Lemma. *Let $\mathbf{A}$ be an arbitrary ring, $B \in \mathbf{A}^{m \times n}$ and $C \in \mathbf{A}^{m \times 1}$. The system of linear equations $BX = C$ admits a solution in $\mathbf{A}^{n \times 1}$ when the following conditions are realized for all $k \in [\![1..\inf(m,n)]\!]$*

1. *The determinantal ideal $\mathcal{D}_k(B)$ is of the form $\delta_k \mathbf{A}$, where δ_k is a minor of order k.*
2. *δ_k satisfies the condition: $\forall y \in \mathbf{A}$ $\big(y\delta_k = 0 \;\Rightarrow\; (\delta_k = 0 \;\vee\; y = 0)\big)$.*
3. *$\mathcal{D}_k([\,B \mid C\,]) = \mathcal{D}_k(B)$.*

D We begin with $k = \inf(m, n)$. We write the identity à la Cramer

$$\delta_k \times C = \delta_k \times \text{(a linear combination of the columns of } B\text{)},$$

which results from the nullity of determinantal ideals of index $k + 1$ and from the fact that $\mathcal{D}_k([\,B \mid C\,])$ is generated by δ_k. Given *2*, we are in one of the following two cases

- we can simplify by dividing everything by δ_k, so $C \in \mathrm{Im}\, B$.
- $\delta_k = 0$, or $k = 1$ in which case $C \in \mathrm{Im}\, B$ (because $B = C = 0$), or $k \geqslant 2$, and we can perform an induction by replacing k by $k - 1$.

□

Extensions of Prüfer rings

The fact that a normal ring is a pf-ring means that locally it behaves like a ring without zerodivisors. Actually the machinery of comaximal localizations at work in the definition of a pf-ring often allows us to return to the integral case, as we have already seen in the proof of Lemma 3.3.

We have the following important theorem, which is a generalization of the analogous result obtained in number theory (Theorem III-8.21).

3.5. Theorem. (Normal integral extension of a Prüfer ring).
Let $\mathbf{A} \subseteq \mathbf{B}$ *with* $\mathbf{B}$ *being normal and integral over* $\mathbf{A}$ *and* $\mathbf{A}$ *being Prüfer. Then* $\mathbf{B}$ *is a Prüfer ring.*

D We will show that every ideal $\langle \alpha, \beta \rangle$ is locally principal.

Let us first consider the case of an ideal $\langle a, \beta \rangle$ with $(a, \beta) \in \mathbf{A} \times \mathbf{B}$. We can then reuse almost word for word the proof "à la Dedekind[1]" of Theorem III-8.21.

Let $f \in \mathbf{A}[X]$ be monic and vanishing at β. We write $f(X) = (X - \beta)h(X)$ where $h \in \mathbf{B}[X]$. We therefore have $f(aX) = (aX - \beta)h(aX)$, which we write as $f_1 = g_1 h_1$. Let $\mathfrak{c} = \mathrm{c}_{\mathbf{A}}(f_1)$, $\mathfrak{b} = \mathrm{c}_{\mathbf{B}}(h_1)$ and $\mathfrak{a} = \mathrm{c}_{\mathbf{B}}(g_1) = \langle a, \beta \rangle$.

If $\deg(f) = n$, we have $a^n \in \mathfrak{c}$. Let $\mathfrak{c}'$ be a finitely generated ideal of $\mathbf{A}$ with $\mathfrak{c}\mathfrak{c}' = a^n \mathbf{A}$.

By using Kronecker's theorem (reformulated in Lemma 2.7), we obtain $\mathfrak{c}\mathbf{B} \subseteq \mathfrak{a}\mathfrak{b} \subseteq \mathrm{Icl}_{\mathbf{B}}(\mathfrak{c})$ and so

$$a^n\mathbf{B} = (\mathfrak{c}\mathbf{B})(\mathfrak{c}'\mathbf{B}) \subseteq \mathfrak{a}\mathfrak{b}(\mathfrak{c}'\mathbf{B}) \subseteq \mathrm{Icl}_{\mathbf{B}}(\mathfrak{c})(\mathfrak{c}'\mathbf{B}) \subseteq \mathrm{Icl}_{\mathbf{B}}(\mathfrak{c}\mathfrak{c}') = \mathrm{Icl}_{\mathbf{B}}(a^n) = a^n\mathbf{B}.$$

Therefore $\mathfrak{a}\mathfrak{b}(\mathfrak{c}'\mathbf{B}) = a^n\mathbf{B}$ and $\mathfrak{a}$ is locally principal by Lemma 3.3.

Let us pass to the general case, with $\alpha, \beta \in \mathbf{B}$. If $\mathbf{B}$ is integral, we can suppose that $\alpha \neq 0$ and we find $\gamma \neq 0$ in $\mathbf{B}$ such that $\alpha\gamma = a \in \mathbf{A}$, which brings us to the problem already treated.

It remains to see the more delicate case where we do not suppose that $\mathbf{B}$ is integral. In this case we have $f_i = h_{i-1} - \alpha h_i$ for $i \in \llbracket 1..n \rrbracket$ (by convention, $h_{-1} = 0$ and $h_n = 0$). We let $\beta_i = -\beta h_i$ for $i \in \llbracket 0..n-1 \rrbracket$. Then using the first case, we know how to compute principal localization matrices M_i for the pairs $(f_i, \beta_i) \in \mathbf{A} \times \mathbf{B}$:

$$\forall i \in \llbracket 0..n-1 \rrbracket \quad \left\{ \begin{array}{l} \mathrm{Tr}(M_i) = 1 \\ M_i \cdot {}^t(-\beta_i, f_i) = 0 \end{array} \right.$$

But $(-\beta_i, f_i) \equiv h_i(\beta, -\alpha) \bmod h_{i-1}\mathbf{B}^2$, so we have

$$\forall i \in \llbracket 0..n-1 \rrbracket \quad h_i M_i \cdot {}^t(\beta, -\alpha) \equiv 0 \bmod h_{i-1}\mathbf{B}^2. \tag{3}$$

Let us prove by induction that there exist elements $\zeta_0, \dots, \zeta_{n-1} \in \mathbf{B}$ and matrices $\widetilde{M_0}, \dots, \widetilde{M_{n-1}} \in M_2(\mathbf{B})$ such that

[1] This would also work with the proof à la Kronecker.

$$\forall i \in [\![0..n-1]\!] \quad \begin{cases} \mathrm{Tr}(\widetilde{M_i}) = 1 - \zeta_0 \cdots \zeta_i \\ \widetilde{M_i} \cdot {}^t(\beta, -\alpha) = 0 \\ \zeta_i h_i = 0 \end{cases}$$

The result is true for $i = 0$: we take $\widetilde{M_0} = M_0$, and we get ζ_0 from equation (3) because $\mathbf{B}$ is a pf-ring. In order to go from rank i to rank $i+1$, we multiply $h_{i+1}M_{i+1} \cdot {}^t(\beta, -\alpha) \equiv 0 \bmod h_i\mathbf{B}^2$ par ζ_i. We get

$$h_{i+1}\zeta_i M_{i+1}.{}^t(\beta, -\alpha) = 0 \ \text{ et a fortiori } \ h_{i+1}\zeta_0 \cdots \zeta_i M_{i+1}.{}^t(\beta, -\alpha) = 0$$

in $\mathbf{B}$.

So there exists $\zeta_{i+1} \in \mathbf{B}$ such that

$$0 = (1 - \zeta_{i+1})\zeta_0 \cdots \zeta_i M_{i+1} \cdot {}^t(\beta, -\alpha) \quad \text{and} \quad 0 = \zeta_{i+1}h_{i+1}$$

We let $\widetilde{M_{i+1}} = \widetilde{M_i} + (1-\zeta_{i+1})\zeta_0 \cdots \zeta_i M_{i+1}$. One verifies equalities $\mathrm{Tr}(\widetilde{M_{i+1}}) = 1 - \zeta_0 \cdots \zeta_{i+1}$ et $\widetilde{M_{i+1}} \cdot {}^t(\beta, -\alpha) = 0$. So the induction hypothesis is satisfied for $i+1$.

Finally, in rank $n-1$, we have $h_{n-1} = f_n = 1$, so $\zeta_{n-1} = \zeta_{n-1}h_{n-1} = 0$, which gives $\mathrm{Tr}(\widetilde{M_{n-1}}) = 1$, and the matrix $\widetilde{M_{n-1}}$ is a principal localization matrix for the pair (α, β). □

Remark. This proof, like that of Lemma 3.3, is more formidable than it seems. It manages to treat in a single way the case where $\alpha = 0$, the case where α is regular, and "all the intermediary cases." ■

We also have the following easy result.

3.6. Theorem. *Let* $\mathbf{A} \subseteq \mathbf{B} \subseteq \mathrm{Frac}\,\mathbf{A}$.

1. *If* $\mathbf{A}$ *is a pf-ring, the same goes for* $\mathbf{B}$.
2. *If* $\mathbf{A}$ *is arithmetic, the same goes for* $\mathbf{B}$.
3. *If* $\mathbf{A}$ *is a Prüfer ring, the same goes for* $\mathbf{B}$.

D Item *1* is left to the reader.

2. Let $x, y \in \mathbf{B}$. There exists a $d \in \mathrm{Reg}(\mathbf{A})$ such that $x_1 = dx$, and $y_1 = dy$ are in $\mathbf{A}$. Then $d(x, y) = (x_1, y_1)$, and a principal localization matrix in $\mathbf{A}$ for (x_1, y_1) is also a principal localization matrix for (x, y). □

The two previous theorems are linked to two classic results in the Noetherian framework (cf. [Freid & Jarden, page 17]):

Krull-Akizuki theorem. *If* $\mathbf{A}$ *is a Dedekind ring and* $\mathbf{L}$ *is a finite extension of the quotient field of* $\mathbf{A}$*, then the integral closure of* $\mathbf{A}$ *in* $\mathbf{L}$ *is a Dedekind ring.*

Grell-Noether theorem. *If* $\mathbf{A}$ *is a Dedekind ring, then every ring contained between* $\mathbf{A}$ *and its quotient field is a Dedekind ring.*

Given the characterization of Dedekind rings (in classical mathematics) as integral Noetherian Prüfer rings, we see that we have established the non-Noetherian and non-integral versions of these two theorems.

We will later prove that in the analogous circumstances, the Krull dimension of $\mathbf{B}$ is always less than or equal to that of $\mathbf{A}$, which this time is linked to the characterization of Dedekind rings as integrally closed Noetherian rings of dimension at most 1.

4. Coherent Prüfer rings

First properties

Recall that over a pp-ring a finitely generated ideal is faithful if and only if it contains a regular element (see Corollary IV-6.5). Actually every finitely generated ideal contains an element that has the same annihilator. In particular, over a pp-ring a projective finitely generated ideal is invertible if and only if it is faithful.

After having provided characterizations of Prüfer rings (see Proposition and Definition VIII-4.4 and Theorem 3.2), here are some for coherent Prüfer rings; the reader will find others in Exercise 16.

4.1. Theorem. (Characterizations of coherent Prüfer rings)
For any ring $\mathbf{A}$*, the following properties are equivalent.*

1. $\mathbf{A}$ *is a coherent Prüfer ring.*
2. $\mathbf{A}$ *is an arithmetic pp-ring.*
3. *Every finitely generated ideal is projective.*
4. *Every ideal with two generators is projective.*
5. $\mathbf{A}$ *is a pp-ring and every ideal* $\langle a, b\rangle$ *with* $a \in \operatorname{Reg}\mathbf{A}$ *is invertible.*
6. $\mathbf{A}$ *is a pp-ring and every faithful finitely generated ideal is a projective module of constant rank* 1*.*

D *1* ⇔ *2.* Use Fact VIII-3.5.
3 ⇒ *4.* Trivial.
4 ⇒ *2.* Theorem 1.6 gives the implication for the locally principal character of ideals. Moreover a ring is a pp-ring if and only if the principal ideals are projective.
The implications *1* ⇒ *3*, *5*, *6* come from the characterization of projective ideals as locally principal ideals whose annihilator is an idempotent and that of the invertible ideals as locally principal ideals containing a regular element (Lemma V-7.7, items *2* and *6*).
For the converses, recall that a principal ideal is projective if and only if its annihilator is generated by an idempotent (Lemma V-7.5), and we can look at the solution of Exercise 16. We can also examine these converses in the integral case, where they are clear, and use the elementary local-global machinery of pp-rings. □

In the local case we obtain the following result (trivial in classical mathematics, but meaningful from a constructive point of view).

4.2. Fact. *A valuation ring is coherent if and only if it is integral. We call it a* valuation domain*.*

D A Prüfer ring is coherent if and only if it is a pp-ring. A local ring is connected. A connected ring is integral if and only if it is a pp-ring. □

In this case $\mathbf{K} = \operatorname{Frac} \mathbf{A}$ is a discrete field and for all $x \in \mathbf{K}^{\times}$, x or $1/x$ is in $\mathbf{A}$. Generally, we call a subring satisfying the preceding property a *valuation ring of the discrete field* $\mathbf{K}$. It is clear that it is a valuation domain.

The following stability properties are easy.

4.3. Fact.

1. *A reduced zero-dimensional ring is a coherent Prüfer ring.*
2. *A ring obtained by localization of a coherent Prüfer ring is a coherent Prüfer ring. A reduced quotient ring of a coherent Prüfer ring by a finitely generated ideal is a coherent Prüfer ring.*
3. *A ring is a coherent Prüfer ring if and only if it has the same property after localization at comaximal monoids.*

Recall: item *1* is valid for pp-rings and item *2* for arithmetic rings.

4.4. Fact. *Let* $\mathbf{A}$ *be a coherent Prüfer ring.*

1. $\mathbf{A}$ *is discrete if and only if* $\mathbb{B}(\mathbf{A})$ *is discrete.*
2. $\mathbf{A}$ *is strongly discrete if and only if it is with explicit divisibility.*

Kernel, image and cokernel of a matrix

4.5. Theorem. *Let* $\mathbf{A}$ *be a coherent Prüfer ring.*

1. *The image of a matrix* $F \in \mathbf{A}^{n\times m}$ *is isomorphic to a direct sum of* n *finitely generated ideals.*
2. *Every finitely generated submodule of a finitely generated projective module is a finitely generated projective module.*
3. *The kernel of a linear map between finitely generated projective modules is a direct summand (therefore finitely generated projective).*
4. *Every finitely presented module is a direct sum of its torsion submodule (which is finitely presented) and of a finitely generated projective submodule.*
5. *Every projective module of rank* $k \geqslant 0$ *is isomorphic to a direct sum of* k *invertible ideals.*
6. *Every projective module of rank* $\leqslant k$ *is isomorphic to a direct sum of* k *finitely generated ideals.*

Note: we do not require that $\mathbf{A}$ be discrete.

D Consider an arbitrary linear map $\varphi : \mathbf{A}^m \to \mathbf{A}^n$.

1. We treat the case of the module $M = \operatorname{Im} \varphi \subseteq \mathbf{A}^n$. Let $\pi_n : \mathbf{A}^n \to \mathbf{A}$ be the last coordinate form. The ideal $\pi_n(M) = \mathfrak{a}_n$ is finitely generated therefore projective, and the surjective induced map $\pi'_n : M \to \mathfrak{a}_n$ is split, and

$$M \simeq \operatorname{Ker} \pi'_n \oplus \operatorname{Im} \pi'_n = (M \cap \mathbf{A}^{n-1}) \oplus \mathfrak{a}_n.$$

We end the proof by induction on n: $M \cap \mathbf{A}^{n-1}$ is finitely generated since it is isomorphic to a quotient of M. We therefore obtain $M \simeq \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_n$.

2. Results immediately from *1.*

3. This results from the image of the linear map being a finitely generated projective module.

4. We treat the case of the module $N = \operatorname{Coker} \varphi$.

Let us first consider the case where $\mathbf{A}$ *is local*, i.e. it is a valuation domain. The matrix of φ is put in Smith form (Proposition IV-7.2). Since the ring is integral, N is a direct sum of a free module (corresponding to the zero diagonal elements in the reduced Smith form) and of a torsion submodule, itself a direct sum of submodules $\mathbf{A}/\langle d_i \rangle$ corresponding to the regular diagonal elements.

Next let us consider the case where $\mathbf{A}$ *is integral.*

By means of a finite number of localizations at comaximal elements, say s_1, …, s_r, we are brought back to the situation of the local case (Smith reduction of the matrix). Since $\operatorname{Ann}_{\mathbf{A}}(s_i) = \langle 0 \rangle$ or $\langle 1 \rangle$, and since the localizations at 0 are useless, we can suppose that the s_i's are in $\operatorname{Reg}(\mathbf{A})$.

Denote by T the torsion submodule of N and take a look at what happens after localization at $S_i = s_i^{\mathbb{N}}$. We easily observe that the torsion submodule of N_{S_i} is equal to T_{S_i}. Thus, T is finitely presented because it is finitely presented after localization at the S_i's. It is a direct summand in N because T_{S_i} is a direct summand in N_{S_i} for each i: the canonical injection $T \to N$ admits a left-inverse by the local-global principle IV-3.1. Finally, the module N/T, which is finitely generated projective after localization at the S_i's, is indeed finitely generated projective.

We therefore obtain what we wanted, with a little bonus: the module T becomes, after localization at each of the elements s_j of a comaximal system $(s_1, \ldots, s_r)$, a direct sum of cyclic torsion modules, i.e. isomorphic to $\mathbf{A}[1/s_j]/\langle u_{k,j} \rangle$, with $u_{k,j} \in \operatorname{Reg}(\mathbf{A})$.

Finally, let us consider the general case, where $\mathbf{A}$ *is a pp-ring.*

Starting from the proof of the integral case, the elementary local-global machinery of pp-rings produces a fundamental system of orthogonal idempotents $(e_1, \ldots, e_r)$ such that the result is attained in each of the components $e_i N$ (regarded as $\mathbf{A}[1/e_i]$-module). This immediately gives the global result.

5. In the case where $\mathbf{A}$ is integral, this results from item *1* since each ideal in the decomposition into a direct sum is of rank 0 or 1.
We can deduce the general case by the elementary local-global machinery of pp-rings. Here is another proof,[2] independent of the proof of item *1.* If M is of constant rank $k \geqslant 1$, then its dual $M^\star$ is also of constant rank, their annihilators are null, and there exists a $\mu \in M^\star$ such that $\mathrm{Ann}(\mu) = \langle 0 \rangle$ (see Lemma IV-6.4). Then $\mu(M)$ is an invertible ideal of $\mathbf{A}$ because its annihilator is also null. Moreover, $M \simeq \mathrm{Ker}\,\mu \oplus \mathrm{Im}\,\mu$, which proves that $\mathrm{Ker}\,\mu$ is finitely generated projective of constant rank $k - 1$. We finish by induction.

6. Consider M as a direct sum of its components of constant rank, and apply item *4* to each of them. □

Extensions of coherent Prüfer rings

An element x of an $\mathbf{A}$-algebra $\mathbf{B}$ is said to be *primitively algebraic over* $\mathbf{A}$ if it annihilates a primitive polynomial of $\mathbf{A}[X]$. After a change of base ring, a primitively algebraic element remains primitively algebraic. The property for an element to be primitively algebraic is local in the following sense.

4.6. Concrete local-global principle. (Primitively algebraic elements) *Let S_1, …, S_n be comaximal monoids of a ring $\mathbf{A}$, $\mathbf{B}$ be an $\mathbf{A}$-algebra and $x \in \mathbf{B}$. Then x is primitively algebraic over $\mathbf{A}$ if and only if it is primitively algebraic over each of the $\mathbf{A}_{S_i}$'s.*

D We need to show that the condition is sufficient. We have comaximal elements s_1, …, s_n ($s_i \in S_i$) and polynomials $f_i \in \mathbf{A}[X]$ such that $s_i \in \mathrm{c}(f_i)$ and $f_i(x) = 0$. If $d_i \geqslant \deg_X(f_i) + 1$, we consider the polynomial

$$f = f_1 + X^{d_1} f_2 + X^{d_1+d_2} f_3 + \cdots .$$

We then have $f(x) = 0$ and $\mathrm{c}(f) = \sum_{i=1}^n \mathrm{c}(f_i) = \langle 1 \rangle$. □

4.7. Lemma. (Emmanuel's trick) *Let $\mathbf{B}$ be a ring and $\mathbf{A}$ be a subring. Let $\mathbf{A}'$ be the integral closure of $\mathbf{A}$ in $\mathbf{B}$ and s be an element of $\mathbf{B}$ which annihilates a polynomial $f(X) = \sum_{k=0}^n a_k X^k \in \mathbf{A}[X]$.*
Let $g(X) = \sum_{k=1}^n b_k X^{k-1}$ be the polynomial $f(X)/(X - s)$.

1. *The elements b_i and $b_i s$ are in $\mathbf{A}'$.*
2. *In $\mathbf{A}'$ we obtain*
$$\langle a_0, \dots, a_n \rangle = \mathrm{c}(f) \subseteq \mathrm{c}(g) + \mathrm{c}(sg) = \langle b_1, \dots, b_n, b_1 s, \dots, b_n s \rangle .$$
3. *In $\mathbf{A}'[s]$ the two ideals are equal.*

[2] More scholarly or less scholarly, it is difficult to say. This is a matter of taste.

D Since $f(X) = (X - s)g(X)$, Kronecker's theorem tells us that the b_i's and b_is's are integral over $\mathbf{A}$. We have

$$b_n = a_n,\ b_{n-1} = b_ns + a_{n-1},\ \ldots,\ b_1 = b_2s + a_1,\ 0 = b_1s + a_0.$$

Therefore each $a_i \in \mathrm{c}(g) + \mathrm{c}(sg)$ and, in $\mathbf{A}'[s]$, step by step, we obtain $b_n \in \mathrm{c}(f)$, $b_{n-1} \in \mathrm{c}(f)$, ..., $b_1 \in \mathrm{c}(f)$. □

4.8. Theorem. (Another characterization of coherent Prüfer rings, see also Exercises 15 and 16) *A ring* $\mathbf{A}$ *is a coherent Prüfer ring if and only if it is a pp-ring, integrally closed in* $\mathrm{Frac}\,\mathbf{A}$*, and if every element of* $\mathrm{Frac}\,\mathbf{A}$ *is primitively algebraic over* $\mathbf{A}$*.*

D Suppose that $\mathbf{A}$ is a coherent Prüfer ring. It remains to show that every element of $\mathrm{Frac}\,\mathbf{A}$ is primitively algebraic over $\mathbf{A}$. Let $x = a/b \in \mathrm{Frac}\,\mathbf{A}$. There is a principal localization matrix for (b, a): $\begin{bmatrix} s & u \\ v & t \end{bmatrix} \in \mathbb{M}_2(\mathbf{A})$, with $s + t = 1$, $sa = ub$ and $va = tb$.

This gives $sx - u = 0$ and $t = vx$. Thus, x annihilates the primitive polynomial $-u + sX + X^2(t - vX)$, or if we prefer $t - (u + v)X + sX^2$.

Let us prove the converse. It suffices to consider only the integral case. We need to show that every ideal $\langle a, b\rangle$ is locally principal. Suppose without loss of generality that a, $b \in \mathrm{Reg}(\mathbf{A})$. The element $s = a/b$ annihilates a primitive polynomial $f(X)$. Since $\mathrm{c}(f) = \langle 1\rangle$ in $\mathbf{A}$, by Lemma 4.7 (items *1* and *2*), we have comaximal elements b_1, ..., b_n, b_1s, ..., b_ns in $\mathbf{A}$.

We then have $s \in \mathbf{A}[1/b_i]$ and $1/s \in \mathbf{A}[1/(b_is)]$: in each of the comaximal localizations, a divides b or b divides a. □

The theorem that follows contains a new proof of the stability of the integral Prüfer rings by integral and integrally closed extension (see Theorem 3.5). It seems disconcertingly easy when compared to that given without the coherence hypothesis.

4.9. Theorem. *If* $\mathbf{B}$ *is a normal pp-ring, and an integral extension of a coherent Prüfer ring* $\mathbf{A}$*, then* $\mathbf{B}$ *is a coherent Prüfer ring.*

D Let us first consider the case where $\mathbf{B}$ *is integral and nontrivial.* Let $s \in \mathrm{Frac}\,\mathbf{B}$. It suffices to show that s is primitively algebraic over $\mathbf{B}$. We have a nonzero polynomial $f(X) \in \mathbf{A}[X]$ such that $f(s) = 0$.

Case where $\mathbf{A}$ *is a Bézout domain.* We divide f by $\mathrm{c}(f)$ and we obtain a primitive polynomial which annihilates s.

Case of a Prüfer domain. After localization at comaximal elements, the ideal $\mathrm{c}(f)$ is generated by one of the coefficients of f, the first case applies.

In the general case, the elementary local-global machinery of pp-rings brings us back to the integral case. □

Now here is the analogue of Proposition III-8.17, which described the ring of integers of a number field. In the case where $\mathbf{A}$ is a Bézout domain, we could have repeated almost word for word the same proofs. Also note that Theorem VI-3.18 studies a similar situation with a slightly weaker hypothesis. See also item *1* of Problem III-9.

4.10. Theorem. (Ring of integers in an algebraic extension)
Let $\mathbf{A}$ *be a coherent Prüfer ring,* $\mathbf{K} = \mathrm{Frac}(\mathbf{A})$*,* $\mathbf{L} \supseteq \mathbf{K}$ *be a reduced ring integral over* $\mathbf{K}$ *and* $\mathbf{B}$ *be the integral closure of* $\mathbf{A}$ *in* $\mathbf{L}$*.*

1. $\mathrm{Frac}\,\mathbf{B} = \mathbf{L} = (\mathrm{Reg}\,\mathbf{A})^{-1}\mathbf{B}$ *and* $\mathbf{B}$ *is a coherent Prüfer ring.*
2. *If* $\mathbf{L}$ *is strictly finite over* $\mathbf{K}$ *and if* $\mathbf{A}$ *is strongly discrete,* $\mathbf{B}$ *is strongly discrete.*

If in addition $\mathbf{L}$ *is étale over* $\mathbf{K}$*, we obtain*

3. *If* $\mathbf{A}$ *is Noetherian, the same goes for* $\mathbf{B}$*.*
4. *If* $\mathbf{A}$ *is a Dedekind ring (Definition 7.7), so is* $\mathbf{B}$*.*
5. *If* $\mathbf{L} = \mathbf{K}[x] = \mathbf{K}[X]/\langle f\rangle$ *with* $f \in \mathbf{A}[X]$ *monic and* $\mathrm{disc}_X(f) \in \mathrm{Reg}\,\mathbf{A}$*, then* $\frac{1}{\Delta}\mathbf{A}[x] \subseteq \mathbf{B} \subseteq \mathbf{A}[x]$ *(*$\Delta = \mathrm{disc}_X(f)$*).*
In particular $\mathbf{A}[x][\frac{1}{\Delta}] = \mathbf{B}[\frac{1}{\Delta}]$.
6. *If in addition* $\mathrm{disc}_X(f) \in \mathbf{A}^\times$*, we have* $\mathbf{B} = \mathbf{A}[x]$ *strictly étale over* $\mathbf{A}$*.*

D *1.* Direct consequence of Fact VI-3.16 and of Theorem 4.9.

2. Since $\mathbf{B}$ is a Prüfer ring, it suffices to know how to test the divisibility in $\mathbf{B}$, i.e. testing that an element of $\mathbf{L}$ is a member of $\mathbf{B}$. Let $y \in \mathbf{L}$ and $Q \in \mathbf{K}[Y]$ be its (monic) minimal polynomial over $\mathbf{K}$. Then y is integral over $\mathbf{A}$ if and only if $Q \in \mathbf{A}[Y]$: in the non-immediate sense, let $P \in \mathbf{A}[Y]$ be monic such that $P(y) = 0$, then Q divides P in $\mathbf{K}[Y]$ and Lemma III-8.10 implies that $Q \in \mathbf{A}[Y]$.

Note: we might as well have used the characteristic polynomial, but the proof that uses the minimal polynomial works in a more general framework (it suffices for $\mathbf{L}$ to be algebraic over $\mathbf{K}$ and for us to know how to compute the minimal polynomials).

5. In the case where $\mathbf{A}$ is a Bézout domain and $\mathbf{L}$ is a field, we apply Theorem VI-3.18. The result in the general case is then obtained from this proof by using the local-global machineries of pp-rings and of arithmetic rings.

3. We carry out the proof under the hypotheses of item *5*. This is not restrictive because by Theorem VI-1.9, $\mathbf{L}$ is a product of monogenic étale $\mathbf{K}$-algebras.

Let $\mathfrak{b}_1 \subseteq \mathfrak{b}_2 \subseteq \cdots \subseteq \mathfrak{b}_n \subseteq \dots$ be a sequence of finitely generated ideals of $\mathbf{B}$ that we write as $\mathfrak{b}_n = \langle G_n\rangle_{\mathbf{B}}$ with $G_n \subseteq G_{n+1}$; we define

$$L_n = \mathrm{disc}_X(f) \cdot \Big(\textstyle\sum_{g \in G_n} \mathbf{A}g\Big) \subseteq \mathbf{A}[x].$$

Then $L_1 \subseteq L_2 \subseteq \cdots \subseteq L_n \subseteq \dots$ is a sequence of finitely generated $\mathbf{A}$-submodules of $\mathbf{A}[x]$. However, $\mathbf{A}[x]$ is a free $\mathbf{A}$-module of finite rank (equal to deg(f)), so Noetherian. We finish by noting that if $L_m = L_{m+1}$, then $\mathfrak{b}_m = \mathfrak{b}_{m+1}$.

4. Results from *2* and *3.*

6. It is clear that $\mathbf{B} = \mathbf{A}[x]$. □

Remark. The previous theorem applies in two important cases in the history of commutative algebra.

The first case is that of the rings of integers of number fields, with $\mathbf{A} = \mathbb{Z}$ and $\mathbf{B}$ being the ring of integers of a number field (a case already examined in Section III-8).

The second case is that of algebraic curves. Consider a discrete field $\mathbf{k}$, the PID $\mathbf{A} = \mathbf{k}[x]$ and a polynomial $f(x, Y) \in \mathbf{k}[x, Y]$ monic in Y, irreducible, with $\text{disc}_Y(f) \neq 0$. Let $\mathbf{K} = \mathbf{k}(x)$.

The ring $\mathbf{A}[y] = \mathbf{k}[x, y] = \mathbf{k}[x, Y]/\langle f\rangle$ is integral. The planar curve $\mathcal{C}$ of equation $f(x, Y) = 0$ can have singular points, in which case $\mathbf{A}[y]$ is not arithmetic. But the integral closure $\mathbf{B}$ of $\mathbf{A}$ in $\mathbf{K}[y] = \mathbf{K}[Y]/\langle f\rangle$ is indeed a Prüfer domain (Theorem 6.2). The field $\mathbf{K}[y]$ is called the field of functions of $\mathcal{C}$. The ring $\mathbf{B}$ corresponds to a curve (which is no longer necessarily plane) without a singular point, with the same field of functions as $\mathcal{C}$. ■

5. pp-rings of dimension at most 1

Most "classical" theorems regarding Dedekind domains are already valid for coherent Prüfer rings of dimension at most 1, or even for arithmetic rings. We prove a certain number of them in this and the following section.

In this section the results relate to the pp-rings of dimension at most 1.

The following theorem is a special case of Bass' "stable range" for which we will give general versions (Theorems XIV-1.4 and XIV-2.6).

5.1. Theorem. *Let $n \geqslant 3$ and ${}^{\mathrm{t}}[\,x_1 \;\cdots\; x_n\,]$ be a unimodular vector over a pp-ring $\mathbf{A}$ of dimension at most 1. This vector is the first column of a matrix of $\mathbb{E}_n(\mathbf{A})$. In particular, $\mathbb{SL}_n(\mathbf{A})$ is generated by $\mathbb{E}_n(\mathbf{A})$ and $\mathbb{SL}_2(\mathbf{A})$ for $n \geqslant 3$. For $n \geqslant 2$ every unimodular vector is the first column of a matrix of $\mathbb{SL}_n(\mathbf{A})$.*

D The annihilator of $\langle x_1, \ldots, x_n\rangle$ is null, so we can by elementary operations transform the vector $v = {}^{\mathrm{t}}[\,x_1 \;\cdots\; x_n\,]$ into a unimodular vector ${}^{\mathrm{t}}[\,y_1\; x_2 \;\cdots\; x_n\,]$, with $y_1 \in \text{Reg}(\mathbf{A})$ (cf. Lemma IV-6.4).

Consider the ring $\mathbf{B} = \mathbf{A}/\langle y_1\rangle$. This ring is zero-dimensional and the vector v becomes equal to ${}^{\mathrm{t}}[\,0\; x_2 \;\cdots\; x_n\,]$ still unimodular. Since $n \geqslant 3$, we can transform ${}^{\mathrm{t}}[\,x_2 \;\cdots\; x_n\,]$ into ${}^{\mathrm{t}}[\,1\; 0 \;\cdots\; 0\,]$ by elementary operations in $\mathbf{B}$ (Exercise IX-10). This gives in $\mathbf{A}$: ${}^{\mathrm{t}}[\,y_1\; 1 + ay_1\; z_3 \;\cdots\; z_n\,]$, hence, still by elementary operations, ${}^{\mathrm{t}}[\,y_1\; 1\; z_3 \;\cdots\; z_n\,]$, then ${}^{\mathrm{t}}[\,1\; 0 \;\cdots\; 0\,]$. □

The following theorem generalizes the analogous result already obtained in number theory (Corollary V-3.2). Item *1* concerns the invertible ideals. Item *2* applies to all the finitely generated ideals of a coherent Prüfer ring of dimension at most 1. A generalization is proposed in Theorem XIII-3.4.

5.2. Theorem. (One and a half theorem)
Let $\mathbf{A}$ be a pp-ring of dimension at most 1 and $\mathfrak{a}$ be a locally principal ideal (thus finitely generated projective).

1. *If $a \in \mathfrak{a} \cap \mathrm{Reg}(\mathbf{A})$, there exists a $b \in \mathfrak{a}$ such that $\mathfrak{a} = \langle a^n, b\rangle$ for every $n \geqslant 1$.*
2. *There exists an $a \in \mathfrak{a}$ such that $\mathrm{Ann}(a) = \mathrm{Ann}(\mathfrak{a})$. For such an a there exists a $b \in \mathfrak{a}$ such that $\mathfrak{a} = \langle a^n, b\rangle$ for every $n \geqslant 1$.*

D The proof of item *1* is identical to that of Corollary V-3.2 which gave the result in number theory.
2. Every finitely generated ideal $\mathfrak{a}$ contains an element a such that $\mathrm{Ann}(a) = \mathrm{Ann}(\mathfrak{a})$ (Corollary IV-6.5). We pass to the quotient $\mathbf{A}/\langle 1-e\rangle$ where e is the idempotent such that $\mathrm{Ann}(a) = \mathrm{Ann}(e)$ and we apply item *1.* □

5.3. Proposition. *Let $\mathbf{A}$ be a pp-ring of dimension at most 1, whose Jacobson radical contains a regular element, and $\mathfrak{a}$ be an invertible ideal. Then $\mathfrak{a}$ is principal.*

D Let $y \in \mathrm{Rad}(\mathbf{A})$ and $x \in \mathfrak{a}$ both be regular. Then $\mathfrak{a} \cap \mathrm{Rad}(\mathbf{A})$ contains $a = xy$ which is regular. By the one and a half theorem, there exists a $z \in \mathfrak{a}$ such that $\mathfrak{a} = \left\langle a^2, z\right\rangle$. Therefore $a = ua^2 + vz$ which gives $a(1-ua) = vz$ and since $a \in \mathrm{Rad}(\mathbf{A})$, $a \in \langle z\rangle$ so $\mathfrak{a} = \langle z\rangle$. □

We now revisit the following classical result, in which we will get rid of the Noetherian hypothesis: *if $\mathbf{A}$ is an integral Noetherian ring of dimension at most* 1 *and $\mathfrak{a}$, $\mathfrak{b}$ are two ideals with $\mathfrak{a}$ invertible and $\mathfrak{b} \neq 0$, then there exists a $u \in \mathrm{Frac}(\mathbf{A})$ such that $u\,\mathfrak{a} \subseteq \mathbf{A}$ and $u\mathfrak{a} + \mathfrak{b} = \langle 1\rangle$.*

5.4. Lemma. *Let $\mathbf{A}$ be a pp-ring (for example a coherent Prüfer ring) of dimension at most* 1*. Let $\mathfrak{a}$ be an invertible ideal of $\mathbf{A}$ and $\mathfrak{b}$ be an ideal containing a regular element. Then there exists an invertible element u in* $\mathrm{Frac}(\mathbf{A})$ *such that $u\mathfrak{a} \subseteq \mathbf{A}$ and $u\mathfrak{a} + \mathfrak{b} = \langle 1\rangle$.*

D We carry out the proof in the integral case, leaving it to the readers to apply the elementary local-global machinery of pp-rings. To facilitate this task, we do not assume $\mathbf{A}$ to be nontrivial and we put "regular" when in the nontrivial case we would have put "nonzero."
We look for a and b regular such that $\frac{b}{a}\,\mathfrak{a} \subseteq \mathbf{A}$, i.e. $b\,\mathfrak{a} \subseteq a\mathbf{A}$, and $\mathbf{A} = \frac{b}{a}\,\mathfrak{a} + \mathfrak{b}$. If c is a regular element of $\mathfrak{b}$, as the condition should also be realized when $\mathfrak{b}$ is the ideal $c\mathbf{A}$, we must find a and b regular such that $b\,\mathfrak{a} \subseteq a\mathbf{A}$ and $\mathbf{A} = \frac{b}{a}\,\mathfrak{a} + c\mathbf{A}$. If steps are taken so that $a \in \mathfrak{a}$, we will have $b \in \frac{b}{a}\mathfrak{a}$, and it

therefore suffices to realize the conditions $b\,\mathfrak{a} \subseteq a\mathbf{A}$ and $\mathbf{A} = \langle b, c\rangle$. This is what we will do.

Let $c \in \mathfrak{a} \cap \mathfrak{b}$ be a regular element (for example the product of two regular elements, one in $\mathfrak{a}$ and the other in $\mathfrak{b}$). By the one and a half theorem, there exists an $a \in \mathfrak{a}$ such that $\mathfrak{a} = \left\langle a, c^2 \right\rangle = \langle a, c\rangle$. If $a = 0$ the ideal $\mathfrak{a} = \langle c\rangle$ is idempotent therefore equal to $\langle 1\rangle$ and there was therefore no need to overexert ourselves:[3] we could have chosen $b = a = 1$.

We therefore suppose that a is regular. Since $c \in \mathfrak{a}$, we have an equality $c = \alpha a + \beta c^2$ which gives $c(1 - \beta c) = \alpha a$. Let $b = 1 - \beta c$ such that $\mathbf{A} = \langle b, c\rangle$. We obtain $b\,\mathfrak{a} = b\,\langle a, c\rangle = \langle ba, bc\rangle = a\,\langle b, \alpha\rangle \subseteq a\mathbf{A}$. If b is regular we therefore have won, and if $b = 0$, then $1 \in \langle c\rangle$ and there was no need to tire ourselves. □

5.5. Proposition. *Let $\mathfrak{a}$ be an invertible ideal of an integral ring $\mathbf{A}$ of dimension at most 1. For every nonzero ideal $\mathfrak{b}$ of $\mathbf{A}$, we have an isomorphism of $\mathbf{A}$-modules $\mathfrak{a}/\mathfrak{a}\mathfrak{b} \simeq \mathbf{A}/\mathfrak{b}$.*

D By Lemma 5.4, there exists an integral ideal $\mathfrak{a}'$ in the class[4] of $\mathbf{A} \div \mathfrak{a}$ such that $\mathfrak{a}' + \mathfrak{b} = \mathbf{A}$; we have $\mathfrak{a}\mathfrak{a}' = x\mathbf{A}$ with $x \in \operatorname{Reg}\mathbf{A}$. The multiplication by x, $\mu_x : \mathbf{A} \to \mathbf{A}$, induces an isomorphism

$$\mathbf{A}/\mathfrak{b} \xrightarrow{\sim} x\mathbf{A}/x\mathfrak{b} = \mathfrak{a}'\mathfrak{a}/\mathfrak{a}'\mathfrak{a}\mathfrak{b}.$$

Let us now consider the canonical map

$$f : \mathfrak{a}'\mathfrak{a} \to \mathfrak{a}/\mathfrak{a}\mathfrak{b}$$

which associates to $y \in \mathfrak{a}'\mathfrak{a} \subseteq \mathfrak{a}$ the class of y modulo $\mathfrak{a}\mathfrak{b}$. Let us show that f is surjective: indeed, $\mathfrak{a}' + \mathfrak{b} = \mathbf{A} \Rightarrow \mathfrak{a}'\mathfrak{a} + \mathfrak{a}\mathfrak{b} = \mathfrak{a}$, so every element of $\mathfrak{a}$ is congruent to an element of $\mathfrak{a}'\mathfrak{a}$ modulo $\mathfrak{a}\mathfrak{b}$. Let us finally examine $\operatorname{Ker} f = \mathfrak{a}'\mathfrak{a} \cap \mathfrak{a}\mathfrak{b}$. Since $\mathfrak{a}$ is invertible, $\mathfrak{a}'\mathfrak{a} \cap \mathfrak{a}\mathfrak{b} = \mathfrak{a}(\mathfrak{a}' \cap \mathfrak{b})$, and finally $\mathfrak{a}' + \mathfrak{b} = \mathbf{A}$ entails that $\mathfrak{a}' \cap \mathfrak{b} = \mathfrak{a}'\mathfrak{b}$, so $\operatorname{Ker} f = \mathfrak{a}'\mathfrak{a}\mathfrak{b}$. We thus have isomorphisms of $\mathbf{A}$-modules

$$\mathbf{A}/\mathfrak{b} \simeq x\mathbf{A}/x\mathfrak{b} = \mathfrak{a}'\mathfrak{a}/\mathfrak{a}'\mathfrak{a}\mathfrak{b} \simeq \mathfrak{a}/\mathfrak{a}\mathfrak{b},$$

hence the result. □

5.6. Corollary. *Let $\mathbf{A}$ be an integral ring with $\mathsf{Kdim}\,\mathbf{A} \leqslant 1$, $\mathfrak{a}$ be an invertible ideal and $\mathfrak{b}$ be a nonzero ideal. We then have an exact sequence of $\mathbf{A}$-modules*

$$0 \to \mathbf{A}/\mathfrak{b} \to \mathbf{A}/\mathfrak{a}\mathfrak{b} \to \mathbf{A}/\mathfrak{a} \to 0.$$

[3] Note however that we are not supposed to know in advance if an invertible ideal of $\mathbf{A}$ contains 1, therefore we have not tired ourselves entirely for nothing, the computation has told us that $1 \in \mathfrak{a}$.

[4] See page 573.

5.7. Lemma. (Jacobson radical of a domain of dimension at most 1) *Let* $\mathbf{A}$ *be an integral ring of dimension at most* 1.

1. *For every nonzero* a *in* $\mathbf{A}$ *we have* $\mathrm{Rad}(\mathbf{A}) \subseteq \sqrt[\mathbf{A}]{a\mathbf{A}}$.
2. *For finitely generated* $\mathfrak{b}$ *containing* $\mathrm{Rad}(\mathbf{A})$*, we have*
$$\mathrm{Rad}(\mathbf{A}) = \mathfrak{b}\big(\,\mathrm{Rad}(\mathbf{A}) : \mathfrak{b}\big).$$
3. *If* $\mathrm{Rad}(\mathbf{A})$ *is an invertible ideal,* $\mathbf{A}$ *is a Bézout domain.*

D Let $\mathfrak{a} = \mathrm{Rad}(\mathbf{A})$.
1. Let $x \in \mathfrak{a}$. The ring $\mathbf{A}/\langle a\rangle$ is zero-dimensional, so there exist y, $z \in \mathbf{A}$ and $m \in \mathbb{N}$ such that $x^m(1+xz) = ay$. As $x \in \mathrm{Rad}(\mathbf{A})$, we have $1+xz \in \mathbf{A}^\times$, therefore $x^m \in a\mathbf{A}$ and $x \in \sqrt[\mathbf{A}]{a\mathbf{A}}$.
2. If $\mathfrak{a} = 0$ it is clear, otherwise the ring $\mathbf{A}/\mathfrak{a}$ is reduced zero-dimensional, so the finitely generated ideal $\mathfrak{b}$ is equal to an ideal $\langle e\rangle$ modulo $\mathfrak{a}$, with e idempotent modulo $\mathfrak{a}$. Therefore $\mathfrak{b} = \mathfrak{b} + \mathfrak{a} = \mathfrak{a} + \langle e\rangle$, then $(\mathfrak{a} : \mathfrak{b}) = \mathfrak{a} + \langle 1 - e\rangle$, and finally
$$\mathfrak{b}(\mathfrak{a} : \mathfrak{b}) = (\mathfrak{a} + \langle e\rangle)(\mathfrak{a} + \langle 1 - e\rangle) = \mathfrak{a}.$$

3. Let $\mathfrak{c}_1$ be a nonzero finitely generated ideal. We define $\mathfrak{b}_1 = \mathfrak{c}_1 + \mathfrak{a}$ and $\mathfrak{c}_2 = (\mathfrak{c}_1 : \mathfrak{b}_1)$. By item *2* since $\mathfrak{a}$ is invertible, so is $\mathfrak{b}_1$. If $\mathfrak{b}_1\mathfrak{b}' = \langle b\rangle$ (b is regular), all the elements of $\mathfrak{c}_1\mathfrak{b}'$ are divisible by b. We then consider $\mathfrak{d} = \frac{1}{b}\mathfrak{c}_1\mathfrak{b}'$, therefore $\mathfrak{d}\mathfrak{b}_1 = \mathfrak{c}_1$ and $\mathfrak{d}$ is finitely generated. Clearly we have $\mathfrak{d} \subseteq \mathfrak{c}_2$. Conversely, if $x\mathfrak{b}_1 \subseteq \mathfrak{c}_1$ then $bx = x\mathfrak{b}_1\mathfrak{b}' \subseteq b\mathfrak{d}$, so $x \in \mathfrak{d}$. In short $\mathfrak{c}_2 = \mathfrak{d}$ and we have established the equality $\mathfrak{b}_1\mathfrak{c}_2 = \mathfrak{c}_1$, with $\mathfrak{c}_2$ finitely generated. By iterating the procedure we obtain an ascending sequence of finitely generated ideals $(\mathfrak{c}_k)_{k\in\mathbb{N}}$ with $\mathfrak{c}_{k+1} = (\mathfrak{c}_k : \mathfrak{b}_k)$ and $\mathfrak{b}_k = \mathfrak{c}_k + \mathfrak{a}$.
Actually $\mathfrak{c}_2 = \big(\mathfrak{c}_1 : (\mathfrak{c}_1 + \mathfrak{a})\big) = (\mathfrak{c}_1 : \mathfrak{a})$, then $\mathfrak{c}_3 = (\mathfrak{c}_2 : \mathfrak{a}) = (\mathfrak{c}_1 : \mathfrak{a}^2)$ and more generally $\mathfrak{c}_{k+1} = (\mathfrak{c}_1 : \mathfrak{a}^k)$.
Let $a \neq 0$ in $\mathfrak{c}_1$. By item *1*, $\mathfrak{a} \subseteq \sqrt{a\mathbf{A}}$. However, $\mathfrak{a}$ is finitely generated, therefore the inclusion $\mathfrak{a} \subseteq \sqrt{a\mathbf{A}}$ implies that for a certain k, $\mathfrak{a}^k \subseteq a\mathbf{A} \subseteq \mathfrak{c}_1$, therefore $\mathfrak{c}_{k+1} = \langle 1\rangle$.
When $\mathfrak{c}_{k+1} = \langle 1\rangle$, we have $\mathfrak{c}_1 = \prod_{i=1}^{k} \mathfrak{b}_i$, which is invertible as a product of invertible ideals.
We have shown that every nonzero finitely generated ideal is invertible, so the ring is a Prüfer domain, and by Proposition 5.3 it is a Bézout ring. □

6. Coherent Prüfer rings of dimension $\leqslant 1$

When a Prüfer ring is a Bézout ring

We now generalize a classical result often formulated as follows:[5] *an integral Dedekind ring having a finite number of maximal ideals is a PID.*

[5] See the constructive definition of a Dedekind ring on page 713.

6.1. Theorem. *Let* $\mathbf{A}$ *be a coherent Prüfer ring of dimension at most* 1 *and whose Jacobson radical contains a regular element. Then* $\mathbf{A}$ *is a Bézout ring.*

D Let $\mathfrak{b}$ be a finitely generated ideal. There exists a $b \in \mathfrak{b}$ such that $\operatorname{Ann}\mathfrak{b} = \operatorname{Ann} b = \langle e \rangle$ with e idempotent. Then $\mathfrak{a} = \mathfrak{b} + \langle e \rangle$ contains the regular element $b + e$: it is invertible and $\mathfrak{b} = (1 - e)\mathfrak{a}$. It suffices to show that $\mathfrak{a}$ is principal. This results from Proposition 5.3. □

The previous theorem and the following are to be compared with Theorem XI-3.12 which affirms that a GCD-domain of dimension at most 1 is a Bézout ring.

An important characterization

The result given in Theorem 6.2 below is important: the three computational machineries of normality, coherence and dimension at most 1 combine to provide the machinery of principal localization of finitely generated ideals.

6.2. Theorem. *A normal, coherent ring* $\mathbf{A}$ *of dimension at most* 1 *is a Prüfer ring.*

D Let us start by noticing that $(\mathbf{A} \div \mathfrak{a}\mathfrak{b}) = (\mathbf{A} \div \mathfrak{a}) \div \mathfrak{b}$.
Since $\mathbf{A}$ is a pp-ring, it suffices to treat the integral case and to finish with the elementary local-global machinery of pp-rings. We therefore suppose that $\mathbf{A}$ is a domain and we show that every finitely generated ideal $\mathfrak{a}$ containing a regular element is invertible.
Let us consider $(\mathbf{A} \div \mathfrak{a}) \in \operatorname{Ifr}\mathbf{A}$ and $\mathfrak{b} = \mathfrak{a}(\mathbf{A} \div \mathfrak{a})$, which is a finitely generated (integral) ideal of $\mathbf{A}$; we want to show that $\mathfrak{b} = \mathbf{A}$. Let us first show that $\mathbf{A} \div \mathfrak{b} = \mathbf{A}$. Let $y \in \mathbf{A} \div \mathfrak{b}$, hence $y(\mathbf{A} \div \mathfrak{a}) \subseteq (\mathbf{A} \div \mathfrak{a})$. Since $\mathbf{A} \div \mathfrak{a}$ is a faithful module (it contains 1) and is finitely generated, y is integral over $\mathbf{A}$ (see Fact III-8.2) so $y \in \mathbf{A}$ because $\mathbf{A}$ is normal.
By induction, by using $\mathbf{A} \div \mathfrak{b}^{k+1} = (\mathbf{A} \div \mathfrak{b}) \div \mathfrak{b}^k$, we obtain $\mathbf{A} \div \mathfrak{b}^k = \mathbf{A}$ for every $k \geqslant 1$.

Let us fix a regular element $x \in \mathfrak{b}$. By Lemma XI-3.10, there exists a $k \in \mathbb{N}^\star$ such that $\mathfrak{b}' := \langle x \rangle + \mathfrak{b}^k$ is invertible. Consequently $\mathfrak{b}'(\mathbf{A} \div \mathfrak{b}') = \mathbf{A}$. Finally, as $\mathfrak{b}^k \subseteq \mathfrak{b}' \subseteq \mathfrak{b}$, we have $\mathbf{A} \div \mathfrak{b}' = \mathbf{A}$, hence $\mathfrak{b}' = \mathbf{A}$ then $\mathfrak{b} = \mathbf{A}$. □

Example. Other than the example of the valuation rings given on page 691, which can have an arbitrary Krull dimension, there are other natural examples of Prüfer domains which are not of dimension $\leqslant 1$.
The *ring of integer-valued polynomials* is the subring of $\mathbb{Q}[X]$ formed by the polynomials $f(X)$ such that $f(x) \in \mathbb{Z}$ for all $x \in \mathbb{Z}$. We easily show that it is a free $\mathbb{Z}$-module admitting as its basis the combinatorial polynomials $\binom{x}{n}$ for $n \in \mathbb{N}$. The ideal generated by the $\binom{x}{n}$'s for $n \geqslant 1$ is not finitely generated.

One can show that an integer-valued polynomial can be evaluated at an arbitrary p-adic integer, which provides an uncountable set of prime ideals. This ring is a Prüfer domain of dimension two, but the proof of this result is not simple, especially if we ask that it be constructive. On this subject see [70, Ducos] and [130, Lombardi]. ■

The structure of finitely presented modules

6.3. Theorem. *Let* $\mathbf{A}$ *be a coherent Prüfer ring of dimension at most* 1. *Every projective module* M *of constant rank* $k \geqslant 1$ *is isomorphic to* $\mathbf{A}^{k-1} \oplus \mathfrak{a}$, *where* $\mathfrak{a}$ *is an invertible ideal. In particular, it is generated by* $k+1$ *elements. Finally, since* $\mathfrak{a} \simeq \bigwedge^k M$, *the isomorphism class of* M *as an* $\mathbf{A}$*-module determines that of* $\mathfrak{a}$.

D By Theorem 4.5, M is a direct sum of k invertible ideals. It therefore suffices to treat the case $M \simeq \mathfrak{a} \oplus \mathfrak{b}$, with invertible ideals $\mathfrak{a}$ and $\mathfrak{b}$. By Lemma 5.4, we can find an ideal $\mathfrak{a}_1$ such that $\mathfrak{a}_1 \simeq \mathfrak{a}$ (as $\mathbf{A}$-modules) and $\mathfrak{a}_1 + \mathfrak{b} = \langle 1 \rangle$ (as ideals). We then have the short exact sequence

$$\langle 0 \rangle \longrightarrow \mathfrak{a}_1\mathfrak{b} = \mathfrak{a}_1 \cap \mathfrak{b} \xrightarrow{\delta} \mathfrak{a}_1 \oplus \mathfrak{b} \xrightarrow{\sigma} \mathfrak{a}_1 + \mathfrak{b} = \mathbf{A} \longrightarrow \langle 0 \rangle\,,$$

where $\delta(x) = (x, -x)$ and $\sigma(x, y) = x + y$. Finally, since this sequence is split, we obtain $M \simeq \mathfrak{a} \oplus \mathfrak{b} \simeq \mathfrak{a}_1 \oplus \mathfrak{b} \simeq \mathbf{A} \oplus (\mathfrak{a}_1 \cap \mathfrak{b}) = \mathbf{A} \oplus (\mathfrak{a}_1\mathfrak{b})$. □

An immediate consequence is the following structure theorem.

6.4. Corollary. *Let* $\mathbf{A}$ *be a coherent Prüfer ring of dimension at most* 1. *Every finitely generated projective module is isomorphic to a direct sum*

$$r_1\mathbf{A} \oplus r_2\mathbf{A}^2 \oplus \cdots \oplus r_n\mathbf{A}^n \oplus \mathfrak{a},$$

where the r_i*'s are orthogonal idempotents (some can be null) and* $\mathfrak{a}$ *is a finitely generated ideal.*

6.5. Proposition. *Let* $\mathbf{A}$ *be a zero-dimensional arithmetic ring. Every matrix admits a reduced Smith form. Consequently every finitely presented* $\mathbf{A}$*-module is isomorphic to a direct sum of cyclic modules* $\mathbf{A}/\langle a_k \rangle$.

D If $\mathbf{A}$ is local, it is a local Bézout ring and the matrix admits a reduced Smith form (Proposition IV-7.2), which gives the result. By following the proof of the local case, and by applying the local-global machinery of arithmetic rings (page 463), we produce a family of comaximal elements $(s_1, \ldots, s_r)$ such that the result is guaranteed over each ring $\mathbf{A}[1/s_i]$.
Since $\mathbf{A}$ is zero-dimensional, every principal filter is generated by an idempotent (Lemma IV-8.2 *2*). Consider the idempotents e_i corresponding to the s_i's, then a fundamental system of orthogonal idempotents (r_j) such that each e_i is a sum of certain r_j's.
The ring is written as a finite product $\prod \mathbf{A}_j$ with the Smith reduction over each $\mathbf{A}_j$. The result is therefore guaranteed. □

Remarks. For the uniqueness of the decomposition, see Theorem IV-5.1. Moreover, the proof shows that the reduction can be done with products of elementary matrices. Finally, a generalization is proposed in Exercise 17. ∎

6.6. Corollary. *Let* $\mathbf{A}$ *be an arithmetic ring of dimension at most* 1*. Every finitely presented torsion* $\mathbf{A}$*-module is isomorphic to a direct sum of cyclic modules* $\mathbf{A}/\langle b, a_k\rangle$ *with* $b \in \mathrm{Reg}(\mathbf{A})$*.*

D The module is annihilated by an element $b \in \mathrm{Reg}(\mathbf{A})$. We consider it as an $\mathbf{A}/\langle b\rangle$-module and we apply Proposition 6.5. □

We can now synthesize Theorems 6.3 and 4.5, and Corollary 6.6 as follows. We leave it up to the reader to give the statement for the pp-ring case (i.e. for coherent Prüfer rings).

6.7. Theorem. (Theorem of the invariant factors)
Over a Prüfer domain $\mathbf{A}$ *of dimension at most* 1*, every finitely presented module is a direct sum*

- *of a finitely generated projective* $\mathbf{A}$*-module, null or of the form* $\mathbf{A}^r \oplus \mathfrak{a}$ *(*$r \geqslant 0$*,* $\mathfrak{a}$ *an invertible ideal),*
- *and of its torsion submodule, which is isomorphic to a direct sum of cyclic modules* $\mathbf{A}/\langle b, a_k\rangle$ *with* $b \in \mathrm{Reg}(\mathbf{A})$*.*

In addition

- *the ideal* $\mathfrak{a}$ *is uniquely determined by the module,*
- *we can assume that the ideals* $\langle b, a_k\rangle$ *are totally ordered with respect to the inclusion relation, and the decomposition of the torsion submodule is then unique in the precise sense given in Theorem IV-5.1.*

Remarks. 1) In particular, the structure theorem for finitely presented modules over a PID (Proposition IV-7.3) is valid for every Bézout domain of dimension at most 1.
2) For a torsion module M, the ideals $\langle b, a_k\rangle$ of the previous theorem are the *invariant factors* of M, in accordance with the definition given in Theorem IV-5.1. ∎

Reduction of matrices

The following theorem gives a reduced form for a column matrix, à la Bézout. It would be interesting to generalize it to an arbitrary matrix.

6.8. Theorem. *Let* $\mathbf{A}$ *be a coherent Prüfer ring of dimension at most* 1 *and* $x_1, \ldots, x_n \in \mathbf{A}$. *There exists a matrix* $M \in \mathbb{GL}_n(\mathbf{A})$ *such that*

$$M\ {}^{\mathrm{t}}[\,x_1\ \cdots\ x_n\,] = {}^{\mathrm{t}}[\,y_1\ y_2\ 0\ \cdots\ 0\,].$$

D It suffices to treat the case where $n = 3$.
If e is an idempotent, then $\mathbb{GL}_n(\mathbf{A}) \simeq \mathbb{GL}_n(\mathbf{A}_e) \times \mathbb{GL}_n(\mathbf{A}_{1-e})$: even if it entails localizing by inverting both the annihilating idempotent of $\langle x_1, x_2, x_3\rangle$ and its complement, we can therefore assume that $\mathrm{Ann}(\langle x_1,x_2,x_3\rangle) = \langle 0\rangle$.
Let A be a principal localization matrix for (x_1, x_2, x_3).
The module $K = \mathrm{Im}(\mathrm{I}_3 - A)$ is the kernel of linear form associated with the row vector $X = [\,x_1\ x_2\ x_3\,]$ and it is a projective module of rank 2 as a direct summand in $\mathbf{A}^3$. Theorem 6.3 tells us that K contains a free submodule of rank 1 as a direct summand in $\mathbf{A}^3$, that is a module $\mathbf{A}v$ where v is a unimodular vector of $\mathbf{A}^3$. By Theorem 5.1, this vector is the last column of an invertible matrix U; the last coefficient of XU is null and the matrix $M = {}^{\mathrm{t}}U$ is the matrix we were looking for. □

7. Factorization of finitely generated ideals

General factorizations

In a general arithmetic ring it seems that we do not have any factorization results that go beyond what stems from the fact that the invertible ideals (i.e. the finitely generated ideals containing a regular element) form a GCD-monoid, and more precisely the non-negative submonoid of an l-group.

For example the Riesz theorem can be reread as follows.

7.1. Theorem. (Riesz theorem for arithmetic rings)
Let $\mathbf{A}$ *be an arithmetic ring,* $(\mathfrak{a}_i)_{i\in[\![1..n]\!]}$ *and* $(\mathfrak{b}_j)_{j\in[\![1..m]\!]}$ *be invertible ideals such that* $\prod_{i=1}^{n} \mathfrak{a}_i = \prod_{j=1}^{m} \mathfrak{b}_j$. *Then there exist invertible ideals* $(\mathfrak{c}_{i,j})_{i\in[\![1..n]\!],j\in[\![1..m]\!]}$ *such that we have for all* i *and all* j,

$$\mathfrak{a}_i = \textstyle\prod_{j=1}^{m} \mathfrak{c}_{i,j} \ \text{ and } \ \mathfrak{b}_j = \prod_{i=1}^{n} \mathfrak{c}_{i,j}.$$

Factorizations in dimension 1

7.2. Theorem. *In a coherent Prüfer ring of dimension at most* 1, *we consider two finitely generated ideals* $\mathfrak{a}$ *and* $\mathfrak{b}$ *with* $\mathfrak{a}$ *invertible.*
Then we can write

$$\mathfrak{a} = \mathfrak{a}_1\mathfrak{a}_2 \ \text{ with } \ \mathfrak{a}_1 + \mathfrak{b} = \langle 1\rangle \ \text{ and } \ \mathfrak{b}^n \subseteq \mathfrak{a}_2,$$

for some suitable integer n. *This expression is unique and we have*

$$\mathfrak{a}_1 + \mathfrak{a}_2 = \langle 1\rangle\,,\ \ \mathfrak{a}_2 = \mathfrak{a} + \mathfrak{b}^n = \mathfrak{a} + \mathfrak{b}^{n+1}.$$

D This is a special case of Lemma XI-3.10. □

Remark. We do not need to assume that the ideals are detachable.

7.3. Theorem. *We consider in a coherent Prüfer ring of dimension at most* 1 *some pairwise comaximal finitely generated ideals* $\mathfrak{p}_1$, …, $\mathfrak{p}_n$, *and an invertible ideal* $\mathfrak{a}$.
We can write $\mathfrak{a} = \mathfrak{a}_0 \cdot \mathfrak{a}_1 \cdots \mathfrak{a}_n$ *with the pairwise comaximal finitely generated ideals* $\mathfrak{a}_0$, …, $\mathfrak{a}_n$ *and, for* $j \geqslant 1$, $\mathfrak{p}_j^{m_j} \subseteq \mathfrak{a}_j$ *with* m_j *as the suitable integer. This expression is unique and we have* $\mathfrak{a}_j = \mathfrak{a} + \mathfrak{p}_j^{m_j} = \mathfrak{a} + \mathfrak{p}_j^{1+m_j}$.

D By induction by using Theorem 7.2 with $\mathfrak{b} \in \{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}$. □

Prüfer rings admitting partial factorizations

Let us re-express the definition of partial decompositions (given for l-groups) in the framework of the monoid of invertible ideals of a coherent Prüfer ring $\mathbf{A}$ (this is the non-negative submonoid of the l-group formed by the invertible elements of $\operatorname{Ifr}(\mathbf{A})$).

7.4. Definition. Let $F = (\mathfrak{a}_1, \dots, \mathfrak{a}_n)$ be a finite family of invertible ideals in a ring $\mathbf{A}$. We say that F admits a *partial factorization* if there exists a family $P = (\mathfrak{p}_1, \dots, \mathfrak{p}_k)$ of pairwise comaximal invertible ideals such that every ideal $\mathfrak{a}_j$ can be written in the form: $\mathfrak{a}_j = \mathfrak{p}_1^{m_{1j}} \cdots \mathfrak{p}_k^{m_{kj}}$ (certain m_{ij}'s can be null). We then say that P is a *partial factorization basis* for the family F.

For the monoid $\operatorname{Ifr}(\mathbf{A})$ to be discrete we need to assume that $\mathbf{A}$ is strongly discrete. This leads to the following definition.

7.5. Definition. A ring is called a *partial factorization Prüfer ring* if it is a strongly discrete coherent Prüfer ring[6] and if every finite family of invertible ideals admits a partial factorization.

7.6. Lemma. *A partial factorization Prüfer ring is of dimension at most* 1.

D We consider a regular element y. We want to show that $\mathbf{A}/\langle y\rangle$ is zero-dimensional.
For this we take a regular x and we want to find $a \in \mathbf{A}$ and $n \in \mathbb{N}$ such that $x^n(1 - ax) \equiv 0 \bmod y$. The partial factorization of (x, y) gives

$$\langle x\rangle = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_i^{\alpha_i} \mathfrak{q}_1^{\beta_1} \cdots \mathfrak{q}_j^{\beta_j} = \mathfrak{a}\mathfrak{b}, \text{ and } \langle y\rangle = \mathfrak{p}_1^{\gamma_1} \cdots \mathfrak{p}_i^{\gamma_i} \mathfrak{h}_1^{\delta_1} \cdots \mathfrak{h}_k^{\delta_k} = \mathfrak{c}\mathfrak{d}$$

[6] By Proposition 1.5 an arithmetic ring is strongly discrete if and only if the divisibility relation is explicit.

with all the exponents > 0. There exists an $n \geqslant 0$ such that $\mathfrak{a}^n$ is a multiple of $\mathfrak{c}$ which gives $\langle x^n \rangle = \mathfrak{c}\mathfrak{g}$. As $\langle x \rangle + \mathfrak{d} = 1$, there exists some $a \in \mathbf{A}$ such that $1 - ax \in \mathfrak{d}$. We therefore have $\langle y \rangle = \mathfrak{c}\mathfrak{d} \supseteq \mathfrak{c}\mathfrak{g}\mathfrak{d} = \langle x^n \rangle \, \mathfrak{d} \supseteq \langle x^n(1 - ax) \rangle$, i.e. $x^n(1 - ax) \equiv 0 \bmod y$. □

Dedekind rings

7.7. Definition. We call a strongly discrete and Noetherian coherent Prüfer ring a *Dedekind ring*. A *Dedekind domain* is an integral Dedekind ring (or yet again a connected Dedekind ring).

7.8. Theorem. *A Dedekind ring is a partial factorization Prüfer ring, so of dimension at most* 1*.*

D Theorem XI-2.16 gives the partial factorization result in the framework of distributive lattices and we finish with Lemma 7.6. □

7.9. Theorem. (Characterizations of Dedekind rings)
For some ring $\mathbf{A}$ *the following properties are equivalent.*

1. $\mathbf{A}$ *is a Dedekind ring.*
2. $\mathbf{A}$ *is an arithmetic, Noetherian, pp-ring with explicit divisibility.*
3. $\mathbf{A}$ *is a normal pp-ring of dimension at most* 1*, with explicit divisibility, which is coherent and Noetherian.*

D Since $\mathbf{A}$ is a coherent Prüfer ring if and only if it is arithmetic and a pp-ring, and since an arithmetic ring is strongly discrete if and only if it is with explicit divisibility, items *1* and *2* are equivalent.
The implication *1* ⇒ *3* results from Theorem 7.8, and Theorem 6.2 gives the converse (it simply suffices to add strongly discrete and Noetherian in the hypothesis and the conclusion). □

7.10. Definition. Let $\mathfrak{a}$ be an ideal of a ring $\mathbf{A}$. We say that $\mathfrak{a}$ admits a *total factorization* if it is of the form $\mathfrak{a} = \mathfrak{p}_1^{m_1} \cdots \mathfrak{p}_k^{m_k}$ ($m_i > 0$, $k > 0$) where ideals $\mathfrak{p}_i$ are detachable, strict and maximal (in other words, each ring $\mathbf{A}/\mathfrak{p}_i$ is a nontrivial discrete field).

7.11. Theorem and definition. (Total factorization Dedekind ring)
For a nontrivial strongly discrete pp-ring $\mathbf{A}$*, the following properties are equivalent.*

1. *Every principal ideal* $\langle a \rangle \neq \langle 1 \rangle$ *with* $a \in \operatorname{Reg} \mathbf{A}$ *admits a total factorization.*
2. *The ring* $\mathbf{A}$ *is a Dedekind ring, and every invertible ideal* $\neq \langle 1 \rangle$ *admits a total factorization.*

Such a ring is called a total factorization Dedekind ring.

D We need to show that *1* implies *2*. We treat the integral case (the pp-ring case is then easily deduced).

We refer to Exercise III-22 and its solution. We see that every finitely generated ideal containing a regular element is invertible, and that it admits a total factorization. Theorem 4.1 then tells us that $\mathbf{A}$ is a coherent Prüfer ring. It remains to see that it is Noetherian. Consider a finitely generated ideal and its total factorization $\mathfrak{a} = \mathfrak{p}_1^{m_1} \cdots \mathfrak{p}_k^{m_k}$. Every finitely generated ideal $\mathfrak{b} \supseteq \mathfrak{a}$ is of the form $\mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_k^{n_k}$ with all the $n_i \in [\![0..m_i]\!]$. Every ascending sequence of finitely generated ideals starting with $\mathfrak{a}$ therefore admits two consecutive equal terms. □

Remark. Exercise III-22 uses no complex theoretical paraphernalia. So it is possible to expose the theory of Dedekind rings by starting with the previous theorem, which promptly leads to the essential results. The main drawback of this approach is that it is based on a total factorization property which is not generally satisfied from a constructive point of view, even by the PIDs, and which does not generally extend to the integral extensions. ■

Recall that we have already established Theorem 4.10 regarding the finite extensions of Dedekind rings.

We can add the following more precise result.

7.12. Theorem. (A computation of integral closure)
Let $\mathbf{A}$ *be a Dedekind ring,* $\mathbf{K} = \mathrm{Frac}(\mathbf{A})$*,* $\mathbf{L} \supseteq \mathbf{K}$ *be an étale* $\mathbf{K}$*-algebra and* $\mathbf{B}$ *be the integral closure of* $\mathbf{A}$ *in* $\mathbf{L}$*.*
Suppose that $\mathbf{L} = \mathbf{K}[X]/\langle f\rangle$ *with monic* $f \in \mathbf{A}[X]$ *and* $\mathrm{disc}_X(f) \in \mathrm{Reg}\,\mathbf{A}$ *(which is not really restrictive). If* $\langle \mathrm{disc}_X(f)\rangle$ *admits a total factorization, and if for each maximal ideal* $\mathfrak{m}$ *of this factorization, the residual field* $\mathbf{A}/\mathfrak{m}$ *is perfect, then* $\mathbf{B}$ *is a finitely generated projective* $\mathbf{A}$*-module.*

D As $\mathbf{A}$ is a pp-ring, it suffices to treat the case where $\mathbf{A}$ is integral (elementary local-global machinery of pp-rings), so $\mathbf{K}$ is a discrete field. The hypothesis $\mathbf{L} = \mathbf{K}[X]/\langle f\rangle$ with monic $f \in \mathbf{A}[X]$ and $\mathrm{disc}_X(f) \in \mathrm{Reg}\,\mathbf{A}$ is not really restrictive because by Theorem VI-1.9, $\mathbf{L}$ is a product of monogenic étale $\mathbf{K}$-algebras. We can even suppose that $\mathbf{L}$ is an étale field over $\mathbf{K}$ (elementary local-global machinery of reduced zero-dimensional rings).

Let $\Delta = \mathrm{disc}_X(f)$. By item *5* of Theorem 4.10 we have the inclusions

$$\mathbf{A}[x] \subseteq \mathbf{B} \subseteq \tfrac{1}{\Delta}\,\mathbf{A}[x].$$

Thus $\mathbf{B}$ is a submodule of the finitely generated $\mathbf{A}$-module $\frac{1}{\Delta}\mathbf{A}[x]$. By Theorem 4.5, if $\mathbf{B}$ is finitely generated, it is finitely generated projective.

We have $\mathbf{A}[x, \frac{1}{\Delta}] = \mathbf{B}[\frac{1}{\Delta}]$, so $\mathbf{B}$ is finitely generated after localization at $\Delta^{\mathbb{N}}$. It remains to show that $\mathbf{B}$ is finitely generated after localization at $S = 1 + \Delta\mathbf{A}$. The ring $\mathbf{A}_S$ is a Bézout ring (Theorem 6.1). If $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are the maximal ideals that intervene in the total factorization of Δ, the monoids $1 + \mathfrak{p}_i$ are comaximal in $\mathbf{A}_S$, and it suffices to show that $\mathbf{B}$ is finitely generated after localization at each of the $1 + \mathfrak{p}_i$. We are thus brought back to the case treated in Lemma 7.13 that follows. □

Note that a local Dedekind domain $\mathbf{V}$ is just as much a strongly discrete Noetherian valuation domain, as a local PID with detachable $\mathbf{V}^{\times}$. The following lemma in addition requires that the radical be principal (which is automatic in classical mathematics). In this case we will also say that $\mathbf{V}$ is a *discrete valuation ring* or a *DVR*, according to the classical terminology; and any generator of $\operatorname{Rad}\mathbf{V}$ is called a *regular parameter.*

7.13. Lemma. *Let* $\mathbf{V}$ *be a local Dedekind domain with* $\operatorname{Rad}\mathbf{V} = p\mathbf{V}$ *and with perfect residual field* $\mathbf{k} = \mathbf{V}/\langle p\rangle$*. Let* $f \in \mathbf{V}[X]$ *be an irreducible monic, therefore* $\Delta = \operatorname{disc}_X(f) \in \operatorname{Reg}\mathbf{V}$*. Let* $\mathbf{K} = \operatorname{Frac}(\mathbf{V})$*,* $\mathbf{L} = \mathbf{K}[x] = \mathbf{K}[X]/\langle f\rangle$*, and* $\mathbf{W}$ *be the integral closure of* $\mathbf{V}$ *in* $\mathbf{L}$*. Then* $\mathbf{W}$ *is finitely generated over* $\mathbf{V}$*.*

D Since $\mathbf{k}$ is perfect, by Lemma VI-1.16, for every monic polynomial f_i of $\mathbf{V}[X]$ we know how to compute the "squarefree subset" of $\overline{f_i}$ (f_i taken modulo p), i.e. a separable polynomial $\overline{g_i}$ in $\mathbf{k}[X]$ which divides $\overline{f_i}$, and whose power is a multiple of $\overline{f_i}$.
The strategy is to add some elements $x_i \in \mathbf{W}$ to $\mathbf{V}[x]$ until we obtain a ring $\mathbf{W}'$ whose radical is an invertible ideal. When this is realized, we know by Lemma 5.7 that $\mathbf{W}'$ is a Prüfer domain, therefore that it is integrally closed, thus equal to $\mathbf{W}$.
To "construct" $\mathbf{W}'$ (finitely generated over $\mathbf{V}$) we will use in an induction the following fact, initialized with $\mathbf{W}_1 = \mathbf{V}[x]$ ($x_1 = x$, $r_1 = 1$).
Fact. Let $\mathbf{W}_k = \mathbf{V}[x_1, \ldots, x_{r_k}] \subseteq \mathbf{W}$*, then*

$$\operatorname{Rad}(\mathbf{W}_k) = \big\langle p, g_1(x_1), \ldots, g_k(x_{r_k})\big\rangle,$$

where $\overline{g_i}$ *is the squarefree subset of* $\overline{f_i}$ *and* f_i *is the minimal polynomial over* $\mathbf{K}$ *of the integer* x_i*.*

Theorem IX-1.8 states that $\operatorname{Rad}(\mathbf{W}_k) = \mathrm{D}_{\mathbf{W}_k}(p\mathbf{W}_k)$. This ideal is the inverse image of $\mathrm{D}_{\mathbf{W}_k/p\mathbf{W}_k}(0)$ and we have $\mathbf{W}_k/p\mathbf{W}_k = \mathbf{k}[\overline{x_1}, \ldots, \overline{x_{r_k}}]$. As the $g_i(x_i)$'s are nilpotent modulo p by construction, they are in the nilradical $\mathrm{D}_{\mathbf{W}_k}(p\mathbf{W}_k)$. Now it suffices to verify that the $\mathbf{k}$-algebra

$$\mathbf{k}[\overline{x_1}, \ldots, \overline{x_{r_k}}]/\big\langle \overline{g_1}(\overline{x_1}), \ldots, \overline{g_{r_k}}(\overline{x_{r_k}})\big\rangle$$

is reduced. Actually $\mathbf{W}_k$ is a finitely generated $\mathbf{V}$-submodule of $\frac{1}{\Delta}\mathbf{V}[x]$, therefore is free finite over $\mathbf{V}$. Consequently $\mathbf{W}_k/p\mathbf{W}_k$ is strictly finite over $\mathbf{k}$, and it is étale because it is generated by some elements that annihilate separable polynomials over $\mathbf{k}$ (Theorem VI-1.7). □

Given this, since $\mathbf{W}$ is a Prüfer domain, we know how to invert the finitely generated ideal $\mathrm{Rad}(\mathbf{W}_k)$ in $\mathbf{W}$.

This means computing some elements $x_{r_k+1}, \ldots, x_{r_{k+1}}$ of $\mathbf{W}$ and a finitely generated ideal $\mathfrak{g}_k$ in the new ring $\mathbf{W}_{k+1}$ such that the ideal $\mathfrak{g}_k \,\mathrm{Rad}(\mathbf{W}_k)$ is principal (and nonzero). However, it is possible that the generators of $\mathrm{Rad}(\mathbf{W}_k)$ do not generate the ideal $\mathrm{Rad}(\mathbf{W}_{k+1})$ of $\mathbf{W}_{k+1}$, which forces an iteration of the process.

The ascending sequence of $\mathbf{W}_k$'s is an ascending sequence of finitely generated $\mathbf{V}$-modules contained in $\frac{1}{\Delta}\mathbf{V}[x]$, therefore it admits two equal consecutive terms. In this case we have reached the required goal. □

7.14. Concrete local-global principle. (Dedekind rings)
Let $s_1, \ldots, s_n$ be comaximal elements of a ring $\mathbf{A}$. Then

1. *The ring $\mathbf{A}$ is strongly discrete Noetherian coherent if and only if each of the $\mathbf{A}_{s_i}$'s is strongly discrete Noetherian coherent.*
2. *The ring $\mathbf{A}$ is a Dedekind ring if and only if each of the $\mathbf{A}_{s_i}$'s is a Dedekind ring.*

D We already know that the concrete local-global principle works for the Prüfer rings and for the coherent rings with comaximal monoids. The same goes for the rings or Noetherian modules (a proof is given with the local-global principle XV-2.2).

It remains to examine the "strongly discrete" property in the case of comaximal elements. Let $\mathfrak{a}$ be a finitely generated ideal and $x \in \mathbf{A}$. It is clear that if we have a test for $x \in \mathfrak{a}\mathbf{A}_{s_i}$ for each of the s_i's, this provides a test for $x \in \mathfrak{a}\mathbf{A}$. The difficulty is in the other direction: if $\mathbf{A}$ is strongly discrete and if $s \in \mathbf{A}$, then $\mathbf{A}[1/s]$ is strongly discrete. It is not true in general, but it is true for the Noetherian coherent rings. Indeed, the membership $x \in \mathfrak{a}\mathbf{A}[1/s]$ is equivalent to $x \in (\mathfrak{a} : s^\infty)_\mathbf{A}$. However, the ideal $(\mathfrak{a} : s^\infty)_\mathbf{A}$ is the union of the ascending sequence of finitely generated ideals $(\mathfrak{a} : s^n)_\mathbf{A}$, and as soon as $(\mathfrak{a} : s^n)_\mathbf{A} = (\mathfrak{a} : s^{n+1})_\mathbf{A}$, the sequence becomes constant. □

Exercises and problems

Exercise 1. *(Another "determinant trick")*
Let E be a faithful $\mathbf{A}$-module generated by n elements and $\mathfrak{a} \subseteq \mathfrak{b}$ be two ideals of $\mathbf{A}$ satisfying $\mathfrak{a}E = \mathfrak{b}E$. Show that $\mathfrak{a}\mathfrak{b}^{n-1} = \mathfrak{b}^n$.

Exercise 2. *(Principal localization matrices in* $\mathbb{M}_2(\mathbf{A})$*)* Let x, $y \in \mathbf{A}$.

1. Show that the ideal $\langle x, y\rangle$ is locally principal if and only if there exists a matrix $B \in \mathbb{M}_2(\mathbf{A})$ of trace 1 satisfying $[\,x\ y\,]B = 0$; in this case, $A = \widetilde{B}$ is a principal localization matrix for (x, y).

2. Let $z \in \mathbf{A}$; suppose that there exists an ideal $\mathfrak{b}$ such that $\langle x, y\rangle\,\mathfrak{b} = \langle z\rangle$. Show that there exists a $B \in \mathbb{M}_2(\mathbf{A})$ such that $z[x\ y]B = 0$ and $z\big(1 - \mathrm{Tr}(B)\big) = 0$.

3. Deduce from the previous questions another proof of Lemma 3.3.

Exercise 3. *(***A** *is arithmetic* $\Leftrightarrow$ $\mathbf{A}(X)$ *is a Bézout ring)* See also Exercise XVI-5. Let $\mathbf{A}$ be a ring and $\mathbf{A}(X)$ be the Nagata ring.

1. Show that for $a, b \in \mathbf{A}$, $a \mid b$ in $\mathbf{A}$ if and only if $a \mid b$ in $\mathbf{A}(X)$.

2. If $\mathbf{A}$ is an arithmetic ring and $f \in \mathbf{A}[X]$, we have in $\mathbf{A}(X)$

$$\langle f\rangle = \mathrm{c}_{\mathbf{A}}(f)\mathbf{A}(X).$$

Also show that $\mathbf{A}(X)$ is a Bézout ring.

3. Let x, $y \in \mathbf{A}$. Show that if $\langle x, y\rangle$ is locally principal in $\mathbf{A}(X)$, it is locally principal in $\mathbf{A}$ (use Exercise 2). In particular, if $\mathbf{A}(X)$ is arithmetic, the same goes for $\mathbf{A}$. A fortiori, if $\mathbf{A}\langle X\rangle$ is arithmetic, the same goes for $\mathbf{A}$.

4. Conclude the result.

Note. Concerning the ring $\mathbf{A}(X)$ see Fact IX-6.7 and Exercise IX-20.

Exercise 4. *(A few other characteristic properties of arithmetic rings)* For any ring $\mathbf{A}$, the following properties are equivalent.

(1) The ring $\mathbf{A}$ is an arithmetic ring.

(2.1) For all ideals $\mathfrak{a}$, $\mathfrak{b}$ and $\mathfrak{c}$ we have $\mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c}) = (\mathfrak{a} \cap \mathfrak{b}) + (\mathfrak{a} \cap \mathfrak{c})$.

(2.2) As above but limiting ourselves to the principal ideals.

(2.3) As above but limiting ourselves to the case $\mathfrak{b} = \langle x\rangle$, $\mathfrak{c} = \langle y\rangle$ and $\mathfrak{a} = \langle x + y\rangle$.

(3.1) For all ideals $\mathfrak{a}$, $\mathfrak{b}$ and $\mathfrak{c}$ we have $\mathfrak{a} + (\mathfrak{b} \cap \mathfrak{c}) = (\mathfrak{a} + \mathfrak{b}) \cap (\mathfrak{a} + \mathfrak{c})$.

(3.2) As above but limiting ourselves to the principal ideals.

(3.3) As above but limiting ourselves to the case $\mathfrak{a} = \langle x\rangle$, $\mathfrak{b} = \langle y\rangle$ and $\mathfrak{c} = \langle x + y\rangle$.

(4.1) For all finitely generated ideals $\mathfrak{a}$, $\mathfrak{b}$ and $\mathfrak{c}$ we have $(\mathfrak{b}+\mathfrak{c}) : \mathfrak{a} = (\mathfrak{b} : \mathfrak{a})+(\mathfrak{c} : \mathfrak{a})$.

(4.2) As above with principal ideals $\mathfrak{b}$ and $\mathfrak{c}$, and $\mathfrak{a} = \mathfrak{b} + \mathfrak{c}$.

(5.1) For every ideal $\mathfrak{a}$ and all the finitely generated ideals $\mathfrak{b}$ and $\mathfrak{c}$ we have the equality

$$\mathfrak{a} : (\mathfrak{b} \cap \mathfrak{c}) = (\mathfrak{a} : \mathfrak{b}) + (\mathfrak{a} : \mathfrak{c}).$$

(5.2) As above with principal ideals $\mathfrak{b}$ and $\mathfrak{c}$, and $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$.

Hint: to prove that the conditions are necessary we use the general method explained on page 463.

Exercise 5. Prove in classical mathematics that a ring is normal if and only if it becomes normal when we localize at an arbitrary prime ideal (recall that in the integral case, normal means integrally closed in its quotient field).

Exercise 6. *(Algebraic closure: a theorem due to Zariski)*
Let $\mathbf{K} \subseteq \mathbf{L}$ be two discrete fields, $\mathbf{K}'$ be the algebraic closure of $\mathbf{K}$ in $\mathbf{L}$. Then the algebraic closure of $\mathbf{K}(X_1, \dots, X_n)$ in $\mathbf{L}(X_1, \dots, X_n)$ is $\mathbf{K}'(X_1, \dots, X_n)$; an analogous result holds if we replace algebraic closure by separable algebraic closure.

Exercise 7. *(A lack of integrality by scalar extension)*
Let $\mathbf{k}$ be a discrete field of characteristic $p \geqslant 3$, $a \in \mathbf{k}$ and $f = Y^2 - f(X) \in \mathbf{k}[X, Y]$ with $f(X) = X^p - a$.

1. Show that $Y^2 - f(X)$ is *absolutely irreducible*, that is that for every overfield $\mathbf{k}' \supseteq \mathbf{k}$, the polynomial $Y^2 - f(X)$ is irreducible in $\mathbf{k}'[X, Y]$.

Let $\mathbf{k}[x, y] = \mathbf{k}[X, Y] \big/ \big\langle Y^2 - f(X) \big\rangle$ and $\mathbf{k}(x, y) = \mathrm{Frac}(\mathbf{k}[x, y])$.

2. Show that $\mathbf{k}$ is algebraically closed in $\mathbf{k}(x, y)$ and that for every algebraic extension $\mathbf{k}'$ of $\mathbf{k}$, we have $\mathbf{k}' \otimes_{\mathbf{k}} \mathbf{k}(x, y) = \mathbf{k}'(x, y)$.

3. Suppose that $a \notin \mathbf{k}^p$. Show that $\mathbf{k}[x, y]$ is integrally closed and that $\mathbf{k}(x, y)$ is not a field of rational fractions with one indeterminate over $\mathbf{k}$.

4. Suppose $a \in \mathbf{k}^p$ (for example $a = 0$). Show that $\mathbf{k}[x, y]$ is not integrally closed and explicate $t \in \mathbf{k}(x, y)$ such that $\mathbf{k}(x, y) = \mathbf{k}(t)$.

Exercise 8. *(The ring of functions over the projective line minus a finite number of points)*
We informally use in this exercise the notions of an affine scheme and of a projective line which have already been discussed in Sections VI-3 and X-4 (see pages 558 to 561).

If $\mathbf{k}$ is a discrete field, the $\mathbf{k}$-algebra of polynomial functions defined over the affine line $\mathbb{A}^1(\mathbf{k})$ is $\mathbf{k}[t]$. If we think of $\mathbb{A}^1(\mathbf{k}) \cup \{\infty\} = \mathbb{P}^1(\mathbf{k})$, the elements of $\mathbf{k}[t]$ are then the rational fractions over $\mathbb{P}^1(\mathbf{k})$ which are "defined everywhere, except maybe at ∞."

Let $t_1, \dots, t_r$ be points of this affine line (we can have $r = 0$). We equip $\mathbb{A}^1(\mathbf{k}) \setminus \{t_1, \dots, t_r\}$ (affine line minus r points) with a structure of an affine variety by forcing the invertibility of the $t - t_i$'s, i.e. by defining

$$\mathbf{B} = \mathbf{k}\big[t, (t - t_1)^{-1}, \dots, (t - t_r)^{-1}\big] \simeq \mathbf{k}[t, x] / \langle F(t, x) \rangle,$$

with $F(t, x) = (t - t_1) \cdots (t - t_r) \cdot x - 1$. This $\mathbf{k}$-algebra $\mathbf{B}$ then appears as the algebra of rational fractions over $\mathbb{P}^1(\mathbf{k})$ defined everywhere except at the points ∞ and t_i. It is an integrally closed ring and even a Bézout ring (indeed, it is a localized ring of $\mathbf{k}[t]$).

Analogously, for n points $t_1, \dots, t_n$ of the affine line (with $n \geqslant 1$ this time), we can consider the $\mathbf{k}$-algebra

$$\mathbf{A} = \mathbf{k}\big[(t - t_1)^{-1}, \dots, (t - t_n)^{-1}\big] \subseteq \mathbf{k}(t).$$

This ring $\mathbf{A}$ is a localized ring of $\mathbf{k}[(t - t_1)^{-1}]$ (which is isomorphic to $\mathbf{k}[X]$) since by letting $v = (t - t_1)^{-1}$, we have $t - t_i = \big((t_1 - t_i)v + 1\big)/v$. So,

$$\mathbf{A} = \mathbf{k}\Big[v, \big((t_1 - t_2)v + 1\big)^{-1}, \dots, \big((t_1 - t_n)v + 1\big)^{-1}\Big] \subseteq \mathbf{k}(v) = \mathbf{k}(t).$$

The $\mathbf{k}$-algebra $\mathbf{A}$ is therefore an integrally closed ring (and even a Bézout domain).

By letting $p(t) = (t - t_1) \cdots (t - t_n)$, we easily have the equality

$$\mathbf{A} = \mathbf{k}[1/p, t/p, \ldots, t^{n-1}/p].$$

The $\mathbf{k}$-algebra $\mathbf{A}$, constituted of rational fractions u/p^s with $\deg(u) \leqslant ns$, appears as that of rational fractions defined everywhere over $\mathbb{P}_1(\mathbf{k})$ (including at the point $t = \infty$) except eventually at the points t_i. In short, we can agree that $\mathbf{A}$ is the $\mathbf{k}$-algebra of the "functions" defined over the projective line minus the points t_1, $\ldots$, t_n.

We study in this exercise a more general case where p is a monic polynomial of degree $n \geqslant 1$.

Let $\mathbf{k}$ be a discrete field and $p(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0 \in \mathbf{k}[t]$ $(n \geqslant 1)$, where t is an indeterminate. Let $x_i = t^i/p$.
Show that the integral closure of $\mathbf{k}[x_0]$ in $\mathbf{k}(t)$ is the $\mathbf{k}$-algebra

$$\mathbf{A} = \mathbf{k}[x_0, \ldots, x_{n-1}] = \{\, u/p^s \mid s \in \mathbb{N},\, u \in \mathbf{k}[t],\ \deg(u) \leqslant ns \,\}.$$

In addition, $\mathrm{Frac}(\mathbf{A}) = \mathbf{k}(t)$.

Exercise 9. *(A presentation of the algebra of functions over the projective line minus a finite number of points)*
The context is that of Exercise 8, but this time $\mathbf{k}$ is an arbitrary ring. Let $p = a_n t^n + \cdots + a_1 t + a_0 \in \mathbf{k}[t]$ be a monic polynomial $(a_n = 1)$ and

$$\mathbf{A} = \mathbf{k}[1/p, t/p, \ldots, t^{n-1}/p].$$

Let $x_i = t^i/p$ for $i \in [\![0..n-1]\!]$. We can write $\mathbf{A} = \mathbf{k}[\underline{X}]/\mathfrak{a}$ where $(\underline{X}) = (X_0, \ldots, X_{n-1})$ and $\mathfrak{a}$ is the ideal of the relators between $(x_0, \ldots, x_{n-1})$. It will be convenient to define x_n by $x_n = t^n/p$; we therefore have $x_j = x_0 t^j$ and

$$\textstyle\sum_{i=0}^{n} a_i x_i = 1 \quad \text{or yet} \quad x_n = 1 - \sum_{i=0}^{n-1} a_i x_i.$$

The equality on the right-hand side proves that $x_n \in \mathbf{A}$.

1. Prove that the following family R gives relators between the x_j's.

$$R \ : \quad x_i x_j = x_k x_\ell \qquad \text{for } i + j = k + \ell, \qquad 0 \leqslant i, j, k, \ell \leqslant n.$$

We define the subfamily $R_{\min}$ with $\frac{n(n-1)}{2}$ relators.

$$R_{\min} \ : \quad x_i x_j = x_{i-1} x_{j+1}, \qquad 1 \leqslant i \leqslant j \leqslant n-1.$$

2. Show that the family $R_{\min}$ (so R also) generates the ideal of the relators between the x_i's for $i \in [\![0..n-1]\!]$. In other words, if we let $\varphi : \mathbf{k}[\underline{X}] \to \mathbf{k}[t, 1/p]$ be the morphism defined by $X_i \mapsto x_i$ for $i \in [\![0..n-1]\!]$, this means that $\operatorname{Ker} \varphi$ is generated by

$$X_i X_j - X_{i-1} X_{j+1}, \qquad 1 \leqslant i \leqslant j \leqslant n-1 \quad (\text{with } X_n := 1 - \textstyle\sum_{i=0}^{n-1} a_i X_i).$$

You may use the $\mathbf{k}$-module $\mathbf{k}[X_0] \oplus \mathbf{k}[X_0]X_1 \oplus \cdots \oplus \mathbf{k}[X_0]X_{n-1}$.

Exercise 10. *(Emmanuel's trick)*
Give a direct proof of item *1* of Lemma 4.7 without using Kronecker's theorem.

Exercise 11. *(Another proof of Kronecker's theorem)*
Consider the polynomials

$$f(T) = a_0T^n + \cdots + a_n, \quad g(T) = b_0T^m + \cdots + b_m \text{ and}$$
$$h(T) = f(T)g(T) = c_0T^{n+m} + \cdots + c_{n+m}.$$

Kronecker's theorem III-3.3 affirms that each product a_ib_j is integral over the ring $\mathbf{A} = \mathbb{Z}[c_0, \ldots, c_{n+m}]$.
It suffices to treat the case where the a_i's and b_j's are indeterminates. Then in a ring containing $\mathbb{Z}[a_0, \ldots, a_n, b_0, \ldots, b_m]$ we have

$$f(T) = a_0(T - x_1)\cdots(T - x_n), \qquad g(T) = b_0(T - y_1)\cdots(T - y_m).$$

1. By using Emmanuel's trick (Lemma 4.7, with the proof given in Exercise 10, independent of Kronecker's theorem), show that for all $I \subseteq [\![1..n]\!]$, $J \subseteq [\![1..m]\!]$, the product $a_0b_0 \prod_{i \in I} x_i \prod_{j \in J} y_j$ is integral over $\mathbf{A}$.

2. Conclude the result.

Exercise 12. *(Intermediary ring $\mathbf{A} \subseteq \mathbf{B} \subseteq \mathrm{Frac}(\mathbf{A})$, Bézout case)*
Let $\mathbf{A}$ be a Bézout domain, $\mathbf{K}$ be its quotient field and $\mathbf{B}$ be an intermediary ring $\mathbf{A} \subseteq \mathbf{B} \subseteq \mathbf{K}$. Show that $\mathbf{B}$ is a localized ring of $\mathbf{A}$ (therefore a Bézout ring).

Exercise 13. *(Intermediary ring, Prüfer case)*
In this exercise we generalize the result of Exercise 12 in the case where $\mathbf{A}$ is a Prüfer domain and we detail Theorem 3.6. This is therefore a variation around the Grell-Noether theorem (page 696).

1. Let $x \in \mathbf{K} = \mathrm{Frac}\,\mathbf{A}$.

a. Show that there exists an $s \in \mathrm{Reg}(\mathbf{A})$ such that $sx \in \mathbf{A}$ and $1 - s \in \mathbf{A}x$.

b. Let $t \in \mathbf{A}$ such that $tx = 1 - s$. For every intermediary ring $\mathbf{A}'$ between $\mathbf{A}$ and $\mathbf{K}$, show that $\mathbf{A}'[x] = \mathbf{A}'_s \cap \mathbf{A}'_t$. In particular, $\mathbf{A}[x] = \mathbf{A}_s \cap \mathbf{A}_t$. Consequently, $\mathbf{A}[x]$ is integrally closed, and it is a Prüfer domain.

2. Show that every finitely generated $\mathbf{A}$-subalgebra $\mathbf{B}$ of $\mathbf{K}$ is the intersection of a finite number of localized rings of $\mathbf{A}$ of the form $\mathbf{A}_s$ with $s \in \mathbf{A}$. Consequently, $\mathbf{B}$ is integrally closed, and it is a Prüfer domain.

3. Deduce that every intermediary ring between $\mathbf{A}$ and $\mathbf{K}$ is a Prüfer domain.

4. Give an example of an integrally closed ring $\mathbf{A}$, with an intermediary ring $\mathbf{B}$ between $\mathbf{A}$ and $\mathrm{Frac}(\mathbf{A})$ which is not integrally closed (in particular, $\mathbf{B}$ is not a localized ring of $\mathbf{A}$).

Exercise 14. *(To be primitively algebraic)*
Let $\mathbf{A} = \mathbb{Z}[A, B, U, V]/\langle AU + BV - 1\rangle = \mathbb{Z}[a, b, u, v]$ and $\mathbf{B} = \mathbf{A}[1/b]$.
Let $x = a/b$. Show that x is primitively algebraic over $\mathbf{A}$, but that $y = 2x$ is not.

Exercise 15. *(Characterizations of the coherent Prüfer rings, 1)*
Let $\mathbf{A}$ be a pp-ring and $\mathbf{K} = \mathrm{Frac}\,\mathbf{A}$. The following properties are equivalent.

1. $\mathbf{A}$ is a Prüfer ring.

2. $\mathbf{A}$ is normal and $x \in \mathbf{A}[x^2]$ for every $x \in \mathbf{K}$.

3. Every ring $\mathbf{A}[y]$ where $y \in \mathbf{K}$ is normal.

4. Every intermediary ring between $\mathbf{A}$ and $\mathbf{K}$ is normal.

5. $\mathbf{A}$ is normal and $x \in \mathbf{A} + x^2\mathbf{A}$ for every $x \in \mathbf{K}$.

Exercise 16. *(Characterizations of the coherent Prüfer rings, 2)*
For any pp-ring $\mathbf{A}$, the following properties are equivalent.

1. $\mathbf{A}$ is a Prüfer ring.
2. Every finitely generated ideal containing a regular element is invertible.
3. Every ideal $\mathfrak{a} = \langle x_1, x_2 \rangle$ with x_1, $x_2 \in \mathrm{Reg}(\mathbf{A})$ is invertible.
4. For all a, $b \in \mathbf{A}$, we have $\langle a, b \rangle^2 = \left\langle a^2, b^2 \right\rangle = \left\langle a^2 + b^2, ab \right\rangle$.
5. For all f, $g \in \mathbf{A}[X]$, we have $\mathrm{c}(f)\mathrm{c}(g) = \mathrm{c}(fg)$.

Exercise 17. *(A generalization of Proposition 6.5)*
Let $\mathbf{A}$ be a local-global coherent Prüfer ring (e.g. residually zero-dimensional).

1. Every matrix is equivalent to a matrix in Smith form (i.e. $\mathbf{A}$ is a Smith ring).
2. Every finitely presented $\mathbf{A}$-module is characterized, up to isomorphism, by its Fitting ideals. Actually it is isomorphic to a direct sum of cyclic modules $\mathbf{A}/\mathfrak{a}_k$ with principal ideals $\mathfrak{a}_1 \subseteq \cdots \subseteq \mathfrak{a}_n$ $(n \geqslant 0)$.
   Note: We can naturally deduce an analogous generalization of Corollary 6.6.

Exercise 18. *(Reduction ideal of another ideal)*

1. Let E be an $\mathbf{A}$-module generated by n elements, $b \in \mathbf{A}$ and $\mathfrak{a}$ be an ideal such that $bE \subseteq \mathfrak{a}E$. Show that there exists a $d = b^n + a_1 b^{n-1} + \cdots + a_{n-1} b + a_n$, with the $a_i \in \mathfrak{a}^i$, that annihilates E.

We say that an ideal $\mathfrak{a}$ is a *reduction* of an ideal $\mathfrak{b}$ if $\mathfrak{a} \subseteq \mathfrak{b}$ and if $\mathfrak{b}^{r+1} = \mathfrak{a}\mathfrak{b}^r$ for a certain exponent r (it is then true for all the larger exponents).

2. Let f, $g \in \mathbf{A}[\underline{X}]$. Prove that $\mathrm{c}(fg)$ is a reduction of $\mathrm{c}(f)\mathrm{c}(g)$.
3. In $\mathbf{A}[X, Y]$, show that $\mathfrak{a} = \left\langle X^2, Y^2 \right\rangle$ is a reduction of $\mathfrak{b} = \langle X, Y \rangle^2$.
   Show that $\mathfrak{a}_1 = \left\langle X^7, Y^7 \right\rangle$ and $\mathfrak{a}_2 = \left\langle X^7, X^6 Y + Y^7 \right\rangle$ are reductions of the ideal $\mathfrak{b}' = \left\langle X^7, X^6 Y, X^2 Y^5, Y^7 \right\rangle$. Give the smallest possible exponents.
4. Let $\mathfrak{a} \subseteq \mathfrak{b}$ be two ideals with $\mathfrak{b}$ finitely generated. Show that $\mathfrak{a}$ is a reduction of $\mathfrak{b}$ if and only if $\mathrm{Icl}(\mathfrak{a}) = \mathrm{Icl}(\mathfrak{b})$.

Exercise 19. *(Normal pp-ring)*
Here is a light generalization of Fact 2.2. By Problem XIII-1 the hypothesis is satisfied for the strongly discrete reduced coherent Noetherian rings (in classical mathematics they are the reduced Noetherian rings).

Consider a reduced ring $\mathbf{A}$. Suppose that its total ring of fractions is zero-dimensional.

1. If $\mathbf{A}$ is normal, it is a pp-ring.
2. The ring $\mathbf{A}$ is normal if and only if it is integrally closed in $\mathrm{Frac}\,\mathbf{A}$.

Exercise 20. *(Integral polynomial over $\mathfrak{a}[X]$)*
Let $\mathbf{A} \subseteq \mathbf{B}$ be two rings, $\mathfrak{a}$ be an ideal of $\mathbf{A}$ and $\mathfrak{a}[X]$ be the ideal of $\mathbf{A}[X]$ constituting of polynomials with coefficients in $\mathfrak{a}$. For $F \in \mathbf{B}[X]$, show that F is integral over $\mathfrak{a}[X]$ if and only if each coefficient of F is integral over $\mathfrak{a}$.

Exercise 21. *(Indecomposable modules)*

We say that a module M is *indecomposable* if the only direct summand submodules of M are 0 and M. The goal of the exercise is to prove that over a total factorization Dedekind domain, every finitely presented module is a direct sum of a finite number of indecomposable modules, this decomposition being unique up to the order of terms when the module is a torsion module.

1. Let $\mathbf{A}$ be a ring and $\mathfrak{a}$ be an ideal. If the $\mathbf{A}$-module $M = \mathbf{A}/\mathfrak{a}$ is a direct sum of two submodules N and P we have $N = \mathfrak{b}/\mathfrak{a}$, $P = \mathfrak{c}/\mathfrak{a}$ with comaximal $\mathfrak{b} \supseteq \mathfrak{a}$ and $\mathfrak{c} \supseteq \mathfrak{a}$. More precisely, $\mathfrak{b} = \langle b \rangle + \mathfrak{a}$, $\mathfrak{c} = \langle c \rangle + \mathfrak{a}$, where b and c are complementary idempotents modulo $\mathfrak{a}$.

2. Let $\mathbf{Z}$ be a Dedekind domain.

2a. Show that a projective module of constant rank 1 is indecomposable.

2b. Show that a cyclic module $\mathbf{Z}/\mathfrak{a}$ with $\mathfrak{a}$ finitely generated, $\neq \langle 0 \rangle, \langle 1 \rangle$ is indecomposable if and only if $\mathfrak{a} = \mathfrak{p}^m$ for some maximal ideal $\mathfrak{p}$ and some $m \geqslant 1$.

2c. Deduce that if $\mathbf{Z}$ admits total factorizations, every finitely presented module is a direct sum of a finite number of indecomposable modules.

3. When the module is a torsion module, show the uniqueness of the decomposition with a meaning to be specified.

Problem 1. *(Subring of invariants under a finite group action and arithmetic character)* Note: See also Problem III-8.

1. If $\mathbf{A}$ is a normal ring, every locally principal ideal is integrally closed. Consequently, if f, $g \in \mathbf{A}[X]$ with $\mathrm{c}(fg)$ locally principal, then $\mathrm{c}(f)\mathrm{c}(g) = \mathrm{c}(fg)$.

2. Suppose that $\mathbf{A}$ is normal and that $\mathbf{B} \supseteq \mathbf{A}$ is integral over $\mathbf{A}$. If $\mathfrak{a}$ is a locally principal ideal of $\mathbf{A}$, then $\mathfrak{a}\mathbf{B} \cap \mathbf{A} = \mathfrak{a}$.

3. Let $(\mathbf{B}, \mathbf{A}, G)$ where $G \subseteq \mathrm{Aut}(\mathbf{B})$ is a finite group and $\mathbf{A} = \mathrm{Fix}_{\mathbf{B}}(G) = \mathbf{B}^G$. If $\mathfrak{b}$ is an ideal of $\mathbf{B}$, let $\mathrm{N}'_G(\mathfrak{b}) = \prod_{\sigma \in G} \sigma(\mathfrak{b})$ (it is an ideal of $\mathbf{B}$) and $\mathrm{N}_G(\mathfrak{b}) = \mathbf{A} \cap \mathrm{N}'_G(\mathfrak{b})$.

Suppose that $\mathbf{B}$ is normal and that $\mathbf{A}$ is a Prüfer ring (therefore normal).

a. For $b \in \mathbf{B}$, prove that $\mathrm{N}'_G(b\mathbf{B}) = \mathrm{N}_G(b)\mathbf{B}$ and $\mathrm{N}_G(b\mathbf{B}) = \mathrm{N}_G(b)\mathbf{A}$.

b. If $\mathfrak{b}$ is a finitely generated ideal of $\mathbf{B}$, show that $\mathrm{N}_G(\mathfrak{b})$ is a finitely generated ideal of $\mathbf{A}$ and that $\mathrm{N}'_G(\mathfrak{b}) = \mathrm{N}_G(\mathfrak{b})\mathbf{B}$. You can write $\mathfrak{b} = \langle b_1, \ldots, b_n \rangle$ and introduce n indeterminates $\underline{X} = (X_1, \ldots, X_n)$ and consider the normic polynomial $h(\underline{X})$

$$h(\underline{X}) = \prod\nolimits_{\sigma \in G} h_\sigma(\underline{X}) \quad \text{with} \quad h_\sigma(\underline{x}) = \sigma(b_1)X_1 + \cdots + \sigma(b_n)X_n.$$

c. For finitely generated ideals $\mathfrak{b}_1$, $\mathfrak{b}_2$ of $\mathbf{B}$, we obtain $\mathrm{N}_G(\mathfrak{b}_1\mathfrak{b}_2) = \mathrm{N}_G(\mathfrak{b}_1)\mathrm{N}_G(\mathfrak{b}_2)$.

d. A finitely generated ideal $\mathfrak{b}$ of $\mathbf{B}$ is invertible if and only if $\mathrm{N}_G(\mathfrak{b})$ is invertible in $\mathbf{A}$.

Note: We know that $\mathbf{B}$ is a Prüfer ring (Theorem 3.5); in the case where $\mathbf{B}$ is integral, question *3d* provides a new proof for it.

4. Let $\mathbf{k}$ be a discrete field with $2 \in \mathbf{k}^\times$ and $f(X) \in \mathbf{k}[X]$ be a separable monic polynomial. The polynomial $Y^2 - f(X) \in \mathbf{k}[X, Y]$ is absolutely irreducible (see

Exercise 7); let $\mathbf{k}[x,y] = \mathbf{k}[X,Y]\big/\big\langle Y^2 - f(X)\big\rangle$. Show that $\mathbf{k}[x,y]$ is a Prüfer ring.

Problem 2. *(Full submonoids of* $\mathbb{N}^n$*)*
Let $M \subseteq \mathbb{N}^n$ be a submonoid; for a ring $\mathbf{k}$, let $\mathbf{k}[M]$ be the $\mathbf{k}$-algebra of the monoid M. It is the $\mathbf{k}$-subalgebra of $\mathbf{k}[\mathbb{N}^n] \simeq \mathbf{k}[\underline{x}] = \mathbf{k}[x_1,\dots,x_n]$ generated by the monomials $\underline{x}^m = x_1^{m_1}\cdots x_n^{m_n}$ for $m \in M$. We say that M is a *full submonoid* of $\mathbb{N}^n$ if for $m \in M$, $m' \in \mathbb{N}^n$, we have $m + m' \in M \Rightarrow m' \in M$.

1. The subgroup of $\mathbb{Z}^n$ generated by M is equal to $M - M$, and if M is full, then $M = (M - M) \cap \mathbb{N}^n$. Conversely, if $L \subseteq \mathbb{Z}^n$ is a subgroup, then the monoid $M = L \cap \mathbb{N}^n$ is a full submonoid of $\mathbb{N}^n$.

2. Let $M \subseteq \mathbb{N}^n$ be a full submonoid and $\mathbf{k}$ be a discrete field.

- *a)* Let $\mathbf{A} = \mathbf{k}[M] \subseteq \mathbf{B} = \mathbf{k}[\underline{x}]$. Show that if $a \in \mathbf{A} \setminus \{0\}$, $b \in \mathbf{B}$, and $ab \in \mathbf{A}$, then $b \in \mathbf{A}$.
- *b)* Let $\mathbf{A} \subseteq \mathbf{B}$ be two domains satisfying: if $a \in \mathbf{A} \setminus \{0\}$, $b \in \mathbf{B}$, and $ab \in \mathbf{A}$, then $b \in \mathbf{A}$.
  - *i.* Show that $\mathbf{A} = \mathbf{B} \cap \mathrm{Frac}(\mathbf{A})$; deduce that if $\mathbf{B}$ is integrally closed, the same goes for $\mathbf{A}$.
  - *ii.* In particular, if $M \subseteq \mathbb{N}^n$ is a full submonoid, then $\mathbf{k}[M]$ is integrally closed for every discrete field $\mathbf{k}$.
  - *iii.* More generally, if $\mathbf{B} \subseteq \mathbf{C}$ is integrally closed in $\mathbf{C}$, then $\mathbf{A}$ is integrally closed in $\mathbf{C} \cap \mathrm{Frac}(\mathbf{A})$.

3. Let $M \subseteq \mathbb{N}^n$ be the submonoid of magic squares (see Exercise VII-4); then $\mathbf{k}[M]$ is integrally closed for every discrete field $\mathbf{k}$.

Problem 3. *(Normal basis at infinity)*
A valuation domain $\mathbf{B}$ with quotient field $\mathbf{K}$ is a DVR if $\mathbf{K}^\times\big/\mathbf{B}^\times \simeq \mathbb{Z}$ (isomorphism of ordered groups). A regular parameter is every element $b \in \mathbf{B}$ such that $v(b) = 1$, where $v : \mathbf{K}^\times \to \mathbb{Z}$ is the map defined via the previous isomorphism (this map v is also called a *valuation*). Every element z of $\mathbf{K}^\times$ is then of the form $ub^{v(z)}$ with $u \in \mathbf{B}^\times$.

Let $\mathbf{k}$ be a discrete field, t be an indeterminate over $\mathbf{k}$, $\mathbf{A} = \mathbf{k}[t]$, $\mathbf{A}_\infty = \mathbf{k}[t^{-1}]_{\langle t^{-1}\rangle}$, and $\mathbf{K} = \mathrm{Frac}(\mathbf{A}) = \mathbf{k}(t) = \mathrm{Frac}(\mathbf{A}_\infty) = \mathbf{k}(t^{-1})$. If L is a finite dimensional $\mathbf{K}$-vector space, we study in this problem the intersection of an $\mathbf{A}$-lattice of L and of an $\mathbf{A}_\infty$-lattice of L (see the definitions question *2*), an intersection which is always a finite dimensional $\mathbf{k}$-vector space.

In the theory of algebraic function fields this study is at the basis of the determination of Riemann-Roch spaces, however, when certain integral closures are known by bases; as a subproduct, we determine the algebraic closure of $\mathbf{k}$ in a finite extension of $\mathbf{k}(t)$.

The ring $\mathbf{A}_\infty$ is a DVR; let $v : \mathbf{K} \to \mathbb{Z} \cup \{\infty\}$ be the corresponding valuation, defined by $v = -\deg_t$, and we fix $\pi = t^{-1}$ as regular parameter. If $x = {}^{\mathrm{t}}[x_1,\dots,x_n]$, let $v(x) = \min_i v(x_i)$. This allows us to define a *modular reduction*

$$\mathbf{K}^n \setminus \{0\} \to \mathbf{k}^n \setminus \{0\}\,, \qquad x \mapsto \xi = \overline{x},$$

with $\xi_i = (x_i/\pi^{v(x)}) \bmod \pi \in \mathbf{k}$.
Generally, if $\mathbf{V}$ is a valuation ring of a discrete field $\mathbf{K}$, of residual field $\mathbf{k}$, we have a *reduction*

$$\mathbb{P}^m(\mathbf{K}) \to \mathbb{P}^m(\mathbf{k}), \qquad (x_0 : \ldots : x_m) \mapsto (\xi_0 : \ldots : \xi_m) \quad \text{with } \xi_i = \overline{x_i/x_{i_0}},$$

where $x_{i_0} \,|\, x_i$ for all i; the element $(\xi_0 : \ldots : \xi_n) \in \mathbb{P}^m(\mathbf{k})$ is well-defined: it corresponds to a unimodular vector of $\mathbf{V}^{m+1}$. In short we have an "isomorphism" $\mathbb{P}^m(\mathbf{V}) \simeq \mathbb{P}^m(\mathbf{K})$ and a reduction $\mathbb{P}^m(\mathbf{V}) \to \mathbb{P}^m(\mathbf{k})$.
Here the choice of the regular parameter $\pi = t^{-1}$ gives a direct definition of the reduction $\mathbf{K}^n \setminus \{0\} \to \mathbf{k}^n \setminus \{0\}$, without having to change the coordinates on the projective line to understand what is happening at infinity.

We will say that a matrix $A \in \mathbb{GL}_n(\mathbf{K})$ with columns $(A_1, \ldots, A_n)$ is $\mathbf{A}_\infty$*-reduced* if the matrix $\overline{A} \in \mathbb{M}_n(\mathbf{k})$ is in $\mathbb{GL}_n(\mathbf{k})$.

1. Let $A \in \mathbb{GL}_n(\mathbf{K})$ of columns $A_1, \ldots, A_n$. Show that $\sum_{j=1}^n v(A_j) \leqslant v(\det A)$.

2. Let $A \in \mathbb{GL}_n(\mathbf{K})$; compute $Q \in \mathbb{GL}_n(\mathbf{A})$ such that AQ is $\mathbf{A}_\infty$-reduced. Or yet again, let $E \subset \mathbf{K}^n$ be an $\mathbf{A}$-lattice, i.e. a free $\mathbf{A}$-module of rank n; then E admits an $\mathbf{A}_\infty$-reduced $\mathbf{A}$-basis (a basis $(A_1, \ldots, A_n)$ such that $(\overline{A_1}, \ldots, \overline{A_n})$ is a $\mathbf{k}$-basis of $\mathbf{k}^n$). You can start with the example $A = \begin{bmatrix} \pi^2 & \pi \\ 1 & 1 \end{bmatrix}$.

3. For $P \in \mathbb{GL}_n(\mathbf{A}_\infty)$, prove the following points.

- *a.* P is a v-isometry, i.e. $v(Px) = v(x)$ for every $x \in \mathbf{K}^n$.
- *b.* For $x \in \mathbf{K}^n \setminus \{0\}$, $\overline{Px} = \overline{P}\,\overline{x}$.
- *c.* If $A \in \mathbb{GL}_n(\mathbf{K})$ is $\mathbf{A}_\infty$-reduced, the same goes for PA.

4. Let $A \in \mathbb{GL}_n(\mathbf{K})$ be triangular. What is the meaning of "A is $\mathbf{A}_\infty$-reduced"?

5. Let $A \in \mathbb{GL}_n(\mathbf{K})$. Show that there exists a $Q \in \mathbb{GL}_n(\mathbf{A})$, $P \in \mathbb{GL}_n(\mathbf{A}_\infty)$ and integers $d_i \in \mathbb{Z}$ such that $PAQ = \mathrm{Diag}(t^{d_1}, \ldots, t^{d_n})$; moreover, if we order the d_i's by increasing order, they are unique.

6. Let L be a $\mathbf{K}$-vector space of dimension n, $E \subset L$ be an $\mathbf{A}$-lattice, and $E' \subset L$ be an $\mathbf{A}_\infty$-lattice.

- *a.* Show that there exist an $\mathbf{A}$-basis $(e_1, \ldots, e_n)$ of E, an $\mathbf{A}_\infty$-basis $(e'_1, \ldots, e'_n)$ of E' and integers $d_1, \ldots, d_n \in \mathbb{Z}$ satisfying $e'_i = t^{d_i} e_i$ for $i \in [\![1..n]\!]$. Moreover, the d_i's ordered in increasing order only depend on (E, E').
- *b.* Deduce that $E \cap E'$ is a finite dimensional $\mathbf{k}$-vector space. More precisely,
$$E \cap E' = \bigoplus\nolimits_{d_i \geqslant 0} \bigoplus\nolimits_{j=0}^{d_i} \mathbf{k} t^j e_i,$$
and in particular,
$$\dim_{\mathbf{k}}(E \cap E') = \sum\nolimits_{d_i \geqslant 0}(1 + d_i) = \sum\nolimits_{d_i \geqslant -1}(1 + d_i).$$

7. Suppose that $\mathbf{L}$ is a finite $\mathbf{K}$-extension of degree n. We define integral closures in $\mathbf{L}$: $\mathbf{B}$ that of $\mathbf{A}$, $\mathbf{B}_\infty$ that of $\mathbf{A}_\infty$ and $\mathbf{k}'$ that of $\mathbf{k}$. We say that a basis $(\underline{e}) = (e_1, \dots, e_n)$ of $\mathbf{B}$ over $\mathbf{A}$ is *normal at infinity* if there exist $r_1, \dots, r_n \in \mathbf{K}^*$ such that $(r_1 e_1, \dots, r_n e_n)$ is an $\mathbf{A}_\infty$-basis of $\mathbf{B}_\infty$. Show that the elements of the basis $(\underline{e})$ "integral at infinity," that is which are members of $\mathbf{B}_\infty$, form a $\mathbf{k}$-basis of the extension $\mathbf{k}'$.

8. Let $\mathbf{k} = \mathbb{Q}$, $\mathbf{L} = \mathbf{k}[X, Y] \big/ \big\langle X^2 + Y^2 \big\rangle = \mathbf{k}[x, y]$, $\mathbf{A} = \mathbf{k}[x]$.
Show that $(y + 1, y/x)$ is an $\mathbf{A}$-basis of $\mathbf{B}$ but that it is not normal at infinity. Explicate an $\mathbf{A}$-basis of $\mathbf{B}$ normal at infinity.

Problem 4. *(Ring of functions of an affine hyper-elliptic curve having a single point at infinity)*
Here we will use a notion of a *norm of an ideal* in the following context: $\mathbf{B}$ being a free $\mathbf{A}$-algebra of finite rank n and $\mathfrak{b}$ being a finitely generated ideal of $\mathbf{B}$, the norm of $\mathfrak{b}$ is the ideal

$$\mathrm{N}_{\mathbf{B}/\mathbf{A}}(\mathfrak{b}) = \mathrm{N}(\mathfrak{b}) \overset{\mathrm{def}}{=} \mathcal{F}_{\mathbf{A},0}(\mathbf{B}/\mathfrak{b}) \subseteq \mathbf{A}.$$

It is clear that for $b \in \mathbf{B}$, $\mathrm{N}(b\mathbf{B}) = \mathrm{N}_{\mathbf{B}/\mathbf{A}}(b)\mathbf{A}$, that $\mathrm{N}(\mathfrak{a}\mathbf{B}) = \mathfrak{a}^n$ for $\mathfrak{a}$ a finitely generated ideal of $\mathbf{A}$ and that $\mathfrak{b}_1 \subseteq \mathfrak{b}_2 \Rightarrow \mathrm{N}(\mathfrak{b}_1) \subseteq \mathrm{N}(\mathfrak{b}_2)$.

Let $\mathbf{k}$ be a field of characteristic $\neq 2$ and $f = f(X) \in \mathbf{k}[X]$ be a separable monic polynomial of odd degree $2g+1$. The polynomial $Y^2 - f(X) \in \mathbf{k}[X, Y]$ is absolutely irreducible; let $\mathbf{B} = \mathbf{k}[X, Y] \big/ \big\langle Y^2 - f(X) \big\rangle = \mathbf{k}[x, y]$ and $\mathbf{A} = \mathbf{k}[x] \simeq \mathbf{k}[X]$. The ring $\mathbf{B}$ is integral, it is a free $\mathbf{A}$-module of basis $(1, y)$. For $z = a + by$ with a, $b \in \mathbf{A}$, let $\overline{z} = a - yb$, and $\mathrm{N} = \mathrm{N}_{\mathbf{B}/\mathbf{A}}$: $\mathrm{N}(z) = z\overline{z} = a^2 - fb^2$.
The goal of the problem is to parameterize the nonzero finitely generated ideals of $\mathbf{B}$, to show that $\mathbf{B}$ is a Prüfer ring and to study the group $\mathrm{Cl}(\mathbf{B})$ of classes of invertible ideals of $\mathbf{B}$.
If $\mathfrak{b}$ is a finitely generated ideal of $\mathbf{B}$, its *content* is the Fitting ideal $\mathcal{F}_{\mathbf{A},1}(\mathbf{B}/\mathfrak{b})$.
To two elements u, $v \in \mathbf{A}$ satisfying $v^2 \equiv f \bmod u$, we associate the $\mathbf{A}$-submodule of $\mathbf{B}$: $\mathfrak{b}_{u,v} = \mathbf{A}u + \mathbf{A}(y - v)$. We have $u \neq 0$ because f is separable. We will sometimes make the polynomial $w \in \mathbf{A}$ intervene so that $v^2 - uw = f$ and we will write $\mathfrak{b}_{u,v,w}$ instead of $\mathfrak{b}_{u,v}$ (even if w is completely determined by u, v).

1. Show that $\mathfrak{b}_{u,v}$ is an ideal of $\mathbf{B}$ and that $\mathfrak{b}_{u,v} = \mathbf{A}u \oplus \mathbf{A}(y - v)$. Conversely, for $u, v \in \mathbf{A}$, if $\mathbf{A}u + \mathbf{A}(y - v)$ is an ideal of $\mathbf{B}$, then $v^2 \equiv f \bmod u$.

2. Show that $\mathbf{A} \to \mathbf{B}/\mathfrak{b}_{u,v}$ induces an isomorphism $\mathbf{A}/\mathbf{A}u \simeq \mathbf{B}/\mathfrak{b}_{u,v}$; consequently, $\mathrm{Ann}_{\mathbf{A}}(\mathbf{B}/\mathfrak{b}_{u,v}) = \mathbf{A}u$. Deduce "the uniqueness of u"

$$u_1,\ u_2 \text{ monic and } \mathfrak{b}_{u_1,v_1} = \mathfrak{b}_{u_2,v_2} \implies u_1 = u_2.$$

Also prove that $\mathrm{N}(\mathfrak{b}_{u,v}) = u\mathbf{A}$ and that v is unique modulo u

$$\mathfrak{b}_{u,v_1} = \mathfrak{b}_{u,v_2} \iff v_1 \equiv v_2 \bmod u.$$

3. Show that

$$\mathfrak{b}_{u,v,w}\mathfrak{b}_{w,v,u} = \langle y - v \rangle_{\mathbf{B}}, \qquad \mathfrak{b}_{u,v}\mathfrak{b}_{u,-v} = \langle u \rangle_{\mathbf{B}}.$$

Consequently, the ideal $\mathfrak{b}_{u,v}$ is invertible.
In addition, for $u = u_1 u_2$ satisfying $v^2 \equiv f \bmod u$, we have $\mathfrak{b}_{u,v} = \mathfrak{b}_{u_1,v}\, \mathfrak{b}_{u_2,v}$.

4. Let $\mathfrak{b}$ be a nonzero finitely generated ideal of $\mathbf{B}$.

a. Show that there exist two unique monic polynomials d, $u \in \mathbf{A}$ and $v \in \mathbf{A}$ with $v^2 \equiv f \bmod u$, so that $\mathfrak{b} = d\,\mathfrak{b}_{u,v}$. Consequently, $\mathfrak{b}$ is an invertible ideal (so $\mathbf{B}$ is a Prüfer ring). In addition, v is unique modulo u, therefore unique if we impose $\deg v < \deg u$.

b. Deduce that $\mathfrak{b}\overline{\mathfrak{b}} = \mathrm{N}(\mathfrak{b})\mathbf{B}$ then that the norm is multiplicative over the ideals.

c. Show that $\mathbf{B}/\mathfrak{b}$ is a finite dimensional $\mathbf{k}$-vector space.
Show that $\dim_{\mathbf{k}}(\mathbf{B}/\mathfrak{b}) = \dim_{\mathbf{k}}(\mathbf{A}/\mathfrak{a})$ with $\mathfrak{a} = \mathrm{N}(\mathfrak{b})$. This integer will be denoted by $\deg(\mathfrak{b})$. Prove that $\deg(\mathfrak{b}_{u,v}) = \deg u$, that $\deg(\mathfrak{b}) = \deg \mathrm{N}(\mathfrak{b})$, and finally that deg is additive, i.e. $\deg(\mathfrak{b}_1\mathfrak{b}_2) = \deg(\mathfrak{b}_1) + \deg(\mathfrak{b}_2)$.

Let u, $v \in \mathbf{A}$ with $v^2 \equiv f \bmod u$. We say that *the pair* (u, v) *is reduced* if u is monic and $\boxed{\deg v < \deg u \leqslant g}$. By abuse of language, we also say that $\mathfrak{b}_{u,v}$ is reduced. For example, if (x_0, y_0) is a point of the hyper-elliptic curve $y^2 = f(x)$, its ideal $\langle x - x_0, y - y_0\rangle$ is a reduced ideal (take $u(x) = x - x_0$, $v = y_0$).

5. Show that every nonzero finitely generated ideal of $\mathbf{B}$ is associated with a reduced ideal of $\mathbf{B}$ (two ideals $\mathfrak{a}$ and $\mathfrak{a}'$ are said to be *associated* if there exist two regular elements a and a' such that $a\mathfrak{a}' = a'\mathfrak{a}$, we then let $\mathfrak{a} \sim \mathfrak{a}'$).

6. In this question, for a nonzero finitely generated ideal $\mathfrak{b}$ of $\mathbf{B}$, we designate by $\mathrm{N}(\mathfrak{b})$ the monic polynomial generator of the ideal $\mathrm{N}_{\mathbf{B}/\mathbf{A}}(\mathfrak{b})$. Let $\mathfrak{b}_{u,v}$ be a reduced ideal.

a. Let $z \in \mathfrak{b}_{u,v} \setminus \{0\}$ such that $u = \mathrm{N}(\mathfrak{b}_{u,v}) \mid \mathrm{N}(z)$, i.e. $\mathrm{N}(z)/\mathrm{N}(\mathfrak{b}_{u,v})$ is a polynomial. Show that

$$\deg\left(\mathrm{N}(z)/\mathrm{N}(\mathfrak{b}_{u,v})\right) \geqslant \deg u,$$

with equality if and only if $z \in \mathbf{k}^\times u$.

b. Let $\mathfrak{b}'$ be a finitely generated ideal of $\mathbf{B}$ satisfying $\mathfrak{b}' \sim \mathfrak{b}_{u,v}$. Show that $\deg(\mathfrak{b}') \geqslant \deg(\mathfrak{b}_{u,v})$ with equality if and only if $\mathfrak{b}' = \mathfrak{b}_{u,v}$. In summary, in a class of invertible ideals of $\mathbf{B}$, there is therefore one and only one ideal of minimum degree: it is the unique reduced ideal of the class.

7a. Show that the affine curve $y^2 = f(x)$ is smooth; more precisely, by letting $F(X, Y) = Y^2 - f(X) \in \mathbf{k}[X, Y]$, show that $1 \in \langle F, F'_X, F'_Y\rangle$; this uniquely uses the fact that f is separable and that the characteristic of $\mathbf{k}$ is not 2, not the fact that f is of odd degree.
If $\mathbf{k}$ is algebraically closed, we thus obtain a biunivocal correspondence between the points $p_0 = (x_0, y_0)$ of the affine curve $y^2 = f(x)$ and the DVRs $\mathbf{W}$ of $\mathbf{k}(x, y)$ containing $\mathbf{B} = \mathbf{k}[x, y]$: to p_0, we associate its local ring $\mathbf{W}$ and in the other direction, to $\mathbf{W}$ we associate the point $p_0 = (x_0, y_0)$ such that $\langle x - x_0, y - y_0\rangle_{\mathbf{B}} = \mathbf{B} \cap \mathfrak{m}(\mathbf{W})$.

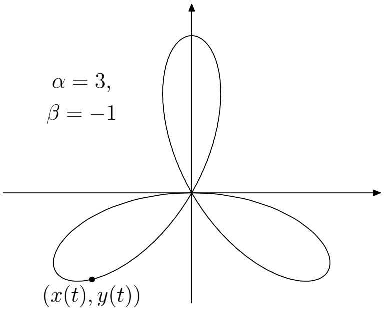
b. We now study "the points at infinity of the smoothed projective curve," at infinity relative to the model $y^2 = f(x)$. Algebraically, these are valuation rings for $\mathbf{k}(x, y)$ not containing $\mathbf{B}$ (but containing $\mathbf{k}$ of course). Let $\mathbf{A}_\infty = \mathbf{k}[x^{-1}]_{\langle x^{-1}\rangle}$ be the DVR. Show that there exists one and only one ring $\mathbf{B}_\infty$, $\mathbf{A}_\infty \subseteq \mathbf{B}_\infty \subsetneq \mathrm{Frac}(\mathbf{B}) = \mathbf{k}(x, y)$, having $\mathrm{Frac}(\mathbf{B})$ as quotient field. Show that $\mathbf{B}_\infty$ is a DVR, that $\mathbf{B}_\infty/\mathfrak{m}(\mathbf{B}_\infty) \simeq \mathbf{A}_\infty/\mathfrak{m}(\mathbf{A}_\infty) \simeq \mathbf{k}$ and that it is the only point at infinity.

Problem 5. *(Trifolium: integral closure and parameterization)*
Let $\mathbf{k}$ be a discrete field and

$$F(X,Y) = (X^2+Y^2)^2 + \alpha X^2 Y + \beta Y^3,$$

with $\alpha \neq \beta$ in $\mathbf{k}$.

We study the curve $F(x,y)=0$, its singular points, its field of functions
$$\mathbf{L} = \mathbf{k}(x,y)$$
(we will show that F is irreducible), its ring of functions $\mathbf{k}[x,y]$, the integral closure $\mathbf{B}$ of $\mathbf{k}[x,y]$ in $\mathbf{L}$ … etc …
Note that $F(-X,Y) = F(X,Y)$ and therefore that the involution $(x,y) \mapsto (-x,y)$ leaves the curve $F(x,y)=0$ invariant.
Opposite is an example of such a curve.



1. Show that F is an absolutely irreducible polynomial. More generally: let $\mathbf{k}$ be an integral ring, $\mathbf{k}[\underline{T}]$ be a polynomial ring with several indeterminates and $F \in \mathbf{k}[\underline{T}]$, $F = F_N + F_{N+1}$ with nonzero homogeneous F_N, F_{N+1}, of degrees N, $N+1$, respectively. Then, in every factorization $F = GH$, one of the two polynomials G or H is homogeneous; finally, if $\mathbf{k}$ is a field, then F is irreducible if and only if F_N, F_{N+1} are coprime.

2. Determine the singular points of the curve $F=0$.

Let $\mathbf{L} = \mathbf{k}(x,y)$ and $\mathbf{B}$ be the integral closure of $\mathbf{k}[x,y]$ in $\mathbf{L}$.

3. Let $t = y/x$ be such that $\mathbf{L} = \mathbf{k}(x,t)$.

a. Determine a primitive algebraic equation of t over $\mathbf{k}[x]$.
Let $G(X,T) = a_4T^4 + \cdots + a_1T + a_0 \in \mathbf{k}[X][T]$, with $a_i = a_i(X) \in \mathbf{k}[X]$, such a primitive polynomial, therefore satisfying $G(x,t)=0$. Prove that $(x,t)=(0,0)$ is a nonsingular point of the curve $G=0$.

b. Using Emmanuel's trick (Lemma 4.7), determine the integral elements b_4, …, b_1 associated with (G,t) with $\mathbf{A} = \mathbf{k}[x]$ as a base ring. Deduce a principal localization matrix for (x,y) and describe the ideal $\mathfrak{q}$ of $\mathbf{B}$ such that $\langle x\rangle_{\mathbf{B}} = \mathfrak{q}\,\langle x,y\rangle_{\mathbf{B}}$.

4. Show that $\mathbf{L} = \mathbf{k}(t)$ and express x, y as elements of $\mathbf{k}(t)$.

5. Determine the integral closure $\mathbf{B}$ of $\mathbf{k}[x,y]$ in $\mathbf{L}$.

a. Show that $\mathbf{B} = \mathbf{k}[g_0,g_1]$ with $g_0 = 1/(1+t^2)$ and $g_1 = tg_0$. Express x, y in $\mathbf{k}[g_0,g_1]$. What is "the equation" relating g_0 and g_1?

b. Show that $(1, y, b_3t, b_2t)$ is an $\mathbf{A}$-basis of $\mathbf{B}$.

c. Prove that $\dim_{\mathbf{k}} \mathbf{B}\big/\langle x,y\rangle_{\mathbf{B}} = 3$.

6. Let $\mathbf{V}$ be the valuation ring[7] of $\mathbf{L}$ defined by the nonsingular point $(0,0)$ of the curve $G = 0$. It is the only valuation ring of $\mathbf{L}$ containing $\mathbf{k}$ and such that x, $t \in \operatorname{Rad}\mathbf{V}$ (and so $y \in \operatorname{Rad}\mathbf{V}$ also).
Consider the prime ideal $\mathfrak{p}_1 = (\operatorname{Rad}\mathbf{V}) \cap \mathbf{B}$. Show that

$$\mathfrak{p}_1 = \langle x, y, b_4t, b_3t, b_2t, b_1t\rangle = \langle g_0 - 1, g_1\rangle \quad \text{and} \quad \mathbf{B}/\mathfrak{p}_1 = \mathbf{k},$$

and prove that $\mathfrak{p}_1^2 = \left\langle g_0 - 1, g_1^2\right\rangle$.

7. Determine the factorization in $\mathbf{B}$ of the ideal $\langle x, y\rangle_{\mathbf{B}}$ as a product of prime ideals. The response is not uniform at (α, β), unlike the determination of the integral closure $\mathbf{B}$ of $\mathbf{A}$.

8. Repeat the questions by only assuming that $\mathbf{k}$ is an integrally closed ring and that $\beta - \alpha \in \mathbf{k}^\times$.

Some solutions, or sketches of solutions

Exercise 1. We need to show the inclusion $\mathfrak{b}^n \subseteq \mathfrak{a}\mathfrak{b}^{n-1}$. Let $(x_1, \dots, x_n)$ be a generator set of E, $X = {}^{\mathrm{t}}[\,x_1 \ \cdots \ x_n\,]$, $b_1, \dots, b_n \in \mathfrak{b}$ and $B = \operatorname{Diag}(b_1, \dots, b_n)$. Since $b_ix_i \in \mathfrak{a}E$ ($i \in [\![1..n]\!]$), there exists an $A \in \mathbb{M}_n(\mathfrak{a})$ such that $B\,X = A\,X$. Let $C = B - A$. We have $C\,X = 0$, and since E is faithful, $\det C = 0$. Expanding this determinant, we obtain $b_1 \cdots b_n + a = 0$ with $a \in \mathfrak{a}\mathfrak{b}^{n-1}$ (since $\mathfrak{a} \subseteq \mathfrak{b}$).

Exercise 2. *(Principal localization matrices in* $\mathbb{M}_2(\mathbf{A})$*)*

1. Immediate, because if $B = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix}$, then $\widetilde{B} = \begin{bmatrix} b_{22} & -b_{12} \\ -b_{21} & b_{11} \end{bmatrix}$ and $[x\ y\,]B = [x'\ y'\,]$ with

$$x' = -\begin{vmatrix} -b_{21} & b_{11} \\ x & y \end{vmatrix}, \quad y' = \begin{vmatrix} b_{22} & -b_{12} \\ x & y \end{vmatrix}.$$

2. We have u, $v \in \mathfrak{b}$ with $z = ux + vy$ and ux, uy, vx, vy are multiples of z, which we write as $\begin{bmatrix} y \\ -x \end{bmatrix}[v\ \ -u\,] = zB$. As $[x\ y\,]\begin{bmatrix} y \\ -x \end{bmatrix} = 0$, we have $[x\ y\,]zB = 0$; in addition $\operatorname{Tr}(zB) = yv + xu = z$.

3. In the lemma in question, $z = x^n$ and the ring is a pf-ring. The equalities $x^n[x\ y\,]B = 0$ and $x^n\big(1 - \operatorname{Tr}(B)\big) = 0$ provide two comaximal localizations of $\mathbf{A}$: one in which $x^n = 0$, in which case $x = 0$ because the ring $\mathbf{A}$ and its localized rings are reduced, and the other in which $[x\ y\,]B = 0$ and $\operatorname{Tr}(B) = 1$. In each one of them, $\langle x, y\rangle$ is locally principal therefore it is locally principal in $\mathbf{A}$.

Exercise 3. *1.* Indeed, $\mathbf{A}(X)$ is faithfully flat over $\mathbf{A}$.

2. Let $f = \sum_{k=0}^n a_kX^k \in \mathbf{A}[X]$. For each k, we have, in $\mathbf{A}$, an equality

$$\langle a_0, \dots, a_n\rangle\, \langle b_{0,k}, \dots, b_{n,k}\rangle = \langle a_k\rangle \text{ with } a_0b_{0,k} + \cdots + a_nb_{n,k} = a_k.$$

Consider then the polynomial $g_k = \sum_{j=0}^n b_{j,k}X^{n-j}$. All of the coefficients of fg_k are in $\langle a_k\rangle$. We can therefore write $fg_k = a_kh_k$ with the coefficient of degree k

[7] A subring $\mathbf{V}$ of a discrete field $\mathbf{L}$ is called a *valuation ring of* $\mathbf{L}$ if for all $x \in \mathbf{L}^\times$ we have $x \in \mathbf{V}$ or $x^{-1} \in \mathbf{V}$.

in h_k equal to 1. This implies that in $\mathbf{A}(X)$, $a_k \in \langle f \rangle$. However, we have $f \in \langle a_0, \ldots, a_n \rangle$ in $\mathbf{A}[X]$. Thus, in $\mathbf{A}(X)$, $\langle f \rangle = \langle a_0, \ldots, a_n \rangle$.
We deduce that $\mathbf{A}(X)$ is a Bézout ring, because for $f_0, \ldots, f_m \in \mathbf{A}[X]$ of degrees $< d$, a consequence of the previous result is that in $\mathbf{A}(X)$

$$\langle f_0, \ldots, f_m \rangle = \left\langle f_0 + X^d f_1 + \cdots + X^{dm} f_m \right\rangle.$$

3. By Exercise 2, (x, y) admits a principal localization matrix over $\mathbf{B}$ if and only if there exists a $B \in \mathbb{M}_2(\mathbf{B})$ of trace 1 satisfying $[\,x\ y\,]B = [\,0\ 0\,]$.
So let $B \in \mathbb{M}_2\big(\mathbf{A}(X)\big)$ satisfy $[\,x\ y\,]B = [\,0\ 0\,]$ and $\mathrm{Tr}(B) = 1$.
By multiplying the coefficients of B by a common denominator, we obtain some elements p, q, r, s of $\mathbf{A}[X]$ such that $[\,x\ y\,]\begin{bmatrix} p & q \\ r & s \end{bmatrix} = [\,0\ 0\,]$ and $p+s$ is primitive.
We therefore have (with $p = \sum_k p_k X^k, \ldots$): $[\,x\ y\,]\begin{bmatrix} p_i & q_i \\ r_i & s_i \end{bmatrix} = [\,0\ 0\,]$. As $p+s$ is primitive, we have $u_i \in \mathbf{A}$ such that $\sum u_i(p_i + s_i) = 1$. Let $B' = \sum_i u_i \begin{bmatrix} p_i & q_i \\ r_i & s_i \end{bmatrix} \in \mathbb{M}_2(\mathbf{A})$: we obtain $[\,x\ y\,]B' = [\,0\ 0\,]$ with $\mathrm{Tr}(B') = 1$.

4. $\mathbf{A}\langle X \rangle$ is arithmetic $\Rightarrow$ $\mathbf{A}$ is arithmetic and

$$\mathbf{A} \text{ is arithmetic} \iff \mathbf{A}(X) \text{ is arithmetic} \iff \mathbf{A}(X) \text{ is a Bézout ring.}$$

The last equivalence also results from the local-global principle IX-6.10. In addition, the monoid of divisibility in $\mathbf{A}(X)$, i.e. $\mathbf{A}(X)/\mathbf{A}(X)^\times$, is isomorphic to the monoid of finitely generated ideals of $\mathbf{A}$.

Exercise 6. We only show the first item. It is clear that $\mathbf{K}'(\underline{X})$ is algebraic over $\mathbf{K}(\underline{X})$.
Conversely, let $z \in \mathbf{L}(\underline{X})$ be algebraic over $\mathbf{K}(\underline{X})$, then there exists some nonzero $a \in \mathbf{K}[\underline{X}]$ such that az is integral over $\mathbf{K}[\underline{X}]$, a fortiori over $\mathbf{L}[\underline{X}]$. As $\mathbf{L}[\underline{X}]$ is a GCD-domain, we have $az \in \mathbf{L}[\underline{X}]$. Moreover, we know that the integral closure of $\mathbf{K}[\underline{X}]$ in $\mathbf{L}[\underline{X}]$ is $\mathbf{K}'[\underline{X}]$ (Lemma III-8.4); so $az \in \mathbf{K}'[\underline{X}]$ then $z = (az)/a \in \mathbf{K}'(\underline{X})$.

Exercise 7. *1.* Immediate.

In what follows, we will use the fact that $(1, y)$ is a $\mathbf{k}[x]$-basis of $\mathbf{k}[x, y]$; it is also a $\mathbf{k}(x)$-basis of $\mathbf{k}(x, y)$ and the extension $\mathbf{k}(x, y)/\mathbf{k}(x)$ is a Galois extension of the group $\langle \sigma \rangle$ where $\sigma : \mathbf{k}(x, y) \to \mathbf{k}(x, y)$ is the involutive $\mathbf{k}(x)$-automorphism which realizes $y \mapsto -y$.

2. Let $z = u(x) + yv(x) \in \mathbf{k}(x, y)$ be algebraic over $\mathbf{k}$.
Then $z + \sigma(z) = 2u$ and $z\sigma(z) = u^2 - fv^2$ are algebraic over $\mathbf{k}$ and in $\mathbf{k}(x)$ so in $\mathbf{k}$. Hence $u \in \mathbf{k}$, $v = 0$ and $z = u \in \mathbf{k}$.

3. As $a \notin \mathbf{k}^p$, we easily see that $f(X)$ is irreducible in $\mathbf{k}[X]$. Let us show that $\mathbf{k}[x, y]$ is the integral closure of $\mathbf{k}[x]$ in $\mathbf{k}(x, y)$.
Let $z = u(x) + yv(x) \in \mathbf{k}(x, y)$ be integral over $\mathbf{k}[x]$.
Then $z + \sigma(z) = 2u$ and $z\sigma(z) = u^2 - fv^2$ are in $\mathbf{k}(x)$ and integral over $\mathbf{k}[x]$, so in $\mathbf{k}[x]$. Thus u and $fv^2 \in \mathbf{k}[x]$. By using the fact that f is irreducible, we see that $v \in \mathbf{k}[x]$. Recap: $z \in \mathbf{k}[x, y]$.

4. Let $\alpha = a^{1/p} \in \mathbf{k}$, hence $f(X) = (X - \alpha)^p$. Let $t = y/(x - \alpha)^{\frac{p-1}{2}}$.
Then $t^2 = x - \alpha$, therefore $x \in \mathbf{k}[t]$, and $y = t(x - \alpha)^{\frac{p-1}{2}} = t^p \in \mathbf{k}[t]$.

Therefore $\mathbf{k}[x,y] \subseteq \mathbf{k}[t]$ and $\mathbf{k}(x,y) = \mathbf{k}(t)$. We see that t is integral over $\mathbf{k}[x]$, but that $t \notin \mathbf{k}[x,y] = \mathbf{k}[x] \oplus \mathbf{k}[x]y$. The integral closure of $\mathbf{k}[x]$ (or that of $\mathbf{k}[x,y]$) in $\mathbf{k}(x,y)$ is $\mathbf{k}[t]$ (which indeed contains x and y).

Exercise 8. Recall that $x_0 = \frac{1}{p}$. The equality

$$\mathbf{k}[x_0,\dots,x_{n-1}] = \{\, u/p^s \mid u \in \mathbf{k}[t],\ \deg(u) \leqslant ns \,\}$$

is easy by noticing that $t^n x_0 \in \mathbf{k}[x_0,\dots,x_{n-1}]$ since

$$\tfrac{t^n}{p} = 1 + \tfrac{t^n - p}{p} \ \in\ \textstyle\sum_{i=0}^{n-1} \mathbf{k}\, \tfrac{t^i}{p}.$$

Let us write that t is algebraic over $\mathbf{k}(x_0)$ as a root in T of the polynomial

$$p(T)x_0 - 1 = x_0T^n + x_0a_{n-1}T^{n-1} + \cdots + x_0a_1T + (x_0a_0 - 1).$$

The elements determined by "Emmanuel's trick" (see Lemma 4.7 or Exercise 10) are

$$\begin{array}{ll} x_0t, \quad x_0t^2 + x_0a_{n-1}t, & x_0t^3 + x_0a_{n-1}t^2 + x_0a_{n-2}t, \\ \qquad\dots, & x_0t^{n-1} + \cdots + x_0a_2t. \end{array}$$

Thus, $t^k x_0$ is integral over $\mathbf{k}[x_0]$ for $k \in [\![0..n-1]\!]$ and $\mathbf{k}[x_0,\dots,x_{n-1}] \subseteq \mathbf{A}$.

It remains to show that $\mathbf{A} \subseteq \mathbf{k}[x_0,\dots,x_{n-1}]$. We use the inclusion

$$\mathbf{k}[x_0] \subseteq \mathbf{V}_\infty := \mathbf{k}[1/t]_{1+\langle 1/t\rangle}.$$

This last ring is comprised of rational fractions of degree $\leqslant 0$, i.e. defined at $t = \infty$. It is isomorphic to $\mathbf{k}[y]_{1+\langle y\rangle}$ so it is integrally closed, and $\mathbf{A} \subseteq \mathbf{V}_\infty$. The ring $\mathbf{V}_\infty$ is called "the local ring of the point $t = \infty$."

Let $z \in \mathbf{k}(t)$ be an integral rational fraction over $\mathbf{k}[x_0]$. By multiplying an integral dependence relation of z over $\mathbf{k}[x_0]$ by p^N with large enough N, we obtain

$$p^N z^m + b_{m-1}z^{m-1} + \cdots + b_1 + b_0 = 0, \qquad b_i \in \mathbf{k}[t].$$

This entails that $p^N z$ is integral over $\mathbf{k}[t]$ and therefore belongs to $\mathbf{k}[t]$ ($\mathbf{k}[t]$ is integrally closed). Moreover, $z \in \mathbf{V}_\infty$, i.e. $\deg z \leqslant 0$. Ultimately, z is a rational fraction of degree $\leqslant 0$ whose denominator divides a power of p, so $z \in \mathbf{k}[x_0,\dots,x_{n-1}]$.

Finally, we have $x_1 = tx_0$ so $t = x_1/x_0 \in \mathrm{Frac}(\mathbf{A})$ then $\mathbf{k}(t) = \mathrm{Frac}(\mathbf{A})$.

Exercise 9. *1.* Immediate.

2. Let $\mathfrak{b}$ be the ideal generated by each of the $X_iX_j - X_{i-1}X_{j+1}$ for $1 \leqslant i \leqslant j \leqslant n-1$ and E be the $\mathbf{k}$-module

$$E = \mathbf{k}[X_0] \oplus \mathbf{k}[X_0]X_1 \oplus \cdots \oplus \mathbf{k}[X_0]X_{n-1}.$$

We will prove that $E \cap \operatorname{Ker}\varphi = 0$ and that $\mathbf{k}[\underline{X}] = E + \mathfrak{b}$. As $\mathfrak{b} \subseteq \operatorname{Ker}\varphi$, we will obtain $\mathbf{k}[\underline{X}] = E \oplus \mathfrak{b}$. Let $y \in \operatorname{Ker}\varphi$ which we write as $y = y_1 + y_2$ with $y_1 \in E$ and $y_2 \in \mathfrak{b}$. By applying φ, we obtain $\varphi(y_1) = 0$, so $y_1 = 0$, then $y = y_2 \in \mathfrak{b}$. We have obtained $\operatorname{Ker}\varphi \subseteq \mathfrak{b}$, hence the equality $\operatorname{Ker}\varphi = \mathfrak{b}$.

- *Justification of* $E \cap \operatorname{Ker}\varphi = 0$. Let $f \in E$

$$f = f_0(X_0) + f_1(X_0)X_1 + \cdots + f_{n-1}(X_0)X_{n-1}.$$

Let $\varphi(f) = 0$,

$$\varphi(f) = f_0(1/p) + f_1(1/p)t/p + \cdots + f_{n-1}(1/p)t^{n-1}/p = 0.$$

By multiplying each $f_i(1/p)$ by p^N, with large enough N, we obtain $g_i(p) \in \mathbf{k}[p]$,

$$pg_0(p) + g_1(p)t + \cdots + g_{n-1}(p)t^{n-1} = 0.$$

But $(1, t, \dots, t^{n-1})$ is a basis of $\mathbf{k}[t]$ over $\mathbf{k}[p]$, so the g_k's $= 0$, then $f = 0$.

- *Justification of* $\mathbf{k}[\underline{X}] = E + \mathfrak{b}$.

Letting $\mathbf{k}[x_0, \dots, x_{n-1}] = \mathbf{k}[\underline{X}]/\mathfrak{b}$ and $E' = \mathbf{k}[x_0] + \mathbf{k}[x_0]x_1 + \cdots + \mathbf{k}[x_0]x_{n-1}$, this amounts to showing that $\mathbf{k}[\underline{x}] = E'$. Moreover E' contains $x_n = 1 - \sum_{i=0}^{n-1} a_i x_i$. It therefore suffices to prove that E' is a subring, or that $x_i x_j \in E'$ for i, $j \in [\![0..n-1]\!]$. By definition, it contains x_0^2, x_0x_1, …, x_0x_{n-1} and therefore also contains x_0x_n. But $x_1x_j = x_0x_{j+1}$ for $j \in [\![1..n-1]\!]$, so E' contains these x_1x_j's and therefore also contains x_1x_n, and by using $x_2x_j = x_1x_{j+1}$ for $j \in [\![2..n-1]\!]$, we see that E' contains all the x_2x_j's. And so forth.

Remark. The author of the exercise proceeded as follows, for some discrete field $\mathbf{k}$: he used an additional indeterminate X_n and chose, for $\mathbf{k}[X_0, X_1, \dots, X_n]$, the graded monomial reversed lexicographical order by ordering the indeterminates as follows: $X_0 < X_1 < \cdots < X_n$. We then observe that the trivial ideal of the ideal $\langle R_{\min}\rangle + \left\langle 1 - \sum_{i=0}^{n} a_i X^i \right\rangle$ is the monomial ideal generated by the monomials

$$(\star) \qquad X_n \text{ and } X_iX_j \text{ for } 1 \leqslant i \leqslant j \leqslant n-1.$$

The $\mathbf{k}$-vector space generated by the monomials wich are nondivisible by a monomial of $(\star)$ is the $\mathbf{k}$-vector space $E = \mathbf{k}[X_0] \oplus \mathbf{k}[X_0]X_1 \oplus \cdots \oplus \mathbf{k}[X_0]X_{n-1}$. It is the space that appears in the above solution (in which $\mathbf{k}$ is an arbitrary ring, not necessarily a discrete field). ∎

Exercise 10. By multiplying the initial equation by a_n^{n-1}, we obtain $a_n s$ integral over $\mathbf{A}$. Let us then express the initial equation as follows

$$(a_n s + a_{n-1})s^{n-1} + a_{n-2}s^{n-2} + \cdots + a_1 s + a_0 = 0, \text{ with } b = b_{n-1} = a_n s + a_{n-1},$$

and let us consider the ring $\mathbf{A}[b]$. Thus, s annihilates a polynomial of $\mathbf{A}[b][X]$ whose leading coefficient is b; by what precedes, bs is integral over $\mathbf{A}[b]$. But b is integral over $\mathbf{A}$ so $bs = a_n s^2 + a_{n-1}s$ is integral over $\mathbf{A}$.

The following step consists in writing the initial equation in the form

$$cs^{n-2} + a_{n-3}s^{n-3} + \cdots + a_1 s + a_0 = 0, \text{ with } c = b_{n-2} = a_n s^2 + a_{n-1}s + a_{n-2}.$$

Exercise 11. *1.* We write $[\![1..n]\!] \setminus I = \{i_1, i_2, \dots\}$. By using Lemma 4.7, we see that the coefficients of $h_1(T) = h(T)/(T - x_{i_1})$ are integral over $\mathbf{A}$, that those of $h_2(T) = h_1(T)/(T - x_{i_2})$ are integral over $\mathbf{A}$[coeffs. of h_1], therefore integral over $\mathbf{A}$ and so on and so forth. Therefore by letting $q(T) = \prod_{i' \notin I}(T - x_{i'}) \prod_{j' \notin J}(T - y_{j'})$, the coefficients of the polynomial $h(T)/q(T)$ are integral over $\mathbf{A}$. The constant coefficient of this last polynomial is $\pm a_0 b_0 \prod_{i \in I} x_i \prod_{j \in J} y_j$.

2. Elementary symmetric functions: we have $a_i = \pm a_0 S_i(\underline{x})$, $b_j = \pm b_0 S_j(\underline{y})$, so $a_i b_j$ is integral over $\mathbf{A}$.

Exercise 12. Let $S \subseteq \mathbf{A} \setminus \{0\}$ be the set of denominators b of the elements of $\mathbf{B}$ written in the form a/b with $a, b \in \mathbf{A}$, $b \neq 0$ and $1 \in \langle a, b\rangle$. It is clearly a monoid. To show that $\mathbf{B} = \mathbf{A}_S$, it suffices to prove that $S^{-1} \subseteq \mathbf{B}$.

Let $a/b \in \mathbf{B}$ be expressed irreducibly; there exist $u, v \in \mathbf{A}$ such that $1 = ua + vb$ which implies $1/b = u(a/b) + v \in \mathbf{AB} + \mathbf{A} \subseteq \mathbf{B}$.

Exercise 13. We want to show that an intermediary ring between $\mathbf{A}$ and $\mathbf{K}$ is a Prüfer ring. Every element of $\mathbf{K}$ is primitively algebraic over any arbitrary intermediary ring between $\mathbf{A}$ and $\mathbf{K}$. It remains to prove that the intermediary ring is integrally closed in order to apply Theorem 4.8.

1. If $x = a/b$, with a, $b \in \mathbf{A}$, there exists a principal localization matrix for (b, a), $\begin{bmatrix} s & c \\ t & 1-s \end{bmatrix} \in \mathbb{M}_2(\mathbf{A})$, with $sa = cb$ and $ta = (1-s)b$.

Therefore $x = c/s = (1-s)/t$ and $x \in \mathbf{A}'_s \cap \mathbf{A}'_t$. Conversely, if $x' \in \mathbf{A}'_s \cap \mathbf{A}'_t$, there is a', $b' \in \mathbf{A}'$ and n, $m \in \mathbb{N}$ such that $x' = a'/s^n = b'/t^m$. Therefore, for u, $v \in \mathbf{A}$, since $1/t = x/(1-s)$ we have

$$x' = \frac{a'}{s^n} = \frac{b'x^m}{(1-s)^m} = \frac{ua' + vb'x^m}{us^n + v(1-s)^m}\ .$$

It suffices to take $us^n + v(1-s)^m = 1$ to observe that $x' \in \mathbf{A}'[x]$.

2. Let $\mathbf{B} \subseteq \mathbf{K}$ be an $\mathbf{A}$-algebra generated by n elements ($n \geqslant 1$).
We write $\mathbf{B} = \mathbf{A}'[x]$, where $\mathbf{A}'$ is an $\mathbf{A}$-algebra generated by $n-1$ elements. By item *1*, there exist s, $t \in \mathbf{A}$ such that $\mathbf{A}'[x] = \mathbf{A}'_s \cap \mathbf{A}'_t$.
By induction, there exist $u_1, \ldots, u_k \in \mathbf{A}$ such that $\mathbf{A}' = \mathbf{A}_{u_1} \cap \cdots \cap \mathbf{A}_{u_k}$.
Then, $\mathbf{A}'_s = \mathbf{A}_{su_1} \cap \cdots \cap \mathbf{A}_{su_k}$ and $\mathbf{A}'_t = \mathbf{A}_{tu_1} \cap \cdots \cap \mathbf{A}_{tu_k}$, so

$$\mathbf{B} = \mathbf{A}_{su_1} \cap \cdots \cap \mathbf{A}_{su_k} \cap \mathbf{A}_{tu_1} \cap \cdots \cap \mathbf{A}_{tu_k}.$$

3. Let $\mathbf{B}$ be an intermediary ring and $x \in \mathbf{K}$ be integral over $\mathbf{B}$. Then x is integral over a finitely generated $\mathbf{A}$-subalgebra, therefore it belongs to this finitely generated $\mathbf{A}$-subalgebra, therefore to $\mathbf{B}$, i.e. $\mathbf{B}$ is integrally closed.

4. Let x, y be two indeterminates over a discrete field $\mathbf{k}$ and $\mathbf{A} = \mathbf{k}[x, y]$.
Let $\mathbf{B} = \mathbf{k}[x, y, (x^2 + y^2)/xy]$. Then $\mathbf{A}$ is integrally closed but not $\mathbf{B}$: indeed, x/y and y/x are integral over $\mathbf{B}$ (their sum and their product are members of $\mathbf{B}$) but x/y and $y/x \notin \mathbf{B}$ as we can easily prove, thanks to a homogeneity argument.

Exercise 14. We have $bx - a = 0$ with $1 = ua + vb$. The reader will check that if $f(Y) \in \mathbf{A}[Y]$ satisfies $f(y) = 0$, then f is a multiple, in $\mathbf{A}[Y]$, of $bY - 2a$. Therefore $\mathrm{c}(f) \subseteq \langle 2a, b \rangle$ and as $1 \notin \langle 2a, b \rangle$, y is not primitively algebraic over $\mathbf{A}$.

Exercise 15. The implications *4* $\Rightarrow$ *3* $\Rightarrow$ *2* and *5* $\Rightarrow$ *2* are trivial. Theorem 3.6 gives *1* $\Rightarrow$ *4* and Theorem 3.2 *4d* (page 692) gives *1* $\Rightarrow$ *5*.

2 $\Rightarrow$ *1*. x is primitively algebraic over $\mathbf{A}$, we apply Theorem 4.8.

Exercise 16. We already know that *1* $\Rightarrow$ *2* $\Rightarrow$ *3* and *1* $\Rightarrow$ *5*.

Let us show that *3* implies that the ring is arithmetic. Consider an ideal with two arbitrary generators $\mathfrak{a} = \langle y_1, y_2 \rangle$ and let r_i be the idempotent annihilator of y_i. Consider the orthogonal idempotents: $e = (1-r_1)(1-r_2)$, $f = r_1(1-r_2)$, and $g = r_2$. We have $e + f + g = 1$. If we invert f or g, one of the y_i's is null and the ideal $\mathfrak{a}$ becomes principal. To see what happens if we invert e, consider the regular elements $x_1 = (1-e) + ey_1$ and $x_2 = (1-e) + ey_2$. The ideal $\mathfrak{b} = \langle x_1, x_2 \rangle$ is invertible in $\mathbf{A}$. Then let u, v, w be such that $ux_1 = vx_2$ and $(1-u)x_2 = wx_1$. We multiply by e and we obtain $uey_1 = vey_2$ and $(1-u)ey_2 = wey_1$, which implies that the ideal $\mathfrak{a}\mathbf{A}_e = \langle ey_1, ey_2 \rangle \mathbf{A}_e$ is locally principal.

5 $\Rightarrow$ *4*. First consider $f = aX + b$, $g = aX - b$, then $f = aX + b$, $g = bX + a$.

4 ⇒ *3.* Let $\mathfrak{a} = \langle a, b\rangle$, with regular a and b. Let α, β such that $ab = \alpha a^2 + \beta b^2$, and let $\mathfrak{b} = \langle \alpha a, \beta b\rangle$. We have $ab \in \mathfrak{a}\mathfrak{b}$, therefore

$$a^2b^2 \in \mathfrak{a}^2\mathfrak{b}^2 = \left\langle a^2, b^2\right\rangle \left\langle \alpha^2 a^2, \beta^2 b^2\right\rangle.$$

Let us show the equality $\left\langle a^2b^2\right\rangle = \mathfrak{a}^2\mathfrak{b}^2$, which will imply that $\mathfrak{a}$ is invertible. Letting $u = \alpha a^2$, $v = \beta b^2$, it suffices to show that $u^2 = \alpha^2 a^4$ and $v^2 = \beta^2 b^4$ are in $\left\langle a^2b^2\right\rangle$. By definition, $u + v = ab \in \mathfrak{a}\mathfrak{b}$ and $uv \in \left\langle a^2b^2\right\rangle$.
Therefore $u^2 + v^2 = (u+v)^2 - 2uv \in \left\langle a^2b^2\right\rangle$. As u^2, $v^2 \in \left\langle u^2 + v^2, uv\right\rangle$, we indeed have u^2, $v^2 \in \left\langle a^2b^2\right\rangle$.

Exercise 17. We give the proof for the integral case. The pp-ring case is deduced from it by applying the usual elementary local-global machinery.
1. Let $M \in \mathbf{A}^{n\times m}$, $p = \inf(m, n)$. Proposition VIII-4.7 gives us locally principal ideals $\mathfrak{a}_i$ such that

$\mathcal{D}_{\mathbf{A},1}(M) = \mathfrak{a}_1$, $\mathcal{D}_{\mathbf{A},2}(M) = \mathfrak{a}_1^2\mathfrak{a}_2$, $\mathcal{D}_{\mathbf{A},3}(M) = \mathfrak{a}_1^3\mathfrak{a}_2^2\mathfrak{a}_3$, $\mathcal{D}_{\mathbf{A},4}(M) = \mathfrak{a}_1^4\mathfrak{a}_2^3\mathfrak{a}_3^2\mathfrak{a}_4$, …
Since the ring is local-global, the locally principal ideals $\mathfrak{a}_j$ are principal (local-global principle IX-6.10).
Let $\mathfrak{a}_j = \langle a_j\rangle$ and consider the matrix $M' \in \mathbf{A}^{n\times m}$ in Smith form, whose diagonal elements are a_1, a_1a_2, …, $a_1a_2\cdots a_p$.
As in the proof of Proposition VIII-4.7 the algorithm that produces the reduced Smith form in the local case and the local-global machinery of arithmetic rings provides us with a comaximal system $(s_1, \ldots, s_r)$ such that, over each $\mathbf{A}[1/s_i]$, the matrix M admits a reduced Smith form. By comparing the determinantal ideals we see that this reduced form can always be taken equal to M' (here is where the fact that over an integral ring, two generators of a principal ideal are always associated intervenes).
Thus, M and M' are equivalent over each $\mathbf{A}[1/s_i]$. The result follows by the local-global principle IX-6.8 that they are equivalent.

2. Immediate consequence of *1.*

Exercise 18. *1.* We write $E = \mathbf{A}x_1 + \cdots + \mathbf{A}x_n$ therefore $\mathfrak{a}E = \mathfrak{a}x_1 + \cdots + \mathfrak{a}x_n$. By using $bE \subseteq \mathfrak{a}E$, we obtain a matrix $A \in \mathbb{M}_n(\mathfrak{a})$ such that

$$b\,{}^{\mathrm{t}}[\,x_1 \ \cdots \ x_n\,] = A\,{}^{\mathrm{t}}[\,x_1 \ \cdots \ x_n\,].$$

It then suffices to let $d = \det(b\mathrm{I}_n - A)$.

2. If $\deg(g) \leqslant m$, we know that $\mathrm{c}(f)^{m+1}\mathrm{c}(g) = \mathrm{c}(f)^m\mathrm{c}(fg)$ (Lemma III-2.1). By multiplying by $\mathrm{c}(g)^m$, we obtain $\big(\mathrm{c}(f)\mathrm{c}(g)\big)^{m+1} = \mathrm{c}(fg)\big(\mathrm{c}(f)\mathrm{c}(g)\big)^m$.

3. We have $\mathfrak{b}^2 = \mathfrak{a}\mathfrak{b}$, $\mathfrak{b}'^5 = \mathfrak{a}_1\mathfrak{b}'^4$ and $\mathfrak{b}'^4 = \mathfrak{a}_2\mathfrak{b}'^3$.

4. Suppose $\mathfrak{b}^{r+1} = \mathfrak{a}\mathfrak{b}^r$. We apply the first question with $E = \mathfrak{b}^r$ and $b \in \mathfrak{b}$. We obtain $d = b^n + a_1b^{n-1} + \cdots + a_{n-1}b + a_n \in \mathrm{Ann}(\mathfrak{b}^r)$ with $a_i \in \mathfrak{a}^i$.
As $d \in \mathfrak{b}$ and $d \in \mathrm{Ann}(\mathfrak{b}^r)$, we have $d^{r+1} = 0$, which is an integral dependence relation of b over $\mathfrak{a}$.
For the converse, let $\mathfrak{b}$ be integral over $\mathfrak{a}$. For $b \in \mathfrak{b}$, by writing an integral dependence relation of b over $\mathfrak{a}$. We obtain n such that $b^{n+1} \in \mathfrak{a}\mathfrak{b}^n$. However, if we have two ideals $\mathfrak{b}_1, \mathfrak{b}_2 \subseteq \mathfrak{b}$ with $\mathfrak{b}_i^{n_i+1} \subseteq \mathfrak{a}\mathfrak{b}^{n_i}$, we have $(\mathfrak{b}_1 + \mathfrak{b}_2)^{n_1+n_2+1} \subseteq \mathfrak{a}\mathfrak{b}^{n_1+n_2}$. By using a finite generator set of $\mathfrak{b}$, we obtain an exponent r with the inclusion $\mathfrak{b}^{r+1} \subseteq \mathfrak{a}\mathfrak{b}^r$.

Exercise 19. Let $\mathbf{K} = \operatorname{Frac}\mathbf{A}$.

1. Let $a \in \mathbf{A}$ and e_a be the idempotent of $\mathbf{K}$ such that $\operatorname{Ann}_{\mathbf{K}}(a) = \operatorname{Ann}_{\mathbf{K}}(e_a)$. The element e_a is integral over $\mathbf{A}$, so $e_a \in \mathbf{A}$, and $\operatorname{Ann}_{\mathbf{A}}(b) = \operatorname{Ann}_{\mathbf{K}}(b) \cap \mathbf{A}$ for every $b \in \mathbf{A}$.

2. Direct implication. The computation is immediate.

2. Converse implication. Let a be integral over the principal ideal $\langle b \rangle$ in $\mathbf{A}$. Let us express the integral dependence relation of a over $\langle b \rangle$.

$$a^n = b(u_{n-1}a^{n-1} + u_{n-2}ba^{n-2} + \cdots + u_0b^{n-1}). \qquad (*)$$

We have $(1 - e_b)a^n = 0$, therefore since $\mathbf{A}$ is reduced $(1 - e_b)a = 0$. We introduce the regular element $b_1 = b + (1 - e_b)$. Then the element $c = a/b_1 \in \mathbf{K}$ is integral over $\mathbf{A}$. Indeed, the equality $(*)$ remains true when replacing b by b_1 and the u_i's by e_bu_i's, because in the component $e_b = 1$ we obtain $(*)$ and over the component $e_b = 0$ we obtain $0 = 0$.
Therefore c is in $\mathbf{A}$, and $a = e_ba = e_bb_1c = bc$.

Exercise 20. Let T be a new indeterminate over $\mathbf{B}$. For $b \in \mathbf{B}$, we will use the result (similar to Fact 2.5): b is integral over the ideal $\mathfrak{a}$ if and only if bT is integral over the subring$\mathbf{A}[\mathfrak{a}T] \overset{\text{def}}{=} \mathbf{A} \oplus \mathfrak{a}T \oplus \mathfrak{a}^2T^2 \oplus \ldots$ of $\mathbf{B}[T]$.

Let us take a look at the difficult case. Let $F \in \mathbf{B}[X]$ be integral over $\mathfrak{a}[X]$, we must show that each coefficient of F is integral over $\mathfrak{a}$. We write an integral dependence relation

$$F^n + G_1F^{n-1} + \cdots + G_{n-1}F + G_n = 0, \quad G_k = G_k(X) \in (\mathfrak{a}[X])^k = \mathfrak{a}^k[X].$$

We therefore have an equality in $\mathbf{B}[X][T]$ with some Q_i's in $\mathbf{B}[X]$

$$T^n + G_1T^{n-1} + \cdots + G_{n-1}T + G_n = (T - F)(T^{n-1} + Q_1T^{n-2} + \cdots + Q_{n-1}).$$

We replace T by $1/(TX)$ and we multiply by $(TX)^n = TX \times (TX)^{n-1}$, which gives

$$1 + XTG_1 + \cdots + X^nT^nG_n = (1 - XTF)(1 + XTQ_1 + \cdots + X^{n-1}T^{n-1}Q_{n-1}).$$

We now look at this equality in $\mathbf{B}[T][X]$.
If b is a coefficient of F, bT is a coefficient in X of $1 - XTF$ and 1 is a coefficient in X of $1 + XTQ_1 + \cdots + X^{n-1}T^{n-1}Q_{n-1}$. By Kronecker's theorem, the product $bT = bT \times 1$ is integral over the ring generated by the coefficients (in X) of the polynomial $1 + XTG_1 + \cdots + X^nT^nG_n$. But the coefficient in X^k of this last polynomial is in $\mathbf{A}[\mathfrak{a}T] = \mathbf{A} \oplus \mathfrak{a}T \oplus \mathfrak{a}^2T^2 \oplus \ldots$ and therefore bT is integral over $\mathbf{A}[\mathfrak{a}T]$ and consequently b is integral over $\mathfrak{a}$.

Exercise 21. *(Indecomposable modules)*

1. Everything takes place modulo $\mathfrak{a}$. We therefore consider the quotient ring $\mathbf{B} = \mathbf{A}/\mathfrak{a}$. Then the result is obvious (Lemma II-4.4).

2a. If $M = N \oplus P$, N and P are projective of constant rank and the sum of the ranks is equal to 1, therefore one of the two is null.

2b. We refer to item *1.* If the module is decomposable, we have $\mathfrak{a} \subseteq \mathfrak{b}$ and $\mathfrak{c}$ with $\mathfrak{b}$ and $\mathfrak{c}$ finitely generated comaximal. These ideals are therefore obtained from the total factorization of $\mathfrak{a}$ as two partial products of this factorization.
Thus, we cannot have $\mathfrak{b}$ and $\mathfrak{c}$ comaximal if the total factorization of $\mathfrak{a}$ makes only

one maximal ideal intervene.

Otherwise the total factorization of $\mathfrak{a}$ provides two comaximal ideals $\mathfrak{b}$ and $\mathfrak{c}$ such that $\mathfrak{b}\mathfrak{c} = \mathfrak{a}$. Therefore $\mathfrak{b} + \mathfrak{c} = \mathbf{Z}$ and $\mathfrak{b} \cap \mathfrak{c} = \mathfrak{a}$ which gives $\mathbf{Z}/\mathfrak{a} = \mathfrak{b}/\mathfrak{a} \oplus \mathfrak{c}/\mathfrak{a}$.

Actually, if $\mathfrak{a} = \prod_{i=1}^{k} \mathfrak{q}_i = \prod_{i=1}^{k} \mathfrak{p}_i^{m_i}$ is the total factorization of $\mathfrak{a}$, we obtain by induction on k that $\mathbf{Z}/\mathfrak{a} = \bigoplus_{i=1}^{k} \mathfrak{q}_i/\mathfrak{a}$.

2c. Results from the previous considerations and from the structure theorem for finitely presented modules over a Dedekind domain.

3. The uniqueness can be stated as follows: if M can be expressed in two ways as a sum of indecomposable modules, there is an automorphism of M which sends the modules of the first decomposition to those of the second.

If a torsion finitely presented module M is decomposed into direct sums of indecomposable modules, each term of the sum is itself finitely presented and with torsion. It is therefore of the form $\mathbf{Z}/\mathfrak{p}^m$ by item *1*.

By the Chinese remainder theorem we return to the case where only one maximal ideal intervenes in the direct sum, and the uniqueness then results from Theorem IV-5.1.

Note also that in the case of a total factorization PID, the uniqueness is valid for the decomposition of every finitely presented module.

Problem 1. Hereinafter the word “locally” means “after localization at comaximal elements.”

1. The ideal $\mathfrak{a}$ is locally principal, therefore since $\mathbf{A}$ is normal, locally integrally closed, so it is integrally closed (local-global principle 2.10). We end with Lemma 2.7 (variant of Kronecker's theorem).

2. If $x \in \mathfrak{a}\mathbf{B} \cap \mathbf{A}$, then x is integral over the ideal $\mathfrak{a}$ (Lying Over, Lemma 2.8) therefore in $\mathfrak{a}$ by the previous question.

3a. If $a = \mathrm{N}_G(b)$, we have $\mathrm{N}_G(b\mathbf{B}) = a\mathbf{B} \cap \mathbf{A} = a\mathbf{A}$.

3b and *3c.* The finitely generated ideal $\mathfrak{a} = \mathrm{c}_{\mathbf{A}}(h)$ is locally principal, so $\mathrm{c}_{\mathbf{B}}(h) = \mathfrak{a}\mathbf{B}$ is a locally principal ideal of $\mathbf{B}$. By the first question, we have

$$\textstyle\prod_\sigma \mathrm{c}_{\mathbf{B}}(h_\sigma) = \mathrm{c}_{\mathbf{B}}(h), \quad \text{i.e.} \quad \mathrm{N}'_G(\mathfrak{b}) = \mathfrak{a}\mathbf{B}.$$

By question *2*, $\mathfrak{a} = \mathrm{N}_G(\mathfrak{b})$. Next we note that

$$\mathrm{N}_G(\mathfrak{b}_1\mathfrak{b}_2)\mathbf{B} = \mathrm{N}'_G(\mathfrak{b}_1\mathfrak{b}_2) = \mathrm{N}'_G(\mathfrak{b}_1)\mathrm{N}'_G(\mathfrak{b}_2) = \mathrm{N}_G(\mathfrak{b}_1)\mathrm{N}_G(\mathfrak{b}_2)\mathbf{B},$$

hence the result when taking the intersection with $\mathbf{A}$.

3d. This results from item *2* and from the two following facts.

- If $b \in \mathbf{B}$ is regular then $a = \mathrm{N}_G(b) \in \mathbf{A}$ is regular in $\mathbf{A}$: indeed, it is a product of regular elements in $\mathbf{B}$ therefore it is regular in $\mathbf{B}$.
- If $a \in \mathbf{A}$ is regular in $\mathbf{A}$ then it is regular in $\mathbf{B}$. Indeed, let $x \in \mathbf{B}$ such that $ax = 0$. We want to show that $x = 0$. We consider the polynomial

$$\mathrm{C}_G(x)(T) = \textstyle\prod_{\sigma\in G} \big(T - \sigma(x)\big).$$

As $a\sigma(x) = 0$ for each σ, the coefficients of $\mathrm{C}_G(x)(T)$ are annihilated by a therefore null, except for the leading coefficient. Thus $x^{|G|} = 0$, but $\mathbf{B}$ is normal therefore reduced.

4. Let $\mathbf{k}(x, y) = \operatorname{Frac} \mathbf{k}[x, y]$. We will use the fact that $(1, y)$ is a $\mathbf{k}[x]$-basis of $\mathbf{k}[x, y]$; it is also a $\mathbf{k}(x)$-basis of $\mathbf{k}(x, y)$ and the extension $\mathbf{k}(x, y)/\mathbf{k}(x)$ is a Galois extension of the group $\langle\sigma\rangle$ where $\sigma : \mathbf{k}(x,y) \to \mathbf{k}(x,y)$ is the involutive $\mathbf{k}(x)$-automorphism which realizes $y \mapsto -y$. Let us show that $\mathbf{k}[x,y]$ is the integral closure of $\mathbf{k}[x]$ in $\mathbf{k}(x,y)$. Let $z = u(x) + yv(x) \in \mathbf{k}(x,y)$ be integral over $\mathbf{k}[x]$. Then $z + \sigma(z) = 2u$ and $z\sigma(z) = u^2 - fv^2$ are in $\mathbf{k}(x)$ and integral over $\mathbf{k}[x]$ therefore in $\mathbf{k}[x]$. We therefore have $fv^2 \in \mathbf{k}[x]$. By using the fact that f is separable, we see that $v \in \mathbf{k}[x]$. Recap: $z \in \mathbf{k}[x,y]$. Therefore $\mathbf{k}[x,y]$ is integrally closed. We apply the preceding with $\mathbf{A} = \mathbf{k}[x]$, $\mathbf{B} = \mathbf{k}[x,y]$, $G = \langle\sigma\rangle$.

Problem 2.

2a) Let $a = \sum_\alpha a_\alpha \underline{x}^\alpha$, $b = \sum_\beta b_\beta \underline{x}^\beta$.

We must show that $\beta \in M$ for each β such that $b_\beta \neq 0$. We can assume b nonzero. Let $a_\alpha \underline{x}^\alpha$ be the leading monomial of a for the lexicographical order and $b_\beta \underline{x}^\beta$ be that of b. The leading monomial of ab is $a_\alpha b_\beta \underline{x}^{\alpha+\beta}$, therefore $\alpha + \beta \in M$.

As $\alpha \in M$ and as M is full, we have $\beta \in M$. We then start again by replacing b by $b' = b - b_\beta \underline{x}^\beta$ which satisfies $ab' \in \mathbf{k}[\underline{x}]$. We obtain $b' \in \mathbf{k}[\underline{x}]$ and finally $b \in \mathbf{k}[\underline{x}]$.

Problem 3.

1. If $A = (a_{ij})$, then $\det A = \sum_{\sigma \in \mathrm{S}_n} a_{\sigma(1)1} \cdots a_{\sigma(n)n}$ and

$$v(a_{\sigma(1)1} \cdots a_{\sigma(n)n}) \geqslant v(A_1) + \cdots + v(A_n).$$

We deduce that $v(\det A) \geqslant v(A_1) + \cdots + v(A_n)$.

2. For the matrix given as an example: we have $\det(A) = \pi^2 - \pi \neq 0$.

But $\overline{A} = \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}$ is not invertible. By realizing $A_1 \leftarrow A_1 - A_2$, we obtain the equality $A' = \begin{bmatrix} \pi^2 - \pi & \pi \\ 0 & 1 \end{bmatrix}$ and this time $\overline{A'} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is invertible.

Here is the general method: if $\det \overline{A} \neq 0$, A is $\mathbf{A}_\infty$-reduced and that is all. Otherwise, there are some $\lambda_1, \ldots, \lambda_n \in \mathbf{k}$, not all zero, such that $\lambda_1 \overline{A_1} + \cdots + \lambda_n \overline{A_n} = 0$. We consider a column A_j with $\lambda_j \neq 0$ and $v(A_j)$ minimum; to simplify, we can suppose that it is A_1 and that $\lambda_1 = 1$ (even if it entails dividing the relation by λ_1); we then perform the elementary operation

$$A_1 \leftarrow A_1' = A_1 + \textstyle\sum_{j=2}^n \lambda_j \pi^{v(A_1)-v(A_j)} A_j.$$

In this sum, by only making the A_j's for which $\lambda_j \neq 0$ intervene, each exponent of π is $\geqslant 0$. This is therefore a $\mathbf{k}[\pi^{-1}]$-elementary operation on the columns, i.e. $\mathbf{k}[t]$-elementary, and we do not change the $\mathbf{k}[t]$-module generated by the columns. Moreover, $v(A_1') > v(A_1)$; indeed, (by remembering that $\lambda_1 = 1$):

$$A_1'/\pi^{v(A_1)} = s \overset{\text{def}}{=} \textstyle\sum_{\lambda_j \neq 0} \lambda_j A_j / \pi^{v(A_j)},$$

and $v(s) > 0$ since by hypothesis $\sum_{\lambda_j \neq 0} \lambda_j \overline{A_j} = 0$. We iterate this process which eventually stops because at each step, the sum $\sum_j v(A_j)$ strictly increases while being bounded above by $v(\det A)$, invariant under the above operations.

3. Let $y = Px$, i.e. $y_i = \sum_j p_{ij} x_j$; we have $v(p_{ij}) \geqslant 0$, $v(x_j) \geqslant v(x)$ so $v(y_i) \geqslant v(x)$ then $v(y) \geqslant v(x)$. By symmetry, $v(y) = v(x)$. The remainder poses no more difficulties.

4. A is $\mathbf{A}_\infty$-reduced if and only if every (necessarily nonzero) diagonal coefficient divides (in the $\mathbf{A}_\infty$ sense) all the coefficients of its column.

5. Even if it entails replacing A by AQ with suitable $Q \in \mathbb{GL}_n(\mathbf{A})$, we can suppose that A is $\mathbf{A}_\infty$-reduced. We will realize some operations $A \leftarrow PA$ with $P \in \mathbb{GL}_n(\mathbf{A}_\infty)$ (i.e. consider the $\mathbf{A}_\infty$-lattice generated by the rows of A), which does not modify the $\mathbf{A}_\infty$-reduced character of A. There exists a $P \in \mathbb{GL}_n(\mathbf{A}_\infty)$ such that PA is upper triangular and we replace A by PA. Let $L_1, \ldots, L_n$ be the rows of A; we then realize the $\mathbf{A}_\infty$-elementary operation

$$L_1 \leftarrow L_1 - \tfrac{a_{12}}{a_{22}} L_2 \qquad \text{recall : } a_{22} \mid_{\mathbf{A}_\infty} a_{12},$$

which brings a 0 in position a_{12} (and the new matrix is always triangular and $\mathbf{A}_\infty$-reduced). We continue in order to annihilate all the coefficients of the first row (except a_{11}); we can then pass to the second row and so on and so forth in order to obtain a diagonal matrix (by constantly using the fact that in an $\mathbf{A}_\infty$-reduced triangular matrix, each diagonal coefficient $\mathbf{A}_\infty$-divides all the coefficients of its column). As $\mathbf{A}_\infty$ is a DVR, we can make sure that the final obtained diagonal matrix is $\mathrm{Diag}(\pi^{d_1}, \ldots, \pi^{d_n})$ with $d_i \in \mathbb{Z}$.

6a. Let $\underline{\varepsilon}$ be an $\mathbf{A}$-basis of E, $\underline{\varepsilon'}$ be an $\mathbf{A}_\infty$-basis of E' and $A = \mathrm{Mat}_{\underline{\varepsilon},\underline{\varepsilon'}}(\mathrm{Id}_L)$. Then there exist $P \in \mathbb{GL}_n(\mathbf{A}_\infty)$ and $Q \in \mathbb{GL}_n(\mathbf{A})$ such that $PAQ = \mathrm{Diag}(t^{-d_1}, \ldots, t^{-d_n})$. Let $\underline{e}$ and $\underline{e'}$ be defined by $\mathrm{Mat}_{\underline{e},\underline{\varepsilon}}(\mathrm{Id}_L) = Q$, $\mathrm{Mat}_{\underline{\varepsilon'},\underline{e'}}(\mathrm{Id}_L) = P$.

Then $\underline{e}$ is an $\mathbf{A}$-basis of E, $\underline{e'}$ an $\mathbf{A}_\infty$-basis of E' and $e_i = t^{-d_i} e'_i$.

6b. Since $t^j e_i = t^{j-d_i} e'_i$, it is clear that $t^j e_i \in E \cap E'$ for $0 \leqslant j \leqslant d_i$. Conversely, let $y \in E \cap E'$ which we express as

$$y = \textstyle\sum_i a_i e_i = \sum_i a'_i t^{d_i} e_i, \quad \text{with } a_i \in \mathbf{A} \text{ and } a'_i \in \mathbf{A}_\infty,$$

and therefore $a_i = a'_i t^{d_i}$.

If $d_i < 0$, we obtain $a_i = a'_i = 0$, and if $a_i \neq 0$, $0 \leqslant \deg a_i \leqslant d_i$. Hence the stated $\mathbf{k}$-basis.

7. First of all $\mathbf{k}' = \mathbf{B} \cap \mathbf{B}_\infty$, so $\mathbf{B}$ and $\mathbf{B}_\infty$ are $\mathbf{k}'$-vector spaces. Let us show that each $r_i \in \mathbf{A}_\infty$ and that in addition, if $e_i \notin \mathbf{B}_\infty$, then $v(r_i) > 0$, i.e. $\deg(r_i) < 0$. If $e_i \in \mathbf{B}_\infty$, we have $e_i \in \mathbf{B} \cap \mathbf{B}_\infty = \mathbf{k}'$, so also $e_i^{-1} \in \mathbf{k}'$; consequently $r_i = e_i^{-1}(r_i e_i) \in \mathbf{B}_\infty$ therefore $r_i \in \mathbf{B}_\infty \cap \mathbf{K} = \mathbf{A}_\infty$.

If $e_i \notin \mathbf{B}_\infty$, we write $e_i = r_i^{-1}(r_i e_i)$, an equality which proves that $r_i^{-1} \notin \mathbf{A}_\infty$ (let us not forget that $r_i e_i \in \mathbf{B}_\infty$) so $v(r_i^{-1}) < 0$, i.e. $v(r_i) > 0$.

Now let $c \in \mathbf{k}'$ which we express in the $\mathbf{A}$-basis (e_i) and the $\mathbf{A}_\infty$-basis $(r_i e_i)$

$$c = \textstyle\sum_i a_i e_i = \sum_i a'_i r_i e_i, \quad a_i \in \mathbf{A}, \quad a'_i \in \mathbf{A}_\infty, \quad a_i = a'_i r_i.$$

For the i's such that $e_i \in \mathbf{k}'$, as $r_i \in \mathbf{A}_\infty$, we have $a_i = a'_i r_i \in \mathbf{A} \cap \mathbf{A}_\infty = \mathbf{k}$. It remains to see that for $e_i \notin \mathbf{k}'$, $a_i = 0$; the equality $a_i = a'_i r_i$ and the fact that $a_i \in \mathbf{A}$, $a'_i \in \mathbf{A}_\infty$ and $\deg(r_i) < 0$ then entail $a_i = a'_i = 0$. Recap: the e_i's which are in $\mathbf{k}'$ form a $\mathbf{k}$-basis of $\mathbf{k}'$.

8. By letting $i = y/x$, we have $i^2 = -1$ and

$$\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ i \end{bmatrix} = \begin{bmatrix} y+1 \\ i \end{bmatrix}.$$

The matrix on the left-hand side has determinant 1, therefore $(1, i)$ and $(y+1, i)$ are two bases of the same $\mathbf{A}$-module. But $y+1$ is not integral over $\mathbf{A}_\infty$ (because x is integral over $\mathbf{k}[y] = \mathbf{k}[y+1]$ and is not integral over $\mathbf{A}_\infty$). The basis $(1, i)$ is normal at infinity but not the basis $(y+1, i)$.

Problem 4. *1.* Let $z = y - v$, $(1, z)$ is an $\mathbf{A}$-basis of $\mathbf{B}$ and $\mathbf{A}u \cap \mathbf{A}z = \{0\}$. To show that $\mathfrak{b}_{u,v} = \mathbf{A}u \oplus \mathbf{A}z$ is an ideal, it suffices to see that $z^2 \in \mathfrak{b}_{u,v}$.
However, $y^2 = (z + v)^2 = z^2 + 2vz + v^2$, i.e. $z^2 + 2vz + uw = 0$.

2. As $(1, z)$ is an $\mathbf{A}$-basis of $\mathbf{B}$ and (u, z) is an $\mathbf{A}$-basis of $\mathfrak{b}_{u,v}$, we obtain the equality $\mathbf{A} \cap \mathfrak{b}_{u,v} = u\mathbf{A}$. Moreover, every element of $\mathbf{B}$ is congruent modulo z to an element of $\mathbf{A}$, therefore $\mathbf{A} \to \mathbf{B}/\mathfrak{b}_{u,v}$ is surjective with kernel $u\mathbf{A}$.
The matrix M of $(u, y - v)$ over $(1, y)$ is $M = \begin{bmatrix} u & -v \\ 0 & 1 \end{bmatrix}$ with $\det(M) = u$, which gives $\mathrm{N}(\mathfrak{b}_{u,v}) = u\mathbf{A}$. We also see that the content of $\mathfrak{b}_{u,v}$ is 1. The other points are easy.

3. We have $\mathfrak{b}_{u,v,w} = \mathbf{A}u \oplus \mathbf{A}z$, $\mathfrak{b}_{w,v,u} = \mathbf{A}w \oplus \mathbf{A}z$. The product of these two ideals is generated (as an ideal or $\mathbf{A}$-module) by the four elements uw, uz, wz, z^2, all multiples of z (because $z^2 + 2vz + uw = 0$). It therefore suffices to see that

$$z \in \left\langle uw, uz, wz, z^2 \right\rangle_{\mathbf{B}} = \langle uw, uz, wz, 2vz \rangle_{\mathbf{B}} = \langle uw, uz, wz, vz \rangle_{\mathbf{B}}\,.$$

However, $v^2 - uw = f$ is separable, therefore $1 \in \langle u, w, v \rangle_{\mathbf{A}}$, and $z \in \langle uz, wz, vz \rangle_{\mathbf{B}}$.
As for $\mathfrak{b}_{u,-v}$ it is $\mathbf{A}u \oplus \mathbf{A}\overline{z}$ with $z\overline{z} = uw$ and $z + \overline{z} = -2v$. The product π of the two ideals $\mathfrak{b}_{u,v}$ and $\mathfrak{b}_{u,-v}$ is equal to $\left\langle u^2, u\overline{z}, uz, z\overline{z} \right\rangle$, with $z\overline{z} = uw$, so $\pi \subseteq \langle u \rangle$.
Finally, $-2uv = uz + u\overline{z} \in \pi$ and therefore $\pi \supseteq \left\langle uv, u^2, uw \right\rangle = u \langle v, u, w \rangle = \langle u \rangle$.

Finally, with $u = u_1u_2$, we have $\mathfrak{b}_{u_1,v}\mathfrak{b}_{u_2,v} = \mathbf{A}u + \mathbf{A}u_1z + \mathbf{A}u_2z + \mathbf{A}z^2$ clearly included in $\mathbf{A}u + \mathbf{A}z = \mathfrak{b}_{u,v}$. As $z^2 + 2vz + uw = 0$ we obtain

$$\mathbf{A}u + \mathbf{A}u_1z + \mathbf{A}u_2z + \mathbf{A}z^2 = \mathbf{A}u + \mathbf{A}u_1z + \mathbf{A}u_2z + \mathbf{A}vz = \mathbf{A}u + (\mathbf{A}u_1 + \mathbf{A}u_2 + \mathbf{A}v)z.$$

Hence $\mathfrak{b}_{u_1,v}\mathfrak{b}_{u_2,v} = \mathfrak{b}_{u,v}$; indeed, $1 \in \langle u_1, u_2, v \rangle_{\mathbf{A}}$ because $v^2 - u_1u_2w = f$ is separable, therefore $\langle u_1, u_2, v \rangle_{\mathbf{A}}\, z = \mathbf{A}z$.

4a. Let $\mathfrak{b}$ be a nonzero finitely generated ideal of $\mathbf{B}$. As a free $\mathbf{A}$-module of rank 2, it admits an $\mathbf{A}$-basis (e_1, e_2) and we let $M = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$ be the matrix of (e_1, e_2) over $(1, y)$. We write that $\mathfrak{b}$ is an ideal, i.e. $y\mathfrak{b} \subseteq \mathfrak{b}$: the membership $ye_1 \in \mathbf{A}e_1 \oplus \mathbf{A}e_2$ gives a multiple a of d and the membership $ye_2 \in \mathbf{A}e_1 \oplus \mathbf{A}e_2$ gives a multiple b of d. Ultimately, M is of the form $M = d\begin{bmatrix} u & -v \\ 0 & 1 \end{bmatrix}$ and we obtain $\mathfrak{b} = d\mathfrak{b}_{u,v}$. We see that $\langle d \rangle_{\mathbf{A}}$ is the content of $\mathfrak{b}$, and d is unique if we impose d as unitary.

4b. We have seen that $\mathfrak{b} = d\mathfrak{b}_{u,v}$ therefore $\overline{\mathfrak{b}} = d\mathfrak{b}_{u,-v}$ then $\mathfrak{b}\overline{\mathfrak{b}} = d^2u\mathbf{B}$.
But we also have $\mathrm{N}(\mathfrak{b}) = d^2u\mathbf{A}$ because $d\begin{bmatrix} u & -v \\ 0 & 1 \end{bmatrix}$ is the matrix of an $\mathbf{A}$-basis of $\mathfrak{b}$ over an $\mathbf{A}$-basis of $\mathbf{B}$. We deduce that $\mathfrak{b}\overline{\mathfrak{b}} = \mathrm{N}(\mathfrak{b})\mathbf{A}$. Then, for two nonzero ideals $\mathfrak{b}_1, \mathfrak{b}_2$ of $\mathbf{B}$

$$\mathrm{N}(\mathfrak{b}_1\mathfrak{b}_2)\mathbf{B} = \mathfrak{b}_1\mathfrak{b}_2\overline{\mathfrak{b}_1\mathfrak{b}_2} = \mathfrak{b}_1\overline{\mathfrak{b}_1}\mathfrak{b}_2\overline{\mathfrak{b}_2} = \mathrm{N}(\mathfrak{b}_1)\mathrm{N}(\mathfrak{b}_2)\mathbf{B},$$

hence $\mathrm{N}(\mathfrak{b}_1\mathfrak{b}_2) = \mathrm{N}(\mathfrak{b}_1)\mathrm{N}(\mathfrak{b}_2)$ since the three ideals are principal ideals of $\mathbf{A}$.

4c. First of all, if $\mathfrak{b}$ is a nonzero finitely generated ideal of $\mathbf{B}$, it contains a regular element b and $a = \mathrm{N}(b) = b\widetilde{b}$ is a regular element of $\mathfrak{b}$ contained in $\mathbf{A}$. We then have a surjection $\mathbf{B}/a\mathbf{B} \twoheadrightarrow \mathbf{B}/\mathfrak{b}$ and as $\mathbf{B}/a\mathbf{B}$ is a finite dimensional $\mathbf{k}$-vector space, the same goes for $\mathbf{B}/\mathfrak{b}$.

If $d \in \mathbf{A} \setminus \{0\}$, we have an exact sequence

$$0 \to \mathbf{B}/\mathfrak{b}' \simeq d\mathbf{B}/d\mathfrak{b}' \to \mathbf{B}/d\mathfrak{b}' \to \mathbf{B}/d\mathbf{B} \to 0.$$

We deduce that $\deg(d\mathfrak{b}') = \deg(\mathfrak{b}') + \deg(d\mathbf{B}) = \deg(\mathfrak{b}') + \deg(d^2)$. In particular, for $\mathfrak{b}' = \mathfrak{b}_{u,v}$ and $\mathfrak{b} = d\mathfrak{b}_{u,v}$, we obtain

$$\deg(\mathfrak{b}) = \deg(u) + \deg(d^2) = \deg \mathrm{N}(\mathfrak{b}).$$

This shows that deg is additive.

5. We first provide a reduction algorithm of (u, v) satisfying $v^2 \equiv f \bmod u$. Even if it entails replacing v by $v \bmod u$, we can assume that $\deg v < \deg u$. If $\deg u \leqslant g$, then, by rendering u monic, (u, v) is reduced. Otherwise, with $v^2 - uw = f$ let us show that $\deg w < \deg u$; this will allow us to consider $\widetilde{u} := w$, $\widetilde{v} := (-v) \bmod \widetilde{u}$, having the property $\mathfrak{b}_{u,v} \sim \mathfrak{b}_{\tilde{u},\tilde{v}}$ and to iterate the process $(u, v) \leftarrow (\widetilde{u}, \widetilde{v})$ until we obtain the inegality $\deg u \leqslant g$. To show $\deg u > g \Rightarrow \deg w < \deg u$, we consider the two following cases; either $\deg(uw) > 2g + 1 = \deg f$, in which case the equality $f + uw = v^2$ provides $\deg(uw) = 2 \deg v < 2 \deg u$ so $\deg w < \deg u$; or $\deg(uw) \leqslant 2g + 1$, in which case $\deg w \leqslant 2g + 1 - \deg u < 2g + 1 - g$ so $\deg w \leqslant g < \deg u$.

Every ideal $\mathfrak{b}_{u,v}$ is therefore associated with a reduced ideal and as every nonzero finitely generated ideal $\mathfrak{b}$ of $\mathbf{B}$ is associated with an ideal $\mathfrak{b}_{u,v}$, $\mathfrak{b}$ is therefore associated with a reduced ideal.

6a. Let w satisfy $v^2 - uw = f = y^2$; as (u, v) is reduced, we have

$$\deg v < \deg u \leqslant g < g + 1 \leqslant \deg w \quad \text{and} \quad \deg u + \deg w = 2g + 1.$$

Let $y' = y - v$ and $z = au + by'$ with $a, b \in \mathbf{A}$.
We have $y' + \overline{y'} = -2v$, $y\overline{y'} = -(y^2 - v^2) = uw$, so

$$\mathrm{N}(z) = z\overline{z} = a^2u^2 + aub(y' + \overline{y'}) + b^2y'\overline{y'} = u(a^2u - 2vab + b^2w),$$

hence $\mathrm{N}(z)/\mathrm{N}(\mathfrak{b}_{u,v}) = \mathrm{N}(z)/u = a^2u - 2vab + b^2w$, a polynomial whose degree we need to bound from below. Consider the special case $b = 0$ (therefore $a \neq 0$) in which case $\mathrm{N}(z)/u = a^2u$, of degree $2 \deg a + \deg u \geqslant \deg u$. Here we see that the equality $\deg(\mathrm{N}(z)/u) = \deg u$ is reached if and only if $\deg a = 0$, i.e. if and only if $z \in \mathbf{k}^\times u$.

There is also the special case $a = 0$ (therefore $b \neq 0$) in which case $\mathrm{N}(z)/u = b^2w$, which is of degree $2 \deg b + \deg w > \deg u$.

Therefore it remains to show that for $a \neq 0$, $b \neq 0$, we have $\deg(\mathrm{N}(z)/u) > \deg u$. We introduce $\alpha = \deg a \geqslant 0$, $\beta = \deg b \geqslant 0$ and

$d_1 = \deg(a^2u) = 2\alpha + \deg u$, $d_2 = \deg(vab) = \alpha + \beta + \deg v$, $d_3 = \deg(b^2w) = 2\beta + \deg w$.

We have $d_1 + d_3 \equiv \deg u + \deg w = 2g + 1 \bmod 2$ so $d_1 \neq d_3$. Also, $\alpha \geqslant \beta \Rightarrow d_1 > d_2$ and finally $\beta \geqslant \alpha \Rightarrow d_3 > \max(d_1, d_2)$.
If $d_3 > \max(d_1, d_2)$, then $\deg(\mathrm{N}(z)/u) = d_3 \geqslant \deg w > \deg u$. If $d_3 \leqslant \max(d_1, d_2)$, then $\alpha > \beta$, so $d_1 > d_2$, then $d_1 > \max(d_2, d_3)$.
We therefore have $\deg(\mathrm{N}(z)/u) = d_1 = 2\alpha + \deg u \geqslant 2 + \deg u > \deg u$.

6b. We have $\mathfrak{b}' = d\mathfrak{b}_{u_1,v_1}$ and $\deg(\mathfrak{b}') = 2 \deg(d) + \deg(\mathfrak{b}_{u_1,v_1})$. We can therefore assume that $d = 1$. We have c, $c_1 \in \mathbf{B} \setminus \{0\}$ with $c\mathfrak{b}_{u,v} = c_1\mathfrak{b}_{u_1,v_1}$, which we denote by $\mathfrak{b}$. We have $\mathrm{N}(\mathfrak{b}) = u\mathrm{N}(c) = u_1\mathrm{N}(c_1)$. The minimum degree of the $\mathrm{N}(z)/\mathrm{N}(\mathfrak{b})$'s for $z \in \mathfrak{b} \setminus \{0\}$ is $\deg u$ and it is uniquely reached for $z \in \mathbf{k}^\times cu$. For $z = c_1u_1 \in \mathfrak{b}$, we have $\mathrm{N}(z) = u_1^2\mathrm{N}(c_1)$ therefore $\mathrm{N}(z)/\mathrm{N}(\mathfrak{b}) = \frac{u_1^2\mathrm{N}(c_1)}{u_1\mathrm{N}(c_1)} = u_1$. We therefore have $\deg u_1 \geqslant \deg u$, i.e. $\deg(\mathfrak{b}_{u_1,v_1}) \geqslant \deg(\mathfrak{b}_{u,v})$. The equality is only possible if $c_1u_1 \in \mathbf{k}^\times cu$. In this case, $u\mathfrak{b}_{u_1,v_1} = u_1\mathfrak{b}_{u,v}$. Since the content of $u\mathfrak{b}_{u_1,v_1}$ is u, and since that of $u_1\mathfrak{b}_{u,v}$ is u_1, the previous equality entails $u = u_1$ then $v = v_1$.

7a. We have $F'_X(X,Y) = -f'(X)$, $F'_Y(X,Y) = 2Y$.
As $\mathrm{char}(\mathbf{k}) \neq 2$, we obtain $f(X) \in \langle F, F'_X, F'_Y\rangle$, then $1 \in \langle F, F'_X, F'_Y\rangle$.

7b. We realize the change of variable $\mathbf{x} = 1/x$ in

$$y^2 = f(x) = x^{2g+1} + a_{2g}x^{2g} + \cdots + a_1x + a_0,$$

and we multiply by $\mathbf{x}^{2g+2}$ to obtain

$$\mathbf{y}^2 = \mathbf{x} + a_{2g}\mathbf{x}^2 + \cdots + a_0\mathbf{x}^{2g+2} = \mathbf{x}\big(1 + \mathbf{x}h(\mathbf{x})\big) \quad \text{with} \quad \mathbf{y} = y\mathbf{x}^{g+1}.$$

Recap: the change of variable $\mathbf{x} = 1/x$, $\mathbf{y} = y/x^{g+1}$ gives $\mathbf{k}(x) = \mathbf{k}(\mathbf{x})$ and $\mathbf{k}(x,y) = \mathbf{k}(\mathbf{x},\mathbf{y})$, and $\mathbf{y}$ is integral over $\mathbf{k}[\mathbf{x}]$, a fortiori over $\mathbf{A}_\infty$.
Let $\mathbf{B}_\infty = \mathbf{k}[\mathbf{x},\mathbf{y}]_{\langle \mathbf{x},\mathbf{y}\rangle}$; in this localized ring, we have $\langle \mathbf{x},\mathbf{y}\rangle = \langle \mathbf{y}\rangle$ since $\mathbf{x} = \dfrac{\mathbf{y}^2}{1+\mathbf{x}h(\mathbf{x})}$. Conclusion: $\mathbf{B}_\infty$ is a DVR with regular parameter $\mathbf{y}$.
Finally, let $\mathbf{W}$ be a valuation ring for $\mathbf{k}(x,y)$ containing $\mathbf{k}$.
If $x \in \mathbf{W}$, then $\mathbf{k}[x] \subset \mathbf{W}$. Then y, integral over $\mathbf{k}[x]$, is in $\mathbf{W}$, therefore $\mathbf{B} \subset \mathbf{W}$.
If $x \notin \mathbf{W}$, we have $x^{-1} \in \mathfrak{m}(\mathbf{W})$, so $\mathbf{A}_\infty = \mathbf{k}[x^{-1}]_{\langle x^{-1}\rangle} \subset \mathbf{W}$, and $\mathbf{W} = \mathbf{B}_\infty$.

Problem 5. Let ε be the unit defined by $\boxed{\varepsilon = \beta - \alpha}$.

1. We decompose G and H into homogeneous components G_i, H_j,

$$G = G_a + \cdots + G_b,\ a \leqslant b, \quad H = H_c + \cdots + H_d,\ c \leqslant d.$$

The lower homogeneous component of GH, of degree $a + c$, is G_aH_c while the upper homogeneous component of GH, of degree $b + d$, is G_bH_d. We deduce that $a + c = N$, $b + d = N + 1$; we cannot have $a < b$ and $c < d$ at the same time (because we would then have $a + c + 2 \leqslant b + d$, i.e. $N + 2 \leqslant N + 1$). If $a = b$, then G is homogeneous, if $c = d$ it is H. Suppose that F_N, F_{N+1} are coprime and let $F = GH$ be a factorization; for example, G is homogeneous of degree g; we deduce that $H = H_{N-g} + H_{N+1-g}$ and that $F_N = GH_{N-g}$, $F_{N+1} = GH_{N+1-g}$: G is a common factor of F_N, F_{N+1}, so G is invertible. The converse is easy.

The polynomials $(X^2 + Y^2)^2$ and $\alpha X^2Y + \beta Y^3 = Y(\alpha X^2 + \beta Y^2)$ are coprime if and only if the polynomials $X^2 + Y^2$ and $\alpha X^2 + \beta Y^2$ are coprime; i.e. if and only if $\alpha \neq \beta$.

2. The reader will verify that $(0,0)$ is the only singular point; we have the more precise result

$$\varepsilon^2X^5, \varepsilon^2Y^5 \in \left\langle F, F'_X, F'_Y \right\rangle.$$

3. Let $Y = TX$ in $F(X,Y)$. We obtain $F(X,TX) = X^3G(X,T)$ with

$$G(X,T) = XT^4 + \beta T^3 + 2XT^2 + \alpha T + X.$$

The polynomial G is primitive (in T) and $(x = 0, t = 0)$ is a simple point of the curve $G = 0$. With $a_4 = x$, $a_3 = \beta$, $a_2 = 2x$, $a_1 = \alpha$, $a_0 = x$, we consider the integral elements (by Emmanuel's trick)

$$b_4 = a_4, \quad b_3 = a_3 + tb_4, \quad b_2 = a_2 + tb_3, \quad b_1 = a_1 + tb_2.$$

Thus, $b_4 = x$, $b_3 = \beta + y$ and $b_2 = 2x + (\beta + y)y/x$.

It is clear that a_4, a_3, ..., $a_0 \in \sum_i \mathbf{A}b_i + \sum_i \mathbf{A}tb_i$. As $a_3 - a_1 = \varepsilon$ is invertible, there are $u_i, v_i \in \mathbf{A}$ such that $1 = \sum_i u_i b_i + \sum_i v_i t b_i$. We formally write (without worrying about the nullity of a b_i)

$$t = \tfrac{b_1 t}{b_1} = \cdots = \tfrac{b_4 t}{b_4} = \frac{\sum_i v_i b_i t}{\sum_i v_i b_i} = \frac{\sum_i u_i b_i t}{\sum_i u_i b_i}.$$

Thus, $t = y/x = a/b = c/d$ with a, b, c, $d \in \mathbf{B}$ and $a + d = 1$.

The equalities $by = ax$, $dy = cx$, $a + d = 1$ are those coveted.

Thus we obtain $\mathfrak{q}\,\langle x, y\rangle_{\mathbf{B}} = \langle x\rangle_{\mathbf{B}}$ with $\mathfrak{q} = \langle d, b\rangle_{\mathbf{B}}$. Here by letting

$$a = b_2 t - b_4 t, \quad b = b_2 - b_4, \quad c = b_3 t - b_1 t, \quad d = b_3 - b_1,$$

we have $\varepsilon = a + d$. By letting $g_0 = 1/(1 + t^2)$, $g_1 = tg_0$, we find $b = \varepsilon g_1$, $d = \varepsilon g_0$, so $\mathfrak{q} = \langle g_0, g_1\rangle_{\mathbf{B}}$. We will show (question *5*) that $\mathbf{B} = \mathbf{k}[g_0, g_1]$, so $\mathbf{B}/\mathfrak{q} = \mathbf{k}$.

4. A geometric idea leads to the equality $\mathbf{k}(t) = \mathbf{k}(x, y)$. It is the parameterization of the trifolium. The polynomial defining the curve is of degree 4 and the origin is a singular point of multiplicity 3. Therefore a rational line passing through the origin intersects the curve at a rational point. Algebraically, this corresponds to the fact that the polynomial $G(X, T)$ is of degree 1 in X

$$G(T, X) = (T^4 + 2T^2 + 1)X + \beta T^3 + \alpha T = (T^2 + 1)^2 X + T(\beta T^2 + \alpha),$$

hence

$$x = -\frac{t(\beta t^2 + \alpha)}{(t^2 + 1)^2}, \quad y = tx = -\frac{t^2(\beta t^2 + \alpha)}{(t^2 + 1)^2}.$$

At $t = 0$, we have $(x, y) = (0, 0)$. What are the other values of the parameter t for which $\big(x(t), y(t)\big) = (0, 0)$?

We have to first find the zeros of $x(t)$, a rational fraction of height 4. There is the value $t = \infty$, for which $y(t) = -\beta$.

If $\alpha = 0$, we only have two zeros of x: $t = 0$ (of multiplicity 3) and $t = \infty$ (of multiplicity 1).

If $\beta = 0$, we only have two zeros of x: $t = 0$ (of multiplicity 1) and $t = \infty$ (of multiplicity 3).

If $\beta \neq 0$, we have two other zeros of x (eventually coinciding): $t = \pm\sqrt{-\alpha/\beta}$. We can render this more uniform by making the quadratic character of $-\alpha\beta$ intervene, see question *7*.

Remark: in all the cases, at $t = \infty$, we have $(x, y) = (0, -\beta)$.

5. We know by Exercise 8 that $\mathbf{k}[g_0, g_1]$ is an integrally closed ring, the integral closure of $\mathbf{k}[g_0]$ in $\mathbf{k}(t)$. To obtain a $\mathbf{k}$-relator between g_0 and g_1, we substitute $t = g_1/g_0$ in the expression $g_0 = 1/(1 + t^2)$, which gives $g_0^2 - g_0 + g_1^2 = 0$ and confirms that g_1 is integral over $\mathbf{k}[g_0]$. At $t = 0$, we have $(g_0, g_1) = (1, 0)$; this point is a nonsingular point of the curve $g_0^2 - g_0 + g_1^2 = 0$. Actually the conic $C(g_0, g_1) = g_0^2 - g_0 + g_1^2$ is smooth over every ring since

$$1 = -4C + (2g_0 - 1)\tfrac{\partial C}{\partial g_0} + 2g_1\tfrac{\partial C}{\partial g_1}.$$

The same goes for the homogenized conic denoted by C, $C = g_0^2 - g_0 g_2 + g_1^2$, which satisfies $\langle g_0, g_1, g_2 \rangle^2 \subseteq \left\langle C, \frac{\partial C}{\partial g_0}, \frac{\partial C}{\partial g_1}, \frac{\partial C}{\partial g_2} \right\rangle$

$$g_0 = -\frac{\partial C}{\partial g_2}, \quad g_1^2 = C + (g_0 - g_2)\frac{\partial C}{\partial g_2}, \quad g_2 = -\frac{\partial C}{\partial g_0} - 2\frac{\partial C}{\partial g_2}.$$

We dispose of $\mathbb{P}^1 \to \mathbb{P}^2$ defined by $(u : v) \mapsto (g_0 : g_1 : g_2) = (u^2 : uv : u^2 + v^2)$ whose image is the homogeneous conic $C = 0$; more or less, this is a Veronese embedding $\mathbb{P}^1 \to \mathbb{P}^2$ of degree 2.

Moreover, the decomposition into simple elements provides the following expressions of x, y, $b_3 t$, $b_2 t$ in $\mathbf{k}[g_0, g_1]$

$$x = \varepsilon g_0 g_1 - \beta g_1, \quad y = \varepsilon g_0^2 + (2\beta - \alpha) g_0 - \beta = (g_0 - 1)(\beta - \varepsilon g_0)$$
$$b_2 t = 2y + (\beta + y)t^2 = -\alpha + \beta g_0 - \varepsilon g_0^2, \quad b_3 t = (2\beta - \alpha) g_1 - \varepsilon g_0 g_1.$$

We see that g_0 is integral over $\mathbf{k}[y]$, therefore integral over $\mathbf{k}[x]$; as g_1 is integral over $\mathbf{k}[g_0]$, it also is integral over $\mathbf{k}[x]$. We have just obtained the equality $\mathbf{B} = \mathbf{k}[g_0, g_1]$.

First consider $\mathbf{k}[y] \subset \mathbf{k}[g_0] \subset \mathbf{k}[g_0, g_1]$; it is clear that $(1, g_0)$ is a basis of $\mathbf{k}[g_0]$ over $\mathbf{k}[y]$ and $(1, g_1)$ is a basis of $\mathbf{k}[g_0, g_1]$ over $\mathbf{k}[g_0]$, therefore $(1, g_0, g_1, g_0 g_1)$ is a basis of $\mathbf{k}[g_0, g_1]$ over $\mathbf{k}[y]$ (but not over $\mathbf{A} = \mathbf{k}[x]$).

Let us show that $(1, y, b_3 t, b_2 t)$ is an $\mathbf{A}$-basis, let E be the generated $\mathbf{A}$-module. By using $y - b_2 t = \varepsilon(g_0 - 1)$ and $x + b_3 t = \varepsilon g_1$, we see that g_0, $g_1 \in E$. Finally, E contains $x + \beta g_1 = \varepsilon g_0 g_1$, so $g_0 g_1 \in E$ and $E = \mathbf{k}[g_0, g_1] = \mathbf{B}$.

An invertible ideal $\mathfrak{b}$ of $\mathbf{B}$ contains a regular element therefore $\mathbf{B}/\mathfrak{b}$ is a finite dimensional $\mathbf{k}$-vector space, which allows us to define $\deg \mathfrak{b}$ by $\deg \mathfrak{b} = \dim_{\mathbf{k}} \mathbf{B}/\mathfrak{b}$; we then have (see Proposition 5.5 and its Corollary 5.6) $\deg(\mathfrak{b}\mathfrak{b}') = \deg(\mathfrak{b}) + \deg(\mathfrak{b}')$. We deduce that $\deg \langle x, y \rangle_{\mathbf{B}} = 4 - 1 = 3$.

6. We have $\mathfrak{p}_1 = \langle g_0 - 1, g_1 \rangle$, therefore to show the equality $\mathfrak{p}_1^2 = \left\langle g_0 - 1, g_1^2 \right\rangle$, it suffices to see that $g_0 - 1 \in \left\langle (g_0 - 1)^2, g_1^2 \right\rangle$. This results from the equality $1 - g_0 = (1 - g_0)^2 + g_1^2$ which stems from $g_0^2 - g_0 + g_1^2 = 0$.

7. Let $X = UY$ in $F(X, Y)$. We obtain $F(UY, Y) = U^3 H(U, Y)$ with

$$H(U, Y) = YU^4 + (2Y + \alpha)U^2 + Y + \beta, \qquad H(U, 0) = \alpha U^2 + \beta.$$

This polynomial $H = a_4' U^4 + a_2' U^2 + a_0'$ is primitive in U (we have $a_2' = 2a_4' + \alpha$ and $a_0' = a_4' + \beta$ therefore $\epsilon = a_0' - a_2' + a_4'$). It satisfies $H(u, y) = 0$ with $u = x/y$; the associated element b_3' determined by Emmanuel's trick is x and we therefore have $b_3' u \in \mathbf{B}$ with

$$b_3' u = x^2/y = \varepsilon g_0 - \beta - y.$$

In root t of $\beta t^2 + \alpha = 0$, we have $g_0 = \beta/\varepsilon$ and $g_1^2 = -\alpha\beta/\varepsilon^2$, which renders the introduction of the ideal $\mathfrak{a} = \left\langle \varepsilon g_0 - \beta, \varepsilon^2 g_1^2 + \alpha\beta \right\rangle$ natural. We verify the equality

$$\left\langle y, x^2/y \right\rangle_{\mathbf{B}} = \left\langle \varepsilon g_0 - \beta, \varepsilon^2 g_1^2 + \alpha\beta \right\rangle.$$

We then have $\langle x, y \rangle_{\mathbf{B}} = \mathfrak{p}_1 \mathfrak{a}$ and $\deg \mathfrak{a} = 2$. If $-\alpha\beta$ is not a square, then $\mathfrak{a}$ is prime. Otherwise, we have $\mathfrak{a} = \mathfrak{p}_2 \mathfrak{p}_3$ with $\mathfrak{p}_2, \mathfrak{p}_3$ expressed with the two square roots of $-\alpha\beta$. We have $\mathfrak{p}_2 = \mathfrak{p}_3$ if and only if the two square roots are confused; this happens when $\alpha\beta = 0$ for example or in characteristic 2. Finally, for $\alpha = 0$, we have $\mathfrak{p}_1 = \mathfrak{p}_2 = \mathfrak{p}_3$.

Bibliographic comments

Regarding the genesis of the theory of ideals of number fields developed by Dedekind, we can read the articles of H. Edwards [73] and of J. Avigad [4].

The Prüfer domains were introduced by H. Prüfer in 1932 in [153]. Their central role in the multiplicative theory of ideals is highlighted in the reference book on the subject [Gilmer]. See also the bibliographic comments at the end of Chapter VIII.

In the classical literature a coherent Prüfer ring is often called a *semi-hereditary ring* (according to item *3* in Theorem 4.1), which is not very pretty. These rings are signaled as important in [Cartan & Eilenberg]. The constructive proof of item *1* of Theorem 4.5 is given in Chapter 1, Proposition 6.1.

A *hereditary ring* is a ring in which every ideal is projective. This notion is badly defined in constructive mathematics because of the non-legitimate quantification "every ideal." An example of such a non-Noetherian ring is the subring of a countable product of the field $\mathbb{F}_2$, formed by the sequences which are either null almost everywhere, or equal to 1 almost everywhere. The most interesting case is that of Noetherian coherent Prüfer rings, which we described in classical mathematics as the rings in which every ideal is finitely generated projective. Our definition of a Dedekind ring (freed from the integrity constraint) corresponds exactly (in classical mathematics) to the notion of a Noetherian hereditary ring.

Fairly comprehensive presentations on arithmetic rings and Prüfer rings written in the style of constructive mathematics can be found in the articles [71, Ducos&al.] and [128, Lombardi].

"Emmanuel's trick" of Lemma 4.7 appears in Emmanuel Hallouin's PhD thesis [99].

Theorem 4.8 is due to Gilmer and Hoffmann [94]. Theorem 6.1 for the case of a Prüfer domain is given by Heitman and Levy in [102]. Theorem 6.2 has been proven in classical mathematics by Quentel in [154]. The constructive proof is due to I. Yengui.

Theorem 6.3 is classical (Steinitz's theorem) for Dedekind rings. It has been generalized for the Prüfer domains having the one and a half property in [119, Kaplansky] and [102, Heitmann&Levy]. A detailed inspection of our proof actually shows that the hypothesis "ring of dimension at most 1" could be weakened to "ring having the one and a half property."

We find Theorem 6.7 (see also Exercise 17) in [24, Brewer&Klinger] for the integral case. It has been generalized to the case of a pp-ring in [55, Couchot].

Lemma 5.7 and Theorem 7.12 are due to Claire Tête and Lionel Ducos.

Problem 3 is based on the article [104, Hess].

Theorem III-8.12 says that if $\mathbf{A}$ is integrally closed, the same goes for $\mathbf{A}[X]$. A constructive proof of the same result for normal rings is given in [45].

Chapter XIII

Krull dimension

Contents

Introduction

In this chapter we introduce the Krull dimension in its elementary constructive version and we compare it to the corresponding classical notion.

Next we establish the first properties of this dimension. The ease with which we obtain the Krull dimension of a polynomial ring over a discrete field shows that the constructive version of the Krull dimension can be seen as a conceptual simplification of the usual classical version.

We then apply the same type of ideas to define the Krull dimension of a distributive lattice, that of a morphism of commutative rings, then the valuative dimension of commutative rings.

We establish a few basic important theorems regarding these notions.

We finish by indicating the constructive versions of the usual classical notions of Lying Over, Going Up, Going Down and Incomparability, with some applications.

1. Spectral spaces

In this section, we describe the classical approach to Krull dimension.

For us, this is above all a matter of heuristics. It is for this reason that we give no proofs. This will have no incidence in the rest of the book. Indeed, the constructive aspect of the spectral spaces is entirely concentrated in the distributive lattices obtained by duality. In particular, the constructive aspect of the Krull dimension is entirely concentrated in the Krull dimension of the distributive lattices and it can be defined completely independently from the spectral spaces.

Nevertheless the heuristic given by the spectral spaces is essential to the understanding of the small miracle that will happen with the introduction of the dual constructive notions. This small miracle will only fully be realized in the following chapters, where we will see the transformation of many beautiful abstract theorems into algorithms.

The Zariski lattice and the Zariski spectrum

Recall that we denote by $\mathrm{D}_{\mathbf{A}}(\mathfrak{a})$ the nilradical of the ideal $\mathfrak{a}$ in the ring $\mathbf{A}$ and that the Zariski lattice $\mathsf{Zar}\,\mathbf{A}$ is the set of the $\mathrm{D}_{\mathbf{A}}(x_1,\ldots,x_n)$'s (for $n \in \mathbb{N}$ and $x_1, \ldots, x_n \in \mathbf{A}$). We therefore have $x \in \mathrm{D}_{\mathbf{A}}(x_1,\ldots,x_n)$ if and only if a power of x belongs to $\langle x_1,\ldots,x_n\rangle$. The set $\mathsf{Zar}\,\mathbf{A}$, ordered by the inclusion relation, is a distributive lattice with

$$\mathrm{D}_{\mathbf{A}}(\mathfrak{a}_1) \vee \mathrm{D}_{\mathbf{A}}(\mathfrak{a}_2) = \mathrm{D}_{\mathbf{A}}(\mathfrak{a}_1 + \mathfrak{a}_2) \text{ and } \mathrm{D}_{\mathbf{A}}(\mathfrak{a}_1) \wedge \mathrm{D}_{\mathbf{A}}(\mathfrak{a}_2) = \mathrm{D}_{\mathbf{A}}(\mathfrak{a}_1\,\mathfrak{a}_2).$$

1.1. Definition. We call the set of strict prime ideals of the ring $\mathbf{A}$ the *Zariski spectrum* of $\mathbf{A}$ and we denote it by $\mathsf{Spec}\,\mathbf{A}$. We equip it with the topology that has as its basis of open sets the $\mathfrak{D}_{\mathbf{A}}(a) = \{\, \mathfrak{p} \in \mathsf{Spec}\,\mathbf{A} \mid a \notin \mathfrak{p} \,\}$. We denote by $\mathfrak{D}_{\mathbf{A}}(x_1,\ldots,x_n)$ the set $\mathfrak{D}_{\mathbf{A}}(x_1) \cup \cdots \cup \mathfrak{D}_{\mathbf{A}}(x_n)$.

For $\mathfrak{p} \in \mathsf{Spec}\,\mathbf{A}$ and $S = \mathbf{A} \setminus \mathfrak{p}$, we denote $\mathbf{A}_S$ by $\mathbf{A}_{\mathfrak{p}}$ (the ambiguity between the two contradictory notations $\mathbf{A}_{\mathfrak{p}}$ and $\mathbf{A}_S$ is removed in practice by the context).

In classical mathematics, we then obtain the following result.

1.2. Theorem*.

1. *The compact-open subspaces of* $\mathsf{Spec}\,\mathbf{A}$ *are the open sets* $\mathfrak{D}_{\mathbf{A}}(x_1,\ldots,x_n)$.
2. *The map* $\mathrm{D}_{\mathbf{A}}(x_1,\ldots,x_n) \mapsto \mathfrak{D}_{\mathbf{A}}(x_1,\ldots,x_n)$ *is well-defined.*
3. *It is an isomorphism of distributive lattices.*

Spectrum of a distributive lattice

The Zariski spectrum is the paradigmatic example of a *spectral space.* Spectral spaces were introduced by Stone [181] in 1937.

They can be characterized as the topological spaces satisfying the following properties

- the space is quasi-compact,
- every open set is a union of compact-open subspaces,
- the intersection of two compact-open subspaces is a compact-open subspace,
- for two distinct points, there is an open set containing one of them but not the other,
- every irreducible closed set is the adherence of a point.

The compact-open subspaces then form a distributive lattice, the supremum and the infimum being the union and the intersection, respectively. A continuous map between spectral spaces is said to be *spectral* if the inverse image of every compact-open subspace is a compact-open subspace. Stone's fundamental result can be stated as follows.

In classical mathematics the category of spectral spaces and spectral maps is anti-equivalent to the category of distributive lattices.

Here is how this works.

First of all if $\mathbf{T}$ is a distributive lattice, a *prime ideal* is an ideal $\mathfrak{p}$ which satisfies

$$x \wedge y \in \mathfrak{p} \;\Rightarrow\; (x \in \mathfrak{p} \text{ or } y \in \mathfrak{p}), \qquad 1_{\mathbf{T}} \notin \mathfrak{p}.$$

The *spectrum* of $\mathbf{T}$, denoted by $\mathsf{Spec}\,\mathbf{T}$, is then defined as the space whose points are the prime ideals of $\mathbf{T}$ and which has a basis of open sets given by the subsets $\mathfrak{D}_{\mathbf{T}}(a) := \{\, \mathfrak{p} \in \mathsf{Spec}\,\mathbf{T} \mid a \notin \mathfrak{p} \,\}$ for $a \in \mathbf{T}$.
If $\varphi : \mathbf{T} \to \mathbf{V}$ is a morphism of distributive lattices, we define the map

$$\mathsf{Spec}\,\varphi : \mathsf{Spec}\,\mathbf{V} \to \mathsf{Spec}\,\mathbf{T}, \quad \mathfrak{p} \mapsto \varphi^{-1}(\mathfrak{p}).$$

It is a spectral map and all of this defines Spec as a contravariant functor.
We show that the $\mathfrak{D}_{\mathbf{T}}(a)$'s are all the compact-open subspaces of $\mathsf{Spec}\,\mathbf{T}$.
Actually Theorem* 1.2 applies to every distributive lattice $\mathbf{T}$:

1. *The compact-open subspaces of* $\mathsf{Spec}\,\mathbf{T}$ *are exactly the* $\mathfrak{D}_{\mathbf{T}}(u)$*'s.*
2. *The map* $u \mapsto \mathfrak{D}_{\mathbf{T}}(u)$ *is well-defined and it is an isomorphism of distributive lattices.*

In the other direction, if X is a spectral space we let $\mathsf{Oqc}(X)$ be the distributive lattice formed by its compact-open subspaces. If $\xi : X \to Y$ is a spectral map, the map

$$\mathsf{Oqc}(\xi) : \mathsf{Oqc}(Y) \to \mathsf{Oqc}(X), \quad U \mapsto \xi^{-1}(U)$$

is a homomorphism of distributive lattices. This defines Oqc as a contravariant functor.

The stated anti-equivalence of categories is defined by the functors Spec and Oqc. It generalizes the anti-equivalence given in the finite case by Theorem XI-5.6.

Note that the empty spectral space corresponds to the lattice $\mathbf{1}$, and that a reduced spectral space at a point corresponds to the lattice $\mathbf{2}$.

Spectral subspaces

By definition, a subset Y of a spectral space X is a *spectral subspace* if Y is a spectral space by the induced topology and if the canonical injection $Y \to X$ is spectral.
This notion is actually exactly the dual notion of the notion of a quotient distributive lattice. In other words a spectral map $\alpha : Y \to X$ identifies Y with a spectral subspace of X if and only if the homomorphism of distributive lattices $\mathsf{Oqc}(\alpha)$ identifies $\mathsf{Oqc}(Y)$ to a quotient distributive lattice of $\mathsf{Oqc}(X)$.

The closed subspaces of X are spectral and correspond to the quotients by the ideals. More precisely an ideal $\mathfrak{a}$ of $\mathsf{Oqc}(X) = \mathbf{T}$ defines the closed set $\mathfrak{V}_{\mathbf{T}}(\mathfrak{a}) = \{\, \mathfrak{p} \in X \,|\, \mathfrak{a} \subseteq \mathfrak{p} \,\}$, (provided we identify the points of X with the prime ideals of $\mathsf{Oqc}(X)$) and we then have a canonical isomorphism

$$\mathsf{Oqc}\big(\mathfrak{V}_{\mathbf{T}}(\mathfrak{a})\big) \simeq \mathsf{Oqc}(X)/(\mathfrak{a} = 0) \ .$$

The irreducible closed sets correspond to the prime ideals of $\mathsf{Oqc}(X)$.

Finally, the compact-open subspaces correspond to the quotients by principal filters

$$\mathsf{Oqc}\big(\mathfrak{D}_{\mathbf{T}}(u)\big) \simeq \mathsf{Oqc}(X)/(\uparrow u = 1) \ .$$

A heuristic approach to the Krull dimension

Note moreover that the Zariski spectrum of a commutative ring is naturally identified with the spectrum of its Zariski lattice.

In classical mathematics, the notion of Krull dimension can be defined, for an arbitrary spectral space X, as the maximal length of the strictly increasing chains of irreducible closed sets.

An intuitive way to apprehend this notion of dimension is the following. The dimension can be characterized by induction by saying that on the one hand, the dimension -1 corresponds to the empty space, and on the other hand, for $k \geqslant 0$, a space X is of dimension at most k if and only if for every compact-open subspace Y, the boundary of Y in X is of dimension at most $k-1$ (this boundary is closed therefore it is a spectral subspace of X).

Let us see, for example, for a commutative ring $\mathbf{A}$, how we can define the boundary of the open set $\mathfrak{D}_{\mathbf{A}}(a)$ in $\mathsf{Spec}\,\mathbf{A}$. The boundary is the intersection of the adherence of $\mathfrak{D}_{\mathbf{A}}(a)$ and of the complementary closed set of $\mathfrak{D}_{\mathbf{A}}(a)$, which we denote by $\mathfrak{V}_{\mathbf{A}}(a)$. The adherence of $\mathfrak{D}(a)$ is the intersection of all the $\mathfrak{V}(x)$'s that contain $\mathfrak{D}(a)$, i.e. such that $\mathfrak{D}(x) \cap \mathfrak{D}(a) = \emptyset$.

As $\mathfrak{D}(x) \cap \mathfrak{D}(a) = \mathfrak{D}(xa)$, and as we have $\mathfrak{D}(y) = \emptyset$ if and only if y is nilpotent, we obtain a heuristic approach to the ideal “Krull boundary of a,” which is the ideal generated by a on the one hand (which corresponds to $\mathfrak{V}(a)$), and by all the x's such that xa is nilpotent on the other hand (which corresponds to the adherence of $\mathfrak{D}(a)$).

2. Constructive definition and first consequences

In classical mathematics, the Krull dimension of a commutative ring is defined as the maximum (eventually infinite) of the lengths of the strictly increasing chains of strict prime ideals (beware, a chain $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_\ell$ is said to be of length ℓ). Since the complement of a prime ideal is a prime filter, the Krull dimension is also the maximum of the lengths of the strictly increasing chains of prime filters.

As this definition is impossible to manipulate from an algorithmic point of view, we replace it in constructive mathematics by an equivalent definition (in classical mathematics) but of a more elementary nature.

The quantification over the set of prime ideals of the ring is then replaced by a quantification over the elements of the ring and the non-negative integers. Since this discovery (surprisingly it is very recent) the theorems that make the Krull dimension intervene have been able to become fully integrated into constructive mathematics and into Computer Algebra.

2.1. Definition. Let $\mathbf{A}$ be a commutative ring, $x \in \mathbf{A}$ and $\mathfrak{a}$ be a finitely generated ideal.

(1) The *Krull upper boundary* of $\mathfrak{a}$ in $\mathbf{A}$ is the quotient ring

$$\mathbf{A}_{\mathrm{K}}^{\mathfrak{a}} := \mathbf{A}/\mathcal{J}_{\mathbf{A}}^{\mathrm{K}}(\mathfrak{a}) \quad \text{where} \quad \mathcal{J}_{\mathbf{A}}^{\mathrm{K}}(\mathfrak{a}) := \mathfrak{a} + (\sqrt{0} : \mathfrak{a}). \tag{1}$$

Write $\mathcal{J}_{\mathbf{A}}^{\mathrm{K}}(x)$ for $\mathcal{J}_{\mathbf{A}}^{\mathrm{K}}(x\mathbf{A})$ and $\mathbf{A}_{\mathrm{K}}^{x}$ for $\mathbf{A}_{\mathrm{K}}^{x\mathbf{A}}$. This ring is called the *upper boundary of x in* $\mathbf{A}$.
We will say that $\mathcal{J}_{\mathbf{A}}^{\mathrm{K}}(\mathfrak{a})$ is *the Krull boundary ideal of $\mathfrak{a}$ in $\mathbf{A}$.*

(2) The *Krull lower boundary* of x in $\mathbf{A}$ is the localized ring

$$\mathbf{A}_{x}^{\mathrm{K}} := \mathcal{S}_{\mathbf{A}}^{\mathrm{K}}(x)^{-1}\mathbf{A} \quad \text{where} \quad \mathcal{S}_{\mathbf{A}}^{\mathrm{K}}(x) = x^{\mathbb{N}}(1 + x\mathbf{A}). \tag{2}$$

We will say that $\mathcal{S}_{\mathbf{A}}^{\mathrm{K}}(x)$ is the *Krull boundary monoid of x* in $\mathbf{A}$.

Recall that in classical mathematics the Krull dimension of a ring is -1 if and only if the ring does not admit any prime ideals, which means that it is trivial.

The following theorem then gives in classical mathematics an elementary inductive characterization of the Krull dimension of a commutative ring.

2.2. Theorem*. *For a commutative ring $\mathbf{A}$ and an integer $k \geqslant 0$ the following properties are equivalent.*

1. *The Krull dimension of $\mathbf{A}$ is $\leqslant k$.*
2. *For all $x \in \mathbf{A}$ the Krull dimension of $\mathbf{A}_{\mathrm{K}}^{x}$ is $\leqslant k - 1$.*
3. *For all $x \in \mathbf{A}$ the Krull dimension of $\mathbf{A}_{x}^{\mathrm{K}}$ is $\leqslant k - 1$.*

Note: this is a theorem of classical mathematics which cannot admit a constructive proof. ∎

In the proof that follows all the prime or maximal ideals and filters are taken in the usual sense in classical mathematics: they are strict.

D Let us first show the equivalence of items *1* and *3.* Recall that the prime ideals of $S^{-1}\mathbf{A}$ are of the form $S^{-1}\mathfrak{p}$ where $\mathfrak{p}$ is a prime ideal of $\mathbf{A}$ which

does not intersect S (Fact XI-4.17). The equivalence then clearly results from the two following statements.
(a) Let $x \in \mathbf{A}$, if $\mathfrak{m}$ is a maximal ideal of $\mathbf{A}$ it always intersects $\mathcal{S}_{\mathbf{A}}^{\mathrm{K}}(x)$. Indeed, if $x \in \mathfrak{m}$ it is clear and otherwise, x is invertible modulo $\mathfrak{m}$ which means that $1 + x\mathbf{A}$ intersects $\mathfrak{m}$.
(b) Let $\mathfrak{a}$ be an ideal, $\mathfrak{p}$ be a prime ideal with $\mathfrak{p} \subset \mathfrak{a}$ and $x \in \mathfrak{a} \setminus \mathfrak{p}$; if $\mathfrak{p} \cap \mathcal{S}_{\mathbf{A}}^{\mathrm{K}}(x)$ is nonempty, then $1 \in \mathfrak{a}$. Indeed, let $x^n(1 + xy) \in \mathfrak{p}$; since $x \notin \mathfrak{p}$, we have $1 + xy \in \mathfrak{p} \subset \mathfrak{a}$, which gives, with $x \in \mathfrak{a}$, $1 \in \mathfrak{a}$.
Thus, if $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_\ell$ is a chain with $\mathfrak{p}_\ell$ maximal, it is shortened by at least its last term when we localize at $\mathcal{S}_{\mathbf{A}}^{\mathrm{K}}(x)$, and it is only shortened by its last term if $x \in \mathfrak{p}_\ell \setminus \mathfrak{p}_{\ell-1}$.
The equivalence of items *1* and *2* is proven dually, by replacing the prime ideals by the prime filters. Let $\pi : \mathbf{A} \to \mathbf{A}/\mathfrak{a}$ be the canonical projection. We notice that the prime filters of $\mathbf{A}/\mathfrak{a}$ are exactly the $\pi(S)$'s, where S is a prime filter of $\mathbf{A}$ that does not intersect $\mathfrak{a}$ (Fact XI-4.16). It then suffices to prove the two dual statements of (a) and (b) which are the following.
(a') Let $x \in \mathbf{A}$, if S is a maximal filter of $\mathbf{A}$ it always intersects $\mathcal{J}_{\mathbf{A}}^{\mathrm{K}}(x)$. Indeed, if $x \in S$ it is clear and otherwise, since S is maximal, $Sx^{\mathbb{N}}$ contains 0, which means that there is an integer n and an element s of S such that $sx^n = 0$. Then $(sx)^n = 0$ and $s \in (\sqrt{0} : x) \subseteq \mathcal{J}_{\mathbf{A}}^{\mathrm{K}}(x)$.
(b') Let S' be a prime filter contained in a filter S and $x \in S \setminus S'$. If $S' \cap \mathcal{J}_{\mathbf{A}}^{\mathrm{K}}(x)$ is nonempty, then $S = \mathbf{A}$. Indeed, let $ax + b \in S'$ with $(bx)^n = 0$. Then, since $x \notin S'$, we have $ax \notin S'$ and, given that S' is prime, $b \in S' \subseteq S$. As $x \in S$, we obtain $(bx)^n = 0 \in S$. □

In constructive mathematics we replace the usual definition given in classical mathematics by the following more elementary definition.

2.3. Definition. The *Krull dimension* (denoted by Kdim) of a commutative ring $\mathbf{A}$ is defined by induction as follows

1. $\mathsf{Kdim}\,\mathbf{A} = -1$ if and only if $\mathbf{A}$ is trivial.
2. For $k \geqslant 0$, $\mathsf{Kdim}\,\mathbf{A} \leqslant k$ means $\forall x \in \mathbf{A}$, $\mathsf{Kdim}(\mathbf{A}_x^{\mathrm{K}}) \leqslant k - 1$.

Naturally, we will say that $\mathbf{A}$ is infinite dimensional if and only if for every integer $k \geqslant 0$ we have the implication $\mathsf{Kdim}\,\mathbf{A} \leqslant k \Rightarrow 1 =_{\mathbf{A}} 0$.

The following lemma immediately results from the definitions.

2.4. Lemma. *A ring is zero-dimensional if and only if it is of dimension at most* 0.

Note that the terminology “zero-dimensional ring” therefore constitutes a slight abuse of language because affirming that the dimension is less than or equal to 0 leaves the possibility of a dimension equal to -1 open, which means that the ring is trivial.

Examples.
1) If x is nilpotent or invertible in $\mathbf{A}$, the boundary ideal and the boundary monoid of x in $\mathbf{A}$ are both equal to $\mathbf{A}$. The two boundary rings are trivial.

2) For $x \neq 0$, 1, -1 in $\mathbb{Z}$, the boundary rings $\mathbb{Z}_{\mathrm{K}}^{x} = \mathbb{Z}/x\mathbb{Z}$ and $\mathbb{Z}_{x}^{\mathrm{K}} = \mathbb{Q}$ are zero-dimensional. We therefore find that $\mathsf{Kdim}\,\mathbb{Z} \leqslant 1$ again.

3) Let $\mathbf{K}$ be a field contained in a discrete algebraically closed field $\mathbf{L}$. Let $\mathfrak{a}$ be a finitely generated ideal of $\mathbf{K}[X_1, \dots, X_n]$ and $\mathbf{A} = \mathbf{K}[X_1, \dots, X_n]/\mathfrak{a}$. Let V be the affine variety corresponding to $\mathfrak{a}$ in $\mathbf{L}^n$ and W be the subvariety of V defined by f. Then the "boundary of W in V," defined as the intersection of W with the Zariski closure of its complement in V, is the affine variety corresponding to the ring $\mathbf{A}_{\mathrm{K}}^{f}$. We abbreviate this as

$$\text{boundary}_V\, \mathcal{Z}(f) = \mathcal{Z}_V(\text{boundary of } f).$$

4) Let $\mathbf{A}$ be integral and $k \geqslant 0$: $\mathsf{Kdim}\,\mathbf{A} \leqslant k$ is equivalent to $\mathsf{Kdim}(\mathbf{A}/a\mathbf{A}) \leqslant k-1$ for every regular a (use the Krull boundary ideals).

5) Let $\mathbf{A}$ be a residually discrete local ring and $k \geqslant 0$: $\mathsf{Kdim}\,\mathbf{A} \leqslant k$ is equivalent to $\mathsf{Kdim}\,\mathbf{A}[1/a] \leqslant k-1$ for all $a \in \operatorname{Rad} \mathbf{A}$ (use the Krull boundary monoids). ■

Comments. 1) The advantage of the constructive definition of the Krull dimension with respect to the usual definition is that it is simpler (no quantification over the set of prime ideals) and more general (no need to assume the axiom of choice). However, we have only defined the sentence "$\mathbf{A}$ is of dimension at most k."

2) In the context of classical mathematics. The Krull dimension of $\mathbf{A}$ can be defined as an element of $\{-1\} \cup \mathbb{N} \cup \{+\infty\}$ by letting

$$\mathsf{Kdim}\,\mathbf{A} = \inf \{\, k \in \mathbb{Z},\ k \geqslant -1 \mid \mathsf{Kdim}\,\mathbf{A} \leqslant k \,\},$$

(with $\inf \emptyset_{\mathbb{Z}} = +\infty$). This definition based on the constructive definition 2.3 is equivalent to the usually given definition via chains of prime ideals (see Theorem* 2.2).

3) From the constructive point of view, the previous method does not define the Krull dimension of $\mathbf{A}$ as an element of $\{-1\} \cup \mathbb{N} \cup \{+\infty\}$. Actually it so happens that the concept in question is generally not necessary (but the reader must take our word for it).
The most similar point of view to classical mathematics would be to look at $\mathsf{Kdim}\,\mathbf{A}$ as a subset of $\mathbb{N} \cup \{-1\}$, defined by

$$\{\, k \in \mathbb{Z},\ k \geqslant -1 \mid \mathsf{Kdim}\,\mathbf{A} \leqslant k \,\}.$$

We then reason with (eventually empty) final subsets of $\mathbb{N} \cup \{-1\}$, the order relation is given by the reversed inclusion, the upper bound by the intersection and the lower bound by the union.
This approach finds its limit with the "counterexample" of the real number field (see the comment on page 764). ■

We use in constructive mathematics the following *notations*, to be closer to the classical language

2.5. Notation. Let $\mathbf{A}$, $\mathbf{B}$, $(\mathbf{A}_i)_{i\in I}$, $(\mathbf{B}_j)_{j\in J}$ be commutative rings (with I, J finite).

– $\mathsf{Kdim}\,\mathbf{B} \leqslant \mathsf{Kdim}\,\mathbf{A}$ means $\forall \ell \geqslant -1$ $(\mathsf{Kdim}\,\mathbf{A} \leqslant \ell \;\Rightarrow \mathsf{Kdim}\,\mathbf{B} \leqslant \ell)$.

– $\mathsf{Kdim}\,\mathbf{B} = \mathsf{Kdim}\,\mathbf{A}$ means $\mathsf{Kdim}\,\mathbf{B} \leqslant \mathsf{Kdim}\,\mathbf{A}$ and $\mathsf{Kdim}\,\mathbf{B} \geqslant \mathsf{Kdim}\,\mathbf{A}$.

– $\sup_{j\in J} \mathsf{Kdim}\,\mathbf{B}_j \leqslant \sup_{i\in I} \mathsf{Kdim}\,\mathbf{A}_i$ means
$$\forall \ell \geqslant -1 \quad \big(\&_{i\in I}\ \mathsf{Kdim}\,\mathbf{A}_i \leqslant \ell \;\Rightarrow\; \&_{j\in J}\ \mathsf{Kdim}\,\mathbf{B}_j \leqslant \ell\big).$$

– $\sup_{j\in J} \mathsf{Kdim}\,\mathbf{B}_j = \sup_{i\in I} \mathsf{Kdim}\,\mathbf{A}_i$ means
$$\forall \ell \geqslant -1 \quad \big(\&_{i\in I}\ \mathsf{Kdim}\,\mathbf{A}_i \leqslant \ell \;\Leftrightarrow\; \&_{j\in J}\ \mathsf{Kdim}\,\mathbf{B}_j \leqslant \ell\big).$$

Iterated boundaries, singular sequences, complementary sequences

Definition 2.3 can be rewritten in terms of algebraic identities. For this, we introduce the notion of a *singular sequence.*

2.6. Definition. For a sequence $(\underline{x}) = (x_0, \ldots, x_k)$ in $\mathbf{A}$ we define the iterated Krull boundaries as follows.

1. An "iterated" version of the monoid $\mathcal{S}^{\mathrm{K}}_{\mathbf{A}}(x)$: the set
$$\mathcal{S}^{\mathrm{K}}_{\mathbf{A}}(x_0, \ldots, x_k) := x_0^{\mathbb{N}}(x_1^{\mathbb{N}} \cdots (x_k^{\mathbb{N}}(1 + x_k\mathbf{A}) + \cdots) + x_1\mathbf{A}) + x_0\mathbf{A}) \quad (3)$$
is a monoid. For an empty sequence, we define $\mathcal{S}^{\mathrm{K}}_{\mathbf{A}}() = \{1\}$.

2. We define two variants for the iterated Krull boundary ideal.

— 2a) The ideal $\mathcal{J}^{\mathrm{K}}_{\mathbf{A}}(x_0, \ldots, x_k) = \mathcal{J}^{\mathrm{K}}_{\mathbf{A}}(\underline{x})$ is defined as follows
$$\mathcal{J}^{\mathrm{K}}_{\mathbf{A}}() = \{0\}\,,\ \mathcal{J}^{\mathrm{K}}_{\mathbf{A}}(x_0, \ldots, x_k) = \big(\mathrm{D}_{\mathbf{A}}\big(\mathcal{J}^{\mathrm{K}}_{\mathbf{A}}(x_0, \ldots, x_{k-1})\big) : x_k\big) + \mathbf{A}x_k. \quad (4)$$

— 2b) The ideal $\mathcal{I}^{\mathrm{K}}_{\mathbf{A}}(x_0, \ldots, x_k) = \mathcal{I}^{\mathrm{K}}_{\mathbf{A}}(\underline{x})$ is defined as follows
$$\mathcal{I}^{\mathrm{K}}_{\mathbf{A}}(\underline{x}) := \big\{\, y \in \mathbf{A} \mid 0 \in x_0^{\mathbb{N}}\big(\cdots \big(x_k^{\mathbb{N}}(y + x_k\mathbf{A}) + \cdots\big) + x_0\mathbf{A}\big)\,\big\} \qquad (5)$$

For an empty sequence, we define $\mathcal{I}^{\mathrm{K}}_{\mathbf{A}}() = \{0\}$.

We will show (Lemma 2.13) that the two "iterated boundary" ideals defined above have the same nilradical.

2.7. Definition. A sequence $(x_0, \ldots, x_k)$ in $\mathbf{A}$ is said to be *singular* if $0 \in \mathcal{S}^{\mathrm{K}}_{\mathbf{A}}(x_0, \ldots, x_k)$, in other words if $1 \in \mathcal{I}^{\mathrm{K}}_{\mathbf{A}}(x_0, \ldots, x_k)$, i.e. if there exist a_0, …, $a_k \in \mathbf{A}$ and m_0, …, $m_k \in \mathbb{N}$ such that
$$x_0^{m_0}(x_1^{m_1}(\cdots(x_k^{m_k}(1 + a_kx_k) + \cdots) + a_1x_1) + a_0x_0) = 0 \qquad (6)$$

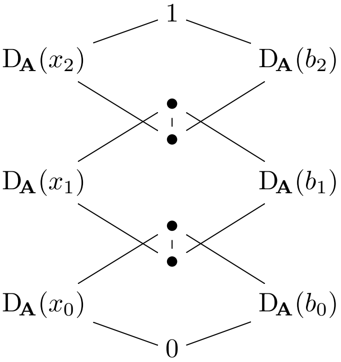
2.8. Proposition. *For a commutative ring $\mathbf{A}$ and an integer $k \geqslant 0$, the following properties are equivalent.*

1. *The Krull dimension of $\mathbf{A}$ is $\leqslant k$.*
2. *For all $x \in \mathbf{A}$ the Krull dimension of $\mathbf{A}^x_{\mathrm{K}}$ is $\leqslant k-1$.*
3. *Every sequence $(x_0, \dots, x_k)$ in $\mathbf{A}$ is singular.*
4. *For all $x_0, \dots, x_k \in \mathbf{A}$ there exist $b_0, \dots, b_k \in \mathbf{A}$ such that*

$$\left.\begin{array}{rcl} \mathrm{D}_{\mathbf{A}}(b_0x_0) & = & \mathrm{D}_{\mathbf{A}}(0), \\ \mathrm{D}_{\mathbf{A}}(b_1x_1) & \leqslant & \mathrm{D}_{\mathbf{A}}(b_0, x_0), \\ \vdots & \vdots & \vdots \\ \mathrm{D}_{\mathbf{A}}(b_kx_k) & \leqslant & \mathrm{D}_{\mathbf{A}}(b_{k-1}, x_{k-1}), \\ \mathrm{D}_{\mathbf{A}}(1) & = & \mathrm{D}_{\mathbf{A}}(b_k, x_k). \end{array}\right\} \tag{7}$$

5. *For all $x_0, \dots, x_k \in \mathbf{A}$, by letting $\pi_i = \prod_{j<i} x_j$ for $i \in \llbracket 0..k+1 \rrbracket$ (so $\pi_0 = 1$), there exists an $n \in \mathbb{N}$ such that* $\pi_{k+1}^n \in \left\langle \pi_k^n x_k^{n+1},\ \pi_{k-1}^n x_{k-1}^{n+1},\ \dots,\ \pi_1^n x_1^{n+1},\ \pi_0^n x_0^{n+1} \right\rangle.$

For example, for $k = 2$ item *4* corresponds to the following graph in $\mathsf{Zar}\,\mathbf{A}$.


1
$\mathrm{D}_{\mathbf{A}}(x_2)$
$\mathrm{D}_{\mathbf{A}}(b_2)$
$\mathrm{D}_{\mathbf{A}}(x_1)$
$\mathrm{D}_{\mathbf{A}}(b_1)$
$\mathrm{D}_{\mathbf{A}}(x_0)$
$\mathrm{D}_{\mathbf{A}}(b_0)$
0

D The equivalences for dimension 0 are immediate by application of the definitions.

1 ⇔ 3. Suppose the equivalence established for dimension at most k and for every commutative ring. We then see that $S^{-1}\mathbf{A}$ is of dimension at most k if and only if we have

for all $x_0, \dots, x_k \in \mathbf{A}$ there exist $a_0, \dots, a_k \in \mathbf{A}$, $s \in S$ and $m_0, \dots, m_k \in \mathbb{N}$ such that

$$x_0^{m_0}(x_1^{m_1} \cdots (x_k^{m_k}(s + a_kx_k) + \cdots + a_1x_1) + a_0x_0) = 0. \tag{8}$$

Note that with respect to Equation (6), some $s \in S$ has replaced the 1 in the center of the expression on the left-hand side.

It therefore remains to replace s by an arbitrary element of $\mathcal{S}^{\mathrm{K}}_{\mathbf{A}}(x_{k+1})$, i.e.

an element of the form $x_{k+1}^{m_{k+1}}(1 + a_{k+1}x_{k+1})$.
The equivalence between *2* and *3* is proven analogously.

3 ⇒ *4*. We take $b_k = 1 + a_k x_k$, then $b_{\ell-1} = x_\ell^{m_\ell} b_\ell + a_{\ell-1}x_{\ell-1}$, successively for $\ell = k, \ldots, 1$.

4 ⇒ *2*. Proof by induction. The implication for dimension $\leqslant 0$ is clear. Suppose it established for dimension $< k$. Assume property *4* and let us show that for all x_0 the dimension of $\mathbf{B} = \mathbf{A}_{\mathrm{K}}^{x_0}$ is $< k$.
By induction hypothesis it suffices to find, for all $x_1, \ldots, x_k$, some elements $b_1, \ldots, b_k$ such that

$$\left.\begin{array}{rcl} \mathrm{D}_{\mathbf{B}}(b_1x_1) & = & \mathrm{D}_{\mathbf{B}}(0) \\ \vdots & \vdots & \vdots \\ \mathrm{D}_{\mathbf{B}}(b_kx_k) & \leqslant & \mathrm{D}_{\mathbf{B}}(b_{k-1}, x_{k-1}) \\ \mathrm{D}_{\mathbf{B}}(1) & = & \mathrm{D}_{\mathbf{B}}(b_k, x_k). \end{array}\right\}$$

However, by hypothesis we have some elements $b_0, \ldots, b_k$ such that

$$\left.\begin{array}{rcl} \mathrm{D}_{\mathbf{A}}(b_0x_0) & = & \mathrm{D}_{\mathbf{A}}(0) \\ \mathrm{D}_{\mathbf{A}}(b_1x_1) & \leqslant & \mathrm{D}_{\mathbf{A}}(b_0, x_0) \\ \vdots & \vdots & \vdots \\ \mathrm{D}_{\mathbf{A}}(b_kx_k) & \leqslant & \mathrm{D}_{\mathbf{A}}(b_{k-1}, x_{k-1}) \\ \mathrm{D}_{\mathbf{A}}(1) & = & \mathrm{D}_{\mathbf{A}}(b_k, x_k). \end{array}\right\}$$

and the inequalities with $\mathrm{D}_{\mathbf{A}}$ imply the same inequalities with $\mathrm{D}_{\mathbf{B}}$. The second inequality means that $(b_1x_1)^m \in \langle b_0, x_0\rangle$ (for a certain m); the first tells us that b_0x_0 is nilpotent therefore $\langle b_0, x_0\rangle \subseteq \mathcal{J}_{\mathbf{A}}^{\mathrm{K}}(x_0)$. Recap: b_1x_1 is nilpotent in $\mathbf{B}$.
We could also prove *4* ⇒ *3* by a direct, slightly more tedious, computation.

3 ⇔ *5*. In the definition of a singular sequence, we can replace all the exponents m_i by their maximum n. Once this is acquired, item *5* is a simple reformulation of item *3*. □

We could therefore have given a definition by induction of the Krull dimension based on the upper boundaries $\mathbf{A}_{\mathrm{K}}^{x}$ rather than on the lower boundaries $\mathbf{A}_{x}^{\mathrm{K}}$: we have just obtained a direct constructive proof (without using Theorem* 2.2) of the equivalence between the two possible inductive definitions.

Remark. The system of inequalities (7) in item *4* of Proposition 2.8 establishes an interesting and symmetric relation between the two sequences $(b_0, \ldots, b_k)$ and $(x_0, \ldots, x_k)$.
When $k = 0$, this means $\mathrm{D}_{\mathbf{A}}(b_0) \wedge \mathrm{D}_{\mathbf{A}}(x_0) = 0$ and $\mathrm{D}_{\mathbf{A}}(b_0) \vee \mathrm{D}_{\mathbf{A}}(x_0) = 1$, that is that the two elements $\mathrm{D}_{\mathbf{A}}(b_0)$ and $\mathrm{D}_{\mathbf{A}}(x_0)$ are complements of one another in the lattice $\mathsf{Zar}\,\mathbf{A}$. In $\mathsf{Spec}\,\mathbf{A}$ this means that the corresponding

basic open sets are complementary.
We therefore introduce the following terminology: when the sequences $(b_0, \dots, b_k)$ and $(x_0, \dots, x_k)$ satisfy the inequalities (7) we say that they are two *complementary sequences.* ■

2.9. Fact. *Let $(\underline{x}) = (x_1, \dots, x_n)$ and $(\underline{y}) = (y_1, \dots, y_m)$ be two sequences of elements of $\mathbf{A}$, $\mathbf{A} \to \mathbf{A}'$ be a morphism and $(\underline{x'})$ be the image of $(\underline{x})$ in $\mathbf{A}'$.*

1. *We have the equivalences*
$$\exists z \in \mathcal{I}^{\mathrm{K}}_{\mathbf{A}}(\underline{x}) \cap \mathcal{S}^{\mathrm{K}}_{\mathbf{A}}(\underline{y}) \iff 1 \in \mathcal{I}^{\mathrm{K}}_{\mathbf{A}}(\underline{x}, \underline{y}) \iff 0 \in \mathcal{S}^{\mathrm{K}}_{\mathbf{A}}(\underline{x}, \underline{y}).$$
2. *If $\mathbf{A} \to \mathbf{A}'$ is surjective, the image of $\mathcal{S}^{\mathrm{K}}_{\mathbf{A}}(\underline{x})$ is $\mathcal{S}^{\mathrm{K}}_{\mathbf{A}'}(\underline{x'})$.*
3. *If $\mathbf{A}' = S^{-1}\mathbf{A}$, with S being a monoid of $\mathbf{A}$, then $S^{-1}\mathcal{I}^{\mathrm{K}}_{\mathbf{A}}(\underline{x}) = \mathcal{I}^{\mathrm{K}}_{\mathbf{A}'}(\underline{x'})$.*

2.10. Fact. *Let $\mathfrak{a}$ be an ideal of $\mathbf{A}$, $Z \subseteq \mathbf{A}$ be an arbitrary subset and $x \in \mathbf{A}$.*
$$x^{\mathbb{N}}(Z + \mathbf{A}x) \text{ meets } \mathfrak{a} \iff Z \text{ meets } (\mathfrak{a} : x^{\infty}) + \mathbf{A}x.$$

2.11. Lemma. (Krull boundary ideals à la Richman)
For a sequence $(\underline{x}) = (x_1, \dots, x_n)$ of elements of $\mathbf{A}$, the iterated boundary ideal $\mathcal{I}^{\mathrm{K}}_{\mathbf{A}}(\underline{x})$ can be defined recursively as follows
$$\mathcal{I}^{\mathrm{K}}_{\mathbf{A}}() = \{0\}\,, \qquad \mathcal{I}^{\mathrm{K}}_{\mathbf{A}}(x_1, \dots, x_n) = \big(\mathcal{I}^{\mathrm{K}}_{\mathbf{A}}(x_1, \dots, x_{n-1}) : x_n^{\infty}\big) + \mathbf{A}x_n.$$
For example,
$$\mathcal{I}^{\mathrm{K}}_{\mathbf{A}}(x_1) = (0 : x_1^{\infty}) + \mathbf{A}x_1,\ \mathcal{I}^{\mathrm{K}}_{\mathbf{A}}(x_1, x_2) = \big(\big((0 : x_1^{\infty}) + \mathbf{A}x_1\big) : x_2^{\infty}\big) + \mathbf{A}x_2.$$

D We temporarily define
$$N() = \{0\}, \quad N(x_1, \dots, x_n) = \big(N(x_1, \dots, x_{n-1}) : x_n^{\infty}\big) + \mathbf{A}x_n$$
Take $n = 3$ to fix the ideas. Then, for $y \in \mathbf{A}$, we have the equivalences
$$\begin{array}{ll}
0 \in x_1^{\mathbb{N}}\big(x_2^{\mathbb{N}}\big(x_3^{\mathbb{N}}(y + \mathbf{A}x_3) + \mathbf{A}x_2\big) + \mathbf{A}x_1\big) & \iff \\
x_2^{\mathbb{N}}\big(x_3^{\mathbb{N}}(y + \mathbf{A}x_3) + \mathbf{A}x_2\big) \text{ meets } N(x_1) & \iff \\
x_3^{\mathbb{N}}(y + \mathbf{A}x_3) \text{ meets } \big(N(x_1) : x_2^{\infty}\big) + \mathbf{A}x_2 \overset{\mathrm{def}}{=} N(x_1, x_2) & \iff \\
y \in \big(N(x_1, x_2) : x_3^{\infty}\big) + \mathbf{A}x_3 \overset{\mathrm{def}}{=} N(x_1, x_2, x_3), &
\end{array}$$
which proves that $\mathcal{I}^{\mathrm{K}}_{\mathbf{A}}(x_1, x_2, x_3) = N(x_1, x_2, x_3)$. □

2.12. Lemma. Iterating boundary ideals
Let $(\underline{x}) = (x_1, \dots, x_n)$ and $(\underline{y}) = (y_1, \dots, y_m)$ be two sequences of elements of $\mathbf{A}$. Let $\mathbf{A}' = \mathbf{A}/\mathcal{I}^{\mathrm{K}}_{\mathbf{A}}(\underline{x})$ and let $(\underline{y'}) = (y'_1, \dots, y'_m)$ be the image of $(\underline{y})$ in $\mathbf{A}'$.

1. *The kernel of the (surjective) canonical morphism $\mathbf{A} \to \mathbf{A}'/\mathcal{I}^{\mathrm{K}}_{\mathbf{A}'}(\underline{y'})$ is the ideal $\mathcal{I}^{\mathrm{K}}_{\mathbf{A}}(\underline{x}, \underline{y})$.*

2. *We define* $\mathbf{A}_0 = \mathbf{A}$ *and* $\mathbf{A}_i = \mathbf{A}_{i-1}/\mathcal{I}^{\mathrm{K}}_{\mathbf{A}_{i-1}}(x_i)$ *for* $i \in [\![1..n]\!]$*. Then the kernel of the (surjective) canonical morphism* $\mathbf{A} \to \mathbf{A}_n$ *is the ideal* $\mathcal{I}^{\mathrm{K}}_{\mathbf{A}}(\underline{x})$*.*

D It suffices to prove the first item for $n = 1$. Let $x = x_1$.
Let $z \in \mathbf{A}$ and z' be its image in $\mathbf{A}' = \mathbf{A}/\mathcal{I}^{\mathrm{K}}_{\mathbf{A}}(x)$. We have the equivalences

$$\begin{array}{ll}
z = 0 \text{ in } \mathbf{A}'/\mathcal{I}^{\mathrm{K}}_{\mathbf{A}'}(\underline{y'}) & \iff \\
0 \in {y'_1}^{\mathbb{N}}\big(\cdots\big({y'_m}^{\mathbb{N}}(z' + y'_m\mathbf{A}') + \cdots\big) + y'_1\mathbf{A}'\big) & \iff \\
{y_1}^{\mathbb{N}}\big(\cdots\big({y_m}^{\mathbb{N}}(z + y_m\mathbf{A}) + \cdots\big) + y_1\mathbf{A}\big) \text{ rencontre } \mathcal{I}^{\mathrm{K}}_{\mathbf{A}}(x) & \iff \\
0 \in x^{\mathbb{N}}({y_1}^{\mathbb{N}}\big(\cdots\big({y_m}^{\mathbb{N}}(z + y_m\mathbf{A}) + \cdots\big) + y_1\mathbf{A}) + x\mathbf{A}\big) & \iff \\
z \in \mathcal{I}^{\mathrm{K}}_{\mathbf{A}}(x, \underline{y}). & \square
\end{array}$$

2.13. Fact. *For every sequence* $(\underline{x})$ *of elements of* $\mathbf{A}$*, the ideals* $\mathcal{I}^{\mathrm{K}}_{\mathbf{A}}(\underline{x})$ *and* $\mathcal{J}^{\mathrm{K}}_{\mathbf{A}}(\underline{x})$ *have the same nilradical.*

D For every ideal $\mathfrak{a}$ and all $x \in \mathbf{A}$, we easily prove that the nilradical of the ideal $(\mathfrak{a} : x^{\infty})$ is $(\mathrm{D}_{\mathbf{A}}(\mathfrak{a}) : x)$. By using $\mathrm{D}_{\mathbf{A}}(\mathfrak{b} + \mathfrak{c}) = \mathrm{D}_{\mathbf{A}}(\mathrm{D}_{\mathbf{A}}(\mathfrak{b}) + \mathfrak{c})$, we deduce that the ideals $(\mathfrak{a} : x^{\infty}) + \mathbf{A}x$ and $(\mathrm{D}_{\mathbf{A}}(\mathfrak{a}) : x) + \mathbf{A}x$ have the same nilradical. The stated result is then deduced by induction on the length of the sequence $(\underline{x})$ by using the recursive definition of the two iterated boundary ideals. □

2.14. Lemma. *Let* S *be a monoid of* $\mathbf{A}$*,* $\mathbf{A}' = S^{-1}\mathbf{A}$*,* $x \in \mathbf{A}$*,* x' *be its image in* $\mathbf{A}'$ *and* $V = \mathcal{S}^{\mathrm{K}}_{\mathbf{A}'}(x')$*. Then the canonical morphism* $\mathbf{A} \to V^{-1}\mathbf{A}'$ *is a localization morphism*[1] *and induces an isomorphism of* $T^{-1}\mathbf{A}$ *over* $V^{-1}\mathbf{A}'$*, where* T *is the monoid* $x^{\mathbb{N}}(S + \mathbf{A}x)$*.*

D The image in $V^{-1}\mathbf{A}'$ of the element $s + ax \in S + \mathbf{A}x$ is invertible since we can write $s + ax = s(1 + ax/s)$ (with a few notation abuses). Hence a (canonical) morphism $\varphi : T^{-1}\mathbf{A} \to V^{-1}\mathbf{A}'$.
Moreover, since $S \subseteq T$, we have a morphism $\mathbf{A}' \to T^{-1}\mathbf{A}$. The image under this morphism of $1 + xa/s \in 1 + x\mathbf{A}'$ is invertible because $1 + xa/s = (s + xa)/s$, hence a morphism $\varphi' : V^{-1}\mathbf{A}' \to T^{-1}\mathbf{A}$.
We prove without difficulty that φ and φ' are inverses of one another. □

2.15. Corollary. Iterating boundary monoids
Let $(\underline{x}) = (x_1, \ldots, x_n)$ *and* $(\underline{y}) = (y_1, \ldots, y_m)$ *in* $\mathbf{A}$*,* $\mathbf{A}' = \mathcal{S}^{\mathrm{K}}_{\mathbf{A}}(\underline{y})^{-1}\mathbf{A}$*, and* $(\underline{x'}) = (x'_1, \ldots, x'_n)$ *be the image of* $(\underline{x})$ *in* $\mathbf{A}'$*.*
Then, the morphism $\mathbf{A} \to \mathcal{S}^{\mathrm{K}}_{\mathbf{A}'}(\underline{x'})^{-1}\mathbf{A}'$ *gives by factorization an isomorphism* $\mathcal{S}^{\mathrm{K}}_{\mathbf{A}}(\underline{x}, \underline{y})^{-1}\mathbf{A} \xrightarrow{\sim} \mathcal{S}^{\mathrm{K}}_{\mathbf{A}'}(\underline{x'})^{-1}\mathbf{A}'$*.*

[1] See Definition XV-4.5.

A regular sequence “is not” singular

Item *4* of the following proposition implies that a regular sequence that does not generate the ideal $\langle 1\rangle$ is nonsingular, which explains the title of this subsection.

An advantage of the iterated Krull boundaries à la Richman is that over a coherent Noetherian ring they are finitely generated ideals. Another advantage is given by item *1* in the following proposition.

2.16. Proposition. (Regular sequences and Krull dimension)
Let $(x_1,\dots,x_n)$ be a regular sequence in $\mathbf{A}$ and $(y_1,\dots,y_r)$ be another sequence.

1. *We have $\mathcal{I}^{\mathrm{K}}_{\mathbf{A}}(x_1,\dots,x_n)=\langle x_1,\dots,x_n\rangle$.*
2. *The sequence $(x_1,\dots,x_n,y_1,\dots,y_r)$ is singular in $\mathbf{A}$ if and only if the sequence $(y_1,\dots,y_r)$ is singular in $\mathbf{A}/\langle x_1,\dots,x_n\rangle$.*
3. *The following implication is satisfied for every $k\geqslant -1$,*
$$\mathsf{Kdim}\,\mathbf{A}\leqslant n+k \implies \mathsf{Kdim}\,\mathbf{A}/\langle x_1,\dots,x_n\rangle\leqslant k.$$
If $1\notin\langle x_1,\dots,x_n\rangle$, we have $n+\mathsf{Kdim}\,\mathbf{A}/\langle x_1,\dots,x_n\rangle\leqslant\mathsf{Kdim}\,\mathbf{A}$.
4. *If the sequence $(x_1,\dots,x_n)$ is also singular, we have $\langle x_1,\dots,x_n\rangle=\langle 1\rangle$. Consequently if $\mathsf{Kdim}\,\mathbf{A}\leqslant n-1$ every regular sequence of length n generates the ideal $\langle 1\rangle$.*

D *1.* Immediate computation taking into account the recursive definition given in Lemma 2.12 (item *2*).
2. We apply item *1* of Lemma 2.12.
3. Results from item *2*.
4. Special case of item *2*, with the empty sequence $(y_1,\dots,y_r)$. □

Lower bounds of the Krull dimension

It can be comfortable, sometimes even useful, to define the statement “$\mathbf{A}$ is of Krull dimension $\geqslant k$.”

First of all $\mathsf{Kdim}\,\mathbf{A}\geqslant 0$ must mean $1\neq 0$. For $k\geqslant 1$, a possibility would be to ask: “there exists a sequence $(x_1,\dots,x_k)$ which is not singular.” Note that from the constructive point of view this affirmation is stronger than the negation of “every sequence $(x_1,\dots,x_k)$ is singular.”

A ring then has a well-defined Krull dimension if there exists an integer k such that the ring is both of Krull dimension $\geqslant k$ and of Krull dimension $\leqslant k$.

The annoying thing is the negative character of the assertion

“the sequence $(x_1,\dots,x_k)$ is not singular.”

Anyway here it seems impossible to avoid the use of the negation, because we do not see how we could define $\mathsf{Kdim}\,\mathbf{A}\geqslant 0$ other than by the negation $1\neq 0$. Naturally, in the case where $\mathbf{A}$ is a discrete set, “$x\neq 0$” loses its negative character, and the statement "there exists a sequence $(\underline{x}) = (x_1, \ldots, x_k)$ such that $0 \notin \mathcal{I}^{\mathrm{K}}_{\mathbf{A}}(\underline{x})$" does not strictly speaking contain any negation.

However, note that the definitions of $\mathsf{Kdim}\,\mathbf{A} \leqslant k$ and $\mathsf{Kdim}\,\mathbf{A} \geqslant k$ use an alternation of quantifiers that introduces an infinity (for an infinite ring). Consequently the definition cannot generally be certified by a simple computation: a proof is needed.

Note that for the ring $\mathbb{R}$, if we use the strong negation (of positive character), for which $x \neq 0$ means "x is invertible," to define the sentence $\mathsf{Kdim}\,\mathbb{R} \geqslant k$, then it is absurd that $\mathsf{Kdim}\,\mathbb{R} \geqslant 1$. But we cannot constructively prove $\mathsf{Kdim}\,\mathbb{R} \leqslant 0$ (see the comment on page 764).

3. A few elementary properties of the Krull dimension

The stated facts in the following proposition are easy (note that we use the notation introduced in 2.5).

3.1. Proposition. *Let $\mathbf{A}$ be a ring, $\mathfrak{a}$ be an ideal and S be a monoid.*

1. *A singular sequence remains singular in $\mathbf{A}/\mathfrak{a}$ and $\mathbf{A}_S$.*
2. $\mathsf{Kdim}\,\mathbf{A}/\mathfrak{a} \leqslant \mathsf{Kdim}\,\mathbf{A}$, $\mathsf{Kdim}\,\mathbf{A}_S \leqslant \mathsf{Kdim}\,\mathbf{A}$.
3. $\mathsf{Kdim}(\mathbf{A} \times \mathbf{B}) = \sup(\mathsf{Kdim}\,\mathbf{A}, \mathsf{Kdim}\,\mathbf{B})$.
4. $\mathsf{Kdim}\,\mathbf{A} = \mathsf{Kdim}\,\mathbf{A}_{\mathrm{red}}$.
5. *If a is regular in $\mathbf{A}_{\mathrm{red}}$ (a fortiori if it is regular in $\mathbf{A}$), then* $\mathsf{Kdim}\,\mathbf{A}/a\mathbf{A} \leqslant \sup(\mathsf{Kdim}\,\mathbf{A}, 0) - 1$.
6. *If $a \in \operatorname{Rad}\mathbf{A}$, then* $\mathsf{Kdim}\,\mathbf{A}[1/a] \leqslant \sup(\mathsf{Kdim}\,\mathbf{A}, 0) - 1$.

Example. We give a ring $\mathbf{B}$ for which $\operatorname{Frac}(\mathbf{B})$ is of Krull dimension $n > 0$, but $\mathbf{B}_{\mathrm{red}} = \operatorname{Frac}(\mathbf{B}_{\mathrm{red}})$ is zero-dimensional.

Consider $\mathbf{B} = \mathbf{A}/x\mathfrak{m}$, where $\mathbf{A}$ is local residually discrete, $\mathfrak{m} = \operatorname{Rad}\mathbf{A}$ and $x \in \mathfrak{m}$. The ring $\mathbf{B}$ is local, $\operatorname{Rad}\mathbf{B} = \mathfrak{m}' = \mathfrak{m}/x\mathfrak{m}$ and $\mathbf{B}/\mathfrak{m}' = \mathbf{A}/\mathfrak{m}$. If $\overline{x} = 0$, then $x \in x\mathfrak{m}$, i.e. $x(1-m) = 0$ with $m \in \mathfrak{m}$, which implies $x = 0$. For $y \in \mathfrak{m}$ we have $\overline{y}\,\overline{x} = 0$. Therefore if $\overline{y} \in \operatorname{Reg}\mathbf{B} \cap \mathfrak{m}'$, we obtain $x = 0$. However, we have $\overline{y} \in \mathfrak{m}'$ or $\overline{y} \in \mathbf{B}^\times$, therefore if $x \neq 0$ and $\overline{y} \in \operatorname{Reg}\mathbf{B}$, we obtain $\overline{y} \in \mathbf{B}^\times$. In other words, if $x \neq 0$, $\mathbf{B} = \operatorname{Frac}(\mathbf{B})$.

Take $\mathbf{A} = \mathbf{k}[x_0, \ldots, x_n]_{\langle x_0, \ldots, x_n \rangle}$ where $\mathbf{k}$ is a nontrivial discrete field, and $x = x_0$. We then have

$$\mathbf{A}/\langle x_0 \rangle \simeq \mathbf{k}[x_1, \ldots, x_n]_{\langle x_1, \ldots, x_n \rangle} \text{ and } \mathsf{Kdim}\,\mathbf{A}/\langle x_0 \rangle = n.$$

As $\overline{x_0}^2 = 0$ in $\mathbf{B}$, we have $\mathbf{B}_{\mathrm{red}} \simeq \mathbf{A}/\langle x_0 \rangle$ and therefore $\mathsf{Kdim}\,\mathbf{B} = n$.

Finally, $\operatorname{Frac}(\mathbf{B}_{\mathrm{red}}) = \mathbf{k}(x_1, \ldots, x_n)$ is a zero-dimensional discrete field.

Geometrically, we have considered the ring of a variety "with multiplicities" consisting at a point immersed in a hyperplane of dimension n, and we have

localized at this immersed point.
Note: in classical mathematics, if $\mathbf{C}$ is Noetherian and reduced, $\mathrm{Frac}(\mathbf{C})$ is a finite product of fields, therefore zero-dimensional. For a constructive version we refer to Problem 1 and to [51, Coquand&al.]. ■

3.2. Concrete local-global principle. (For the Krull dimension)
Let S_1, …, S_n be comaximal monoids of a ring $\mathbf{A}$ and $k \in \mathbb{N}$.

1. *A sequence is singular in $\mathbf{A}$ if and only if it is singular in each of the $\mathbf{A}_{S_i}$'s.*
2. *The ring $\mathbf{A}$ is of dimension at most k if and only if the $\mathbf{A}_{S_i}$'s are of dimension at most k.*

We could have written $\mathsf{Kdim}\,\mathbf{A} = \sup_i \mathsf{Kdim}\,\mathbf{A}_{S_i} = \mathsf{Kdim} \prod_i \mathbf{A}_{S_i}$.

D It suffices to prove the first item. Consider a sequence $(x_0, \dots, x_k)$ in $\mathbf{A}$. We look for a_0, …, $a_k \in \mathbf{A}$, and m_0, …, $m_k \in \mathbb{N}$ such that

$$x_0^{m_0}\big(x_1^{m_1}\cdots\big(x_k^{m_k}(1 + a_k x_k) + \cdots + a_1 x_1\big) + a_0 x_0\big) = 0.$$

An equation of this type at the a_j's can be solved in each of the $\mathbf{A}_{S_i}$'s. We notice that if in a ring $\mathbf{A}_{S_i}$ we have a solution for certain exponents m_0, …, m_k then we also have a solution for any system of larger exponents. Therefore by taking a system of exponents that bound from above each of those obtained separately for each $\mathbf{A}_{S_i}$, we obtain a unique linear equation in the a_j's which has a solution in each $\mathbf{A}_{S_i}$. We can therefore apply the basic local-global principle II-2.3. □

As the property for a sequence to be singular is of finite character, item *1* in the previous concrete local-global principle actually always applies with a family of comaximal elements, which corresponds to a finite covering of the Zariski spectrum by basic open sets.

In the case of a finite covering by closed sets, the result still holds.

3.3. Closed covering principle. (Krull dimension)
Let $\mathbf{A}$ be a ring, k be an integer $\geqslant 0$, and $\mathfrak{a}_1$, …, $\mathfrak{a}_r$ be ideals of $\mathbf{A}$.
First we assume that the $\mathfrak{a}_i$'s form a closed covering of $\mathbf{A}$.

1. *A sequence $(x_0, \dots, x_k)$ is singular in $\mathbf{A}$ if and only if it is singular in each of the $\mathbf{A}/\mathfrak{a}_i$'s.*
2. *The ring $\mathbf{A}$ is of dimension at most k if and only if each of the $\mathbf{A}/\mathfrak{a}_i$'s is of dimension at most k.*

More generally, without a hypothesis on the $\mathfrak{a}_i$'s we have

3. *The ring $\mathbf{A}/\bigcap_i \mathfrak{a}_i$ is of dimension at most k if and only if each of the $\mathbf{A}/\mathfrak{a}_i$'s is of dimension at most k.*
   This can be abbreviated to
   $$\mathsf{Kdim}\,\mathbf{A}/\textstyle\prod_i \mathfrak{a}_i = \mathsf{Kdim}\,\mathbf{A}/\bigcap_i \mathfrak{a}_i = \sup_i \mathsf{Kdim}\,\mathbf{A}/\mathfrak{a}_i = \mathsf{Kdim} \prod_i \mathbf{A}/\mathfrak{a}_i\ .$$

D It suffices to prove item *1.* The sequence $(x_0, \ldots, x_k)$ is singular if and only if the monoid $\mathcal{S}^{\mathrm{K}}(x_0, \ldots, x_k)$ contains 0.
In addition, $\mathcal{S}^{\mathrm{K}}_{\mathbf{A}/\mathfrak{a}_i}(x_0, \ldots, x_k)$ is none other than $\mathcal{S}^{\mathrm{K}}_{\mathbf{A}}(x_0, \ldots, x_k)$ considered modulo $\mathfrak{a}_i$. The result follows by the closed covering principle XI-4.18. □

3.4. Theorem. (One and a half theorem)

1. *a. If* $\mathbf{A}$ *is zero-dimensional, or more generally if* $\mathbf{A}$ *is local-global, every locally cyclic module is cyclic.*

   b. If $\mathbf{A}$ *is zero-dimensional, every finitely generated projective ideal is generated by an idempotent.*
2. *Let* $\mathbf{A}$ *be of dimension at most* k*, let* $(x_1, \ldots, x_k)$ *be a regular sequence and* $\mathfrak{b}$ *be a locally principal ideal containing* $\mathfrak{a} = \langle x_1, \ldots, x_k \rangle$*. Then there exists a* $y \in \mathfrak{b}$ *such that*
$$\mathfrak{b} = \langle y, x_1, \ldots, x_k \rangle = \langle y \rangle + \mathfrak{b}\mathfrak{a} = \langle y \rangle + \mathfrak{a}^m$$
for any exponent $m \geqslant 1$.
3. *Let* $\mathbf{A}$ *be such that* $\mathbf{A}/\mathrm{Rad}\,\mathbf{A}$ *is of dimension at most* k*, let* $(x_1, \ldots, x_k)$ *be a regular sequence in* $\mathbf{A}/\mathrm{Rad}\,\mathbf{A}$ *and* $\mathfrak{b}$ *be a finitely generated projective ideal of* $\mathbf{A}$ *containing* $\mathfrak{a} = \langle x_1, \ldots, x_k \rangle$ *then there exists a* $y \in \mathfrak{b}$ *such that*
$$\mathfrak{b} = \langle y, x_1, \ldots, x_k \rangle = \langle y \rangle + \mathfrak{b}\mathfrak{a} = \langle y \rangle + \mathfrak{a}^m$$
for any exponent $m \geqslant 1$.

D Item *1a* is a reminder (see item *4* of Theorem V-3.1 for the zero-dimensional rings and item *2* of Theorem IX-6.10 for the local-global rings).
1b. Recall that in an arbitrary ring a finitely generated projective ideal $\mathfrak{a}$ has as its annihilator an idempotent h. In $\mathbf{A}/\langle h \rangle$, $\mathfrak{a}$ is faithful, therefore so is $\mathfrak{a}^k$, for all $k \geqslant 1$. In $\mathbf{A}[1/h]$, $\mathfrak{a} = 0$. Therefore $\mathrm{Ann}(\mathfrak{a}^k) = \mathrm{Ann}(\mathfrak{a}) = \langle h \rangle$ for $k \geqslant 1$.
In the zero-dimensional case, since a finitely generated projective ideal is locally principal, it is principal by item *1a*, let us denote it by $\langle x \rangle$. We know that for large enough k, $\langle x \rangle^k = \langle e \rangle$ with e idempotent. By the preliminary remark $\mathrm{Ann}(x) = \mathrm{Ann}(e) = \langle 1 - e \rangle$. In $\mathbf{A}/\langle 1 - e \rangle$, x is invertible, so $\langle x \rangle = \langle 1 \rangle$; in $\mathbf{A}/\langle e \rangle$, x is null; thus in $\mathbf{A}$, $\langle x \rangle = \langle e \rangle$.
3. Results from *2* by Nakayama's lemma.
2. The ideal $\mathfrak{b}$ seen as an $\mathbf{A}$-module, after scalar extension to $\mathbf{A}/\mathfrak{a}$, becomes the module $\mathfrak{b}/\mathfrak{b}\mathfrak{a}$ and it remains locally cyclic. Since the quotient ring $\mathbf{A}/\mathfrak{a}$ is zero-dimensional, item *1a* tells us that $\mathfrak{b}/\mathfrak{b}\mathfrak{a}$ is generated by an element y. This means that $\mathfrak{b} = \langle y \rangle + \mathfrak{b}\mathfrak{a}$ and the other equalities immediately follow.□

Remark. In the case of dimension 1 and of an invertible ideal, item *2* of the previous theorem is often called the "One and a half theorem." See Corollary V-3.2 and Theorem XII-5.2. ■

4. Integral extensions

4.1. Proposition. *Let* $\mathbf{A} \subseteq \mathbf{B}$ *be rings with* $\mathbf{B}$ *integral over* $\mathbf{A}$*. Every finite sequence of elements of* $\mathbf{A}$ *that is singular in* $\mathbf{B}$ *is singular in* $\mathbf{A}$*. In particular,* $\mathsf{Kdim}\,\mathbf{A} \leqslant \mathsf{Kdim}\,\mathbf{B}$*.*

Note: the opposite inequality is proven a little later (Theorem 7.16).

D Suppose for example that the sequence $(x, y) \in \mathbf{A}$ is singular in $\mathbf{B}$, i.e.

$$\exists a, b \in \mathbf{B},\ \exists m, \ell \in \mathbb{N},\ x^\ell\big(y^m(1 + ay) + bx\big) = 0.$$

We want to realize the same type of equality, with some elements a', b' of $\mathbf{A}$ instead of elements a, b in $\mathbf{B}$. The intuitive idea is to transform the previous equality by the "norm" operation. Consider some monic polynomials f, $g \in \mathbf{A}[T]$ that annihilate a and b. Let $\mathbf{B}_1 = \mathbf{A}[T, T']/\langle f(T), g(T')\rangle$. Let α and β be the classes of T and T' in $\mathbf{B}_1$. The subring $\mathbf{A}[a, b]$ of $\mathbf{B}$ is a quotient of $\mathbf{B}_1 = \mathbf{A}[\alpha, \beta]$, via an $\mathbf{A}$-homomorphism which sends α and β to a and b. In addition, $\mathbf{B}_1$ is a free module of finite rank over $\mathbf{A}$ which allows for a definition of the norm and the cotransposed element of an arbitrary element of $\mathbf{B}_1[X, Y]$. Then let

$$U(\alpha, \beta, X, Y) = X^\ell\big(Y^m(1 + \alpha Y) + \beta X\big) \text{ and}$$
$$V(X, Y) = \mathrm{N}_{\mathbf{B}_1[X,Y]/\mathbf{A}[X,Y]}(U).$$

By Lemma 4.2, $V(X, Y)$ is of the form

$$X^p\big(Y^q\big(1 + A(Y)Y\big) + B(X, Y)X\big),$$

with $A \in \mathbf{A}[Y]$, $B \in \mathbf{A}[X, Y]$. Moreover let $W(\alpha, \beta, X, Y) \in \mathbf{B}_1[X, Y]$ be the cotransposed element of $U(\alpha, \beta, X, Y)$. By specializing X, Y, α, β at x, y in $\mathbf{A}$ and a, b in $\mathbf{B}$, we obtain an equality in $\mathbf{B}$

$$V(x, y) = x^p\big(y^q\big(1 + A(y)y\big) + B(x, y)x\big) = U(a, b, x, y)W(a, b, x, y),$$

which ends the proof since $V(x, y) = 0$ is an equality in $\mathbf{A}$: note that we have $U(a, b, x, y) = 0$ in $\mathbf{B}$ but that $U(\alpha, \beta, x, y)$ is perhaps nonzero in $\mathbf{B}_1$.□

4.2. Lemma. *Let* $\mathbf{C}$ *be a free* $\mathbf{A}$*-algebra of finite rank over* $\mathbf{A}$*,* $(c_0, \dots, c_n)$ *in* $\mathbf{C}$ *and* $(X_0, \dots, X_n) = (\underline{X})$ *be a list of indeterminates. Let*

$$U(\underline{X}) = X_0^{k_0}\big(X_1^{k_1}\big(\cdots(X_n^{k_n}(1 + c_nX_n) + \cdots\big) + c_1X_1\big) + c_0X_0\big) \in \mathbf{C}[\underline{X}].$$

Then $V(\underline{X}) \overset{\text{def}}{=} \mathrm{N}_{\mathbf{C}[\underline{X}]/\mathbf{A}[\underline{X}]}\big(U(\underline{X})\big)$ *is of the form*

$$V(\underline{X}) = X_0^{\ell_0}\big(X_1^{\ell_1}\big(\cdots(X_n^{\ell_n}(1 + a_nX_n) + \cdots\big) + a_1X_1\big) + a_0X_0\big) \in \mathbf{A}[\underline{X}],$$

with $a_n \in \mathbf{A}[X_n]$*,* $a_{n-1} \in \mathbf{A}[X_n, X_{n-1}]$*,* $\dots$*,* $a_0 \in \mathbf{A}[\underline{X}]$*.*

D First of all the norm $\mathrm{N}(1 + c_nX_n)$ is a polynomial $h(X_n) \in \mathbf{A}[X_n]$ which satisfies $h(0) = 1$, therefore which can be expressed in the form $1 + a_n(X_n)X_n$. Next we use the multiplicativity of the norm, and an evaluation at $X_{n-1} = 0$ to show that $\mathrm{N}\big(X_n^{k_n}(1 + c_nX_n) + c_{n-1}X_{n-1}\big)$ is of the form

$$X_n^{\ell_n}\big(1 + a_n(X_n)X_n\big) + a_{n-1}(X_n, X_{n-1})X_{n-1}.$$

And so on and so forth. The skeptical or meticulous reader can formulate a proof by induction in good and due form. □

5. Dimension of geometric rings

Polynomial rings over a discrete field

A first important result in the theory of Krull dimension is the dimension of polynomial rings over a discrete field.

5.1. Theorem. *If* $\mathbf{K}$ *is a nontrivial discrete field, the Krull dimension of the polynomial ring* $\mathbf{K}[X_1, \ldots, X_\ell]$ *is equal to* ℓ.

We first establish the following result which needs a precise definition. Some elements x_1, …, x_ℓ of a $\mathbf{K}$-algebra with zero-dimensional $\mathbf{K}$ are said to be *algebraically dependent over* $\mathbf{K}$ if they annihilate a primitive polynomial[2] $f \in \mathbf{K}[X_1, \ldots, X_\ell]$.

5.2. Proposition. *Let* $\mathbf{K}$ *be a discrete field, or more generally a zero-dimensional ring,* $\mathbf{A}$ *be a* $\mathbf{K}$*-algebra, and* x_1, …, $x_\ell \in \mathbf{A}$ *be algebraically dependent over* $\mathbf{K}$. *Then the sequence* $(x_1, \ldots, x_\ell)$ *is singular.*

D We treat the case of a discrete field. The general case is then deduced by applying the elementary local-global machinery no. 2 (page 213).
Let $Q(x_1, \ldots, x_\ell) = 0$ be an algebraic dependence relation over $\mathbf{K}$. Let us put a lexicographical order on the nonzero monomials $\alpha_{p_1,\ldots,p_\ell} x_1^{p_1} x_2^{p_2} \cdots x_\ell^{p_\ell}$ of Q, in accordance with the "words" $p_1 p_2 \ldots p_\ell$. We can assume that the coefficient of the smallest nonzero monomial equal to 1 (here we use the hypothesis that the field is discrete, because we assume that we can determine for each $\alpha_{p_1,\ldots,p_\ell}$ wether it is null or invertible). Let $x_1^{m_1} x_2^{m_2} \cdots x_\ell^{m_\ell}$ be this monomial. By following the lexicographical order, we see that we can express Q in the form

$$\begin{aligned} Q = {} & x_1^{m_1} \cdots x_\ell^{m_\ell} + x_1^{m_1} \cdots x_\ell^{1+m_\ell} R_\ell + x_1^{m_1} \cdots x_{\ell-1}^{1+m_{\ell-1}} R_{\ell-1} \\ & + \cdots + x_1^{m_1} x_2^{1+m_2} R_2 + x_1^{1+m_1} R_1 \end{aligned}$$

where $R_j \in \mathbf{K}[x_k\,;\, k \geqslant j]$. Then $Q = 0$ is the desired equality. □

Proof of Theorem 5.1. We first note that the sequence $(X_1, \ldots, X_\ell)$ is regular, which shows that the Krull dimension of $\mathbf{K}[X_1, \ldots, X_\ell]$ is $\geqslant \ell$. We

[2] The notion introduced here generalizes the notion of a primitively algebraic element introduced on page 701. If $\mathbf{K}$ were not zero-dimensional, it would be reasonable to use a more restrictive terminology such as "primitively algebraic dependence relation." It is also clear that the local-global principle XII-4.6 can be generalized in the case of ℓ elements.

can also directly see that it is nonsingular: in Equality (6) (page 753) with $x_i = X_i$ the left-hand side is nonzero (consider the coefficient of $X_1^{m_1} X_2^{m_2} \cdots X_\ell^{m_\ell}$). To prove that the dimension of $\mathbf{K}[X_1, \ldots, X_\ell]$ is $\leqslant \ell$, it suffices, given Proposition 5.2, to show that $\ell + 1$ elements of $\mathbf{K}[X_1, \ldots, X_\ell]$ are always algebraically dependent over $\mathbf{K}$. Here is an elementary proof of this classical result. Let $y_1, \ldots, y_{\ell+1}$ be these elements, and d be a bound on their degrees. For some integer $k \geqslant 0$ consider the list L_k of all the $y_1^{\delta_1} \cdots y_{\ell+1}^{\delta_{\ell+1}}$ such that $\sum_{i=1}^{\ell+1} \delta_i \leqslant k$. The number of elements of the list L_k is equal to $\binom{k+\ell+1}{k}$: this is a polynomial of degree $\ell + 1$ in k. The elements of L_k live in the vector space $E_{\ell,kd}$ of the elements of $\mathbf{K}[X_1, \ldots, X_\ell]$ of degree $\leqslant k\,d$, which is of dimension $\binom{kd+\ell}{kd}$: this is a polynomial of degree ℓ in k. Thus for large enough k, the cardinal of L_k is greater than the dimension of the vector space $E_{\ell,kd}$ containing L_k, therefore there is a linear dependence relation between the elements of L_k. This provides an algebraic dependence relation between the y_i's. □

Comment. The proof of Proposition 5.2 cannot constructively provide the same result for the field of reals $\mathbb{R}$ (which *is not* discrete). Actually it is impossible to realize the test of zero-dimensionality for $\mathbb{R}$:

$$\forall x \in \mathbb{R} \;\; \exists a \in \mathbb{R} \;\; \exists n \in \mathbb{N},\, x^n\,(1 - ax) = 0.$$

This would indeed mean that for every real number x, we know how to find a real a such that $x(1 - ax) = 0$. If we have found such an a, we obtain

- if ax is invertible then x is invertible,
- if $1 - ax$ is invertible then $x = 0$.

However, the alternative "ax or $1 - ax$ is invertible" is explicit over $\mathbb{R}$. Thus providing the test of zero-dimensionality amounts to the same as providing the test for "is x null or invertible ?" But this is not possible from the constructive point of view. Moreover, we can show that it is impossible to have a nonsingular sequence of length 1, if we take $y \neq 0$ in the strong sense of "y is invertible" (in the definition of "nonsingular"). Indeed, if we have some x such that for all $a \in \mathbb{R}$ and $n \in \mathbb{N}$, $x^n\,(1 - ax) \in \mathbb{R}^\times$, we get a contradiction: if $a = 0$ then $x \in \mathbb{R}^\times$, therefore there exists a b such that $1 - bx = 0$. ■

An interesting corollary

5.3. Lemma. *A ring generated by k elements is of finite Krull dimension.*

D Since the dimension can only decrease by passage to a quotient, it suffices to show that $\mathbb{Z}[X_1, \ldots, X_k]$ is of Krull dimension $\leqslant 2k + 1$ (actually this ring is of Krull dimension $k + 1$ by Theorem 8.20).

Let $(h_1, \ldots, h_{2k+2})$ be a sequence of $2k+2$ elements in $\mathbb{Z}[X_1, \ldots, X_k] = \mathbb{Z}[\underline{X}]$.

We need to show that it is singular.
The sequence $(h_1, \ldots, h_{k+1})$ is singular in $\mathbb{Q}[X_1, \ldots, X_k] = \mathbb{Q}[\underline{X}]$. This means that the iterated boundary ideal $\mathcal{I}^{\mathrm{K}}_{\mathbb{Q}[\underline{X}]}(h_1, \ldots, h_{k+1})$ contains 1.

By getting rid of the denominators we obtain that $\mathcal{I}^{\mathrm{K}}_{\mathbb{Z}[\underline{X}]}(h_1, \ldots, h_{k+1})$ contains an integer $d > 0$. Therefore the ring $\mathbf{B} = \mathbb{Z}[\underline{X}]/\mathcal{I}^{\mathrm{K}}_{\mathbb{Z}[\underline{X}]}(h_1, \ldots, h_{k+1})$ is a quotient of the ring $\mathbf{C} = (\mathbb{Z}/\langle d\rangle)[\underline{X}]$. As $\mathbb{Z}/\langle d\rangle$ is zero-dimensional, the sequence $(h_{k+2}, \ldots, h_{2k+2})$ is singular in $\mathbf{C}$ (Proposition 5.2), in other words the ideal $\mathcal{I}^{\mathrm{K}}_{\mathbf{C}}(h_{k+2}, \ldots, h_{2k+2})$ contains 1. A fortiori $\mathcal{I}^{\mathrm{K}}_{\mathbf{B}}(h_{k+2}, \ldots, h_{2k+2})$ contains 1. Finally, the ring

$$\mathbb{Z}[\underline{X}]\Big/\mathcal{I}^{\mathrm{K}}_{\mathbb{Z}[\underline{X}]}(h_1, \ldots, h_{2k+2}) = \mathbf{B}/\mathcal{I}^{\mathrm{K}}_{\mathbf{B}}(h_{k+2}, \ldots, h_{2k+2})$$

is trivial. □

Geometric rings

We call a *geometric ring* a ring $\mathbf{A}$ that is a finitely presented $\mathbf{K}$-algebra with $\mathbf{K}$ as a nontrivial discrete field.

Theorem VII-1.5 of Noether position affirms that such a quotient ring is a finite integral extension of a ring $\mathbf{B} = \mathbf{K}[Y_1, \ldots, Y_r]$ contained in $\mathbf{A}$ (here, Y_1, ..., Y_r are elements of $\mathbf{A}$ algebraically independent over $\mathbf{K}$).

5.4. Theorem. *Under the previous hypotheses, the Krull dimension of the ring* $\mathbf{A}$ *is equal to* r.

D Theorem 5.1 shows that $\mathsf{Kdim}\,\mathbf{B} \leqslant r$. We can get the fact that $r + 1$ elements of $\mathbf{A}$ are algebraically dependent over $\mathbf{K}$ in the same style as described on page 764 for a polynomial algebra. This will give $\mathsf{Kdim}\,\mathbf{A} \leqslant r$. For the Krull dimension to be $\geqslant r$ results from Proposition 4.1.
NB: Theorem 7.16, which implies $\mathsf{Kdim}\,\mathbf{A} = \mathsf{Kdim}\,\mathbf{B}$, gives another proof.□

6. Krull dimension of distributive lattices

As previously mentioned, the Krull dimension of a commutative ring $\mathbf{A}$ is none other than that Krull dimension of the spectral space $\mathsf{Spec}\,\mathbf{A}$, at least in classical mathematics.

In constructive mathematics we introduce the Krull dimension of a distributive lattice $\mathbf{T}$ so that it is equal, in classical mathematics, to the Krull dimension of its spectrum $\mathsf{Spec}\,\mathbf{T}$. The proof of this equality is very nearly identical to the one which we gave for commutative rings. We will not repeat it, since in any case, we will always use the Krull dimension of a distributive lattice via the constructive definition that follows.

6.1. Definition.

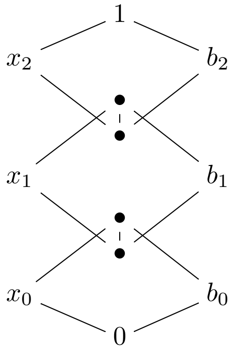
1. Two sequences $(x_0, \dots, x_n)$ and $(b_0, \dots, b_n)$ in a distributive lattice $\mathbf{T}$ are said to be *complementary* if

$$\left.\begin{array}{rcl} b_0 \wedge x_0 & = & 0 \\ b_1 \wedge x_1 & \leqslant & b_0 \vee x_0 \\ \vdots & \vdots & \vdots \\ b_n \wedge x_n & \leqslant & b_{n-1} \vee x_{n-1} \\ 1 & = & b_n \vee x_n \end{array}\right\} \tag{9}$$

   A sequence that has a complementary sequence will be said to be *singular.*

2. For $n \geqslant 0$ we will say that the distributive lattice $\mathbf{T}$ is *of Krull dimension at most n* if every sequence $(x_0, \dots, x_n)$ in $\mathbf{T}$ is singular. Moreover, we will say that the distributive lattice $\mathbf{T}$ is of Krull dimension -1 if it is trivial, i.e. if $1_{\mathbf{T}} = 0_{\mathbf{T}}$.

For example, for $k = 2$ item *1* corresponds to the following graph in $\mathbf{T}$.



We will write $\mathsf{Kdim}\,\mathbf{T} \leqslant n$ when the Krull dimension is at most n.

It is obvious that a lattice has the same Krull dimension as the opposite lattice. We also immediately see that a lattice is zero-dimensional if and only if it is a Boolean algebra.

Also, a totally ordered set of n elements has for Krull dimension $n - 2$.

6.2. Fact. *Let S be a subset of $\mathbf{T}$ that generates $\mathbf{T}$ as a distributive lattice. Then $\mathbf{T}$ is of dimension at most n if and only if every sequence $(x_0, \dots, x_n)$ in S admits a complementary sequence in $\mathbf{T}$.*

D Let us illustrate the computations on a sufficiently general example in the case $n = 4$.

We verify that if $(x_0, x_1, x_2, x_3, x_4)$ admits $(a_0, a_1, a_2, a_3, a_4)$ as a complementary sequence, and if $(x_0, x_1, y_2, x_3, x_4)$ admits $(b_0, b_1, b_2, b_3, b_4)$ as a complementary sequence, then the sequence $(x_0, x_1, x_2 \vee y_2, x_3, x_4)$ admits the complementary sequence $(a_0 \vee b_0, a_1 \vee b_1, a_2 \wedge b_2, a_3 \wedge b_3, a_4 \wedge b_4)$.

Dually, the sequence $(x_0, x_1, x_2 \wedge y_2, x_3, x_4)$ admits the complementary sequence $(a_0 \vee b_0, a_1 \vee b_1, a_2 \vee b_2, a_3 \wedge b_3, a_4 \wedge b_4)$.

The same computation would work for an arbitrary x_i (instead of x_2 above) in an arbitrary finite sequence. Thus if each sequence $(z_0, \dots, z_n)$ in S admits a complementary sequence in $\mathbf{T}$, the same will hold for every sequence of $n + 1$ terms in the lattice generated by S. □

6.3. Fact. *A commutative ring has the same Krull dimension as its Zariski lattice.*

D The proof, based on Fact 6.2, is left to the reader. Another proof will be given later in the form of Lemma XIV-4.7. □

We can also access the Krull dimension via the Krull boundary ideals as for the commutative rings.

6.4. Definition.

1. The lattice $\mathbf{T}^x_{\mathrm{K}} = \mathbf{T}/(\mathcal{J}^{\mathrm{K}}_{\mathbf{T}}(x) = 0)$, where
$$\mathcal{J}^{\mathrm{K}}_{\mathbf{T}}(x) \;=\; \downarrow x \vee (0 : x)_{\mathbf{T}} \tag{10}$$
is called *the (Krull) upper boundary of x in* $\mathbf{T}$. We also say that the ideal $\mathcal{J}^{\mathrm{K}}_{\mathbf{T}}(x)$ is *the Krull boundary ideal of x in* $\mathbf{T}$.
2. More generally, for a sequence $(\underline{x})$ in $\mathbf{T}$, the iterated Krull boundary ideal $\mathcal{J}^{\mathrm{K}}_{\mathbf{T}}(\underline{x})$ is defined by induction as follows: $\mathcal{J}^{\mathrm{K}}_{\mathbf{T}}() = \{0\}$, and
$$\mathcal{J}^{\mathrm{K}}_{\mathbf{T}}(x_0, \dots, x_k) = \big(\mathcal{J}^{\mathrm{K}}_{\mathbf{T}}(x_0, \dots, x_{k-1}) : x_k\big)_{\mathbf{T}} \vee \downarrow x_k\,. \tag{11}$$

6.5. Fact. *Let $n \in \mathbb{N}$ and $\mathbf{T}$ be a distributive lattice.*

1. *A sequence $(x_0, \dots, x_n)$ in $\mathbf{T}$ is singular if and only if the iterated boundary ideal $\mathcal{J}^{\mathrm{K}}_{\mathbf{T}}(x_0, \dots, x_n)$ contains* 1.
2. *We have* $\mathsf{Kdim}\,\mathbf{T} \leqslant n$ *if and only if for every x,* $\mathsf{Kdim}\,\mathbf{T}^x_{\mathrm{K}} \leqslant n - 1$.

6.6. Fact. *In a Heyting algebra, every iterated Krull boundary ideal is principal: $\mathcal{J}^{\mathrm{K}}_{\mathbf{T}}(x) = \downarrow\big(x \vee \neg x\big)$ and more generally,*

$$\mathcal{J}^{\mathrm{K}}_{\mathbf{T}}(x_0, \dots, x_n) = \downarrow\big(x_n \vee \big(x_n \to (\cdots (x_1 \vee (x_1 \to (x_0 \vee \neg x_0))) \cdots)\big)\big) \tag{12}$$

6.7. Lemma. *Let $\mathfrak{a}$ and $\mathfrak{b}$ be two finitely generated ideals of a ring $\mathbf{A}$. In the lattice* $\mathsf{Zar}\,\mathbf{A}$*, the element $\mathrm{D}_{\mathbf{A}}(\mathfrak{a}) \to \mathrm{D}_{\mathbf{A}}(\mathfrak{b})$ exists if and only if the ideal $(\mathfrak{b} : \mathfrak{a}^\infty)$ has the same radical as a finitely generated ideal.*

D In a distributive lattice, the element $u \to v$ exists if the ideal $(v : u)$ is principal (its generator is then denoted by $u \to v$). However, for some finitely generated ideal $\mathfrak{a}$, $\big(\mathrm{D}_{\mathbf{A}}(\mathfrak{b}) : \mathrm{D}_{\mathbf{A}}(\mathfrak{a})\big) = \mathrm{D}_{\mathbf{A}}(\mathfrak{b} : \mathfrak{a}^\infty)$. Hence the stated result. □

6.8. Lemma. *Suppose that* $\mathsf{Zar}\,\mathbf{A}$ *is a Heyting algebra.*
For $(x_0, \dots, x_n)$ in $\mathbf{A}$, we have the equality
$$\mathrm{D}_{\mathbf{A}}\big(\mathcal{J}^{\mathrm{K}}_{\mathbf{A}}(x_0, \dots, x_n)\big) = \mathcal{J}^{\mathrm{K}}_{\mathsf{Zar}\,\mathbf{A}}\big(\mathrm{D}_{\mathbf{A}}(x_0), \dots, \mathrm{D}_{\mathbf{A}}(x_n)\big).$$

D The proof is left to the reader. □

6.9. Proposition. *Let* $\mathbf{A}$ *be a Noetherian coherent ring.*

1. *If* $\mathfrak{a}$ *and* $\mathfrak{b}$ *are two finitely generated ideals, the ideal* $(\mathfrak{b} : \mathfrak{a}^\infty)$ *is finitely generated.*
2. $\mathsf{Zar}\,\mathbf{A}$ *is a Heyting algebra, with* $\mathrm{D}_{\mathbf{A}}(\mathfrak{a}) \to \mathrm{D}_{\mathbf{A}}(\mathfrak{b}) = \mathrm{D}_{\mathbf{A}}(\mathfrak{b} : \mathfrak{a}^\infty)$.
3. *The iterated Krull boundary ideals defined on page 753 have the same radical as the finitely generated ideals.*
4. *If in addition* $\mathbf{A}$ *is strongly discrete,* $\mathsf{Zar}\,\mathbf{A}$ *is discrete and we dispose of a test to decide if a sequence in* $\mathbf{A}$ *admits a complementary sequence.*

D *1.* Let $\mathfrak{a}$, $\mathfrak{b} \in \mathsf{Zar}\,\mathbf{A}$. Let $\mathfrak{J}_k = (\mathfrak{b} : \mathfrak{a}^k)$. Since $\mathbf{A}$ is coherent, each ideal $\mathfrak{J}_k$ is finitely generated. Since $\mathbf{A}$ is Noetherian, the sequence admits two consecutive equal terms, for example of indices p and $p+1$, from which it is clear that it becomes stationary. We then have $\mathfrak{J}_p = (\mathfrak{b} : \mathfrak{a}^\infty)$.
2. Consequence of *1* given Lemma 6.7.
3. Results by induction of *2* given Fact 6.6 and Lemma 6.8.
4. Results from *2*, from Fact 6.6 and from Lemma 6.8. □

7. Dimension of morphisms

Definition and first properties

7.1. Definition. Let $\rho : \mathbf{A} \to \mathbf{B}$ is a ring homomorphism. *The Krull dimension of the morphism* ρ is the Krull dimension of the ring $\mathbf{A}^\bullet \otimes_{\mathbf{A}} \mathbf{B}$ obtained by scalar extension (Theorem VI-3.9) from $\mathbf{A}$ to its reduced zero-dimensional closure $\mathbf{A}^\bullet$ (Theorem XI-4.25).

Examples.
1) If $\mathbf{k}$ is zero-dimensional, we have seen that $\mathsf{Kdim}\,\mathbf{k}[X_1, \ldots, X_n] \leqslant n$. We deduce that the Krull dimension of the morphism $\mathbf{A} \to \mathbf{A}[X_1, \ldots, X_n]$ is $\leqslant n$, with equality if $\mathbf{A}$ is nontrivial.
2) If $\mathbf{B}$ is an integral $\mathbf{A}$-algebra, after scalar extension the algebra is integral over $\mathbf{A}^\bullet$, therefore zero-dimensional. Thus, the morphism $\mathbf{A} \to \mathbf{B}$ is zero-dimensional. ■

7.2. Lemma. *Let* $\mathbf{B}$ *and* $\mathbf{C}$ *be two* $\mathbf{A}$*-algebras. Then by scalar extension we obtain* $\mathsf{Kdim}(\mathbf{C} \to \mathbf{C} \otimes_{\mathbf{A}} \mathbf{B}) \leqslant \mathsf{Kdim}(\mathbf{A} \to \mathbf{B})$ *in the following cases.*

1. $\mathbf{C}$ *is a quotient of* $\mathbf{A}$*, or a localized ring of* $\mathbf{A}$*, or the quotient of a localized ring of* $\mathbf{A}$*.*
2. $\mathbf{C}$ *is a finite product of rings of the previous type.*
3. $\mathbf{C}$ *is a filtering colimit of rings of the previous type.*

D We use the observation $\mathbf{C}^\bullet \otimes_\mathbf{C} (\mathbf{C} \otimes_\mathbf{A} \mathbf{B}) \simeq \mathbf{C}^\bullet \otimes_\mathbf{A} \mathbf{B} \simeq \mathbf{C}^\bullet \otimes_{\mathbf{A}^\bullet} (\mathbf{A}^\bullet \otimes_\mathbf{A} \mathbf{B})$. We then prove that the functor $\mathbf{B} \mapsto \mathbf{B}^\bullet$ transforms a quotient into a quotient, a localized ring into a localized ring (Proposition XI-4.27), a finite product into a finite product, and a filtering colimit into a filtering colimit. Moreover, the scalar extension also commutes with all these constructions. Finally, the Krull dimension can only decrease by these constructions. □

Remark. It is not true that $\mathbf{C} \otimes_\mathbf{A} \mathbf{B}$ is zero-dimensional as soon as the three rings are zero-dimensional. For example we can take $\mathbf{A}$ to be a discrete field and $\mathbf{B} = \mathbf{C} = \mathbf{A}(X)$. Then $\mathsf{Kdim}(\mathbf{C} \otimes_\mathbf{A} \mathbf{B}) = 1$ (see Exercise 13). It follows that the scalar extension, even in the case of a faithfully flat extension, can strictly increase the Krull dimension of morphisms. A contrario we have the following concrete local-global principle. ■

7.3. Concrete local-global principle. *Let S_1, …, S_n be comaximal monoids of a ring $\mathbf{A}$, $k \geqslant -1$ be an integer and $\mathbf{B}$ be an $\mathbf{A}$-algebra. The Krull dimension of the morphism $\mathbf{A} \to \mathbf{B}$ is $\leqslant k$ if and only if the Krull dimension of each of the morphisms $\mathbf{A}_{S_i} \to \mathbf{B}_{S_i}$ is $\leqslant k$.*

D As $(\mathbf{A}_{S_i})^\bullet \simeq (\mathbf{A}^\bullet)_{S_i}$ (Proposition XI-4.27), we obtain

$$(\mathbf{A}_{S_i})^\bullet \otimes_{\mathbf{A}_{S_i}} \mathbf{B}_{S_i} \simeq (\mathbf{A}^\bullet \otimes_\mathbf{A} \mathbf{B})_{S_i},$$

and we are brought back to the local-global principle 3.2. □

The goal of this section is to show, for a morphism $\rho : \mathbf{A} \to \mathbf{B}$, the inequality

$$\boxed{1 + \mathsf{Kdim}\,\mathbf{B} \leqslant (1 + \mathsf{Kdim}\,\mathbf{A})(1 + \mathsf{Kdim}\,\rho)}.$$

Note that for $\mathsf{Kdim}\,\mathbf{A} \leqslant 0$ we trivially have $\mathsf{Kdim}\,\mathbf{B} = \mathsf{Kdim}\,\rho$. We then treat a simple but nontrivial case to get a clear picture. The truly simple case would be the one where $\mathbf{A}$ is integral and $\mathsf{Kdim}\,\mathbf{A} \leqslant 1$. As the proof is unchanged, we will only suppose that $\mathbf{A}$ is a pp-ring, which will make the rest easier.

7.4. Proposition. *Let $\rho : \mathbf{A} \to \mathbf{B}$ be a morphism, with $\mathbf{A}$ a pp-ring. If $\mathsf{Kdim}\,\rho \leqslant n$ and $\mathsf{Kdim}\,\mathbf{A} \leqslant 1$, then $\mathsf{Kdim}\,\mathbf{B} \leqslant 2n + 1$.*

D Let $\underline{h} = (h_0, \dots, h_{2n+1})$ be a sequence of $2n + 2$ elements in $\mathbf{B}$. We need to show that it is singular.
By hypothesis the ring $\mathbf{A}^\bullet \otimes_\mathbf{A} \mathbf{B}$ is of dimension at most n.
Let $\mathbf{K} = \operatorname{Frac}\mathbf{A}$ be the total ring of fractions. It is reduced zero-dimensional and generated by $\mathbf{A}$ as a reduced zero-dimensional ring, therefore it is a quotient of $\mathbf{A}^\bullet$. We conclude that the sequence $(h_0, \dots, h_n)$ is singular in $\widetilde{\mathbf{B}} = \mathbf{K} \otimes_\mathbf{A} \mathbf{B}$.
This means that the iterated boundary ideal $\mathcal{I}^{\mathrm{K}}_{\widetilde{\mathbf{B}}}(h_0, \dots, h_n)$ contains 1, and by getting rid of the denominators, that $\mathcal{I}^{\mathrm{K}}_{\mathbf{B}}(h_0, \dots, h_n)$ contains some

$a \in \mathrm{Reg}(\mathbf{A})$.
Therefore $\mathbf{B}_0 = \mathbf{B}/\mathcal{I}^{\mathrm{K}}_{\mathbf{B}}(h_0, \dots, h_n)$ is a quotient of $\mathbf{B}/a\mathbf{B} = \mathbf{A}/a\mathbf{A} \otimes_{\mathbf{A}} \mathbf{B}$. Since a is regular and $\mathsf{Kdim}\,\mathbf{A} \leqslant 1$, the quotient $\mathbf{A}/a\mathbf{A}$ is zero-dimensional, so $(\mathbf{A}/a\mathbf{A})_{\mathrm{red}}$ is a quotient of $\mathbf{A}^\bullet$ and the ring $(\mathbf{B}_0)_{\mathrm{red}}$ is a quotient of $\mathbf{A}^\bullet \otimes_{\mathbf{A}} \mathbf{B}$. We deduce that the sequence $(h_{n+1}, \dots, h_{2n+1})$ is singular in $(\mathbf{B}_0)_{\mathrm{red}}$, therefore also in $\mathbf{B}_0$.
Therefore the ring $\mathbf{B}/\mathcal{I}^{\mathrm{K}}_{\mathbf{B}}(\underline{h}) = \mathbf{B}_0/\mathcal{I}^{\mathrm{K}}_{\mathbf{B}_0}(h_{n+1}, \dots, h_{2n+1})$ is trivial. □

To pass from the pp-ring case to the general case we want to say that every reduced ring can behave in the computations like an integral ring provided we replace $\mathbf{A}$ with

$$\mathbf{A}/\mathrm{Ann}_{\mathbf{A}}(a) \times \mathbf{A}/\mathrm{Ann}_{\mathbf{A}}(\mathrm{Ann}_{\mathbf{A}}(a))$$

when an algorithm asks to know if the annihilator of a is equal to 0 or 1. The important thing in this construction is that the closed covering principle for the singular sequences applies since the product of the two ideals $\mathrm{Ann}_{\mathbf{A}}(a)$ and $\mathrm{Ann}_{\mathbf{A}}(\mathrm{Ann}_{\mathbf{A}}(a))$ is null.

This type of proof will probably be easier to grasp when we will familiarize ourselves with the basic local-global machinery explained on page 871. Here we do not proceed by successive comaximal localizations but by successive "closed coverings."

Actually we will not introduce a dynamic computation tree as such, we will instead construct a universal object. This universal object is a "constructive finitary approximation" of the product of all the quotients of $\mathbf{A}$ by its minimal prime ideals, a slightly too ideal object of classical mathematics to be considered constructively, at least in the form that we just defined: actually, if $\mathbf{B}$ is this product and if $\mathbf{A}_1$ is the natural image of $\mathbf{A}$ in $\mathbf{B}$, then the universal ring that we are constructing should be equal to the pp-ring closure of $\mathbf{A}_1$ in $\mathbf{B}$, at least in classical mathematics.

The minimal pp-ring closure of a reduced ring

In what follows we denote by $a^\perp$ the annihilator ideal of the element a when the context is clear (here the context is simply the ring in which we must consider a). We will also use the notation $\mathfrak{a}^\perp$ for the annihilator of an ideal $\mathfrak{a}$.

The facts stated below are immediate.

$$\mathfrak{a} \ \subseteq \ (\mathfrak{a}^\perp)^\perp \tag{13}$$

$$\mathfrak{a} \subseteq \mathfrak{b} \Longrightarrow \mathfrak{b}^\perp \subseteq \mathfrak{a}^\perp \tag{14}$$

$$\mathfrak{a}^\perp \ = \ \big((\mathfrak{a}^\perp)^\perp\big)^\perp \tag{15}$$

$$(\mathfrak{a} + \mathfrak{b})^\perp \ = \ \mathfrak{a}^\perp \cap \mathfrak{b}^\perp \tag{16}$$

$$\mathfrak{a}^\perp \subseteq \mathfrak{b}^\perp \iff (\mathfrak{a}+\mathfrak{b})^\perp = \mathfrak{a}^\perp \tag{17}$$

$$\mathfrak{a}^\perp \subseteq \mathfrak{b}^\perp \iff (\mathfrak{b}^\perp)^\perp \subseteq (\mathfrak{a}^\perp)^\perp \tag{18}$$

$$(\mathfrak{a}^\perp : \mathfrak{b}) \ = \ (\mathfrak{a}\mathfrak{b})^\perp \tag{19}$$

$$(\mathbf{A}/\mathfrak{a}^\perp)/\ \overline{\mathfrak{b}}^{\ \perp} \ = \ \mathbf{A}/(\mathfrak{a}\mathfrak{b})^\perp \tag{20}$$

Remarks. 1) An ideal $\mathfrak{a}$ is an annihilator (of another ideal) if and only if $\mathfrak{a} = (\mathfrak{a}^\perp)^\perp$.
2) The inclusion $\mathfrak{a}^\perp + \mathfrak{b}^\perp \subseteq (\mathfrak{a} \cap \mathfrak{b})^\perp$ can be strict, even if $\mathfrak{a} = \mathfrak{a}_1^\perp$ and $\mathfrak{b} = \mathfrak{b}_1^\perp$. Take for example $\mathbf{A} = \mathbb{Z}[x,y] = \mathbb{Z}[X,Y]/\langle XY \rangle$, $\mathfrak{a}_1 = \langle x \rangle$ and $\mathfrak{b}_1 = \langle y \rangle$. Then, $\mathfrak{a} = \mathfrak{a}_1^\perp = \langle y \rangle$, $\mathfrak{b} = \mathfrak{b}_1^\perp = \langle x \rangle$, $\mathfrak{a}^\perp + \mathfrak{b}^\perp = \langle x, y \rangle$, and $(\mathfrak{a} \cap \mathfrak{b})^\perp = \langle 0 \rangle^\perp = \langle 1 \rangle$. ■

If we assume that $\mathbf{A}$ is reduced, we also have the following results.

$$\sqrt{\mathfrak{a}^\perp} \quad = \quad \mathfrak{a}^\perp \ = \ (\sqrt{\mathfrak{a}})^\perp \quad = \quad (\mathfrak{a}^2)^\perp \tag{21}$$

$$(\mathfrak{a}\mathfrak{b})^\perp \ = \ (\mathfrak{a} \cap \mathfrak{b})^\perp \tag{22}$$

$$\mathfrak{a}^\perp \subseteq \mathfrak{b}^\perp \iff (\mathfrak{a}\mathfrak{b})^\perp = \mathfrak{b}^\perp \tag{23}$$

7.5. Lemma. *Let $\mathbf{A}$ be a reduced ring and $a \in \mathbf{A}$. We define*

$$\mathbf{A}_{\{a\}} \overset{\mathrm{def}}{=} \mathbf{A}/a^\perp \times \mathbf{A}/(a^\perp)^\perp$$

and we let $\psi_a : \mathbf{A} \to \mathbf{A}_{\{a\}}$ be the canonical homomorphism.

1. *$\psi_a(a)^\perp$ is generated by the idempotent $(\overline{0}, \widetilde{1})$, so $\psi_a(a)^\perp = (\overline{1}, \widetilde{0})^\perp$.*
2. *ψ_a is injective (we can identify $\mathbf{A}$ with a subring of $\mathbf{A}_{\{a\}}$).*
3. *Let $\mathfrak{b}$ be an ideal in $\mathbf{A}_{\{a\}}$, then the ideal $\psi_a^{-1}(\mathfrak{b}^\perp) = \mathfrak{b}^\perp \cap \mathbf{A}$ is an annihilator ideal in $\mathbf{A}$.*
4. *The ring $\mathbf{A}_{\{a\}}$ is reduced.*

D *1.* We have $\psi_a(a) = (\overline{a}, \widetilde{0})$, where $\overline{x}$ is the class modulo $a^\perp$ and $\widetilde{x}$ is the class modulo $(a^\perp)^\perp$. If $c = (\overline{y}, \widetilde{z})$, the equality $\psi_a(a)c = 0$ means $\overline{ya} = 0$, i.e. $ya^2 = 0$, or yet $ya = 0$, i.e. $\overline{y} = \overline{0}$.
2. If $xa = 0$ and $xy = 0$ for every $y \in a^\perp$ then $x^2 = 0$ so $x = 0$.
3. Let $\psi_1 : \mathbf{A} \to \mathbf{A}/a^\perp$ and $\psi_2 : \mathbf{A} \to \mathbf{A}/(a^\perp)^\perp$ be the two projections. We have $\mathfrak{b} = \mathfrak{b}_1 \times \mathfrak{b}_2$. If $x \in \mathbf{A}$ we have

$$\psi_a(x) \in \mathfrak{b}^\perp \iff \psi_1(x)\mathfrak{b}_1 = 0 \quad \text{and} \quad \psi_2(x)\mathfrak{b}_2 = 0,$$

i.e. $x \in \psi_1^{-1}(\mathfrak{b}_1^\perp) \cap \psi_2^{-1}(\mathfrak{b}_2^\perp)$. Equality (20) tells us that each $\psi_i^{-1}(\mathfrak{b}_i^\perp)$ is an annihilator ideal. The result follows by Equality (16).
4. In a reduced ring, every annihilator ideal $\mathfrak{b}^\perp$ is radical: indeed, if $x^2\mathfrak{b} = 0$, then $x\mathfrak{b} = 0$. □

7.6. Lemma. *Let* $\mathbf{A}$ *be reduced and* a, $b \in \mathbf{A}$. *Then with the notations of Lemma 7.5 the two rings* $(\mathbf{A}_{\{a\}})_{\{b\}}$ *and* $(\mathbf{A}_{\{b\}})_{\{a\}}$ *are canonically isomorphic.*

D The ring $(\mathbf{A}_{\{a\}})_{\{b\}}$ can be described symmetrically as follows

$$\mathbf{A}_{\{a,b\}} = \mathbf{A}/(ab)^{\perp} \times \mathbf{A}/(ab^{\perp})^{\perp} \times \mathbf{A}/(a^{\perp}b)^{\perp} \times \mathbf{A}/(a^{\perp}b^{\perp})^{\perp} \ ,$$

and if $\psi : \mathbf{A} \to \mathbf{A}_{\{a,b\}}$ is the canonical homomorphism, it is clear that we have $\psi(a)^{\perp} = (1,1,0,0)^{\perp}$ and $\psi(b)^{\perp} = (1,0,1,0)^{\perp}$. □

Remark. The case where $ab = 0$ is typical: when we meet it, we would like to split the ring into components where things are "clear." The previous construction then gives the three components

$$\mathbf{A}/(ab^{\perp})^{\perp} \ , \ \mathbf{A}/(a^{\perp}b)^{\perp} \ \text{ and } \ \mathbf{A}/(a^{\perp}b^{\perp})^{\perp} \ .$$

In the first one, a is regular and $b = 0$, in the second one b is regular and $a = 0$, and in the third one $a = b = 0$. ■

The following lemma regarding pp-rings is copied from Lemma XI-4.22 which concerned reduced zero-dimensional rings (the reader will also be able to just about copy the proof).

7.7. Lemma. *If* $\mathbf{A} \subseteq \mathbf{C}$ *with* $\mathbf{C}$ *a pp-ring, the smallest pp-subring of* $\mathbf{C}$ *containing* $\mathbf{A}$ *is equal to* $\mathbf{A}[(e_a)_{a\in\mathbf{A}}]$, *where* e_a *is the idempotent of* $\mathbf{C}$ *such that* $\mathrm{Ann}_{\mathbf{C}}(a) = \langle 1 - e_a \rangle_{\mathbf{C}}$. *More generally if* $\mathbf{A} \subseteq \mathbf{B}$ *with reduced* $\mathbf{B}$, *and if every element* a *of* $\mathbf{A}$ *admits an annihilator in* $\mathbf{B}$ *generated by an idempotent* $1 - e_a$, *then the subring* $\mathbf{A}[(e_a)_{a\in\mathbf{A}}]$ *of* $\mathbf{B}$ *is a pp-ring.*

7.8. Theorem and definition. (Minimal pp-ring closure)
Let $\mathbf{A}$ *be a reduced ring. We can define a ring* $\mathbf{A}_{\min}$ *as a filtering colimit by iterating the basic construction which consists in replacing* $\mathbf{E}$ *(the "current" ring, which contains* $\mathbf{A}$*) by*

$$\mathbf{E}_{\{a\}} \overset{\text{def}}{=} \mathbf{E}/a^{\perp} \times \mathbf{E}/(a^{\perp})^{\perp} = \mathbf{E}/\mathrm{Ann}_{\mathbf{E}}(a) \times \mathbf{E}/\mathrm{Ann}_{\mathbf{E}}(\mathrm{Ann}_{\mathbf{E}}(a)) \ ,$$

when a *ranges over* $\mathbf{A}$.

1. *This ring* $\mathbf{A}_{\min}$ *is a pp-ring, contains* $\mathbf{A}$ *and is integral over* $\mathbf{A}$.
2. *For all* $x \in \mathbf{A}_{\min}$, $x^{\perp} \cap \mathbf{A}$ *is an annihilator ideal in* $\mathbf{A}$.

This ring $\mathbf{A}_{\min}$ *is called the* minimal pp-ring closure of $\mathbf{A}$.
When $\mathbf{A}$ *is not necessarily reduced, we will take* $\mathbf{A}_{\min} \overset{\text{def}}{=} (\mathbf{A}_{\mathrm{red}})_{\min}$.

D *1.* By Lemma 7.7, it suffices to add an idempotent e_a for each $a \in \mathbf{A}$ to obtain a pp-ring. The colimit is well-defined due to the relation of commutation given by Lemma 7.6.
For item *2* note that x is obtained at a finite stage of the construction, and that $x^{\perp} \cap \mathbf{A}$ stops changing from the moment where x is reached because

the successive homomorphisms are injections. We can therefore call upon item *3* of Lemma 7.5. □

Remark. We can ask ourselves if $\mathbf{A}_{\min}$ could not be characterized by a universal property related to item *2*. ■

By "iterating" the description of $(\mathbf{A}_{\{a\}})_{\{b\}}$ given in the proof of Lemma 7.6 we obtain the following description of each ring obtained at a finite stage of the construction of $\mathbf{A}_{\min}$ (see Exercise 18).

7.9. Lemma. *Let* $\mathbf{A}$ *be a reduced ring and* $(\underline{a}) = (a_1, \dots, a_n)$ *be a sequence of* n *elements of* $\mathbf{A}$*. For* $I \in \mathcal{P}_n$*, let* $\mathfrak{a}_I$ *be the ideal*

$$\mathfrak{a}_I = \big(\textstyle\prod_{i \in I} \langle a_i \rangle^{\perp} \prod_{j \notin I} a_j\big)^{\perp} = \big(\langle a_i, i \in I \rangle^{\perp} \prod_{j \notin I} a_j\big)^{\perp}.$$

Then $\mathbf{A}_{\min}$ *contains the following ring, a product of* 2^n *quotient rings of* $\mathbf{A}$ *(some eventually null)*

$$\mathbf{A}_{\{\underline{a}\}} = \textstyle\prod_{I \in \mathcal{P}_n} \mathbf{A}/\mathfrak{a}_I \ .$$

7.10. Fact.

1. *Let* $\mathbf{A}$ *be a pp-ring.*
   - *a.* $\mathbf{A}_{\min} = \mathbf{A}$*.*
   - *b.* $\mathbf{A}[X]$ *is a pp-ring, and* $\mathbb{B}(\mathbf{A}) = \mathbb{B}(\mathbf{A}[X])$*.*
2. *For every ring* $\mathbf{A}$ *we have a canonical isomorphism*

$$\mathbf{A}_{\min}[X_1, \dots, X_n] \simeq (\mathbf{A}[X_1, \dots, X_n])_{\min}.$$

D *1a.* Results from the construction of $\mathbf{A}_{\min}$.
1b. The result is clear for integral rings. We can apply the elementary local-global machinery no. 1 (page 204). We could also use McCoy's lemma, Corollary III-2.3 *2*.
2. We suppose without loss of generality that $\mathbf{A}$ is a reduced ring. It also suffices to treat the case of a single variable. Given Lemma 7.6 we can "start" the construction of $\mathbf{A}[X]_{\min}$ with the constructions $\mathbf{E} \rightsquigarrow \mathbf{E}_{\{a\}}$ for some $a \in \mathbf{A}$. But if $\mathbf{E} = \mathbf{B}[X]$ and $a \in \mathbf{A} \subseteq \mathbf{B}$ then $\mathbf{E}_{\{a\}} = \mathbf{B}_{\{a\}}[X]$. Thus $\mathbf{A}_{\min}[X]$ can be seen as a first step of the construction of $\mathbf{A}[X]_{\min}$. But since by item *1* $\mathbf{A}_{\min}[X]$ is a pp-ring and that for a pp-ring $\mathbf{C}$ we have $\mathbf{C} = \mathbf{C}_{\min}$, the construction of $\mathbf{A}[X]_{\min}$ is completed with $\mathbf{A}_{\min}[X]$. □

Comment. In practice, to use the ring $\mathbf{A}_{\min}$, we only need the finite stages of the construction. We can however note that even a single stage of the construction is a little mysterious, insofar as the ideals $a^{\perp}$ and $(a^{\perp})^{\perp}$ are difficult to handle. It is only in the case of coherent rings that we know how to describe them with finite generator sets. Actually if the ring is Noetherian, the construction must end in a finite number of steps (at least from the point of view of classical mathematics), and needs to replace the ring with the product of its quotients with the minimal prime ideals. Here we are in a situation where the construction of $\mathbf{A}_{\min}$ meeting the standards of constructive mathematics seems more complicated than the result in classical mathematics (at least if the ring is Noetherian). Nevertheless, since we do not need to know the minimal prime ideals, our method is more general (it does not need **LEM**). In addition, its complication is mostly apparent. When we use $\mathbf{A}\big/a^{\perp}$ for example, we actually make computations in $\mathbf{A}$ by forcing a to be regular, i.e. by forcefully annihilating every x that presents itself and that annihilates a. When we use $\mathbf{A}\big/(a^{\perp})^{\perp}$, things are less easy, because a priori, we need a proof (and not simply the result of a computation) to certify that an element x is in $(a^{\perp})^{\perp}$. It is a fact that the use of minimal prime ideals in a proof of classical mathematics can in general be made innocuous (i.e. constructive) by using $\mathbf{A}_{\min}$ (or another universal ring of the same type[3]), even if we do not dispose of other means to "describe an ideal $(a^{\perp})^{\perp}$" than the one of applying the definition. ■

Application

7.11. Corollary. *Let $\rho : \mathbf{A} \to \mathbf{B}$ be a morphism of finite Krull dimension. We "extend the scalars" from $\mathbf{A}$ to $\mathbf{A}_{\min}$: we obtain $\mathbf{B}' = \mathbf{A}_{\min} \otimes_{\mathbf{A}} \mathbf{B}$ and let $\rho' : \mathbf{A}_{\min} \to \mathbf{B}'$ be the natural morphism.*
Then $\mathsf{Kdim}\,\mathbf{A}_{\min} = \mathsf{Kdim}\,\mathbf{A}$, $\mathsf{Kdim}\,\mathbf{B} = \mathsf{Kdim}\,\mathbf{B}'$ and $\mathsf{Kdim}\,\rho' \leqslant \mathsf{Kdim}\,\rho$.

D The first two items result from the fact that in the construction of the ring $\mathbf{A}_{\min}$, at each elementary step

$$\mathbf{E} \quad \rightsquigarrow \quad \mathbf{E}/\mathrm{Ann}_{\mathbf{E}}(a) \times \mathbf{E}/\mathrm{Ann}_{\mathbf{E}}(\mathrm{Ann}_{\mathbf{E}} a)\ ,$$

the product of the two ideals is null, which is found again after tensorization by $\mathbf{B}$. Therefore, the closed covering principle for the Krull dimension 3.3 applies. Finally, the inequality $\mathsf{Kdim}\,\rho' \leqslant \mathsf{Kdim}\,\rho$ results from Lemma 7.2.□

Remark. Generally the ring $\mathrm{Frac}\,\mathbf{A}_{\min}$ seems a better concept than $\mathbf{A}^{\bullet}$ to replace the quotient field in the case of a non-integral reduced ring. In the case where $\mathbf{A}$ is a pp-ring, we indeed have $\mathbf{A}_{\min} = \mathbf{A}$, so $\mathrm{Frac}\,\mathbf{A}_{\min} = \mathrm{Frac}\,\mathbf{A}$, while $\mathbf{A}^{\bullet}$ is in general significantly more cumbersome (as the example $\mathbf{A} = \mathbb{Z}$ shows). ■

7.12. Corollary. *Let $\rho : \mathbf{A} \to \mathbf{B}$ be a morphism.*
If $\mathsf{Kdim}\,\rho \leqslant n$ and $\mathsf{Kdim}\,\mathbf{A} \leqslant 1$, then $\mathsf{Kdim}\,\mathbf{B} \leqslant 2n+1$.

D This clearly results from Proposition 7.4 and from Corollary 7.11. □

[3] $\mathbf{A}_{\min}$ corresponds to using all the quotients by the minimal prime ideals, $\mathrm{Frac}(\mathbf{A}_{\min})$ corresponds to using all the quotient fields of these quotients.

7.13. Theorem. *Let $\rho : \mathbf{A} \to \mathbf{B}$ be a morphism.*
If $\mathsf{Kdim}\,\rho \leqslant n$ *and* $\mathsf{Kdim}\,\mathbf{A} \leqslant m$*, then* $\mathsf{Kdim}\,\mathbf{B} \leqslant mn + m + n$*.*

D We perform a proof by induction on m. The case $m = 0$ is trivial. The proof given for $m = 1$ in the case where $\mathbf{A}$ is a pp-ring (Proposition 7.4), which relied on the dimension 0 case to prove the result in dimension $m = 1$, can easily be adapted to pass from dimension m to dimension $m + 1$. We copy the proof in the case where $\mathbf{A}$ is a pp-ring.
To pass to the case of an arbitrary ring we use Corollary 7.11.
We therefore suppose that $\mathbf{A}$ is a pp-ring and we consider a sequence $(\underline{h}) = (h_0, \dots, h_p)$ in $\mathbf{B}$ with $p = (m+1)(n+1) - 1$. We need to show that it is singular.
By hypothesis the ring $\mathbf{A}^\bullet \otimes_{\mathbf{A}} \mathbf{B}$ is of dimension at most n. The total ring of fractions $\mathbf{K} = \operatorname{Frac} \mathbf{A}$ is reduced zero-dimensional, and it is generated by $\mathbf{A}$ as a reduced zero-dimensional ring, so it is a quotient of $\mathbf{A}^\bullet$. We conclude that the sequence $(h_0, \dots, h_n)$ is singular in the ring $\widetilde{\mathbf{B}} = \mathbf{K} \otimes_{\mathbf{A}} \mathbf{B}$.
This means that the iterated boundary ideal $\mathcal{I}^{\mathrm{K}}_{\widetilde{\mathbf{B}}}(h_0, \dots, h_n)$ contains 1, and by getting rid of the denominators that $\mathcal{I}^{\mathrm{K}}_{\mathbf{B}}(h_0, \dots, h_n)$ contains some $a \in \operatorname{Reg}(\mathbf{A})$. Therefore the ring $\mathbf{B}_0 = \mathbf{B}/\mathcal{I}^{\mathrm{K}}_{\mathbf{B}}(h_0, \dots, h_n)$ is a quotient of $\mathbf{B}/a\mathbf{B} = \mathbf{A}/a\mathbf{A} \otimes_{\mathbf{A}} \mathbf{B}$. Since a is regular and $\mathsf{Kdim}\,\mathbf{A} \leqslant m$, the quotient $\mathbf{A}/a\mathbf{A}$ is of dimension at most $m-1$. The natural homomorphism $\mathbf{A}/a\mathbf{A} \to \mathbf{B}/a\mathbf{B}$ remains of dimension at most n (Lemma 7.2). Therefore, by induction hypothesis, the sequence $(h_{n+1}, \dots, h_p)$ is singular in $\mathbf{B}/a\mathbf{B}$. Therefore the sequence $(h_{n+1}, \dots, h_p)$ is singular in $\mathbf{B}_0$.
In conclusion, the ring $\mathbf{B}/\mathcal{I}^{\mathrm{K}}_{\mathbf{B}}(\underline{h}) = \mathbf{B}_0/\mathcal{I}^{\mathrm{K}}_{\mathbf{B}_0}(h_{n+1}, \dots, h_p)$ is trivial. □

7.14. Corollary. *Suppose* $\mathsf{Kdim}\,\mathbf{A} \leqslant m$*. Then*

$$\mathsf{Kdim}\,\mathbf{A}[X_1, \dots, X_n] \leqslant mn + m + n.$$

D We know that if $\mathbf{K}$ is reduced zero-dimensional, $\mathsf{Kdim}\,\mathbf{K}[X_1, \dots, X_n] \leqslant n$. Thus $\mathsf{Kdim}(\mathbf{A} \to \mathbf{A}[X_1, \dots, X_n]) \overset{\mathrm{def}}{=} \mathsf{Kdim}\,\mathbf{A}^\bullet[X_1, \dots, X_n] \leqslant n$. We apply Theorem 7.13. □

We dispose equally of a lower bound of $\mathsf{Kdim}\,\mathbf{A}[X_1, \dots, X_n]$.

7.15. Lemma. *For every nontrivial ring* $\mathbf{A}$ *and all* $n > 0$ *we have*

$$n + \mathsf{Kdim}\,\mathbf{A} \leqslant \mathsf{Kdim}\,\mathbf{A}[X_1, \dots, X_n].$$

More precisely, the following implication is satisfied for every $k \geqslant -1$ *and for every ring*

$$\mathsf{Kdim}\,\mathbf{A}[X_1, \dots, X_n] \leqslant n + k \implies \mathsf{Kdim}\,\mathbf{A} \leqslant k$$

D Immediate consequence of Proposition 2.16. □

7.16. Theorem. *Consider an algebra $\rho : \mathbf{A} \to \mathbf{B}$.*

1. *Suppose that $\mathbf{B}$ is generated by elements which are primitively algebraic over $\mathbf{A}$, then $\mathsf{Kdim}\,\rho \leqslant 0$ and so $\mathsf{Kdim}\,\mathbf{B} \leqslant \mathsf{Kdim}\,\mathbf{A}$.*
2. *If ρ is injective and $\mathbf{B}$ is integral over $\mathbf{A}$, then $\mathsf{Kdim}\,\mathbf{B} = \mathsf{Kdim}\,\mathbf{A}$.*

D *1.* Given Fact VII-1.3, the ring $\mathbf{A}^{\bullet} \otimes_{\mathbf{A}} \mathbf{B}$ is zero-dimensional, in other words $\mathsf{Kdim}\,\rho \leqslant 0$. The result follows by Theorem 7.13.
2. By item *1* and Proposition 4.1. □

For a more direct proof of the inequality $\mathsf{Kdim}\,\mathbf{B} \leqslant \mathsf{Kdim}\,\mathbf{A}$, see Exercise 10.

8. Valuative dimension

Dimension of valuation rings

Recall that a valuation ring is a reduced ring in which we have, for all a, b: a divides b or b divides a. In other words it is a Bézout and reduced local ring. A valuation ring is a normal, local ring without zerodivisors. It is integral if and only if it is coherent.

It is clear that the Zariski lattice of a valuation ring is a totally ordered set.

8.1. Fact. *In a distributive lattice if a subsequence of $(\underline{x}) = (x_1, \ldots, x_n)$ is singular, the sequence $(\underline{x})$ is singular.*

D We consider a singular sequence $(y_1, \ldots, y_r)$, with a complementary sequence $(b_1, \ldots, b_r)$. Let us add a term z to $(y_1, \ldots, y_r)$. To obtain a complementary sequence from it, we proceed as follows. If z is placed at the end, we add 1 at the end of $(b_1, \ldots, b_r)$. If z is placed at the start, we add 0 at the start of $(b_1, \ldots, b_r)$. If z is intercalated between y_i and y_{i+1} we intercalate b_i between b_i and b_{i+1}. □

8.2. Fact. *Let $(\underline{x}) = (x_1, \ldots, x_n)$ in a distributive lattice. If we have $x_1 = 0$, or $x_n = 1$, or $x_{i+1} \leqslant x_i$ for some $i \in [\![1..n-1]\!]$, then the sequence $(\underline{x})$ is singular.*

D We apply the previous fact by noting that (0) and (1) are two complementary sequences and that the sequence (x_i, x_{i+1}) with $x_{i+1} \leqslant x_i$ admits $(0, 1)$ as the complementary sequence. □

To recap: the constructive meaning of the phrase "the number of elements of E is bounded by k" (which we denote by $\#E \leqslant k$) is that for every finite list of $k + 1$ elements in E, two of them are equal.

8.3. Lemma. *For a* non-decreasing *sequence* $(\underline{a}) = (a_1, \ldots, a_n)$ *in a totally ordered lattice the following properties are equivalent.*

1. *The sequence is singular.*
2. $a_1 = 0$*, or* $a_n = 1$*, or there exists an* $i \in [\![1..n-1]\!]$ *such that* $a_i = a_{i+1}$*.*
3. *The number of elements in* $(0, a_1, \ldots, a_n, 1)$ *is bounded by* $n+1$*.*

D *1 ⇒ 2.* Let us do the computation for the case $n = 3$ by leaving the induction to the skeptical reader. Consider a complementary sequence (b_1, b_2, b_3). We have

$$\begin{array}{rcl} 1 & \leqslant & a_3 \vee b_3 \\ a_3 \wedge b_3 & \leqslant & a_2 \vee b_2 \\ a_2 \wedge b_2 & \leqslant & a_1 \vee b_1 \\ a_1 \wedge b_1 & \leqslant & 0 \end{array}$$

Thus, $a_1 = 0$ or $b_1 = 0$.
If $b_1 = 0$, then $a_1 \vee b_1 = a_1 \geqslant a_2 \wedge b_2$. Therefore $a_2 \leqslant a_1$ or $b_2 \leqslant a_1$. In the first case, $a_1 = a_2$. In the second case, $b_2 \leqslant a_1 \leqslant a_2$ therefore $a_2 \vee b_2 = a_2$. This implies $a_3 \leqslant a_2$ or $b_3 \leqslant a_2$. In the first case, $a_2 = a_3$. In the second case, $b_3 \leqslant a_2 \leqslant a_3$, therefore $a_3 \vee b_3 = a_3 = 1$.

2 ⇒ 1. By Fact 8.2.

3 ⇒ 2. If we have two equal elements in a non-decreasing sequence, then there are also two consecutively equal elements. □

The following theorem gives a precise and elementary constructive interpretation of the Krull dimension of a totally ordered set. It directly results from Fact 8.2 and from Lemma 8.3.

8.4. Theorem. *For a totally ordered distributive lattice* **T***, the following properties are equivalent.*

1. **T** *is of dimension at most* n*.*
2. *The number of elements of* **T** *is bounded by* $n+2$ *(*$\#\mathbf{T} \leqslant n+2$*).*
3. *For every non-decreasing sequence* $(x_0, \ldots, x_n)$ *in* **T***, we have* $x_0 = 0$*, or* $x_n = 1$*, or* $x_{i+1} = x_i$ *for some* $i \in [\![0, n-1]\!]$*.*

Note that the previous theorem applies to the Zariski lattice of a valuation ring. We now present two very simple and useful facts regarding valuation rings.

8.5. Fact. *In a valuation ring let* $u_1, \ldots, u_m$ *be elements with* $\sum_i u_i = 0$ *(and* $m \geqslant 2$*). Then there exists a* $j \neq k$ *and an invertible element* v *such that* $\langle u_1, \ldots, u_m \rangle = \langle u_j \rangle = \langle u_k \rangle$ *and* $vu_j = u_k$*.*

D First of all there exists a j such that $\langle u_1, \ldots, u_m \rangle = \langle u_j \rangle$. Then for each k let v_k be an element such that $u_k = v_k u_j$, with $v_j = 1$.
We obtain the equality $u_j(1 + \sum_{k \neq j} v_k) = 0$. Therefore $u_j = 0$ or $1 +$

$\sum_{k\neq j} v_k = 0$. If $u_j = 0$, we can take all the v_k's equal to 1.
If $1 + \sum_{k\neq j} v_k = 0$, one of the v_k's is invertible since $\mathbf{V}$ is local. □

8.6. Fact. *Let* $\mathbf{V}$ *be a valuation ring and a sequence* $(a_1, \ldots, a_n)$ *in* $\mathbf{V}^*$*. For exponents* p_i *all* > 0*, let* $a = \prod_{i=1}^n a_i^{p_i}$*. Then there exists some* $j \in [\![1..n]\!]$ *such that* $\mathrm{D}_{\mathbf{V}}(a) = \mathrm{D}_{\mathbf{V}}(a_j)$*.*

D Consider a j such that a_i divides a_j for all $i \in [\![1..n]\!]$. Then a_j divides a which divides a_j^p, where $p = \sum_{i=1}^n p_i$. □

We will need the following combinatorial lemma.

8.7. Lemma. *Let* $E \subseteq F$ *be two sets. We suppose that for every sequence* $(x_0, \ldots, x_m)$ *in* F*, one of the following two alternatives takes place*

- *there exist* $i < j \in [\![0..m]\!]$ *such that* $x_i = x_j$*,*
- *there exists an* $i \in [\![0..m]\!]$ *such that* $x_i \in E$*.*

Then $\#E \leqslant \ell$ *implies* $\#F \leqslant \ell + m$*.*

D We consider a sequence $(y_0, \ldots, y_{\ell+m})$ in F. We need to show that there are two equal terms. We consider the first $m+1$ terms. Either two of them are equal, and the case is closed, or one of the terms is in E. In this case, we delete the term which is in E from the sequence $(y_0, \ldots, y_{\ell+m})$ and we consider the first $m+1$ terms of this new sequence. Either two of them are equal, and the case is closed, or one of the terms is in E ... In the worst case, we follow the procedure till the end and we finally obtain $\ell + 1$ terms in E and two of them are equal. □

8.8. Theorem. *Let* $\mathbf{V}$ *be a valuation domain,* $\mathbf{K}$ *be its quotient field,* $\mathbf{L} \supseteq \mathbf{K}$ *be a discrete field of transcendence degree* $\leqslant m$ *over* $\mathbf{K}$*, and* $\mathbf{W} \supseteq \mathbf{V}$ *be a valuation ring of* $\mathbf{L}$*. Then* $\mathsf{Kdim}\,\mathbf{W} \leqslant \mathsf{Kdim}\,\mathbf{V} + m$*.*

D We need to show that if $\mathsf{Kdim}\,\mathbf{V} \leqslant n$, then $\mathsf{Kdim}\,\mathbf{W} \leqslant n + m$.
Since these are valuation rings, we must simply show that

$$\#\,\mathsf{Zar}\,\mathbf{V} \leqslant n+2 \text{ implies } \#\,\mathsf{Zar}\,\mathbf{W} \leqslant n+m+2.$$

(See Theorem 8.4.) It therefore suffices to show that the hypotheses of Lemma 8.7 are satisfied for the integers $\ell = n+2$ and m, and for the sets $E = \mathsf{Zar}\,\mathbf{V}$ and $F = \mathsf{Zar}\,\mathbf{W}$.
Let $\mathbf{V}' = \mathbf{W} \cap \mathbf{K}$. Since $\mathbf{V}'$ is a localized ring of $\mathbf{V}$, we have $\mathsf{Kdim}\,\mathbf{V}' \leqslant \mathsf{Kdim}\,\mathbf{V}$. We are thus brought back to the case where $\mathbf{V} = \mathbf{W} \cap \mathbf{K}$, which implies $\mathsf{Zar}\,\mathbf{V} \subseteq \mathsf{Zar}\,\mathbf{W}$.
Now let $x_0, \ldots, x_m \in \mathrm{Reg}\,\mathbf{W}$, denoted by $\mathbf{W}^*$.
Consider an algebraic dependence relation over $\mathbf{K}$ for $(x_0, \ldots, x_m)$. We can suppose that the coefficients of the polynomial $P \in \mathbf{K}[X_0, \ldots, X_m]$ which gives this algebraic dependence relation are in $\mathbf{V} \cap \mathbf{K}^\times = \mathbf{V}^*$. By letting, for $p \in \mathbb{N}^{m+1}$, $x^p = x_0^{p_0} \cdots x_m^{p_m}$, Fact 8.5 gives us p and q distinct in $\mathbb{N}^{m+1}$

such that ax^p and bx^q are associated in $\mathbf{W}$ with a, $b \in \mathbf{V}^*$. By simplifying by $x^{p \wedge q}$, we can assume $p \wedge q = 0$. Since a divides b or b divides a, we can assume that $b = 1$. We therefore have ax^p associated with x^q in $\mathbf{W}$. If $q = 0$, then each x_j contained in x^p (there is at least one) is invertible in $\mathbf{W}$, i.e. $\mathrm{D}_{\mathbf{W}}(x_j) = \mathrm{D}_{\mathbf{W}}(1)$. Otherwise, Fact 8.6 applied to x^q gives us some x_j present in x^q such that $\mathrm{D}_{\mathbf{W}}(x^q) = \mathrm{D}_{\mathbf{W}}(x_j)$; applied to ax^p, this tells us that $\mathrm{D}_{\mathbf{W}}(ax^p) = \mathrm{D}_{\mathbf{W}}(a)$ or $\mathrm{D}_{\mathbf{W}}(x_k)$ with x_k present in x^p; we therefore have $\mathrm{D}_{\mathbf{W}}(x_j) = \mathrm{D}_{\mathbf{W}}(a)$, or $\mathrm{D}_{\mathbf{W}}(x_j) = \mathrm{D}_{\mathbf{W}}(x_k)$. The proof is complete. □

Valuative dimension of a commutative ring

8.9. Definition.

1. If $\mathbf{A}$ is a pp-ring, the *valuative dimension* is defined as follows. Let $d \in \mathbb{N} \cup \{-1\}$ and $\mathbf{K} = \operatorname{Frac} \mathbf{A}$. We say that the valuative dimension of $\mathbf{A}$ is less than or equal to d and we write $\mathsf{Vdim}\, \mathbf{A} \leqslant d$ if for every finite sequence $(\underline{x})$ in $\mathbf{K}$ we have $\mathsf{Kdim}\, \mathbf{A}[\underline{x}] \leqslant d$.
2. In the general case we define "$\mathsf{Vdim}\, \mathbf{A} \leqslant d$" by "$\mathsf{Vdim}\, \mathbf{A}_{\min} \leqslant d$."

We immediately have

- $\mathsf{Kdim}\, \mathbf{A} \leqslant \mathsf{Vdim}\, \mathbf{A}$,
- $\mathsf{Vdim}\, \mathbf{A} = -1$ if and only if $\mathbf{A}$ is trivial,
- $\mathsf{Vdim}\, \mathbf{A} \leqslant 0$ if and only if $\mathsf{Kdim}\, \mathbf{A} \leqslant 0$,
- if $\mathbf{A}$ is a pp-ring then
  - $\mathsf{Kdim}\, \mathbf{A} = \mathsf{Vdim}\, \mathbf{A}$ if and only if $\mathsf{Kdim}\, \mathbf{B} \leqslant \mathsf{Kdim}\, \mathbf{A}$ for every intermediary ring $\mathbf{B}$ between $\mathbf{A}$ and $\operatorname{Frac} \mathbf{A}$,
  - if $\mathbf{B}$ is intermediary between $\mathbf{A}$ and $\operatorname{Frac} \mathbf{A}$, we have $\mathsf{Vdim}\, \mathbf{B} \leqslant \mathsf{Vdim}\, \mathbf{A}$.

The following fact results directly from the construction of $\mathbf{A}_{\min}$.

8.10. Fact. *If $\mathbf{A}$ is an arithmetic ring, then so is $\mathbf{A}_{\min}$.*

8.11. Lemma. *If $\mathbf{A}$ is an arithmetic ring, we have $\mathsf{Kdim}\, \mathbf{A} = \mathsf{Vdim}\, \mathbf{A}$.*

D Since $\mathsf{Kdim}\, \mathbf{A} = \mathsf{Kdim}\, \mathbf{A}_{\min}$, and since $\mathbf{A}_{\min}$ is an arithmetic ring if $\mathbf{A}$ is arithmetic, it suffices to treat the case where $\mathbf{A}$ is a pp-ring. We then apply Theorem XII-4.8 which says that every element of $\operatorname{Frac} \mathbf{A}$ is primitively algebraic over $\mathbf{A}$, and Theorem 7.16 which says that in such a case $\mathsf{Kdim}\, \mathbf{B} \leqslant \mathsf{Kdim}\, \mathbf{A}$ for every intermediary ring $\mathbf{B}$ between $\mathbf{A}$ and $\operatorname{Frac} \mathbf{A}$.□

Remark. Here is the end of a less scholarly proof (for the case where $\mathbf{A}$ is an arithmetic pp-ring). We first suppose that $\mathbf{A}$ is local, i.e. it is an integral valuation ring. For every $x = a/b \in \operatorname{Frac} \mathbf{A}$, we have the alternative: b divides a, in which case $x \in \mathbf{A}$, or a divides b, that is, $ac = b$ in which case c

is regular and $x = 1/c$ such that $\mathbf{A}[x]$ is a localized valuation ring of $\mathbf{A}$, so $\mathsf{Kdim}\,\mathbf{A}[x] \leqslant \mathsf{Kdim}\,\mathbf{A}$. We finish by induction on the number of elements of $\mathrm{Frac}\,\mathbf{A}$ which we add to $\mathbf{A}$. Finally, in the general case, we re-express the previous proof. We replace the alternative "b divides a or a divides b" by the creation of two comaximal localizations of $\mathbf{A}$. In the first b divides a, in the second a divides b. ■

8.12. Lemma. *Let* $\mathbf{A}$ *be an integral ring,* $n \geqslant 1$ *and* $k \geqslant -1$.
If $\mathsf{Kdim}\,\mathbf{A}[X_1, \ldots, X_n] \leqslant n + k$, *then for all* $x_1, \ldots, x_n$ *in* $\mathrm{Frac}\,\mathbf{A}$, *we have* $\mathsf{Kdim}\,\mathbf{A}[x_1, \ldots, x_n] \leqslant k$.

D We introduce the intermediary rings

$$\mathbf{B}_0 = \mathbf{A}[X_1, \ldots, X_n],\ \mathbf{B}_1 = \mathbf{A}[x_1, X_2, \ldots, X_n],\ \ldots,\ \mathbf{B}_n = \mathbf{A}[x_1, \ldots, x_n].$$

For $i \in [\![1..n]\!]$, let φ_i be the homomorphism of evaluation $\mathbf{B}_{i-1} \to \mathbf{B}_i$ defined by $X_i \mapsto x_i$. If $x_i = a_i/b_i$, the kernel $\mathrm{Ker}\,\varphi_i$ contains $f_i = b_i X_i - a_i$.
Let $i \in [\![0..n-1]\!]$. Since $b_{i+1} \in \mathrm{Reg}\,\mathbf{A}[(x_j)_{1 \leqslant j \leqslant i}]$, we have $f_{i+1} \in \mathrm{Reg}\,\mathbf{B}_i$ (McCoy's lemma, Corollary III-2.3). Therefore, by item *5* of Proposition 3.1, we have $\mathsf{Kdim}\,\mathbf{B}_i/\langle f_{i+1}\rangle \leqslant \mathsf{Kdim}\,\mathbf{B}_i - 1$. Finally, since $\mathbf{B}_{i+1}$ is a quotient of $\mathbf{B}_i/\langle f_{i+1}\rangle$, we obtain $\mathsf{Kdim}\,\mathbf{B}_{i+1} \leqslant \mathsf{Kdim}\,\mathbf{B}_i - 1$. □

In the following proposition, as we will see a little later, the three properties are actually equivalent (Theorem 8.19 item *2*).

8.13. Proposition. *Let* $\mathbf{A}$ *be an integral ring and* $n \geqslant 1$, *then we have for the following items the implications 1 ⇒ 2 ⇒ 3.*

1. *We have* $\mathsf{Kdim}\,\mathbf{A}[X_1, \ldots, X_n] \leqslant 2n$.
2. *For all* $x_1, \ldots, x_n$ *in* $\mathrm{Frac}\,\mathbf{A}$, *we have* $\mathsf{Kdim}\,\mathbf{A}[x_1, \ldots, x_n] \leqslant n$.
3. *We have* $\mathsf{Vdim}\,\mathbf{A} \leqslant n$.

D *1* ⇒ *2.* Special case of Lemma 8.12.

2 ⇒ *3.* We consider an arbitrary sequence $(y_1, \ldots, y_r)$ in $\mathrm{Frac}\,\mathbf{A}$, then an arbitrary sequence $(x_0, \ldots, x_n)$ in $\mathbf{B} = \mathbf{A}[y_1, \ldots, y_r]$. We need to prove that the sequence $(x_0, \ldots, x_n)$ is singular in $\mathbf{B}$. It suffices to show that it is singular in $\mathbf{C} = \mathbf{A}[x_0, \ldots, x_n]$, or that the sequence $(x_1, \ldots, x_n)$ is singular in $\mathbf{C}/\mathcal{I}^{\mathrm{K}}_{\mathbf{C}}(x_0)$.
We write $x_0 = a_0/b_0$ with $b_0 \in \mathrm{Reg}\,\mathbf{A}$. If $a_0 = 0$, we are done.
If a_0 is regular, then $\mathcal{I}^{\mathrm{K}}_{\mathbf{C}}(x_0) = x_0\mathbf{C} \supseteq a_0\mathbf{C}$. Therefore $\mathbf{C}/\mathcal{I}^{\mathrm{K}}_{\mathbf{C}}(x_0)$ is a quotient of $\mathbf{C}/\langle a_0\rangle$ which is equal to $\mathbf{A}[x_1, \ldots, x_n]/\langle a_0\rangle$, which is of dimension at most $n-1$. Thus $\mathbf{C}/\mathcal{I}^{\mathrm{K}}_{\mathbf{C}}(x_0)$ is of dimension at most $n-1$, and the sequence $(x_1, \ldots, x_n)$ is singular in $\mathbf{C}/\mathcal{I}^{\mathrm{K}}_{\mathbf{C}}(x_0)$. □

Valuative dimension of a polynomial ring

The aim of this subsection is to prove the equality

$$\boxed{\mathsf{Vdim}\,\mathbf{A}[X_1,\dots,X_n] = n + \mathsf{Vdim}\,\mathbf{A}},$$

for all $n \geqslant 1$. We deduce the same equality for the Krull dimensions in the case of an arithmetic ring.

By definition, this equality of dimensions means the following equivalence

$$\boxed{\forall k \geqslant -1,\ \ \mathsf{Vdim}\,\mathbf{A} \leqslant k \iff \mathsf{Vdim}\,\mathbf{A}[X_1,\dots,X_n] \leqslant n+k}. \tag{24}$$

Thus the first framed equality does not quite stick for the trivial ring (we should say that the dimension of the trivial ring is $-\infty$ rather than -1).

Preliminary remark. Given that $\mathsf{Vdim}\,\mathbf{A} = \mathsf{Vdim}\,\mathbf{A}_{\min}$ by definition, and that $\mathbf{A}_{\min}[X_1,\dots,X_n] \simeq (\mathbf{A}[X_1,\dots,X_n])_{\min}$ (Fact 7.10), it suffices to treat the case where $\mathbf{A}$ is a pp-ring, and by the elementary local-global machinery of pp-rings, it suffices to treat the integral case. In the rest of the subsection, we will therefore sometimes use the saving phrase “we can without loss of generality suppose that the ring is integral,” or sometimes, if we want to explain the functioning of the elementary local-global machinery, “we can without loss of generality suppose that the ring is a pp-ring.” ■

8.14. Fact. *In* (24)*, the converse implication (from right to left) is correct.*

D Suppose without loss of generality that $\mathbf{A}$ is integral.
Let $[\underline{X}] = [X_1,\dots,X_n]$. Suppose $\mathsf{Vdim}\,\mathbf{A}[\underline{X}] \leqslant n+k$. Let $\mathbf{B} = \mathbf{A}[y_1,\dots,y_r]$, with $y_i \in \operatorname{Frac}\mathbf{A}$ for $i \in [\![1..n]\!]$. We want to prove that $\mathsf{Kdim}\,\mathbf{B} \leqslant k$.
However, $\mathbf{B}[\underline{X}] = \mathbf{A}[\underline{X}][y_1,\dots,y_r]$ with the y_i's in $\operatorname{Frac}(\mathbf{A}[\underline{X}])$.
Therefore $\mathsf{Kdim}\,\mathbf{B}[\underline{X}] \leqslant n+k$, and by Lemma 7.15, $\mathsf{Kdim}\,\mathbf{B} \leqslant k$. □

We now study the difficult direct implication in (24). In classical mathematics we have the following result:
$(*)$ *the valuative dimension of an integral ring* $\mathbf{A}$ *is also the maximum of the dimensions of valuation rings containing* $\mathbf{A}$ *and contained in its quotient field.*

This affirmation $(*)$ is no longer true in general from a constructive point of view (by lack of valuation rings), but it is a direct consequence (in classical mathematics) of Corollary 8.17, which is therefore a constructive version of $(*)$.

8.15. Lemma. *Let x_0, x_1, …, x_ℓ, u, v, α be indeterminates over a ring $\mathbf{A}$, $P_0(\alpha)$, …, $P_\ell(\alpha) \in \mathbf{A}[\alpha]$ and $Q_0(\alpha^{-1})$, …, $Q_\ell(\alpha^{-1}) \in \mathbf{A}[\alpha^{-1}]$. For some m_i, $n_i \in \mathbb{N}$, we define $P = P(\alpha)$ and $Q = Q(\alpha^{-1})$ as follows*

$$\begin{aligned} P &= x_0^{m_0}(x_1^{m_1}(\cdots(x_\ell^{m_\ell}(u + P_\ell(\alpha)x_\ell) + \cdots) + P_1(\alpha)x_1) + P_0(\alpha)x_0), \\ Q &= x_0^{n_0}(x_1^{n_1}(\cdots(x_\ell^{n_\ell}(v + Q_\ell(\alpha^{-1})x_\ell) + \cdots) + Q_1(\alpha^{-1})x_1) + Q_0(\alpha^{-1})x_0). \end{aligned}$$

If P is of formal degree p (in α), Q of formal degree q (in α^{-1}), we consider the resultant

$$R = \mathrm{Res}_\alpha(\alpha^q Q, q, P, p) \in \mathbf{A}[x_0, \dots, x_\ell, u, v].$$

Then, by letting $r_i = qm_i + pn_i$ and $w = u^q v^p$, R is of the form

$$R = x_0^{r_0}(x_1^{r_1}(\cdots(x_\ell^{r_\ell}(w + a_\ell x_\ell) + \cdots) + a_1 x_1) + a_0 x_0) \quad \textit{with } a_i \in \mathbf{A}[\underline{x}, u, v].$$

D Writing $\mathrm{Res}_{\alpha,q,p}(U, V)$ in place of $\mathrm{Res}_\alpha(U, q, V, p)$, we suppose $n = 1$ and we let $x = x_0$, $y = x_1$, such that $P = x^{m_0} S$, $\alpha^q Q = x^{n_0} T$, with

$$S = y^{m_1}(u + P_1(\alpha)y) + P_0(\alpha)x, \quad T = y^{n_1}(v\alpha^q + T_1(\alpha)y) + T_0(\alpha)x.$$

We obtain $R = x^{r_0}\mathrm{Res}_{\alpha,q,p}(T, S)$, $r_0 = qm_0 + pn_0$. By letting $x := 0$ we have

$$\begin{aligned} \mathrm{Res}_{\alpha,q,p}(T, S)_{x:=0} &= \mathrm{Res}_{\alpha,q,p}(T_{x:=0}, S_{x:=0}) \\ &= \mathrm{Res}_{\alpha,q,p}\big(y^{n_1}(v\alpha^q + T_1(\alpha)y), y^{m_1}(u + P_1(\alpha)y)\big) \\ &= y^{r_1}\mathrm{Res}_{\alpha,q,p}(v\alpha^q + T_1(\alpha)y, u + P_1(\alpha)y), \end{aligned}$$

with $r_1 = qm_1 + pn_1$. By letting $y := 0$ we have

$$\mathrm{Res}_{\alpha,q,p}(v\alpha^q + T_1(\alpha)y, u + P_1(\alpha)y)_{y:=0} = \mathrm{Res}_{\alpha,q,p}(v\alpha^q, u) = u^q v^p,$$

which gives the stated result. □

8.16. Proposition. *Let $\mathbf{A} \subseteq \mathbf{B}$, $(\underline{x}) = (x_0, \dots, x_n)$ be a sequence in $\mathbf{A}$ and α_0, β_0 in $\mathbf{B}$ such that $\alpha_0\beta_0 = 1$. Suppose that the sequence is singular in $\mathbf{A}[\alpha_0]$ and $\mathbf{A}[\beta_0]$, then it is singular in $\mathbf{A}$.*

D We apply the previous lemma by specializing u and v in 1. Since the polynomials $P(\alpha)$ and $\alpha^q Q(\alpha^{-1})$ have a common root α_0 in $\mathbf{B}$, their resultant is null (Lemma III-7.2). □

8.17. Corollary. *Let a and b be regular elements of a pp-ring $\mathbf{A}$. Then $\mathsf{Vdim}\,\mathbf{A} = \sup\big(\mathsf{Vdim}\,\mathbf{A}[\frac{a}{b}], \mathsf{Vdim}\,\mathbf{A}[\frac{b}{a}]\big)$.*

D The inequalities $\mathsf{Vdim}\,\mathbf{A}[\frac{a}{b}] \leqslant \mathsf{Vdim}\,\mathbf{A}$ and $\mathsf{Vdim}\,\mathbf{A}[\frac{b}{a}] \leqslant \mathsf{Vdim}\,\mathbf{A}$ result from the definition of the valuative dimension.
Finally, suppose that $\mathsf{Vdim}\,\mathbf{A}[\frac{a}{b}] \leqslant n$ and $\mathsf{Vdim}\,\mathbf{A}[\frac{b}{a}] \leqslant n$ for some $n \in \mathbb{N}$. Let $(x_0, \dots, x_n)$ be a sequence in $\mathbf{A}$. It is singular in $\mathsf{Vdim}\,\mathbf{A}[\frac{a}{b}]$ and $\mathsf{Vdim}\,\mathbf{A}[\frac{b}{a}]$, therefore it is singular in $\mathbf{A}$ by Proposition 8.16. □

8.18. Proposition. *For every ring* $\mathbf{A}$ *and all* $n \geqslant 1$*, we have*

$$\mathsf{Vdim}\,\mathbf{A}[X_1,\dots,X_n] \leqslant n + \mathsf{Vdim}\,\mathbf{A}.$$

D We need to show that if $\mathsf{Vdim}\,\mathbf{A} \leqslant k$ then $\mathsf{Vdim}\,\mathbf{A}[X_1,\dots,X_m] \leqslant k+m$. By Fact 7.10, it suffices to treat the case where $\mathbf{A}$ is a pp-ring.
We first suppose that $\mathbf{A}$ is integral. We re-express the proof of Theorem 8.8 and we use the dynamic method. Each time that we have a disjunction of the type "a divides b or b divides a" we introduce the rings $\mathbf{C}[\frac{a}{b}]$ and $\mathbf{C}[\frac{b}{a}]$, where $\mathbf{C}$ is the "current" ring. At each leaf of the tree constructed thus we have a ring $\mathbf{A}[u_1,\dots,u_\ell] \subseteq \operatorname{Frac}\mathbf{A}$ in which the considered sequence is singular. We conclude by Proposition 8.16 that the sequence is singular in $\mathbf{A}$.
In the case where $\mathbf{A}$ is a pp-ring we can call upon the elementary local-global machinery of pp-rings. We can also reason more directly: a and b produce the decomposition of "the current ring" $\mathbf{C}$ in a product of four components. In three of them, a or b is null and everything is easy. In the fourth one, a and b are regular and we are brought back to the integral case. □

As corollaries we obtain the following theorems.

8.19. Theorem. *For a ring* $\mathbf{A}$*, we have the following equivalences.*

1. *If* $n \geqslant 1$ *and* $k \geqslant -1$*, then*
$$\mathsf{Vdim}\,\mathbf{A} \leqslant k \iff \mathsf{Vdim}\,\mathbf{A}[X_1,\dots,X_n] \leqslant n+k.$$
In other words, $\mathsf{Vdim}\,\mathbf{A}[X_1,\dots,X_n] = n + \mathsf{Vdim}\,\mathbf{A}$.
2. *If* $n \geqslant 0$*, then*
$$\mathsf{Vdim}\,\mathbf{A} \leqslant n \iff \mathsf{Kdim}\,\mathbf{A}[X_1,\dots,X_n] \leqslant 2n.$$
In the case where $\mathbf{A}$ *is a pp-ring, it is also equivalent to: for all* x_1*, …,* x_n *in* $\operatorname{Frac}\mathbf{A}$*, we have* $\mathsf{Kdim}\,\mathbf{A}[x_1,\dots,x_n] \leqslant n$.

D *1.* Proved in Fact 8.14 and Proposition 8.18.
2. The case $n = 0$ has already been done. Let us look at the case $n \geqslant 1$. The direct implication results from item *1* because $\mathsf{Kdim}\,\mathbf{A}[X_1,\dots,X_n] \leqslant \mathsf{Vdim}\,\mathbf{A}[X_1,\dots,X_n]$. The converse implication is given (in the integral case, but it is not restrictive) in Proposition 8.13. □

8.20. Theorem.

1. *If* $\mathbf{A}$ *is an arithmetic ring of finite Krull dimension we have*
$$\mathsf{Vdim}\,\mathbf{A}[X_1,\dots,X_n] = \mathsf{Kdim}\,\mathbf{A}[X_1,\dots,X_n] \leqslant n + \mathsf{Kdim}\,\mathbf{A}.$$
with equality if $\mathbf{A}$ *is nontrivial.*
2. $\mathsf{Vdim}\,\mathbb{Z}[X_1,\dots,X_n] = \mathsf{Kdim}\,\mathbb{Z}[X_1,\dots,X_n] = 1+n.$
3. *Every ring generated by* n *elements is of valuative dimension (therefore of Krull dimension)* $\leqslant 1+n$.

4. Let $\mathbf{A}$ *be a pp-ring generated by* n *elements and* $\mathbf{B}$ *be an intermediary ring between* $\mathbf{A}$ *and* $\operatorname{Frac}\mathbf{A}$. *Then* $\mathsf{Vdim}\,\mathbf{B} \leqslant 1+n$.

D Item *1* results from the most general theorem (Theorem 8.21) and item *2* is a special case.

3. The ring $\mathbf{A}$ is a quotient of $\mathbb{Z}[X_1,\dots,X_n]$, so $\mathbf{A}[Y_1,\dots,Y_{n+1}]$ is a quotient of $\mathbb{Z}[X_1,\dots,X_n][Y_1,\dots,Y_{n+1}]$ which is of Krull dimension $2n+2$ by item *2* Therefore $\mathsf{Vdim}\,\mathbf{A} \leqslant n+1$ by item *2* of Theorem 8.19.

4. Consequence of item *3* since $\mathsf{Vdim}\,\mathbf{A} \leqslant n+1$. □

8.21. Theorem. *For a ring* $\mathbf{A}$ *of dimension at most* n *(*$n \geqslant 1$*) the following properties are equivalent.*

1. $\mathsf{Vdim}\,\mathbf{A} = \mathsf{Kdim}\,\mathbf{A}$.
2. *For all* $k \geqslant 1$, $\mathsf{Kdim}(\mathbf{A}[X_1,\dots,X_k]) \leqslant k + \mathsf{Kdim}\,\mathbf{A}$.
3. $\mathsf{Kdim}(\mathbf{A}[X_1,\dots,X_n]) \leqslant n + \mathsf{Kdim}\,\mathbf{A}$.

Morevover if $\mathbf{A}$ *is nontrivial we can replace* $\leqslant$ *by* $=$ *in items 2 and 3. When* $\mathsf{Vdim}\,\mathbf{A} = \mathsf{Kdim}\,\mathbf{A}$, *for all* $k \geqslant 1$, *we have the equality*

$$\mathsf{Kdim}(\mathbf{A}[X_1,\dots,X_k]) = \mathsf{Vdim}(\mathbf{A}[X_1,\dots,X_k]).$$

D Note that we do not assume that the Krull dimension of $\mathbf{A}$ is exactly known.

1 ⇒ *2.* We fix some $k \geqslant 1$ and we need to show that for every $m \geqslant -1$, we have $\mathsf{Kdim}\,\mathbf{A} \leqslant m \Rightarrow \mathsf{Kdim}(\mathbf{A}[X_1,\dots,X_k]) \leqslant m+k$.

We have $\mathsf{Vdim}(\mathbf{A}) \leqslant m$, so $\mathsf{Vdim}(\mathbf{A}[X_1,\dots,X_k]) \leqslant m+k$ by Proposition 8.18, therefore $\mathsf{Kdim}(\mathbf{A}[X_1,\dots,X_k]) \leqslant m+k$ because we still have $\mathsf{Kdim}\,\mathbf{B} \leqslant \mathsf{Vdim}\,\mathbf{B}$.

2 ⇒ *3.* This is the special case where $k = n$.

3 ⇒ *1.* Suppose $\mathsf{Kdim}\,\mathbf{A} \leqslant m$ and we need to show $\mathsf{Vdim}\,\mathbf{A} \leqslant m$. Without loss of generality $0 \leqslant m \leqslant n$. If $m = n$ the result follows by item *2* of Theorem 8.19. If $n = m + r$, we have $\mathsf{Kdim}(\mathbf{A}[X_1,\dots,X_n]) \leqslant n + m$ by hypothesis. As $(X_{m+1},\dots,X_n)$ is singular of length r, item *3* of Proposition 2.16 gives us $\mathsf{Kdim}(\mathbf{A}[X_1,\dots,X_m]) \leqslant n+m-r = 2m$ and the result follows by item *2* of Theorem 8.19.

The last statement is left to the reader. □

9. Lying Over, Going Up and Going Down

In this section we are interested in understanding in constructive terms certain properties of commutative rings and of their morphisms which are introduced in classical mathematics via the notions of Zariski spectrum or of spectral morphism (corresponding to a ring homomorphism).

As the goal of the current book is to develop the constructive framework, we will not prove that the elementary definitions that we propose are equivalent to the definitions usually given in classical mathematics.

By making our constructive definitions work we hope to obtain constructive versions of several theorems of classical mathematics, truly usable in practice. Actually, it is what will happen systematically in the following chapters.

Lifting prime ideals (Lying Over)

In classical mathematics we say that a homomorphism $\alpha : \mathbf{T} \to \mathbf{V}$ of distributive lattices "has the lifting property of prime ideals" when the dual homomorphism $\mathsf{Spec}\,\alpha : \mathsf{Spec}\,\mathbf{V} \to \mathsf{Spec}\,\mathbf{T}$ is surjective, in other words when every prime ideal of $\mathsf{Spec}\,\mathbf{T}$ is the inverse image of a prime ideal of $\mathsf{Spec}\,\mathbf{V}$. To abbreviate we also say that the morphism is "Lying Over." We will give a pertinent constructive definition without using the dual homomorphism. For the equivalence in classical mathematics with the definition via the spectra, see Exercise 23.

9.1. Definition.

1. A homomorphism $\alpha : \mathbf{T} \to \mathbf{V}$ of distributive lattices is said to be *Lying Over* when it is injective. It amounts to the same to say that α reflects ineqalities: for all $a, b \in \mathbf{T}$, $\alpha(a) \leqslant \alpha(b)$ implies $a \leqslant b$.
2. A commutative ring homomorphism $\varphi : \mathbf{A} \to \mathbf{B}$ is said to be *Lying Over* when the homomorphism $\mathsf{Zar}\,\varphi : \mathsf{Zar}\,\mathbf{A} \to \mathsf{Zar}\,\mathbf{B}$ is injective.

Remark. We also have the following equivalent formulations for the Lying Over morphisms.

- For the distributive lattices:
  - For all $b \in \mathbf{T}$, $\alpha^{-1}\big(\downarrow\alpha(b)\big) = \downarrow b$.
  - For every ideal $\mathfrak{a}$ of $\mathbf{T}$, $\alpha^{-1}\big(\mathcal{I}_{\mathbf{V}}(\alpha(\mathfrak{a}))\big) = \mathfrak{a}$.
- For the commutative rings:
  - For all the finitely generated ideals $\mathfrak{a}$, $\mathfrak{b}$ of $\mathbf{A}$ we have the implication
$$\varphi(\mathfrak{a}) \subseteq \varphi(\mathfrak{b})\mathbf{B} \implies \mathfrak{a} \subseteq \mathrm{D}_{\mathbf{A}}(\mathfrak{b}).$$
  - For every finitely generated ideal $\mathfrak{a}$ of $\mathbf{A}$ we have $\varphi^{-1}(\langle\varphi(\mathfrak{a})\rangle) \subseteq \mathrm{D}_{\mathbf{A}}(\mathfrak{a})$.
  - For every ideal $\mathfrak{a}$ of $\mathbf{A}$ we have $\varphi^{-1}\big(\mathrm{D}_{\mathbf{B}}(\langle\varphi(\mathfrak{a})\rangle)\big) = \mathrm{D}_{\mathbf{A}}(\mathfrak{a})$. ■

9.2. Fact. *Let $\mathbf{B} \supseteq \mathbf{A}$ be an extension. If $\mathbf{B}$ is integral or faithfully flat (over $\mathbf{A}$), the inclusion morphism $\mathbf{A} \to \mathbf{B}$ is Lying Over.*

D The first case is a simple reformulation of Lemma VI-3.12 (Lying Over). In the second case, for every finitely generated ideal $\mathfrak{a}$ of $\mathbf{A}$, we have $\mathfrak{a}\mathbf{B} \cap \mathbf{A} = \mathfrak{a}$. □

Going Up

In classical mathematics we say that a homomorphism $\alpha : \mathbf{T} \to \mathbf{V}$ of distributive lattices "has the going up property for chains of prime ideals" when we have the following property.

If $\mathfrak{q} \in \mathsf{Spec}\,\mathbf{V}$ *and* $\alpha^{-1}(\mathfrak{q}) = \mathfrak{p}$*, every chain* $\mathfrak{p}_1 \subseteq \cdots \subseteq \mathfrak{p}_n$ *of prime ideals of* $\mathsf{Spec}\,\mathbf{T}$ *with* $\mathfrak{p}_1 = \mathfrak{p}$ *is the inverse image of a chain* $\mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_n$ *of prime ideals of* $\mathsf{Spec}\,\mathbf{V}$ *with* $\mathfrak{q}_1 = \mathfrak{q}$.

Naturally we could limit ourselves to the case $n = 2$. In this case the definition can be reread in the following way.

If $\mathfrak{q} \in \mathsf{Spec}\,\mathbf{V}$ *and* $(\mathsf{Spec}\,\alpha)(\mathfrak{q}) = \mathfrak{p}$*, and if we note*

$$\alpha' : (\mathbf{V}/(\mathfrak{q} = 0) \to \mathbf{T}/(\mathfrak{p} = 0)$$

the induced morphism, then the dual morphism

$$\mathsf{Spec}\,\alpha' : \mathsf{Spec}(\mathbf{V}/(\mathfrak{q} = 0)) \to \mathsf{Spec}(\mathbf{T}/(\mathfrak{p} = 0))$$

is onto.

So we come back to the Lying Over.

Here are the constructive definitions in terms of distributive lattices and of commutative rings.

9.3. Definition.

1. A homomorphism $\alpha : \mathbf{T} \to \mathbf{V}$ of distributive lattices is said to be *Going Up* when for all $a, c \in \mathbf{T}$ and $y \in \mathbf{V}$ we have
$$\alpha(a) \leqslant \alpha(c) \vee y \quad \Longrightarrow \quad \exists x \in \mathbf{T}\ (a \leqslant c \vee x \quad \text{and} \quad \alpha(x) \leqslant y).$$
2. A homomorphism $\varphi : \mathbf{A} \to \mathbf{B}$ of commutative rings is said to be *Going Up* when the homomorphism $\mathsf{Zar}\,\varphi : \mathsf{Zar}\,\mathbf{A} \to \mathsf{Zar}\,\mathbf{B}$ is Going Up.

Remarks. 1) For item *1*, if $\mathfrak{a} = \alpha^{-1}(0_\mathbf{V})$ and $\mathbf{T}_1 = \mathbf{T}/(\mathfrak{a} = 0)$, then α is Going Up if and only if $\alpha_1 : \mathbf{T}_1 \to \mathbf{V}$ is going up.
For item *2*, if $\mathbf{T} = \mathsf{Zar}\,\mathbf{A}$, then $\mathbf{T}_1 \simeq \mathsf{Zar}\big(\varphi(\mathbf{A})\big)$. We deduce, by letting $\mathbf{A}_1 = \varphi(\mathbf{A})$, that φ is Going Up if and only if $\varphi_1 : \mathbf{A}_1 \to \mathbf{B}$ is going up.

2) For the distributive lattices, if $\alpha^{-1}(0) = 0$ and if α is Going Up, then it is Lying Over. For the commutative rings, if $\operatorname{Ker}\varphi \subseteq \mathrm{D}_\mathbf{A}(0)$ and if φ is Going Up, then it is Lying Over. ■

9.4. Proposition. *If* $\mathbf{B}$ *is an integral* $\mathbf{A}$*-algebra, the morphism* $\mathbf{A} \to \mathbf{B}$ *is Going Up.*

D By the previous remark we can assume $\mathbf{A} \subseteq \mathbf{B}$. We then know that the homomorphism is Lying Over, that is we know that $\mathsf{Zar}\,\mathbf{A} \to \mathsf{Zar}\,\mathbf{B}$ is injective, so we can identify $\mathsf{Zar}\,\mathbf{A}$ with a sublattice of $\mathsf{Zar}\,\mathbf{B}$. We need to show that given $a_1, \ldots, a_n, c_1, \ldots, c_q$ in $\mathbf{A}$ and $y_1, \ldots, y_p$ in $\mathbf{B}$ satisfying

$$\mathrm{D}_{\mathbf{B}}(\underline{a}) \leqslant \mathrm{D}_{\mathbf{B}}(\underline{c}) \vee \mathrm{D}_{\mathbf{B}}(\underline{y}),$$

we can find a sequence $(\underline{x})$ in $\mathbf{A}$ such that

$$\mathrm{D}_{\mathbf{A}}(\underline{a}) \leqslant \mathrm{D}_{\mathbf{A}}(\underline{c}) \vee \mathrm{D}_{\mathbf{A}}(\underline{x}) \text{ and } \mathrm{D}_{\mathbf{B}}(\underline{x}) \leqslant \mathrm{D}_{\mathbf{B}}(\underline{y}).$$

Let $\mathfrak{b} = \mathrm{D}_{\mathbf{B}}(\underline{y})$, $\mathfrak{a} = \mathfrak{b} \cap \mathbf{A}$, $\mathbf{B}_1 = \mathbf{B}/\mathfrak{b}$ and $\mathbf{A}_1 = \mathbf{A}/\mathfrak{a}$. We consider the integral extension $\mathbf{B}_1 \supseteq \mathbf{A}_1$. The hypothesis is now that $\mathrm{D}_{\mathbf{B}_1}(\underline{a}) \leqslant \mathrm{D}_{\mathbf{B}_1}(\underline{c})$. By Lying Over we know that this implies that $\mathrm{D}_{\mathbf{A}_1}(\underline{a}) \leqslant \mathrm{D}_{\mathbf{A}_1}(\underline{c})$. This means that for each $i \in [\![1..n]\!]$ we have some $x_i \in \mathfrak{a}$ such that $\mathrm{D}_{\mathbf{A}}(a_i) \leqslant \mathrm{D}_{\mathbf{A}}(\underline{c}) \vee \mathrm{D}_{\mathbf{A}}(x_i)$. We have therefore attained the sought goal with $(\underline{x}) = (x_1, \ldots, x_n)$. □

Going Down

In classical mathematics we say that a homomorphism $\alpha : \mathbf{T} \to \mathbf{V}$ of distributive lattices "has the going down property for chains of prime ideals" when the opposite morphism $\alpha^\circ : \mathbf{T}^\circ \to \mathbf{V}^\circ$ is Going Up. In other words we have the following property.

If $\mathfrak{q} \in \mathsf{Spec}\,\mathbf{V}$ *and* $\alpha^{-1}(\mathfrak{q}) = \mathfrak{p}$*, every chain* $\mathfrak{p}_1 \subseteq \cdots \subseteq \mathfrak{p}_n$ *of prime ideals of* $\mathsf{Spec}\,\mathbf{T}$ *with* $\mathfrak{p}_n = \mathfrak{p}$ *is the inverse image of a chain* $\mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_n$ *of prime ideals of* $\mathsf{Spec}\,\mathbf{V}$ *with* $\mathfrak{q}_n = \mathfrak{q}$.

Naturally we could limit ourselves to the case $n = 2$. And our constructive definition is the notion opposite to Going Up: we reverse the order relation.

9.5. Definition.

1. A homomorphism $\alpha : \mathbf{T} \to \mathbf{V}$ of distributive lattices is said to be *Going Down* when the same homomorphism for the opposite lattices $\mathbf{T}^\circ$ and $\mathbf{V}^\circ$ is Going Up. In other words for all $a, c \in \mathbf{T}$ and $y \in \mathbf{V}$ we have
$$\alpha(a) \geqslant \alpha(c) \wedge y \quad \Longrightarrow \quad \exists x \in \mathbf{T}\ (a \geqslant c \wedge x \quad \text{and} \quad \alpha(x) \geqslant y).$$
2. A homomorphism $\varphi : \mathbf{A} \to \mathbf{B}$ of commutative rings is said to be *Going Down* when the homomorphism $\mathsf{Zar}\,\varphi : \mathsf{Zar}\,\mathbf{A} \to \mathsf{Zar}\,\mathbf{B}$ is Going Down.

Remarks. 1) The definition in item 1 comes down to saying that the image by α of the conductor ideal $(a : c)_{\mathbf{T}}$ generates the ideal $\big(\alpha(a) : \alpha(c)\big)_{\mathbf{V}}$. So if the distributive lattices are Heyting algebras, it means that the lattice homomorphism is also a homomorphism of Heyting algebras.

2) Same remarks as for Going Up.
If $\mathfrak{f} = \alpha^{-1}(1_{\mathbf{V}})$ and $\mathbf{T}_2 = \mathbf{T}/(\mathfrak{f} = 1)$, then α is Going Down if and only if $\alpha_2 : \mathbf{T}_2 \to \mathbf{V}$ is Going Down.
This gives for the commutative rings: if $S = \varphi^{-1}(\mathbf{B}^\times)$ and $\mathbf{A}_2 = \mathbf{A}_S$, then φ is Going Down if and only if $\varphi_2 : \mathbf{A}_2 \to \mathbf{B}$ is Going Down.
For the distributive lattices, if $\alpha^{-1}(1) = 1$ and α is Going Down, then it is Lying Over. For the commutative rings, if $\varphi^{-1}(\mathbf{B}^\times) \subseteq \mathbf{A}^\times$ and φ is Going Down, then it is Lying Over. ■

9.6. Theorem. *If a homomorphism $\alpha : X \to Y$ (of distributive lattices or of commutative rings) is Lying Over and Going Up, or if it is Lying Over and Going Down, we have* $\mathsf{Kdim}\, X \leqslant \mathsf{Kdim}\, Y$.

Remark. This is the case, for example, when the ring $\mathbf{B}$ is an integral extension of $\mathbf{A}$. We thus find Proposition 4.1 again. For the flat extensions, see Proposition 9.8. ■

D It suffices to treat the Going Up case with lattices.
Suppose $\mathsf{Kdim}\, Y \leqslant n$ and consider a sequence $(a_0, \dots, a_n)$ in X. We have in Y a complementary sequence $(y_0, \dots, y_n)$ of $\alpha(\underline{a})$

$$\alpha(a_0) \wedge y_0 \leqslant 0,\ \dots,\ \alpha(a_n) \wedge y_n \leqslant \alpha(a_{n-1}) \vee y_{n-1},\ 1 \leqslant \alpha(a_n) \vee y_n.$$

We will construct a complementary sequence $(x_0, \dots, x_n)$ of $(\underline{a})$ in X. At step n, by Going Up, there exists an $x_n \in X$ such that

$$1 \leqslant a_n \vee x_n \text{ and } \alpha(x_n) \leqslant y_n.$$

This gives at the stage $n-1$ the inequality: $\alpha(a_n \wedge x_n) \leqslant \alpha(a_{n-1}) \vee y_{n-1}$. By Going Up there exists an $x_{n-1} \in X$ such that

$$a_n \wedge x_n \leqslant a_{n-1} \vee x_{n-1} \text{ and } \alpha(x_{n-1}) \leqslant y_{n-1}.$$

We continue in the same way until stage 0, where this time we need to use the Lying Over. □

9.7. Lemma. *For a ring homomorphism $\varphi : \mathbf{A} \to \mathbf{B}$ to be Going Down it is necessary and sufficient that for all c, a_1, …, $a_q \in \mathbf{A}$ and $y \in \mathbf{B}$ such that $\varphi(c)y \in \mathrm{D}_{\mathbf{B}}(\varphi(\underline{a}))$, there exist some elements x_1, …, $x_m \in \mathbf{A}$ such that*

$$\mathrm{D}_{\mathbf{A}}(c) \wedge \mathrm{D}_{\mathbf{A}}(\underline{x}) \leqslant \mathrm{D}_{\mathbf{A}}(\underline{a}) \quad \textit{and} \quad \mathrm{D}_{\mathbf{B}}(y) \leqslant \mathrm{D}_{\mathbf{B}}(\varphi(\underline{x})).$$

D In the definition we have replaced an arbitrary element $\mathrm{D}_{\mathbf{A}}(\underline{c})$ of $\mathsf{Zar}\,\mathbf{A}$ and an arbitrary element $\mathrm{D}_{\mathbf{B}}(\underline{y})$ of $\mathsf{Zar}\,\mathbf{B}$ by generators $\mathrm{D}_{\mathbf{A}}(c)$ and $\mathrm{D}_{\mathbf{B}}(y)$. As the generators $\mathrm{D}_{\mathbf{A}}(c)$ (resp. $\mathrm{D}_{\mathbf{B}}(y)$) generate $\mathsf{Zar}\,\mathbf{A}$ (resp. $\mathsf{Zar}\,\mathbf{B}$) by finite suprema, the rules of distributivity imply that the restriction to these generators is sufficient (computations left to the reader). □

9.8. Proposition. *A homomorphism $\varphi : \mathbf{A} \to \mathbf{B}$ of commutative rings is Going Down in the following two cases.*

1. $\mathbf{B}$ *is a flat* $\mathbf{A}$*-algebra.*
2. $\mathbf{B} \supseteq \mathbf{A}$ *is a domain integral over* $\mathbf{A}$*, and* $\mathbf{A}$ *is integrally closed.*

D We assume the hypotheses of Lemma 9.7, with an equality in $\mathbf{B}$,

$$\varphi(c)^\ell y^\ell + \textstyle\sum_{i=1}^q b_i \varphi(a_i) = 0 \tag{$*$}$$

1. We consider $(*)$ as a $\mathbf{B}$-syzygy between the elements c^ℓ, a_1, …, a_q. We express that it is a $\mathbf{B}$-linear combination of $\mathbf{A}$-syzygies. These relations are written as $x_j c^\ell + \sum_{i=1}^q u_{j,i} a_i = 0$ for $j \in [\![1..m]\!]$, with the x_j's and the $u_{j,i}$'s in $\mathbf{A}$. Hence $\mathrm{D}_{\mathbf{A}}(cx_j) \leqslant \mathrm{D}_{\mathbf{A}}(\underline{a})$, and $\mathrm{D}_{\mathbf{A}}(c) \wedge \mathrm{D}_{\mathbf{A}}(\underline{x}) \leqslant \mathrm{D}_{\mathbf{A}}(\underline{a})$. Finally, y^ℓ is a $\mathbf{B}$-linear combination of the $\varphi(x_j)$'s, hence $\mathrm{D}_{\mathbf{B}}(y) \leqslant \mathrm{D}_{\mathbf{B}}\big(\varphi(\underline{x})\big)$.

2. By $(*)$, $(cy)^\ell \in \langle \underline{a} \rangle\, \mathbf{B}$. By the Lying Over XII-2.8, $(cy)^\ell$, and a fortiori cy, is integral over $\langle \underline{a} \rangle_{\mathbf{A}}$. We write an integral dependence relation for cy over the ideal $\langle \underline{a} \rangle_{\mathbf{A}}$ in the form $f(cy) = 0$ with

$$f(X) = X^k + \textstyle\sum_{j=1}^{k} \mu_j X^{k-j} \qquad \text{where } \mu_j \in \langle \underline{a} \rangle_{\mathbf{A}}^{j}.$$

Moreover, y annihilates a monic polynomial $g(X) \in \mathbf{A}[X]$. Consider in $(\operatorname{Frac}\mathbf{A})[X]$ the monic gcd $h(X) = X^m + x_1 X^{m-1} + \cdots + x_m$ of the two polynomials $f(cX)$ and $g(X)$. Since $\mathbf{A}$ is integrally closed, Kronecker's theorem says that $x_j \in \mathbf{A}$, and the equality $h(y) = 0$ gives $y \in \mathrm{D}_{\mathbf{B}}(\underline{x})$.

It remains to see that $cx_j \in \mathrm{D}_{\mathbf{A}}(\underline{a})$ for $j \in \llbracket 1..m \rrbracket$. By formally replacing X with Y/c, we get that the polynomial

$$h_c(Y) = Y^m + cx_1 Y^{m-1} + \cdots + c^m x_m$$

divides $f(Y)$ in $(\operatorname{Frac}\mathbf{A})[Y]$. Kronecker's theorem (under the form of Lemma XII-2.7) tells us that $cx_j \in \mathrm{D}_{\mathbf{A}}(\mu_1, \ldots, \mu_k)$.

Finally, as $\mathrm{D}_{\mathbf{A}}(\mu_1, \ldots, \mu_k) \leqslant \mathrm{D}_{\mathbf{A}}(\underline{a})$, we indeed have $cx_j \in \mathrm{D}_{\mathbf{A}}(\underline{a})$. □

Incomparability

In classical mathematics we say that a homomorphism $\alpha : \mathbf{T} \to \mathbf{T}'$ of distributive lattices "has the incomparability property" when the fibers of the dual homomorphism $\mathsf{Spec}\,\alpha : \mathsf{Spec}\,\mathbf{T}' \to \mathsf{Spec}\,\mathbf{T}$ are constituted of pairwise incomparable elements. In other words, for $\mathfrak{q}_1$ and $\mathfrak{q}_2$ in $\mathsf{Spec}\,\mathbf{T}'$, if $\alpha^{-1}(\mathfrak{q}_1) = \alpha^{-1}(\mathfrak{q}_2)$ and $\mathfrak{q}_1 \subseteq \mathfrak{q}_2$, then $\mathfrak{q}_1 = \mathfrak{q}_2$.

The corresponding constructive definition is that the morphism $\mathbf{T} \to \mathbf{T}'$ is zero-dimensional.

We have already given the definition of the dimension of a morphism in the case of commutative rings. An analogous definition can be provided for the distributive lattices, but we will not be using it.

The principal consequence of the incomparability situation for a homomorphism $\varphi : \mathbf{A} \to \mathbf{B}$ is the fact that $\mathsf{Kdim}\,\mathbf{B} \leqslant \mathsf{Kdim}\,\mathbf{A}$. This is a special case of Theorem 7.13 with the important Theorem 7.16.

Exercises and problems

Exercise 1. We recommend that the proofs which are not given, or are sketched, or left to the reader, etc, be done. But in particular, we will cover the following cases.

- Prove Proposition 3.1.
- Prove what is stated in Examples on page 752.
- Prove Fact 6.3.

- Prove Facts 6.5 and 6.6.
- Check the details in the proof of Proposition 6.9.
- Prove Lemma 7.7 using the proof of Lemma XI-4.22 as inspiration.
- Check the details in the proof of Lemma 9.7.

Exercise 2. If $\mathfrak{f}$ is a filter of the ring $\mathbf{A}$, let us define its *complement* $\widetilde{\mathfrak{f}}$ as being $\{\, x \in \mathbf{A} \mid x \in \mathfrak{f} \Rightarrow 0 \in \mathfrak{f} \,\}$. In particular, we still have $0 \in \widetilde{\mathfrak{f}}$, even if $0 \in \mathfrak{f}$. Similarly, if $\mathfrak{a}$ is an ideal of the ring $\mathbf{A}$, let us define its *complement* $\bar{\mathfrak{a}}$ as being $\{\, x \in \mathbf{A} \mid x \in \mathfrak{a} \Rightarrow 1 \in \mathfrak{a} \,\}$. Show that if $\mathfrak{f}$ is a prime filter its complement is an ideal. If in addition $\mathfrak{f}$ is detachable, then $\mathfrak{a}$ is a detachable prime ideal. Also show the dual affirmations.

Exercise 3. *1.* If the sequence $(X_1, \ldots, X_n)$ is singular in the ring $\mathbf{A}[X_1, \ldots, X_n]$, then $\mathbf{A}$ is trivial.
2. Let $k \in \mathbb{N}$. Prove that if $\mathbf{A}[X]$ is a ring of dimension at most k then $\mathbf{A}$ is of dimension at most $k-1$. Thus obtain once again item *1.*

Exercise 4. Prove that if $\mathbf{K}$ is a ring of Krull dimension exactly equal to 0 then $\mathbf{K}[X_1, \ldots, X_n]$ is of Krull dimension exactly equal to n.

Exercise 5. *(Partition of unity associated with an open covering of the spectrum)* Let $\mathbf{A}$ be a ring and $(U_i)_i$ be an open covering of $\mathsf{Spec}(\mathbf{A})$. Show in classical mathematics that there exists a family $(f_i)_i$ of elements of $\mathbf{A}$ with $f_i = 0$ except for a finite number of indices i and

$$(\star) \qquad \mathrm{D}_{\mathbf{A}}(f_i) \subseteq U_i, \qquad \textstyle\sum_i f_i = 1.$$

Remark: thus, we replace every open covering of $\mathsf{Spec}(\mathbf{A})$ by a finite system of elements of $\mathbf{A}$ which "cover" $\mathbf{A}$ (since their sum is equal to 1), without "losing information" since $(\star)$ confirms once again that $(U_i)_i$ is a covering.

Exercise 6. For a finitely presented algebra $\mathbf{A}$ over a nontrivial discrete field, let us call the "Noether dimension of $\mathbf{A}$" the number of algebraically independent variables after a Noether position.
1. Let $f \in \mathbf{A} \supseteq \mathbf{K}[Y_1, \ldots, Y_r] = \mathbf{K}[\underline{Y}]$ ($\mathbf{A}$ integral over $\mathbf{K}[\underline{Y}]$).
1a. Show that the boundary ideal of f contains a $g \in \mathbf{K}[\underline{Y}] \setminus \{0\}$.
1b. Deduce that the Krull boundary ring $\mathbf{A}\big/\mathcal{J}_{\mathbf{A}}^{\mathrm{K}}(f)$ is a quotient of a finitely presented algebra whose Noether dimension is $\leqslant r-1$.
2. Deduce a direct proof of the equality of Krull and Noether dimensions of the finitely presented algebras over a nontrivial discrete field.

Exercise 7. *1.* Let $\mathbf{K}$ be a nontrivial discrete field, $\mathbf{K}[\underline{X}] = \mathbf{K}[X_1, \ldots, X_n]$ and $f \in \mathbf{K}[\underline{X}] \setminus \{0\}$, then $\mathsf{Kdim}\,\mathbf{K}[\underline{X}][1/f] = n$.
2. More generally, give a sufficient condition on the polynomial $\delta \in \mathbf{A}[\underline{X}]$ for us to have $\mathsf{Kdim}(\mathbf{A}[\underline{X}][1/\delta]) = \mathsf{Kdim}\,\mathbf{A}[\underline{X}]$ (see the proof of Lemma X-4.6).

Exercise 8. *(Characterization of integral Prüfer rings of dimension at most* 1*)* Let $\mathbf{A}$ be an integrally closed ring.
1. Show that if $\mathsf{Kdim}\,\mathbf{A}[X] \leqslant 2$, then $\mathbf{A}$ is a Prüfer ring, by showing that every element of $\mathrm{Frac}\,\mathbf{A}$ is primitively algebraic over $\mathbf{A}$.
2. Show that $\mathbf{A}$ is a Prüfer ring of dimension at most 1 if and only if $\mathsf{Kdim}\,\mathbf{A}[X] \leqslant 2$.
3. Can we generalize to a normal ring?

Exercise 9. *(A multiplicative property of boundary ideals)*
1. For $a, b \in \mathbf{A}$ and two sequences $(\underline{x})$, $(\underline{y})$ of elements of $\mathbf{A}$, show that

$$\mathcal{I}_{\mathbf{A}}^{\mathrm{K}}(\underline{x}, a, \underline{y})\,\mathcal{I}_{\mathbf{A}}^{\mathrm{K}}(\underline{x}, b, \underline{y}) \subseteq \mathcal{I}_{\mathbf{A}}^{\mathrm{K}}(\underline{x}, ab, \underline{y}).$$

2. Deduce that $\mathcal{I}_{\mathbf{A}}^{\mathrm{K}}(a_1b_1, \ldots, a_nb_n)$ contains the product $\prod_{\underline{c}} \mathcal{I}_{\mathbf{A}}^{\mathrm{K}}(\underline{c})$, in which the sequence $(\underline{c}) = (c_1, \ldots, c_n)$ ranges over the set of 2^n sequences such that $c_i = a_i$ or $c_i = b_i$ for each i.

Exercise 10. *(Boundary ideals and algebraic relations)*
1. We consider the lexicographical order over $\mathbb{N}^n$. Let $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$. Prove, for $\beta > \alpha$, that
$\underline{X}^\beta \in \left\langle X_1^{1+\alpha_1},\ X_1^{\alpha_1} X_2^{1+\alpha_2},\ X_1^{\alpha_1} X_2^{\alpha_2} X_3^{1+\alpha_3},\ \dots,\ X_1^{\alpha_1} X_2^{\alpha_2} \cdots X_{n-1}^{\alpha_{n-1}} X_n^{1+\alpha_n} \right\rangle.$
2. Let $\mathbf{A}$ be a reduced ring, $(\underline{x}) = (x_1, \dots, x_n)$ be a sequence in $\mathbf{A}$ and $P = \sum_\beta a_\beta \underline{X}^\beta$ in $\mathbf{A}[\underline{X}]$, which annihilates $\underline{x}$.

a. Show, for $\alpha \in \mathbb{N}^n$, that $a_\alpha \prod_{\beta<\alpha} \mathrm{Ann}(a_\beta) \subseteq \mathcal{I}^{\mathrm{K}}(\underline{x})$.

b. Deduce
$$\textstyle\prod_\beta \mathcal{I}^{\mathrm{K}}(a_\beta) \subseteq \mathcal{I}^{\mathrm{K}}(\underline{x}) + \prod_\beta \mathrm{Ann}(a_\beta).$$

3. Let $\mathbf{A} \to \mathbf{B}$ be an algebra with reduced $\mathbf{B}$ and let $x \in \mathbf{B}$ be primitively algebraic over $\mathbf{A}$: $\sum_{i=0}^d a_i x^i = 0$ with $a_i \in \mathbf{A}$ and $1 \in \langle a_i, i \in [\![0..d]\!] \rangle$. Deduce from the previous question that $\mathcal{I}_{\mathbf{B}}^{\mathrm{K}}(x)$ contains the image of $\prod_{i=0}^d \mathcal{I}_{\mathbf{A}}^{\mathrm{K}}(a_i)$.
4. Deduce a new proof of Theorem 7.16: if every element of $\mathbf{B}$ is primitively algebraic over $\mathbf{A}$, then $\mathsf{Kdim}\,\mathbf{B} \leqslant \mathsf{Kdim}\,\mathbf{A}$.

Exercise 11. *(Integral extension of the boundary ideal $\mathcal{I}^{\mathrm{K}}$)*
Let $\mathbf{A} \subseteq \mathbf{B}$ be an integral extension of rings.
1. If $\mathfrak{a}$ is an ideal of $\mathbf{A}$, $\mathfrak{b}$ is an ideal of $\mathbf{B}$, show that
$$\mathbf{A} \cap (\mathfrak{b} + \mathfrak{a}\mathbf{B}) \subseteq \mathrm{D}_{\mathbf{A}}(\mathfrak{a} + \mathbf{A} \cap \mathfrak{b}).$$
2. Deduce, for $a_0, \dots, a_d \in \mathbf{A}$,
$$\mathbf{A} \cap \mathcal{I}_{\mathbf{B}}^{\mathrm{K}}(a_0, \dots, a_d) \subseteq \mathrm{D}_{\mathbf{A}}\big(\mathcal{I}_{\mathbf{A}}^{\mathrm{K}}(a_0, \dots, a_d)\big).$$
3. Give a new proof of the fact that $\mathsf{Kdim}\,\mathbf{A} \leqslant \mathsf{Kdim}\,\mathbf{B}$, see Proposition 4.1 and Theorem 9.6. Compare with Exercise 12.

Exercise 12. *(Integral extension of the boundary monoid $\mathcal{S}^{\mathrm{K}}$)*
Let $\mathbf{A} \subseteq \mathbf{B}$ be an integral extension of rings.
1. Let $\mathfrak{a}$ be an ideal of $\mathbf{A}$ and $S \subseteq \mathbf{A}$ be a monoid. Show that
$$S + \mathfrak{a}\mathbf{B} \subseteq (S + \mathfrak{a})^{\mathrm{sat}_{\mathbf{B}}}.$$
2. Deduce, for $a_0, \dots, a_d \in \mathbf{A}$,
$$\mathcal{S}_{\mathbf{B}}^{\mathrm{K}}(a_0, \dots, a_d) \subseteq \mathcal{S}_{\mathbf{A}}^{\mathrm{K}}(a_0, \dots, a_d)^{\mathrm{sat}_{\mathbf{B}}}.$$
3. Give a new proof of the fact that $\mathsf{Kdim}\,\mathbf{A} \leqslant \mathsf{Kdim}\,\mathbf{B}$.

Exercise 13. Let $\mathbf{K}$ be a nontrivial discrete field. Denote $(X_1, \dots, X_n)$ by $(\underline{X})$ and $(Y_1, \dots, Y_m)$ and $(\underline{Y})$ Let $\mathbf{A} = \mathbf{K}(\underline{X}) \otimes_{\mathbf{K}} \mathbf{K}(\underline{Y})$. We intend to determine the Krull dimension of $\mathbf{A}$.

1. $\mathbf{A}$ is the localization of $\mathbf{K}[\underline{X}, \underline{Y}]$ at $S = (\mathbf{K}[\underline{X}])^*(\mathbf{K}[\underline{Y}])^*$. It is also a localization of $\mathbf{K}(\underline{X})[\underline{Y}]$ and of $\mathbf{K}(\underline{Y})[\underline{X}]$. Consequently $\mathsf{Kdim}\,\mathbf{A} \leqslant \inf(m, n)$.
2. Suppose $n \leqslant m$. Show that the sequence $(X_1 - Y_1, \dots, X_n - Y_n)$ is a regular sequence in $\mathbf{A}$.

Conclude that $\mathsf{Kdim}\,\mathbf{A} = \inf(n, m)$.

Exercise 14. *(Prime ideals, boundaries and duality)*
Let $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_{d-1} \subsetneq \mathfrak{p}_d \subsetneq \mathbf{A}$ be a chain of detachable prime ideals with $x_1 \in \mathfrak{p}_1 \setminus \mathfrak{p}_0$, $x_2 \in \mathfrak{p}_2 \setminus \mathfrak{p}_1$, $\ldots$, $x_d \in \mathfrak{p}_d \setminus \mathfrak{p}_{d-1}$, according to the following diagram.

$$\begin{tikzcd}
 & x_1 \arrow[dl, dash, dotted, "\notin"'] \arrow[dr, dash, dotted, "\in"] & & x_2 \arrow[dl, dash, dotted, "\notin"'] \arrow[dr, dash, dotted, "\in"] & & & & x_{d-1} \arrow[dl, dash, dotted, "\notin"'] \arrow[dr, dash, dotted, "\in"] & & x_d \arrow[dl, dash, dotted, "\notin"'] \arrow[dr, dash, dotted, "\in"] & \\
0 \in \mathfrak{p}_0 & \subsetneq & \mathfrak{p}_1 & \subsetneq & \mathfrak{p}_2 & \subsetneq \cdots \subsetneq & \mathfrak{p}_{d-2} & \subsetneq & \mathfrak{p}_{d-1} & \subsetneq & \mathfrak{p}_d \not\ni 1
\end{tikzcd}$$

1. Show that $\mathcal{I}^{\mathrm{K}}(x_1, \ldots, x_i) \subseteq \mathfrak{p}_i$ for $i \in \llbracket 0..d \rrbracket$. Therefore $\mathcal{I}^{\mathrm{K}}(x_1, \ldots, x_d) \subseteq \mathfrak{p}_d$. In addition, if $x_{d+1} \notin \mathfrak{p}_d$, then $\mathcal{I}^{\mathrm{K}}(x_1, \ldots, x_d, x_{d+1}) \subseteq \mathfrak{p}_d + \mathbf{A}x_{d+1}$. Consequently, if $x_{d+1} \notin \mathfrak{p}_d$ and $1 \in \mathcal{I}^{\mathrm{K}}(x_1, \ldots, x_d, x_{d+1})$, then $1 \in \mathfrak{p}_d + \mathbf{A}x_{d+1}$.

2. Consider the complementary prime filters $\mathfrak{f}_i = \mathbf{A} \setminus \mathfrak{p}_i$ for $i \in \llbracket 0..d \rrbracket$. We have the dual diagram of the previous one.

$$\begin{tikzcd}
 & x_d \arrow[dl, dash, dotted, "\notin"'] \arrow[dr, dash, dotted, "\in"] & & x_{d-1} \arrow[dl, dash, dotted, "\notin"'] \arrow[dr, dash, dotted, "\in"] & & & & x_2 \arrow[dl, dash, dotted, "\notin"'] \arrow[dr, dash, dotted, "\in"] & & x_1 \arrow[dl, dash, dotted, "\notin"'] \arrow[dr, dash, dotted, "\in"] & \\
1 \in \mathfrak{f}_d & \subsetneq & \mathfrak{f}_{d-1} & \subsetneq & \mathfrak{f}_{d-2} & \subsetneq \cdots \subsetneq & \mathfrak{f}_2 & \subsetneq & \mathfrak{f}_1 & \subsetneq & \mathfrak{f}_0 \not\ni 0
\end{tikzcd}$$

Show that $\mathcal{S}^{\mathrm{K}}(x_{i+1}, \ldots, x_d) \subseteq \mathfrak{f}_i$ for $i \in \llbracket 0..d \rrbracket$. Therefore $\mathcal{S}^{\mathrm{K}}(x_1, \ldots, x_d) \subseteq \mathfrak{f}_0$. In addition, if $x_0 \notin \mathfrak{f}_0$, i.e. if $x_0 \in \mathfrak{p}_0$, then $\mathcal{S}^{\mathrm{K}}(x_0, x_1, \ldots, x_d) \subseteq x_0^{\mathbb{N}}\mathfrak{f}_0$. Consequently, if $x_0 \notin \mathfrak{f}_0$ and $0 \in \mathcal{S}^{\mathrm{K}}(x_0, x_1, \ldots, x_d)$, then $0 \in x_0^{\mathbb{N}}\mathfrak{f}_0$.

Note: $\mathfrak{p}_d + \mathbf{A}x_{d+1}$ is the ideal generated by $\mathfrak{p}_d$ and x_{d+1}, dually $x_0^{\mathbb{N}}\mathfrak{f}_0$ is the monoid generated by $\mathfrak{f}_0$ and x_0.

Exercise 15. *(Elimination and boundary ideals in polynomial rings)*
Here is a detailed proof of the inequality $\mathsf{Kdim}\,\mathbf{A}[T] \leqslant 1 + 2\,\mathsf{Kdim}\,\mathbf{A}$ (Section 7), with a few further results. Without loss of generality $\mathbf{A}$ is assumed to be reduced.

1. Let $f \in \mathbf{A}[T]$ be a polynomial such that the annihilator of each coefficient is generated by an idempotent. For $g \in \mathbf{A}[T]$, define $R \in \mathbf{A}[X, Y]$ such that $\mathrm{Ann}(R) = 0$ and $R(f, g) = 0$: note that the polynomial $\mathrm{Res}_T\big(f(T) - X, Y - g(T)\big)$ solves the question when f is monic of degree $\geqslant 1$ (why?), and use Lemma IV-6.4.

2. By using Exercise 10, show that if $R = \sum_{i,j} r_{ij} X^i Y^j$, we have

$$\textstyle\prod_{i,j} \mathcal{I}^{\mathrm{K}}_{\mathbf{A}[T]}(r_{ij}) \subseteq \mathcal{I}^{\mathrm{K}}_{\mathbf{A}[T]}(f, g).$$

3. By using a ring of type $\mathbf{A}_{\{\underline{a}\}}$ (Lemma 7.9 and Exercise 18), find the inequality $\mathsf{Kdim}\,\mathbf{A}[T] \leqslant 1 + 2\,\mathsf{Kdim}\,\mathbf{A}$.

4. Show the following more precise result: for a reduced ring $\mathbf{A}$ and f, $g \in \mathbf{A}[T]$, the ideal $\mathrm{D}_{\mathbf{A}[T]}\big(\mathcal{I}^{\mathrm{K}}_{\mathbf{A}[T]}(f, g)\big)$ contains a finite product of boundary ideals $\mathcal{I}^{\mathrm{K}}_{\mathbf{A}}(a)$, $a \in \mathbf{A}$.

5. More generally: if $\mathbf{A}[\underline{T}] = \mathbf{A}[T_1, \ldots, T_r]$ and f_0, $\ldots$, $f_r \in \mathbf{A}[\underline{T}]$, then the nilradical of the boundary ideal $\mathcal{I}^{\mathrm{K}}_{\mathbf{A}[\underline{T}]}(f_0, \ldots, f_r)$ contains a finite product of boundary ideals $\mathcal{I}^{\mathrm{K}}_{\mathbf{A}}(a_i)$, with $a_i \in \mathbf{A}$. We once again deduce that $1 + \mathsf{Kdim}\,\mathbf{A}[\underline{T}] \leqslant (1 + r)(1 + \mathsf{Kdim}\,\mathbf{A})$.

Exercise 16. *(Boundary ideals of polynomials)* Continued from Exercise 15.
1. Let x, $y \in \mathbf{B}$ and (z_j) be a finite family in $\mathbf{B}$ satisfying $\prod_j \mathcal{I}^{\mathrm{K}}(z_j) \subseteq \mathcal{I}^{\mathrm{K}}(x, y)$. Show that for $(b_1, \dots, b_n)$ in $\mathbf{B}$, $\prod_j \mathcal{I}^{\mathrm{K}}(z_j, b_1, \dots, b_n) \subseteq \mathcal{I}^{\mathrm{K}}(x, y, b_1, \dots, b_n)$.

2. Let T be an indeterminate over a ring $\mathbf{A}$.

a. For $(a_1, \dots, a_n)$ in $\mathbf{A}$, prove that $\mathcal{I}^{\mathrm{K}}_{\mathbf{A}}(a_1, \dots, a_n)\mathbf{A}[T] = \mathcal{I}^{\mathrm{K}}_{\mathbf{A}[T]}(a_1, \dots, a_n)$.

b. Show that the boundary ideal of $2d$ polynomials of $\mathbf{A}[T]$ contains, up to radical, a product of boundary ideals of d elements of $\mathbf{A}$.
Consequently $\mathsf{Kdim}\,\mathbf{A} < d \Rightarrow \mathsf{Kdim}\,\mathbf{A}[T] < 2d$; this is another form of the inequality $\mathsf{Kdim}\,\mathbf{A}[T] \leqslant 1 + 2\,\mathsf{Kdim}\,\mathbf{A}$.

3. How can we generalize the first and second item?

Exercise 17. *(Another definition of the Krull dimension of distributive lattices, see [82, Español])* In an ordered set, a sequence $(x_0, \dots, x_n)$ is called a *chain of length n* if we have $x_0 \leqslant x_1 \leqslant \cdots \leqslant x_n$. In a distributive lattice, two chains $(x_0, \dots, x_n)$ and $(b_0, \dots, b_n)$ are said to be *linked*, if there exists a chain $(c_1, \dots, c_n)$ with

$$\left.\begin{array}{rcccl} x_0 \wedge b_0 & = & 0 & & \\ x_1 \wedge b_1 & = & c_1 & = & x_0 \vee b_0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ x_n \wedge b_n & = & c_n & = & x_{n-1} \vee b_{n-1} \\ & & 1 & = & x_n \vee b_n \end{array}\right\} \qquad (25)$$

Please compare with Definition 6.1 for the complementary sequences. Also note that if the sequences $(x_0, \dots, x_n)$, $(b_0, \dots, b_n)$ and $(c_1, \dots, c_n)$ are linked by equations (25), then they are chains.

1. If in a distributive lattice we have $x \leqslant y$ and $x \vee a \geqslant y \wedge b$, then we can explicate a' and b' such that

$$x \wedge a' = x \wedge a, \qquad y \vee b' = y \vee b, \qquad x \vee a' = y \wedge b'.$$

Therefore from a left-configuration (by still assuming that $x \leqslant y$), we can construct a right-configuration

$$\left\{\begin{array}{rcl} x \wedge a & = & p \\ x \vee a & \geqslant & y \wedge b \\ q & = & y \vee b \end{array}\right. \qquad \left\{\begin{array}{rcl} x \wedge a' & = & p \\ x \vee a' & = & y \wedge b' \\ q & = & y \vee b' \end{array}\right.$$

2. In a distributive lattice, a chain $(x_0, \dots, x_n)$ has a complementary sequence if and only if there exists a chain which is linked to it.

3. For a distributive lattice $\mathbf{T}$ the following properties are equivalent.

a. $\mathbf{T}$ has Krull dimension $\leqslant n$.

b. Any chain of length n has a complementary sequence.

c. Any chain of length n has a linked une chain.

Exercise 18. *(A few results on the finite stages of $\mathbf{A}_{\min}$)*
Let $\mathbf{A}$ be a reduced ring. For ideals $\mathfrak{a}$, $\mathfrak{b}$ of $\mathbf{A}$ let $\mathfrak{a} \diamond \mathfrak{b} = (\mathfrak{a}^{\perp}\mathfrak{b})^{\perp} = (\mathfrak{a}^{\perp\perp} : \mathfrak{b})$.

1. Prove that $\mathbf{A}/\mathfrak{a} \diamond \mathfrak{b}$ is a reduced ring in which $\mathfrak{a}$ is null and $\mathfrak{b}$ faithful.

2. Prove that $(\mathbf{A}/\mathfrak{a}_1 \diamond \mathfrak{b}_1)\big/(\overline{\mathfrak{a}_2} \diamond \overline{\mathfrak{b}_2}) \simeq \mathbf{A}/\mathfrak{a}_3 \diamond \mathfrak{b}_3$ with $\mathfrak{a}_3 = \mathfrak{a}_1 + \mathfrak{a}_2$, $\mathfrak{b}_3 = \mathfrak{b}_1\mathfrak{b}_2$.

3. Let $(\underline{a}) = (a_1, \dots, a_n)$ in $\mathbf{A}$. In Lemma 7.9 we have defined (for $I \in \mathcal{P}_n$)

$$\mathfrak{a}_I = \langle a_i, i \in I\rangle \diamond \prod\nolimits_{j \notin I} a_j \qquad \mathbf{A}_{\{\underline{a}\}} = \prod\nolimits_{I \in \mathcal{P}_n} \mathbf{A}/\mathfrak{a}_I \ .$$

Thus, modulo $\mathfrak{a}_I$, a_i is null for $i \in I$ and regular for $i \notin I$. Finally, let ε_i be the idempotent of $\mathbf{A}_{\{\underline{a}\}}$ whose coordinate in $\mathbf{A}/\mathfrak{a}_I$ is 1 if $i \in I$, 0 if $i \notin I$.

- *a.* Prove that the intersection (and a fortiori the product) of the ideals $\mathfrak{a}_I$ is null; consequently, the morphism $\mathbf{A} \to \mathbf{A}_{\{\underline{a}\}}$ is injective and $\mathsf{Kdim}\,\mathbf{A} = \mathsf{Kdim}\,\mathbf{A}_{\{\underline{a}\}}$.
- *b.* Prove that $\mathrm{Ann}_{\mathbf{A}_{\{\underline{a}\}}}(a_i) = \langle \varepsilon_i \rangle_{\mathbf{A}_{\{\underline{a}\}}}$.

Exercise 19. *(A few results on $\mathbf{A}_{\min}$)* See Problem XI-4 for $\mathbf{A}_{\mathrm{pp}}$.
A ring homomorphism $\mathbf{A} \to \mathbf{B}$ is said to be *regular* when the image of every regular element is a regular element. $\boxed{\text{Let } \mathbf{A} \text{ be a reduced ring.}}$

1. Let $\theta : \mathbf{A} \to \mathbf{B}$ be a regular morphism and $a \in \mathbf{A}$. If $a^{\perp}$ is generated by an idempotent e, then $\theta(a)^{\perp}$ is generated by the idempotent $\theta(e)$.
   In particular, as already mentioned in Problem XI-4, a morphism between pp-rings is a pp-ring morphism if and only if it is regular.
2. The natural morphism $\mathbf{A}_{\mathrm{pp}} \to \mathbf{A}_{\min}$ is regular and surjective.
3. For $a \in \mathbf{A}$, the natural morphism $\psi_a : \mathbf{A} \to \mathbf{A}_{\{a\}}$ is regular.
4. The natural morphism $\psi : \mathbf{A} \to \mathbf{A}_{\min}$ is regular and the natural morphism $\mathbb{Z} \to \mathbb{Z}_{\mathrm{qi}}$ is not regular.

Exercise 20. Explicate the proof of Lemma 8.12 in terms of singular sequences.

Exercise 21. *(A generalization of Theorem 8.19)*
For $\mathbf{A} \subseteq \mathbf{B}$ and $\ell \in \mathbb{N}$, if for every sequence $(\underline{x}) = (x_0, \dots, x_\ell)$ in $\mathbf{B}$, we have a primitive polynomial of $\mathbf{A}[\underline{X}]$ which annihilates $(\underline{x})$, then $\mathsf{Vdim}\,\mathbf{B} \leqslant \ell + \mathsf{Vdim}\,\mathbf{A}$.

Exercise 22. *(Lying Over morphism)*
Prove what is affirmed in the remark following the definition of the Lying Over on page 785.

Exercise 23. *(Lying Over morphism, 2)*
In the category of finite ordered sets, it is clear that a morphism is surjective if and only if it is an epimorphism. This therefore corresponds, for the dual distributive lattices, to a monomorphism, which here means an injective homomorphism, i.e. a Lying Over morphism.
Give a proof in classical mathematics of the equivalence, for some homomorphism $\alpha : \mathbf{T} \to \mathbf{T}'$ of distributive lattices, between: α is Lying Over on the one hand, and $\mathsf{Spec}\,\alpha : \mathsf{Spec}\,\mathbf{T}' \to \mathsf{Spec}\,\mathbf{T}$ is surjective, on the other hand.
Idea: use *Krull's lemma*, which can be easily proven à la Zorn: *If in a distributive lattice we have an ideal* $\mathfrak{a}$ *and a filter* $\mathfrak{f}$ *which do not intersect, there exists a prime ideal containing* $\mathfrak{a}$ *whose complement is a filter containing* $\mathfrak{f}$.

Exercise 24. *(Going Up, Going Down morphisms)*
Prove what is stated in the remark following the definition of Going Up on page 786 (use the description of the quotient lattice $\mathbf{T}/(\mathfrak{a}=0)$ given on page 623). Do the same thing for Going Down.

Problem 1. *(Annihilator of an ideal in a reduced Noetherian ring)*
We consider a reduced ring $\mathbf{A}$ such that every ascending sequence of ideals of the form $\mathrm{D}_{\mathbf{A}}(x)$ has two equal consecutive terms.

1. Let $\mathfrak{a}$ be an ideal of $\mathbf{A}$ such that we know how to test for $y \in \mathbf{A}$ if $\mathrm{Ann}(y)\mathfrak{a} = 0$ (and in case of a negative answer provide the corresponding certificate).
1a. If some $x \in \mathfrak{a}$ satisfies $\mathrm{Ann}(x)\mathfrak{a} \neq 0$, determine some $x' \in \mathfrak{a}$ such that $\mathrm{D}_{\mathbf{A}}(x) \subsetneq \mathrm{D}_{\mathbf{A}}(x')$.
1b. Deduce the existence of some $x \in \mathfrak{a}$ such that $\mathrm{Ann}(x) = \mathrm{Ann}(\mathfrak{a})$.

2. Suppose moreover that every regular element of $\mathbf{A}$ is invertible, and that for all y, z we know how to test if $\mathrm{Ann}(y)\mathrm{Ann}(z) = 0$. Show that $\mathsf{Kdim}\,\mathbf{A} \leqslant 0$.

3. Let $\mathbf{B}$ ne a strongly discrete coherent Noetherian ring. Show that $\mathrm{Frac}(\mathbf{B}_{\mathrm{red}})$ is a zero-dimensional ring.
Note: in classical mathematics $\mathbf{B}$ admits a finite number of minimal prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ and $\mathrm{Frac}(\mathbf{B}_{\mathrm{red}})$ is isomorphic to the finite product of corresponding fields: $\mathrm{Frac}(\mathbf{A}/\mathfrak{p}_1) \times \cdots \times \mathrm{Frac}(\mathbf{A}/\mathfrak{p}_k)$. However, in general, we have no algorithmic access to the $\mathfrak{p}_i$'s.

Problem 2. *(Lying Over, Going Up, Going Down, examples)*
1. Let $\mathbf{A} \subseteq \mathbf{B}$ be an inclusion of rings such that, as an $\mathbf{A}$-module, $\mathbf{A}$ is a direct factor in $\mathbf{B}$. Show that $\mathfrak{a}\mathbf{B} \cap \mathbf{A} = \mathfrak{a}$ for every ideal $\mathfrak{a}$ of $\mathbf{A}$. In particular, $\mathbf{A} \hookrightarrow \mathbf{B}$ is Lying Over.

2. Let G be a finite group acting on a ring $\mathbf{B}$ with $|G|\,1_{\mathbf{B}}$ invertible in $\mathbf{B}$. Let $\mathbf{A} = \mathbf{B}^G$ be the subring of fixed points. We define the *Reynolds operator* $R_G : \mathbf{B} \to \mathbf{A}$:

$$R_G(b) = \tfrac{1}{|G|}\sum\nolimits_{g \in G} g(b).$$

Prove that R_G is an $\mathbf{A}$-projector of image $\mathbf{A}$; in particular, $\mathbf{A}$ is a direct summand (as an $\mathbf{A}$-module) in $\mathbf{B}$.

3. Let $\mathbf{A} \hookrightarrow \mathbf{B}$ with $\mathbf{A}$ as a direct summand (as an $\mathbf{A}$-module) in $\mathbf{B}$. Provide a direct proof of $\mathsf{Kdim}\,\mathbf{A} \leqslant \mathsf{Kdim}\,\mathbf{B}$.

4. Let $\mathbf{k}$ be a nontrivial discrete field, $\mathbf{A} = \mathbf{k}[XZ, YZ] \subset \mathbf{B} = \mathbf{k}[X, Y, Z]$. Then $\mathbf{A}$ is a direct summand in $\mathbf{B}$, therefore $\mathbf{A} \hookrightarrow \mathbf{B}$ is Lying Over. But $\mathbf{A} \hookrightarrow \mathbf{B}$ is neither Going Up nor Going Down.

Problem 3. *(Potential chains of prime ideals)*
Over a ring $\mathbf{A}$ we call a *potential chain of prime ideals*, or *potential chain* a list $[(I_0, U_0), \ldots, (I_n, U_n)]$, where the I_j's and U_j's are subsets of $\mathbf{A}$ (i.e. each (I_j, U_j) is a potential prime ideal of $\mathbf{A}$). A potential chain is said to be *finite* if the I_j's and U_j's are finitely enumerated subsets.

A potential chain is said to be *complete* if the following conditions are satisfied

- the I_j's are ideals and the U_j's are monoids,

- $I_0 \subseteq I_1 \subseteq \cdots \subseteq I_n$ and $U_0 \supseteq U_1 \supseteq \cdots \supseteq U_n$,
- $I_j + U_j = U_j$ for each j.

We say that the potential chain $[(I_0, U_0), \dots, (I_n, U_n)]$ *refines* the chain $[(J_0, V_0), \dots, (J_n, V_n)]$ if we have the inclusions $J_k \subseteq I_k$ and $V_k \subseteq U_k$ for each k.

1. Show that every potential chain generates a complete potential chain (in the sense of the refinement relation). More precisely, from $[(I_0, U_0), \dots, (I_n, U_n)]$, we successively construct

- $\mathfrak{a}_j = \langle I_j \rangle$, $\mathfrak{b}_j = \sum_{i \leqslant j} \mathfrak{a}_i$ ($j \in [\![0..n]\!]$),
- $\mathfrak{f}_n = \mathcal{M}(U_n) + \mathfrak{b}_n$,[4] $\mathfrak{f}_{n-1} = \mathcal{M}(U_{n-1} \cup \mathfrak{f}_n) + \mathfrak{b}_{n-1}$, $\dots$, $\mathfrak{f}_0 = \mathcal{M}(U_0 \cup \mathfrak{f}_1) + \mathfrak{b}_0$.

And we consider $[(\mathfrak{b}_0, \mathfrak{f}_0), \dots, (\mathfrak{b}_n, \mathfrak{f}_n)]$.

2. We say that a potential chain $\mathcal{C}$ *collapses* if in the complete chain that it generates $[(\mathfrak{b}_0, \mathfrak{f}_0), \dots]$ we have $0 \in \mathfrak{f}_0$. Show that a sequence $(x_1, \dots, x_n)$ is singular if and only if the potential chain $[(0, x_1), (x_1, x_2), \dots, (x_{n-1}, x_n), (x_n, 1)]$ collapses.

3. Show in classical mathematics that a potential chain $\mathcal{C}$ of $\mathbf{A}$ collapses if and only if it is impossible to find prime ideals $\mathfrak{p}_0 \subseteq \mathfrak{p}_1 \subseteq \cdots \subseteq \mathfrak{p}_n$, such that the chain $[(\mathfrak{p}_0, \mathbf{A} \setminus \mathfrak{p}_0), \dots, (\mathfrak{p}_n, \mathbf{A} \setminus \mathfrak{p}_n)]$ refines the chain $\mathcal{C}$.

4. Given a potential chain $\mathcal{C} = [(I_0, U_0), \dots, (I_n, U_n)]$, we *saturate* it by adding, in I_k, (resp. in U_k) every $x \in \mathbf{A}$ which, added to U_k (resp. to I_k) would lead to a collapse. Thus a potential chain collapses if and only if its saturated chain is $[(\mathbf{A}, \mathbf{A}), \dots, (\mathbf{A}, \mathbf{A})]$.
Show that we obtain thus a potential chain $[(J_0, V_0), \dots, (J_n, V_n)]$ which refines the complete chain generated by $\mathcal{C}$.
Show in classical mathematics that J_k is the intersection of the prime ideals that appear in position k in a chain of prime ideals which refines $\mathcal{C}$ (as in the previous question). Also prove the dual statement for V_k.

Some solutions, or sketches of solutions

Exercise 3. *2.* Consider a sequence of length k in $\mathbf{A}$, to it we add X at the start, and it becomes singular in $\mathbf{A}[X]$. We then get rid of X in the corresponding Equality (6) (page 753).
Note: we can also invoke item *3* of Proposition 2.16.

Exercise 4. We can assume that $\mathbf{K}$ is reduced ($\mathbf{K}_{\mathrm{red}}[\underline{X}] = \mathbf{K}[\underline{X}]_{\mathrm{red}}$ has the same dimension as $\mathbf{K}[X_1, \dots, X_n]$). Two possibilities are then offered. The first is to rewrite the proof given in the case of a discrete field by using Exercise IV-13 and local-global principle 3.2. The second is to apply the elementary local-global machinery no. 2.

[4] Recall that $\mathcal{M}(A)$ is the monoid generated by the subset A.

Exercise 5. We write each U_i in the form $U_i = \bigcup_{j \in J_i} \mathrm{D}_{\mathbf{A}}(g_{ij})$. Saying that the $\mathrm{D}_{\mathbf{A}}(g_{ij})$'s cover $\mathsf{Spec}(\mathbf{A})$ means that $1 \in \langle\, \mathrm{D}_{\mathbf{A}}(g_{ij}) \mid j \in J_i,\ i \in I \rangle$, hence an equality $1 = \sum_{j,i} u_{ji} g_{ij}$, the u_{ji}'s being null except for a finite number of them (i.e. $i \in I_0$, $j \in J_i$, where I_0 and the J_i's are finite). Let $f_i = \sum_{j \in J_i} u_{ji} g_{ij}$. We obtain $\mathrm{D}_{\mathbf{A}}(f_i) \subseteq U_i$ because for $\mathfrak{p} \in \mathrm{D}_{\mathbf{A}}(f_i)$, we have $f_i \notin \mathfrak{p}$, therefore an index j such that $g_{ij} \notin \mathfrak{p}$, i.e. $\mathfrak{p} \in \mathrm{D}_{\mathbf{A}}(g_{ij}) \subseteq U_i$. And $\sum_{i \in I_0} f_i = 1$.

Exercise 6.
1a. We write an integral dependence relation of f over $\mathbf{K}[Y_1, \ldots, Y_r]$

$$f^n + a_{n-1} f^{n-1} + \cdots + a_k f^k = 0,$$

with $n \geqslant 1$, the a_i's in $\mathbf{K}[Y_1, \ldots, Y_r]$ and $a_k \neq 0$. The equality $(a_k + bf) f^k = 0$ shows that $a_k + bf \in (\mathrm{D}_{\mathbf{A}}(0) : f)$ (even if $k = 0$). Therefore $a_k \in \mathcal{J}_{\mathbf{A}}^{\mathrm{K}}(f)$.

Exercise 7.
1. We write $\mathbf{K}[\underline{X}][1/f] = \mathbf{K}[\underline{X}, T]/\langle 1 - fT \rangle$. A Noether position of the nonconstant polynomial $1 - fT$ brings us to an integral extension of $\mathbf{K}[Y_1, \ldots, Y_n]$.
2. We write $\mathbf{A}[\underline{X}][1/\delta] = \mathbf{A}[\underline{X}, T]/\langle 1 - \delta T \rangle$. We seek to apply Theorem 7.16 to integral extensions. On the one hand we want δ to be regular, for the homomorphism $\mathbf{A}[\underline{X}] \to \mathbf{A}[\underline{X}][1/\delta]$ to be injective, and on the other hand we want to be able to put the polynomial $1 - \delta T$ into Noether position, for the ring $\mathbf{A}[\underline{X}][1/\delta]$ to be integral over a ring $\mathbf{A}[Y_1, \ldots, Y_n]$.
The first condition means that the ideal $\mathrm{c}(\delta)$ is faithful (McCoy, Corollary III-2.3). The second condition is satisfied if we are in the same situation as for Lemma X-4.6

- δ is of formal degree d,
- one of the monomials of degree d, relating to a subset of variables $(X_i)_{i \in I}$, has as its coefficient an element of $\mathbf{A}^{\times}$,
- and it is the only monomial of degree d in the variables $(X_i)_{i \in I}$ present in δ.

Indeed, the change of variables "$X_i' = X_i + T$ if $i \in I$, $X_i' = X_i$ otherwise," then renders the polynomial $1 - \delta T$ monic in T (up to inverse). Note that in this case the polynomial δ is primitive and the first condition is also satisfied.

Exercise 8. *1.* Consider $s = a/b \in \operatorname{Frac} \mathbf{A}$ with b regular.
The sequence $(bX - a, b, X)$ is singular in $\mathbf{A}[X]$. This gives an equality in $\mathbf{A}[X]$ of the following type

$$(bX - a)^{k_1} \Big(b^{k_2} \big(X^{k_3} \big(1 + X p_3(X) \big) + b p_2(X) \big) + (bX - a) p_1(X) \Big) = 0.$$

Since $\mathbf{A}[X]$ is integral, we can delete the factor $(bX - a)^{k_1}$, after which we specialize X in s. We get

$$b^{k_2} \big(s^{k_3} \big(1 + s p_3(s) \big) + b p_2(s) \big) = 0,$$

and since b is regular,

$$s^{k_3} \big(1 + s p_3(s) \big) + b p_2(s) = 0.$$

Thus s annihilates $g(X) = X^{k_3} \big(1 + X p_3(X) \big) + b p_2(X)$ and $f(X) = bX - a$.
Finally, since the coefficient of X^{k_3} in g is of the form $1 + bc$, we obtain that $1 \in \mathrm{c}(f) + \mathrm{c}(g) = \mathrm{c}(f + X^2 g)$.

2. Results from *1* and from the general results on the dimension of $\mathbf{A}[X]$, for an arbitrary ring and for a Prüfer ring.

3. The answer seems to be yes.

Exercise 9. *1.* It suffices to show, for two ideals $\mathfrak{a}$, $\mathfrak{b}$ and two elements u, $v \in \mathbf{A}$, that

$$\big((\mathfrak{a} : u^\infty) + \mathbf{A}u\big)\,\big((\mathfrak{b} : u^\infty) + \mathbf{A}u\big) \subseteq (\mathfrak{a}\mathfrak{b} : u^\infty) + \mathbf{A}u \quad \text{and}$$
$$\big((\mathfrak{a} : u^\infty) + \mathbf{A}u\big)\,\big((\mathfrak{a} : v^\infty) + \mathbf{A}v\big) \subseteq (\mathfrak{a} : (uv)^\infty) + \mathbf{A}uv.$$

The first inclusion stems from $(\mathfrak{a} : u^\infty)\,(\mathfrak{b} : u^\infty) \subseteq (\mathfrak{a}\mathfrak{b} : u^\infty)$ and the second from $(\mathfrak{a} : u^\infty) + (\mathfrak{a} : v^\infty) \subseteq (\mathfrak{a} : (uv)^\infty)$.

Exercise 10. *1.* As $\beta > \alpha$, $\underline{X}^\beta$ is a multiple of one of the following monomials

$$X_1^{\alpha_1} X_2^{\alpha_2} \cdots X_{n-1}^{\alpha_{n-1}} X_n^{1+\alpha_n},\ X_1^{\alpha_1} X_2^{\alpha_2} \cdots X_{n-1}^{1+\alpha_{n-1}},\ \ldots,\ X_1^{\alpha_1} X_2^{1+\alpha_2},\ X_1^{1+\alpha_1}.$$

2a. Let $y \in \prod_{\beta<\alpha} \mathrm{Ann}(a_\beta)$; by letting $Q(\underline{X}) = yP(\underline{X})$, we have

$$Q(\underline{X}) = ya_\alpha \underline{X}^\alpha + \textstyle\sum_{\beta>\alpha} ya_\beta \underline{X}^\beta \quad \text{and} \quad Q(\underline{x}) = 0.$$

To show that $ya_\alpha \in \mathcal{I}^{\mathrm{K}}(\underline{x})$, we can therefore suppose that we have $y = 1$ and $P(\underline{X}) = a_\alpha \underline{X}^\alpha + \sum_{\beta>\alpha} a_\beta \underline{X}^\beta$. By using the equality $P(\underline{x}) = 0$ and the first question, we obtain $a_\alpha \in \mathcal{I}^{\mathrm{K}}(\underline{x})$.

2b. First, since $\mathbf{A}$ is reduced, we have $\mathcal{I}^{\mathrm{K}}(a) = \mathrm{Ann}(a) + \mathbf{A}a$, $\forall a \in \mathbf{A}$. Next, we use the following remark: let $\mathfrak{c}$ be an ideal and $2m$ ideals $\mathfrak{a}_1$, $\mathfrak{b}_1$, $\ldots$, $\mathfrak{a}_m$, $\mathfrak{b}_m$ such that $\mathfrak{a}_1 \cdots \mathfrak{a}_{k-1}\mathfrak{b}_k \subseteq \mathfrak{c}$ for every $k \in [\![1..m]\!]$. Then we obtain the inclusion

$$(\mathfrak{a}_1 + \mathfrak{b}_1) \cdots (\mathfrak{a}_m + \mathfrak{b}_m) \subseteq \mathfrak{c} + \mathfrak{a}_1 \cdots \mathfrak{a}_m.$$

Indeed, by induction on m, if $(\mathfrak{a}_1 + \mathfrak{b}_1) \cdots (\mathfrak{a}_{m-1} + \mathfrak{b}_{m-1}) \subseteq \mathfrak{c} + \mathfrak{a}_1 \cdots \mathfrak{a}_{m-1}$, we deduce

$$\mathfrak{a}_1 + \mathfrak{b}_1) \cdots (\mathfrak{a}_m + \mathfrak{b}_m) \subseteq \mathfrak{c} + \mathfrak{a}_1 \cdots \mathfrak{a}_{m-1}\mathfrak{a}_m + \mathfrak{a}_1 \cdots \mathfrak{a}_{m-1}\mathfrak{b}_m \subseteq \mathfrak{c} + \mathfrak{a}_1 \cdots \mathfrak{a}_{m-1}\mathfrak{a}_m + \mathfrak{c},$$

hence the stated inclusion.
Let us apply this to $\mathfrak{c} = \mathcal{I}^{\mathrm{K}}(\underline{x})$ and to the ideals $\mathfrak{a}_\beta = \mathrm{Ann}(a_\beta)$, $\mathfrak{b}_\beta = \mathbf{A}a_\beta$.
As $\mathrm{Ann}(a_\beta) + \mathbf{A}a_\beta = \mathcal{I}^{\mathrm{K}}(a_\beta)$, we obtain the desired inclusion.

3. Direct application with $n = 1$.

4. We can suppose that $\mathbf{A}$, $\mathbf{B}$ are reduced even if it entails replacing $\mathbf{A} \to \mathbf{B}$ with $\mathbf{A}_{\mathrm{red}} \to \mathbf{B}_{\mathrm{red}}$ (every $z \in \mathbf{B}$ remains primitively algebraic). We can also suppose that $\mathbf{A} \subseteq \mathbf{B}$ even if it entails replacing $\mathbf{A}$ with its image in $\mathbf{B}$. Let us show that $\mathsf{Kdim}\,\mathbf{A} \leqslant m \Rightarrow \mathsf{Kdim}\,\mathbf{B} \leqslant m$ by induction on m. It suffices to show, for $x \in \mathbf{B}$, that $\mathsf{Kdim}(\mathbf{B}\big/\mathcal{I}^{\mathrm{K}}_{\mathbf{B}}(x)) \leqslant m-1$; but $\mathcal{I}^{\mathrm{K}}_{\mathbf{B}}(x)$ contains an ideal $\mathfrak{a}$ of $\mathbf{A}$, finite products of boundary ideals $\mathcal{I}^{\mathrm{K}}_{\mathbf{A}}(a)$, $a \in \mathbf{A}$.
We therefore have an algebra $\mathbf{A}/\mathfrak{a} \to \mathbf{B}\big/\mathcal{I}^{\mathrm{K}}_{\mathbf{B}}(x)$ to which we can apply the induction hypothesis since $\mathsf{Kdim}\,\mathbf{A}/\mathfrak{a} \leqslant m-1$.

Exercise 11. *1.* We use the integral extension $\overline{\mathbf{A}} = \mathbf{A}/\mathbf{A} \cap \mathfrak{b} \hookrightarrow \overline{\mathbf{B}} = \mathbf{B}/\mathfrak{b}$.
Let $a \in \mathbf{A} \cap (\mathfrak{b} + \mathfrak{a}\mathbf{B})$; the Lying Over (VI-3.12) with $\overline{\mathbf{A}} \subseteq \overline{\mathbf{B}}$, gives $\overline{a}^n \in \overline{\mathfrak{a}}$, i.e. $a^n \in \mathfrak{a} + \mathfrak{b}$ and as $a \in \mathbf{A}$, $a^n \in \mathfrak{a} + \mathbf{A} \cap \mathfrak{b}$.

2. By induction on d. Let

$$\mathfrak{a} = \mathcal{I}^{\mathrm{K}}_{\mathbf{A}}(a_0, \ldots, a_{d-1}),\ \mathfrak{a}' = \mathcal{I}^{\mathrm{K}}_{\mathbf{A}}(a_0, \ldots, a_d),\ \mathfrak{b} = \mathcal{I}^{\mathrm{K}}_{\mathbf{B}}(a_0, \ldots, a_{d-1}),\ \mathfrak{b}' = \mathcal{I}^{\mathrm{K}}_{\mathbf{B}}(a_0, \ldots, a_d).$$

We therefore have by definition $\mathfrak{a}' = (\mathfrak{a} : a_d^\infty)_{\mathbf{A}} + \mathbf{A}a_d$ and $\mathfrak{b}' = (\mathfrak{b} : a_d^\infty)_{\mathbf{B}} + \mathbf{B}a_d$. We want to show that $\mathbf{A} \cap \mathfrak{b}' \subseteq \mathrm{D}_{\mathbf{A}}(\mathfrak{a}')$. Item *1* gives $\mathbf{A} \cap \mathfrak{b}' \subseteq \mathrm{D}_{\mathbf{A}}(\mathfrak{c})$ with $\mathfrak{c} = \mathbf{A}a_d + \mathbf{A} \cap (\mathfrak{b} : a_d^\infty)_{\mathbf{B}} = \mathbf{A}a_d + (\mathbf{A} \cap \mathfrak{b} : a_d^\infty)_{\mathbf{A}}$.

By induction, $\mathbf{A} \cap \mathfrak{b} \subseteq \mathrm{D}_{\mathbf{A}}(\mathfrak{a})$, therefore

$$\mathfrak{c} \subseteq \mathbf{A}a_d + (\mathrm{D}_{\mathbf{A}}(\mathfrak{a}) : a_d^\infty)_{\mathbf{A}} \subseteq \mathrm{D}_{\mathbf{A}}(\mathbf{A}a_d + (\mathfrak{a} : a_d^\infty)_{\mathbf{A}}) \overset{\mathrm{def}}{=} \mathrm{D}_{\mathbf{A}}(\mathfrak{a}'),$$

hence $\mathbf{A} \cap \mathfrak{b}' \subseteq \mathrm{D}_{\mathbf{A}}(\mathfrak{a}')$.

Exercise 12. *1.* Let $t \in S+\mathfrak{a}\mathbf{B}$; i.e. $t+s \in \mathfrak{a}\mathbf{B}$ with $s \in S$. So, $t+s$ is integral over $\mathfrak{a}$, i.e. is a zero of a monic polynomial $P(X) \in X^n + \mathfrak{a}X^{n-1} + \cdots + \mathfrak{a}^{n-1}X + \mathfrak{a}^n$. We write $P(T+s) = TQ(T) + P(s)$. Thus $P(s) \in s^n + \mathfrak{a}$ and $tQ(t) \in S + \mathfrak{a}$.

2. By induction on d. Let $V = \mathcal{S}_{\mathbf{B}}^{\mathrm{K}}(a_0, \ldots, a_d) = a_0^{\mathbb{N}}(\mathcal{S}_{\mathbf{B}}^{\mathrm{K}}(a_1, \ldots, a_d) + a_0\mathbf{B})$; the induction provides $\mathcal{S}_{\mathbf{B}}^{\mathrm{K}}(a_1, \ldots, a_d) \subseteq \mathcal{S}_{\mathbf{A}}^{\mathrm{K}}(a_1, \ldots, a_d)^{\mathrm{sat}_{\mathbf{B}}}$ so

$$V \subseteq a_0^{\mathbb{N}}(\mathcal{S}_{\mathbf{A}}^{\mathrm{K}}(a_1, \ldots, a_d)^{\mathrm{sat}_{\mathbf{B}}} + a_0\mathbf{B}) \subseteq a_0^{\mathbb{N}}(\mathcal{S}_{\mathbf{A}}^{\mathrm{K}}(a_1, \ldots, a_d) + a_0\mathbf{B})^{\mathrm{sat}_{\mathbf{B}}}.$$

The first question provides

$$V \subseteq a_0^{\mathbb{N}}(\mathcal{S}_{\mathbf{A}}^{\mathrm{K}}(a_1, \ldots, a_d) + a_0\mathbf{A})^{\mathrm{sat}_{\mathbf{B}}} \subseteq \big(a_0^{\mathbb{N}}(\mathcal{S}_{\mathbf{A}}^{\mathrm{K}}(a_1, \ldots, a_d) + a_0\mathbf{A})\big)^{\mathrm{sat}_{\mathbf{B}}},$$

i.e. $V \subseteq \mathcal{S}_{\mathbf{A}}^{\mathrm{K}}(a_0, \ldots, a_d)^{\mathrm{sat}_{\mathbf{B}}}$.

Exercise 13. *2.* The quotient ring $\mathbf{A}/\langle X_1 - Y_1 \rangle$ can be seen as the localization of $\mathbf{K}[X_1, \ldots, X_n, Y_2, \ldots, Y_m]$ at the monoid

$$S_1 = (\mathbf{K}[X_1, \ldots, X_n])^*(\mathbf{K}[X_1, Y_2, \ldots, Y_m])^*.$$

It is therefore integral. In the same way, we describe the successive quotients.

Exercise 14. *1.* Let $\mathfrak{a}_i := \mathcal{I}^{\mathrm{K}}(x_1, \ldots, x_i)$, with $\mathfrak{a}_{i+1} = (\mathfrak{a}_i : x_{i+1}^\infty) + \mathbf{A}x_{i+1}$. By induction, $\mathfrak{a}_i \subseteq \mathfrak{p}_i$: $x_{i+1} \notin \mathfrak{p}_i$ gives $(\mathfrak{p}_i : x_{i+1}^\infty) \subseteq \mathfrak{p}_i$, then $\mathfrak{a}_{i+1} \subseteq \mathfrak{p}_i + \mathbf{A}x_{i+1}$, so $\mathfrak{a}_{i+1} \subseteq \mathfrak{p}_{i+1}$. The rest poses no difficulties.

2. By letting $S_i = \mathcal{S}^{\mathrm{K}}(x_{i+1}, \ldots, x_d)$, we have $S_d = 1$ and $S_{i-1} = x_i^{\mathbb{N}}(S_i + \mathbf{A}x_i)$. Step by step, we prove $S_i \subseteq \mathfrak{f}_i$ by using $x_i \in \mathfrak{p}_i$ and $x_i \in f_{i-1}$:

$$S_{i-1} = x_i^{\mathbb{N}}(S_i + \mathbf{A}x_i) \subseteq x_i^{\mathbb{N}}(\mathfrak{f}_i + \mathfrak{p}_i) = x_i^{\mathbb{N}}\mathfrak{f}_i \subseteq x_i^{\mathbb{N}}\mathfrak{f}_{i-1} \subseteq \mathfrak{f}_{i-1}.$$

The rest poses no difficulties.

Exercise 15. If f is monic of degree $n \geqslant 1$, the polynomial $R(X,Y)$ defined in the statement of the question is Y-monic of degree n, therefore $\mathrm{Ann}(R) = 0$, and $R(f,g) = 0$ because $R \in \langle f(T) - X, Y - g(T) \rangle_{\mathbf{A}[T,X,Y]}$.

1. Let $f = \sum_{k=0}^{n} a_k T^k$. By Lemma IV-6.4 there exists a fundamental system of orthogonal idempotents $(t_n, t_{n-1}, \ldots, t_0, t_{-1})$ such that:

- in the component $t_k = 1$ for $k \in [\![0..n]\!]$, we have $a_i = 0$ for $i > k$ and a_k regular;
- in the component $t_{-1} = 1$, we have $f = 0$, i.e. $t_{-1}f = 0$ and even $\mathrm{Ann}(f) = \langle t_{-1} \rangle$.

Let m be the formal degree of g. For $1 \leqslant k \leqslant n$, we let

$$R_k(X,Y) = t_k \mathrm{Res}_T(t_k f(T) - X, k, Y - g(T), m).$$

We define $R_0(X,Y) = t_0(t_0 f(T) - X)$ and $R_{-1}(X,Y) = t_{-1}X$. For $k \in [\![-1..n]\!]$, we have $\mathrm{Ann}(R_k) = \langle 1 - t_k \rangle$ and $R_k(f,g) = 0$. Thus by letting $R = \sum_{k=-1}^{n} R_k(X,Y)$, we have $\mathrm{Ann}(R) = 0$ and $R(f,g) = 0$.

2. Direct application of the referenced exercise.

3. By induction on the Krull dimension of $\mathbf{A}$. We can replace $\mathbf{A}$ by a ring $\mathbf{A}' := \mathbf{A}_{\{\underline{a}\}}$ such that the annihilator (in $\mathbf{A}'$) of each coefficient of f is generated by an idempotent (recall that $\mathsf{Kdim}\,\mathbf{A} = \mathsf{Kdim}\,\mathbf{A}'$).

Then, if $\mathfrak{a} = \prod_{i,j} \mathcal{I}^{\mathrm{K}}_{\mathbf{A}}(r_{ij})$, the ring $\mathbf{A}[T]\big/\mathcal{I}^{\mathrm{K}}_{\mathbf{A}[T]}(f,g)$ is a quotient of $(\mathbf{A}/\mathfrak{a})[T]$. As $\mathsf{Kdim}(\mathbf{A}/\mathfrak{a}) < \mathsf{Kdim}\,\mathbf{A}$, we obtain by induction hypothesis

$$\mathsf{Kdim}(\mathbf{A}/\mathfrak{a})[T] \leqslant 1 + 2\,\mathsf{Kdim}(\mathbf{A}/\mathfrak{a}) \leqslant 1 + 2(\mathsf{Kdim}\,\mathbf{A} - 1), \text{ then}$$

$$\mathsf{Kdim}\,\mathbf{A}[T] \leqslant 2 + \mathsf{Kdim}\,\mathbf{A}[T]\big/\mathcal{I}^{\mathrm{K}}_{\mathbf{A}[T]}(f,g) \leqslant 2 + 1 + 2(\mathsf{Kdim}\,\mathbf{A} - 1) = 1 + 2\,\mathsf{Kdim}\,\mathbf{A}.$$

4. We preserve the notations of the previous questions. Each $\mathcal{I}^{\mathrm{K}}_{\mathbf{A}'}(r_{ij})$ contains a finite product of boundary ideals of $\mathbf{A}$ (Exercise 10) therefore the product of the $\mathcal{I}^{\mathrm{K}}_{\mathbf{A}'}(r_{ij})$'s contains an ideal $\mathfrak{a}$ of $\mathbf{A}$, a finite product of boundary ideals of $\mathbf{A}$. Thus $\mathfrak{a} \subset \mathbf{A}[T] \cap \mathcal{I}^{\mathrm{K}}_{\mathbf{A}'[T]}(f,g) \subseteq \mathrm{D}_{\mathbf{A}[T]}\big(\mathcal{I}^{\mathrm{K}}_{\mathbf{A}[T]}(f,g)\big)$ (Exercise 11).

Exercise 16. *1.* By induction on n, the case $n = 0$ being the hypothesis. Let us add an element b to $b_1, \dots, b_n$ and let $\mathfrak{b}'_j = \mathcal{I}^{\mathrm{K}}(z_j, b_1, \dots, b_n, b)$.
By definition $\mathfrak{b}'_j = \mathbf{B}b + (\mathfrak{b}_j : b^\infty)$ with $\mathfrak{b}_j = \mathcal{I}^{\mathrm{K}}(z_j, b_1, \dots, b_n)$; the product of the $\mathfrak{b}_j$'s is contained in $\mathcal{I}^{\mathrm{K}}(x, y, b_1, \dots, b_n)$ (by induction). By using inclusions of the type $(\mathfrak{b} : b^\infty)(\mathfrak{b}' : b^\infty) \subseteq (\mathfrak{b}\mathfrak{b}' : b^\infty)$, we obtain

$$\begin{aligned}\textstyle\prod_j \mathfrak{b}'_j \ &\subseteq \ \mathbf{B}b + \textstyle\prod_j (\mathfrak{b}_j : b^\infty) \subseteq \mathbf{B}b + \big(\textstyle\prod_j \mathfrak{b}_j : b^\infty\big) \\ &\subseteq \ \mathbf{B}b + (\mathcal{I}^{\mathrm{K}}(x, y, b_1, \dots, b_n) : b^\infty) = \mathcal{I}^{\mathrm{K}}(x, y, b_1, \dots, b_n, b).\end{aligned}$$

2a. Results from the fact that for two ideals $\mathfrak{a}, \mathfrak{b}$ of $\mathbf{A}$, we have

$$(\mathfrak{a} : \mathfrak{b})_{\mathbf{A}}\, \mathbf{A}[T] = (\mathfrak{a} : \mathfrak{b})_{\mathbf{A}[T]}.$$

2b. For two ideals $\mathfrak{a}, \mathfrak{b}$, let $\mathfrak{a} \Subset \mathfrak{b}$ for $\mathfrak{a} \subseteq \mathrm{D}(\mathfrak{b})$. We reason by induction on d, the case $d = 1$ appearing in Exercise 15.
Consider $2(d+1)$ polynomials p, q, g_1, $\dots$, $g_{2d} \in \mathbf{A}[T]$. There exist a_j's $\in \mathbf{A}$ such that $\prod_j \mathcal{I}^{\mathrm{K}}_{\mathbf{A}}(a_j) \Subset \mathcal{I}^{\mathrm{K}}_{\mathbf{A}[T]}(p, q)$ (the case $d = 1$). By the first question,

$$\textstyle\prod_j \mathcal{I}^{\mathrm{K}}_{\mathbf{A}[T]}(a_j, g_1, \dots, g_{2d}) \Subset \mathcal{I}^{\mathrm{K}}_{\mathbf{A}[T]}(p, q, g_1, \dots, g_{2d}).$$

It suffices therefore to show, for $a \in \mathbf{A}$, that a boundary ideal $\mathcal{I}^{\mathrm{K}}_{\mathbf{A}[T]}(a, g_1, \dots, g_{2d})$ contains, up to radical, a product of boundary ideals of $d + 1$ elements of $\mathbf{A}$. Let $\overline{\mathbf{A}} = \mathbf{A}\big/\mathcal{I}^{\mathrm{K}}(a)$ and $\varphi : \mathbf{A}[T] \to \overline{\mathbf{A}}[T] \simeq \mathbf{A}[T]\big/\big(\mathcal{I}^{\mathrm{K}}_{\mathbf{A}[T]}(a)\big)$ be the homomorphism of passage to the quotient. By induction, the boundary ideal $\mathcal{I}^{\mathrm{K}}_{\overline{\mathbf{A}}[T]}(\overline{g_1}, \dots, \overline{g_{2d}})$ contains, up to radical, a product $\prod_j \mathfrak{a}_j$ where each $\mathfrak{a}_j$ is a boundary ideal of d elements of $\overline{\mathbf{A}}$. By taking the inverse image under φ, we obtain

$$\textstyle\prod_i \varphi^{-1}(\mathfrak{a}_i) \subseteq \varphi^{-1}\big(\prod_i \mathfrak{a}_i\big) \Subset \varphi^{-1}\big(\mathcal{I}^{\mathrm{K}}_{\overline{\mathbf{A}}[T]}(\overline{g_1}, \dots, \overline{g_{2d}})\big).$$

By using Lemma 2.12, we have on the one hand

$$\varphi^{-1}\big(\mathcal{I}^{\mathrm{K}}_{\overline{\mathbf{A}}[T]}(\overline{g_1}, \dots, \overline{g_{2d}})\big) = \mathcal{I}^{\mathrm{K}}_{\mathbf{A}[T]}(a, g_1, \dots, g_{2d}),$$

and on the other hand $\varphi^{-1}(\mathfrak{a}_i)$ is a boundary ideal of $d + 1$ elements of $\mathbf{A}$ (the first element being a). This shows that $\mathcal{I}^{\mathrm{K}}_{\mathbf{A}[T]}(a, g_1, \dots, g_{2d})$ contains up to radical, a product of boundary ideals of $d + 1$ elements of $\mathbf{A}$.

3. If $\mathbf{A}[\underline{T}] = \mathbf{A}[T_1, \dots, T_r]$, the boundary ideal of $(r+1)d$ polynomials of $\mathbf{A}[\underline{T}]$ contains, up to radical, a product of boundary ideals of d elements of $\mathbf{A}$.
Consequently, $\mathsf{Kdim}\,\mathbf{A} < d \Longrightarrow \mathsf{Kdim}\,\mathbf{A}[\underline{T}] < (r+1)d$, i.e.

$$\mathsf{Kdim}\,\mathbf{A}[\underline{T}] + 1 \ \leqslant \ (r+1)(\mathsf{Kdim}\,\mathbf{A} + 1).$$

Exercise 17. *1.* We take $a' = y \wedge a$ and $b' = x \vee b \vee a'$. Then $x \wedge a' = x \wedge y \wedge a = x \wedge a$ (because $x \leqslant y$). Then $y \vee b' = y \vee x \vee b \vee a' = (x \vee a') \vee (y \vee b) = y \vee b$ (the last equality uses $x \vee a' \leqslant y$ which stems from $x \leqslant y$ and $a' \leqslant y$, a fortiori $x \vee a' \leqslant y \vee b$).

Ir remains to see that $y \wedge b' = x \vee a'$; we have the identity for all y, b, z, $y \wedge (b \vee z) = y \wedge z'$ with $z' = (y \wedge b) \vee z$ that we use with $z = x \vee a'$. But we have $y \wedge b \leqslant x \vee a'$ because the hypothesis is $y \wedge b \leqslant x \vee a$, so $y \wedge b \leqslant (x \vee a) \wedge y = (x \wedge y) \vee (y \wedge a) \leqslant x \vee a'$. Therefore $z' = x \vee a'$ and $y \wedge b' = y \wedge (x \vee a')$. Finally, $y \wedge (x \vee a') = x \vee a'$ because $x \vee a' \leqslant y$ (by using $x \leqslant y$ and $a' \leqslant y$).

2. By *1* by induction on n.

3. Item *3a* implies item *3c* by item *2*. Item *3c* implies item *3b* because a linked chain is a particular case of complementary sequence. In order to see that *3b* implies *3a*, let $y_0, \ldots, y_n$ be arbitrary. We define $x_0 = y_0$, $x_i = y_i \vee x_{i-1}$ ($i \in [\![1..n]\!]$). Let $(a_0, \ldots, a_n)$ be a complementary sequence of $(x_0, \ldots, x_n)$. We define $b_0 = a_0$ and $b_i = a_i \vee x_{i-1}$ for $i \in [\![1..n]\!]$. We have $x_i \vee a_i = y_i \vee b_i$ for $i \in [\![0..n]\!]$. Thus $0 = x_0 \wedge a_0 = y_0 \wedge b_0$ and $1 = x_n \vee a_n = y_n \vee b_n$. Let us see the intermediary inequalities. For $i \in [\![1..n]\!]$ we have $x_i \wedge a_i \leqslant x_{i-1} \vee a_{i-1}$, so

$$y_i \wedge a_i \leqslant x_i \wedge a_i \leqslant x_{i-1} \vee a_{i-1} = y_{i-1} \vee b_{i-1}$$

Then we have

$$y_i \wedge b_i = y_i \wedge (a_i \vee x_{i-1}) = (y_i \wedge a_i) \vee (y_i \wedge x_{i-1}) \leqslant (y_i \wedge a_i) \vee x_{i-1}$$

As the two terms after $\leqslant$ are bounded by $x_{i-1} \vee a_{i-1} = y_{i-1} \vee b_{i-1}$ we get the inequality $y_i \wedge b_i \leqslant y_{i-1} \vee b_{i-1}$.

Exercise 18. First of all, for every ideal $\mathfrak{c}$, the ring $\mathbf{A}\big/\mathfrak{c}^{\perp}$ is reduced.

Let us show that $(\mathfrak{a}_1^{\perp}\mathfrak{a}_2^{\perp})^{\perp} = (\mathfrak{a}_1 + \mathfrak{a}_2)^{\perp\perp}$: the equality $\mathfrak{a}_1^{\perp} \cap \mathfrak{a}_2^{\perp} = (\mathfrak{a}_1 + \mathfrak{a}_2)^{\perp}$ implies that the ideals $\mathfrak{a}_1^{\perp} \cap \mathfrak{a}_2^{\perp}$, $\mathfrak{a}_1^{\perp}\mathfrak{a}_2^{\perp}$ and $(\mathfrak{a}_1 + \mathfrak{a}_2)^{\perp}$ have the same nilradical therefore the same annihilator.

We deduce that

$$(\mathfrak{a}_1^{\perp}\mathfrak{a}_2^{\perp}\mathfrak{b})^{\perp} = (\mathfrak{a}_1 + \mathfrak{a}_2) \diamond \mathfrak{b}.$$

Indeed

$$(\mathfrak{a}_1^{\perp}\mathfrak{a}_2^{\perp}\mathfrak{b})^{\perp} = \big((\mathfrak{a}_1^{\perp}\mathfrak{a}_2^{\perp})^{\perp} : \mathfrak{b}\big) = \big((\mathfrak{a}_1 + \mathfrak{a}_2)^{\perp\perp} : \mathfrak{b}\big) = (\mathfrak{a}_1 + \mathfrak{a}_2) \diamond \mathfrak{b}.$$

1. As $\mathfrak{a}^{\perp}\mathfrak{b} \subseteq \mathfrak{a}^{\perp}$, we have $\mathfrak{a} \diamond \mathfrak{b} \supseteq \mathfrak{a}^{\perp\perp} \supseteq \mathfrak{a}$. Let $x \in \mathbf{A}$ such that in the quotient we have $\overline{x}\,\overline{\mathfrak{b}} = 0$, that is $x\mathfrak{b} \subseteq \mathfrak{a} \diamond \mathfrak{b}$, i.e. $x\mathfrak{b}\mathfrak{a}^{\perp}\mathfrak{b} = 0$. We therefore have $x\mathfrak{b}\mathfrak{a}^{\perp} = 0$, that is $x \in \mathfrak{a} \diamond \mathfrak{b}$, i.e. $\overline{x} = 0$.

2. We have

$$(\mathbf{A}/\mathfrak{a}_1 \diamond \mathfrak{b}_1)\big/(\overline{\mathfrak{a}_2} \diamond \overline{\mathfrak{b}_2}) \simeq \mathbf{A}\big/(\mathfrak{a}_1^{\perp}\mathfrak{a}_2^{\perp}\mathfrak{b}_1\mathfrak{b}_2)^{\perp} = \mathbf{A}\big/\big((\mathfrak{a}_1 + \mathfrak{a}_2) \diamond (\mathfrak{b}_1\mathfrak{b}_2)\big) .$$

Exercise 19. *1.* Let $y \in \mathbf{B}$ and suppose $y\theta(a) = 0$. Let $e' = \theta(e)$. We must show that $y = ye'$. Since $e + a$ is regular, $e' + \theta(a)$ is regular. However, $y\big(e' + \theta(a)\big) = ye' = ye'\big(e' + \theta(a)\big)$ because e' is idempotent.

2. The homomorphism $\mathbf{A}_{\mathrm{pp}} \to \mathbf{A}_{\min}$ comes from the universal property of $\mathbf{A}_{\mathrm{pp}}$. It is surjective because $\mathbf{A}_{\min} = \mathbf{A}[(e_x)_{x \in \mathbf{A}}]$ and because the morphism $\mathbf{A}_{\mathrm{pp}} \to \mathbf{A}_{\min}$ is a pp-ring.

3. Let x be regular in $\mathbf{A}$ and $u = (\overline{y}, \widetilde{z}) \in \mathbf{A}_{\{a\}} = \mathbf{A}\big/a^{\perp} \times \mathbf{A}\big/(a^{\perp})^{\perp}$, with $ux = 0$. We must show that $u = 0$, i.e. $\overline{y} = \overline{0}$ and $\widetilde{z} = \widetilde{0}$.
We have $xy \in a^{\perp}$, i.e. $xay = 0$, so $ay = 0$, then $\overline{y} = \overline{0}$.
To see that $\widetilde{z} = \widetilde{0}$ we consider an arbitrary element t of $a^{\perp}$ and we must show that $zt = 0$. However, $\widetilde{xz} = \widetilde{0}$, so $xzt = 0$, then $zt = 0$.

4. If $a \in \mathbf{A}$ is regular, it remains regular at the finite stages of the construction of $\mathbf{A}_{\min}$ by item *3* and this is sufficient for it to be regular in $\mathbf{A}_{\min}$. If the natural homomorphism $\mathbb{Z} \to \mathbb{Z}_{\mathrm{qi}}$ were regular all the homomorphisms from $\mathbb{Z}$ to pp-rings would be regular given the universal property of $\mathbb{Z}_{\mathrm{qi}}$. However, the surjection $\mathbb{Z} \to \mathbb{Z}/\langle n \rangle$ is not a regular homomorphism for $n \geqslant 2$. Note that the argument applies to every ring $\mathbf{A}$ for which there exists a regular element x such that $\mathbf{A}/\langle x \rangle$ is a pp-ring and is nontrivial.

Exercise 20. Let us write the computation for $n = k = 2$.
Let $x_1 = \frac{a_1}{b_1}$, $x_2 = \frac{a_2}{b_2} \in \operatorname{Frac}\mathbf{A}$ and $s = \big(P(x_1, x_2), (Q(x_1, x_2), (R(x_1, x_2)\big)$ be a sequence in $\mathbf{A}[x_1, x_2]$, with P, Q, $R \in \mathbf{A}[X_1, X_2]$. We must show that the sequence s is singular. Let $\mathbf{A}_1 = \mathbf{A}[x_1]$. We know that the sequence

$$(b_1X_1 - a_1, b_2X_2 - a_2, P, Q, R) = (f_1, f_2, P, Q, R)$$

is singular in $\mathbf{A}[X_1, X_2]$, which gives an equality

$$f_1^m(f_2^m(P^m(Q^m(R^m(1 + AR) + BQ) + CP) + Df_2) + Ef_1) = 0$$

in $\mathbf{A}[X_1, X_2]$. Since $b_1 \in \operatorname{Reg}\mathbf{A}$, we have $f_1 \in \operatorname{Reg}\mathbf{A}[X_1, X_2]$ (McCoy's lemma, Corollary III-2.3). We therefore simplify the equality by f_1^m, then we evaluate it in $\mathbf{A}_1[X_2]$ by the morphism $X_1 \mapsto x_1$. We obtain the following equality in $\mathbf{A}_1[X_2]$

$$f_2^m(p^m(q^m(r^m(1 + ar) + bq) + cp) + df_2) = 0,$$

with $p = P(x_1, X_2)$, $q = Q(x_1, X_2)$, …, $d = D(x_1, X_2)$.
Since $b_2 \in \operatorname{Reg}\mathbf{A}_1$, we have $f_2 \in \operatorname{Reg}\mathbf{A}_1[X_2]$. We can therefore simplify the equality by f_2^m, then evaluate it in $\mathbf{A}[x_1, x_2]$ by the morphism $X_2 \mapsto x_2$. We obtain an equality which says that the sequence s is singular.

Exercise 22. Let a, b and c be the three properties for the commutative rings. The equivalence of a and b is easy. The implication $a \Rightarrow c$ has been given as a remark after the Lying Over (Lemma VI-3.12).
$c \Rightarrow a$. In classical mathematics $\mathrm{D}_{\mathbf{A}}(\mathfrak{a})$ is the intersection of the prime ideals that contain $\mathfrak{a}$. We therefore want to show that for every prime ideal $\mathfrak{p}$ such that $\mathfrak{a} \subseteq \mathfrak{p}$, we have $\varphi^{-1}(\langle\varphi(\mathfrak{a})\rangle) \subseteq \mathfrak{p}$. Let $\mathfrak{q}$ be a prime ideal of $\mathbf{B}$ above $\mathfrak{p}$, i.e. $\varphi^{-1}(\mathfrak{q}) = \mathfrak{p}$. Then, $\langle\varphi(\mathfrak{a})\rangle \subseteq \langle\varphi(\mathfrak{p})\rangle \subseteq \mathfrak{q}$, hence $\varphi^{-1}(\langle\varphi(\mathfrak{a})\rangle) \subseteq \mathfrak{p}$.

Problem 1. *1a.* We have some nonzero $a \in \operatorname{Ann}(x)\mathfrak{a}$, in particular $ax = 0$. Let us show that $a \notin \mathrm{D}(x)$: if $a^n \in \langle x \rangle$, then $a^{n+1} \in \langle ax \rangle = 0$, and so $a = 0$. Therefore $\mathrm{D}(x) \subsetneq \mathrm{D}(x, a) = \mathrm{D}(ax, a + x) = \mathrm{D}(a + x)$: we take $x' = a + x$ (which is indeed in $\mathfrak{a}$).

1b. Let $x_0 = 0$. If $\operatorname{Ann}(x_0)\mathfrak{a} = 0$, that is $\mathfrak{a} = 0$, then $\operatorname{Ann}(x_0) \subseteq \operatorname{Ann}(\mathfrak{a})$, so $\operatorname{Ann}(x_0) = \operatorname{Ann}(\mathfrak{a})$. In this case we let $x_i = x_0$ for every $i \geqslant 0$. Otherwise, there is some $x_1 \in \mathfrak{a}$ with $\mathrm{D}(x_0) \subsetneq \mathrm{D}(x_1)$. If $\operatorname{Ann}(x_1)\mathfrak{a} = 0$, then $\operatorname{Ann}(x_1) \subseteq \operatorname{Ann}(\mathfrak{a})$, so $\operatorname{Ann}(x_1) = \operatorname{Ann}(\mathfrak{a})$. In this case we let $x_i = x_1$ for every $i \geqslant 1$. Otherwise, there is some $x_2 \in \mathfrak{a}$ with $\mathrm{D}(x_1) \subsetneq \mathrm{D}(x_2)$ ……

This way we construct a non-decreasing infinite sequence of ideals $\mathrm{D}(x_i)$, which is stationary as soon as two consecutive terms are equal, in which case the initial problem is solved.[5]

2. Let $y \in \mathbf{A}$. By the hypothesis, we apply item *1* with the ideal $\mathfrak{a} = \mathrm{Ann}(y)$ and we know how to determine some $x \in \mathrm{Ann}(y)$ such that $\mathrm{Ann}(x) = \mathrm{Ann}\big(\mathrm{Ann}(y)\big)$, i.e. $xy = 0$ and $\mathrm{Ann}(x)\mathrm{Ann}(y) = 0$. We then have $\big(\mathrm{Ann}(y) \cap \mathrm{Ann}(x)\big)^2 \subseteq \mathrm{Ann}(x)\mathrm{Ann}(y) = 0$, so $\mathrm{Ann}(x) \cap \mathrm{Ann}(y) = 0$ (the ring is reduced). Let us show that $x + y$ is regular; suppose $z(x + y) = 0$. By multiplying by y, $zy^2 = 0$, so $zy = 0$, then $zx = 0$, so $z \in \mathrm{Ann}(x) \cap \mathrm{Ann}(y) = 0$. Consequently, $x+y$ is invertible and this element is in the boundary ideal of y since $x \in \mathrm{Ann}(y)$.

3. For every ring $\mathbf{C}$, every regular element of $\mathrm{Frac}(\mathbf{C})$ is invertible. We can apply the result of item *2* to the ring $\mathbf{C} = \mathrm{Frac}(\mathbf{B}_{\mathrm{red}})$.
Indeed, the first hypothesis that needs to be checked is that every ascending sequence of ideals of the form $\mathrm{D}_{\mathbf{C}}(x_n/y_n)$ ($x_n \in \mathbf{B}_{\mathrm{red}}$, $y_n \in \mathrm{Reg}(\mathbf{B}_{\mathrm{red}})$) admits two equal consecutive terms. However, in $\mathbf{C}$ we have the equality $\mathrm{D}_{\mathbf{C}}(x_n/y_n) = \mathrm{D}_{\mathbf{C}}(x_n)$, and the result follows by the fact that in $\mathbf{B}$, the ascending sequence $\langle x_0, \dots, x_n\rangle_{\mathbf{B}}$ admits two equal consecutive terms.
The second hypothesis is that we know how to test, for $\frac{x}{u}, \frac{y}{v} \in \mathbf{C}$,

$$\mathrm{Ann}\big(\tfrac{x}{u}\big)\mathrm{Ann}\big(\tfrac{y}{v}\big) = 0?$$

which is the same thing as $\mathrm{Ann}(x)\mathrm{Ann}(y) = 0$ in $\mathbf{B}_{\mathrm{red}}$. However, in $\mathsf{Zar}\,\mathbf{B}$ we have the equality $\mathrm{Ann}_{\mathbf{B}_{\mathrm{red}}}(x) = \mathrm{D}_{\mathbf{B}}(x) \to \mathrm{D}_{\mathbf{B}}(0)$, and we know that $\mathsf{Zar}\,\mathbf{B}$ is a discrete Heyting algebra (Proposition 6.9).

Problem 2. *1.* Let $\pi : \mathbf{B} \to \mathbf{A}$ be an $\mathbf{A}$-projector of image $\mathbf{A}$.
Let $a \in \mathfrak{a}\mathbf{B} \cap \mathbf{A}$, $a = \sum_i a_i b_i$ with $a_i \in \mathfrak{a}$, $b_i \in \mathbf{B}$; so $a = \pi(a) = \sum_i a_i \pi(b_i) \in \mathfrak{a}$.
2. It is clear that R_G is $\mathbf{A}$-linear and that $R_G(a) = a$ for all $a \in \mathbf{A}$. The rest stems from this.

3. Let us suppose that $\mathsf{Kdim}\,\mathbf{B} \leqslant d$ and show that $\mathsf{Kdim}\,\mathbf{A} \leqslant d$.
Let $a_0, \dots, a_d \in \mathbf{A}$; as $\mathsf{Kdim} \leqslant d$, there exists an $n \geqslant 0$ such that

$$(a_0 \dots a_d)^n \in \langle c_d, c_{d-1}, \cdots, c_0\rangle_{\mathbf{B}} \quad \text{with} \quad c_i = (a_0 \dots a_{i-1})^n a_i^{n+1}.$$

But $\langle c_d, c_{d-1}, \cdots, c_0\rangle_{\mathbf{B}} \cap \mathbf{A} = \langle c_d, c_{d-1}, \cdots, c_0\rangle_{\mathbf{A}}$. Therefore $\mathsf{Kdim}\,\mathbf{A} \leqslant d$.
4. (Proof in classical mathematics)
We graduate $\mathbf{B}$ by $\deg X = \deg Y = 1$ and $\deg Z = -1$. Then $\mathbf{A}$ is the homogeneous component of degree 0, so is a direct summand in $\mathbf{B}$.
Let $\mathfrak{q}' = \langle Z\rangle_{\mathbf{B}}$ (it is a prime ideal) and $\mathfrak{p}' := \mathbf{A} \cap \mathfrak{q}' = \langle XZ, YZ\rangle$.
Let $\mathfrak{p} = \langle XZ\rangle_{\mathbf{A}}$; it is a prime ideal with $\mathfrak{p} \subset \mathfrak{p}'$ but there does not exist a prime

[5] The proof that the algorithm terminates under the constructive Noetherian hypothesis which has just been given is a little confusing. Spontaneously we would have preferred to say: the algorithm needs to end some day because otherwise, we would have a strictly increasing infinite sequence. The problem with this last argument is that it is an argument by contradiction. Here we have used the Noetherian hypothesis in constructive form and this provided us with the means to know a priori when the algorithm will terminate. This delicate point sends us back to the discussion about the Markov principle (Annex page 974).

ideal $\mathfrak{q}$ of $\mathbf{B}$ contained in $\mathfrak{q}'$ and above $\mathfrak{p}$. Thus $\mathbf{A} \subseteq \mathbf{B}$ is not Going Down.
Let $\mathfrak{q} = \left\langle X, Y^2Z - 1 \right\rangle_{\mathbf{B}}$ (it is a prime ideal) and $\mathfrak{p} := \mathbf{A} \cap \mathfrak{q} = \langle XY \rangle$.
Let $\mathfrak{p}' = \langle XZ, YZ \rangle_{\mathbf{A}}$; it is a prime ideal with $\mathfrak{p} \subset \mathfrak{p}'$ but there does not exist a prime ideal $\mathfrak{q}'$ of $\mathbf{B}$ containing $\mathfrak{q}$ and lying over $\mathfrak{p}'$ (a prime ideal lying over $\mathfrak{p}'$ must contain Z, or X and Y). Thus $\mathbf{A} \subseteq \mathbf{B}$ is not Going Up.

Bibliographic comments

A very good presentation of the Krull dimension from the point of view of classical mathematics is found in [Eisenbud].

The spectral spaces were introduced by Stone [181] in 1937. The theory of spectral spaces is at the heart of this book [Johnstone].

An important Hochster theorem [107] states that every spectral space is homeomorphic to the spectrum of a commutative ring. A pointless version of the Hochster theorem is: every distributive lattice is isomorphic to the Zariski lattice of a commutative ring (for a nonconstructive proof see [5, Banaschewski]). The delicate point is to know how to construct a ring whose Zariski lattice is a given finite ordered set.

The constructive definition of the Krull dimension of distributive lattices and commutative rings dates back to the works of André Joyal [115, 116] and Luis Español [77, 78, 79, 80, 81, 82]. Joyal's idea was to construct for each integer $\ell \geqslant 1$, from the distributive lattice $\mathbf{T}$, a distributive lattice $\mathbf{T}_\ell$, that satisfies an adequate universal property such that, in classical mathematics, the prime ideals of $\mathbf{T}_\ell$ can be identified with the chains $\mathfrak{p}_0 \subseteq \cdots \subseteq \mathfrak{p}_\ell$ of prime ideals of $\mathbf{T}$ (the inclusions being not necessarily strict). This then allows for a definition of $\mathsf{Kdim}\,\mathbf{T} \leqslant \ell$ by means of a property relating $\mathbf{T}_{\ell+1}$ and $\mathbf{T}_\ell$. Finally, the Krull dimension of a commutative ring can be defined in the same way as the dimension of its Zariski lattice. For further details on the subject, see the articles [43, 44, 49, Coquand&al.].

Theorem 2.2, which gives an elementary inductive characterization of the Krull dimension of a commutative ring, is found in [50, Coquand&al.]. The characterization in terms of algebraic identities given in Proposition 2.8 are found in [43, Coquand&Lombardi] and [129, Lombardi].
Even though the characterization in terms of complementary sequences is already present for the distributive lattices in [43], it only appears for the commutative rings in [49, Coquand&al.].

Additional results on the treatment of the Krull dimension in integral extensions are found in [41, Coquand&al.]

The classical theory of valuative dimension can be found in [Jaffard], [Gilmer, Chap. 5, §30] and [26, Cahen]. Regarding the valuative dimension and

Theorem 8.20, a very elegant constructive treatment is given in the integral case by T. Coquand in [38].

The result of Exercise 10 is due to Lionel Ducos. Problem 1 is directly related to the article [51, Coquand&al.]. Problem 3 is drawn from the articles [21, Brenner], [44, Coquand&Lombardi] and [129]. A variant for distributive lattices is found in [43].

Chapter XIV

The number of generators of a module

Contents

Introduction

In this chapter we establish the elementary, non-Noetherian and constructive version of some "grand" theorems of commutative algebra.

These theorems, due in their original version to Kronecker, Bass, Serre, Forster and Swan, regard the number of radical generators of a finitely generated ideal, the number of generators of a module, the possibility of producing a free submodule as a direct summand in a module, and the possibility of simplifying isomorphisms, in the following style: if $M \oplus N \simeq M' \oplus N$, then $M \simeq M'$.

Decisive progress was made by Heitmann [101, (1984)] who proved how to get rid of Noetherian hypotheses.

Further progress was made by T. Coquand who proved in several articles how to obtain all the classical results (sometimes in a stronger form) by means of proofs that are both constructive and elementary.

The proofs given here are essentially those of [35, 37, Coquand] and of [48, 49, Coquand&al.].

1. Kronecker's theorem and Bass' stable range (non-Noetherian versions of Heitmann)

Kronecker's theorem

Kronecker's theorem[1] is usually stated in the following form ([123]): an algebraic variety in $\mathbb{C}^n$ can always be defined by $n+1$ equations.

For Kronecker it was more about replacing a system of arbitrary equations in $\mathbb{Q}[X_1, \ldots, X_n]$ with an "equivalent" system having at most $n+1$ equations. The equivalence of two systems as seen by Kronecker is translated in the current language by the fact that the two ideals have the same nilradical. It is by using the Nullstellensatz that we obtain the above formulation in the language of "algebraic varieties."

In the version proven in this section, we give the formulation à la Kronecker by replacing the ring $\mathbb{Q}[X_1, \ldots, X_n]$ with an arbitrary ring of Krull dimension $\leqslant n$.

The following lemma, although terribly trivial, is an essential key.

[1] This theorem of Kronecker is different from the one given in Chapter III.

1.1. Lemma. *For $u, v \in \mathbf{A}$ we have*

$$\mathrm{D}_{\mathbf{A}}(u,v) = \mathrm{D}_{\mathbf{A}}(u+v, uv) = \mathrm{D}_{\mathbf{A}}(u+v) \vee \mathrm{D}_{\mathbf{A}}(uv)\ .$$

In particular, if $uv \in \mathrm{D}_{\mathbf{A}}(0)$, then $\mathrm{D}_{\mathbf{A}}(u,v) = \mathrm{D}_{\mathbf{A}}(u+v)$.

D We obviously have $\langle u+v, uv\rangle \subseteq \langle u, v\rangle$, therefore $\mathrm{D}_{\mathbf{A}}(u+v, uv) \subseteq \mathrm{D}_{\mathbf{A}}(u,v)$. Moreover, $u^2 = (u+v)u - uv \in \langle u+v, uv\rangle$, so $u \in \mathrm{D}_{\mathbf{A}}(u+v, uv)$.□

Recall that two sequences that satisfy the inequalities (7) in Proposition XIII-2.8 are said to be complementary.

1.2. Lemma. *Let $\ell \geqslant 1$. If $(b_1, \dots, b_\ell)$ and $(x_1 \dots, x_\ell)$ are two complementary sequences in $\mathbf{A}$ then for every $a \in \mathbf{A}$ we have*

$$\mathrm{D}_{\mathbf{A}}(a, b_1, \dots, b_\ell) = \mathrm{D}_{\mathbf{A}}(b_1 + ax_1, \dots, b_\ell + ax_\ell),$$

i.e. $a \in \mathrm{D}_{\mathbf{A}}(b_1 + ax_1, \dots, b_\ell + ax_\ell)$.

D We have the inequalities

$$\begin{aligned}
\mathrm{D}_{\mathbf{A}}(b_1x_1) &= \mathrm{D}_{\mathbf{A}}(0)\\
\mathrm{D}_{\mathbf{A}}(b_2x_2) &\leqslant \mathrm{D}_{\mathbf{A}}(b_1, x_1)\\
\vdots\quad & \vdots \quad \vdots\\
\mathrm{D}_{\mathbf{A}}(b_\ell x_\ell) &\leqslant \mathrm{D}_{\mathbf{A}}(b_{\ell-1}, x_{\ell-1})\\
\mathrm{D}_{\mathbf{A}}(1) &= \mathrm{D}_{\mathbf{A}}(b_\ell, x_\ell).
\end{aligned}$$

We deduce these

$$\begin{aligned}
\mathrm{D}_{\mathbf{A}}(ax_1b_1) &= \mathrm{D}_{\mathbf{A}}(0)\\
\mathrm{D}_{\mathbf{A}}(ax_2b_2) &\leqslant \mathrm{D}_{\mathbf{A}}(ax_1, b_1)\\
\vdots\quad & \vdots \quad \vdots\\
\mathrm{D}_{\mathbf{A}}(ax_\ell b_\ell) &\leqslant \mathrm{D}_{\mathbf{A}}(ax_{\ell-1}, b_{\ell-1})\\
\mathrm{D}_{\mathbf{A}}(a) &\leqslant \mathrm{D}_{\mathbf{A}}(ax_\ell, b_\ell).
\end{aligned}$$

We therefore have by Lemma 1.1

$$\begin{aligned}
\mathrm{D}_{\mathbf{A}}(a) &\leqslant \mathrm{D}_{\mathbf{A}}(ax_\ell + b_\ell) \vee \mathrm{D}_{\mathbf{A}}(ax_\ell b_\ell)\\
\mathrm{D}_{\mathbf{A}}(ax_\ell b_\ell) &\leqslant \mathrm{D}_{\mathbf{A}}(ax_{\ell-1} + b_{\ell-1}) \vee \mathrm{D}_{\mathbf{A}}(ax_{\ell-1}b_{\ell-1})\\
\vdots\quad & \vdots \quad \vdots\\
\mathrm{D}_{\mathbf{A}}(ax_3b_3) &\leqslant \mathrm{D}_{\mathbf{A}}(ax_2 + b_2) \vee \mathrm{D}_{\mathbf{A}}(ax_2b_2)\\
\mathrm{D}_{\mathbf{A}}(ax_2b_2) &\leqslant \mathrm{D}_{\mathbf{A}}(ax_1 + b_1) \vee \mathrm{D}_{\mathbf{A}}(ax_1b_1) = \mathrm{D}_{\mathbf{A}}(ax_1 + b_1).
\end{aligned}$$

Therefore finally

$$\begin{aligned}
\mathrm{D}_{\mathbf{A}}(a) &\leqslant \mathrm{D}_{\mathbf{A}}(ax_1 + b_1) \vee \mathrm{D}_{\mathbf{A}}(ax_2 + b_2) \vee \cdots \vee \mathrm{D}_{\mathbf{A}}(ax_\ell + b_\ell)\\
&= \mathrm{D}_{\mathbf{A}}(ax_1 + b_1, ax_2 + b_2, \dots, ax_\ell + b_\ell).
\end{aligned}$$

□

1.3. Theorem. (Non-Noetherian Kronecker-Heitmann theorem, with the Krull dimension)

1. *Let $n \geqslant 0$. If $\mathsf{Kdim}\,\mathbf{A} < n$ and $b_1, \ldots, b_n \in \mathbf{A}$, there exist $x_1, \ldots, x_n$ such that for every $a \in \mathbf{A}$, $\mathrm{D}_{\mathbf{A}}(a, b_1, \ldots, b_n) = \mathrm{D}_{\mathbf{A}}(b_1 + ax_1, \ldots, b_n + ax_n)$.*
2. *Consequently, in a ring of dimension at most n, every finitely generated ideal has the same nilradical as an ideal generated by at most $n+1$ elements.*

D *1.* Clear by Lemma 1.2 and Proposition XIII-2.8 (if $n = 0$, the ring is trivial and $\mathrm{D}_{\mathbf{A}}(a) = \mathrm{D}_{\mathbf{A}}(\emptyset)$).
2. Stems from *1* because it suffices to iterate the procedure. Actually, if $\mathsf{Kdim}\,\mathbf{A} \leqslant n$ and $\mathfrak{a} = \mathrm{D}_{\mathbf{A}}(b_1, \ldots, b_{n+r})$ $(r \geqslant 2)$, we finally obtain

$$\mathfrak{a} = \mathrm{D}_{\mathbf{A}}(b_1 + c_1, \ldots, b_{n+1} + c_{n+1})$$

with $c_i \in \langle b_{n+2}, \ldots, b_{n+r} \rangle$. □

Bass' "stable range" theorem, 1

1.4. Theorem. (Bass' theorem, with the Krull dimension, without Noetherianity) *Let $n \geqslant 0$. If $\mathsf{Kdim}\,\mathbf{A} < n$, then $\mathsf{Bdim}\,\mathbf{A} < n$.*
Abbreviated to: $\mathsf{Bdim}\,\mathbf{A} \leqslant \mathsf{Kdim}\,\mathbf{A}$. In particular, if $\mathsf{Kdim}\,\mathbf{A} < n$, every stably free $\mathbf{A}$-module of rank $\geqslant n$ is free (see Theorem V-4.10).

D Recall that $\mathsf{Bdim}\,\mathbf{A} < n$ means that for all $b_1, \ldots, b_n \in \mathbf{A}$, there exist some x_i's such that the following implication is satisfied

$$\forall a \in \mathbf{A} \quad (1 \in \langle a, b_1, \ldots, b_n \rangle \Rightarrow 1 \in \langle b_1 + ax_1, \ldots, b_n + ax_n \rangle).$$

This results directly from the first item in Theorem 1.3. □

The local Kronecker theorem

1.5. Proposition and definition. *In a ring we consider two sequences $(a_0, \ldots, a_d)$ and $(x_0, \ldots, x_d)$ such that*

$$\left\{\begin{array}{rcl} a_0x_0 & \in & \mathrm{D}(0) \\ a_1x_1 & \in & \mathrm{D}(a_0, x_0) \\ a_2x_2 & \in & \mathrm{D}(a_1, x_1) \\ a_3x_3 & \in & \mathrm{D}(a_2, x_2) \\ & \vdots & \\ a_dx_d & \in & \mathrm{D}(a_{d-1}, x_{d-1}) \end{array}\right.$$

We will say that these two sequences are disjoint*. Then for $0 \leqslant i < d$, we have*

$$\mathrm{D}(a_0, \ldots, a_i, x_0, \ldots, x_i, a_{i+1}x_{i+1}) = \mathrm{D}(a_0 + x_0, \ldots, a_i + x_i).$$

D An inclusion is obvious. To prove the converse inclusion, we use the equalities $\mathrm{D}(a_i, x_i) = \mathrm{D}(a_i x_i, a_i + x_i)$.
We then successively get

$$\begin{array}{rclcl}
a_0x_0 \in & \mathrm{D}(0) & = & \mathrm{D}() & = \mathrm{D}() \\
 & & & & \quad \cap\!\mathrm{I} \\
a_0, x_0, a_1x_1 \in & \mathrm{D}(a_0, x_0) & = & \mathrm{D}(a_0x_0, a_0+x_0) & = \mathrm{D}(a_0+x_0) \\
 & & & & \qquad\quad \cap\!\mathrm{I} \\
a_1, x_1, a_2x_2 \in & \mathrm{D}(a_1, x_1) & = & \mathrm{D}(a_1x_1, a_1+x_1) & \subseteq \mathrm{D}(a_0+x_0, a_1+x_1) \\
 & & & & \qquad\qquad\qquad \cap\!\mathrm{I} \\
a_2, x_2, a_3x_3 \in & \mathrm{D}(a_2, x_2) & = & \mathrm{D}(a_2x_2, a_2+x_2) & \subseteq \mathrm{D}(a_0+x_0, a_1+x_1, a_2+x_2) \\
\vdots \quad \vdots \quad \vdots & \vdots & & \vdots & \vdots \qquad\qquad \vdots \\
a_i, x_i, a_{i+1}x_{i+1} \in & \mathrm{D}(a_i, x_i) & = & \mathrm{D}(a_ix_i, a_i+x_i) & \subseteq \mathrm{D}(a_0+x_0, \ldots, a_i+x_i).
\end{array}$$

□

Note that the sequences $(a_0, \ldots, a_d)$ and $(x_0, \ldots, x_d)$ are complementary if and only if they are disjoint and $1 \in \langle a_d, x_d \rangle$.

1.6. Theorem. *Let* $\mathbf{A}$ *be a residually discrete local ring of dimension at most* d*, with Jacobson radical* $\mathfrak{m}$*. We suppose that* $\mathfrak{m}$ *is* radically finitely generated*, i.e. there exist* $z_1, \ldots, z_n \in \mathbf{A}$ *such that* $\mathfrak{m} = \mathrm{D}_{\mathbf{A}}(z_1, \ldots, z_n)$*. Then* $\mathfrak{m}$ *is radically generated by* d *elements.*

D Since $\mathsf{Kdim}\,\mathbf{A} \leqslant d$ and $\mathfrak{m}$ is radically finitely generated, Kronecker's theorem 1.3 tells us that $\mathfrak{m} = \mathrm{D}(x_0, \ldots, x_d)$. In addition, there exists a complementary sequence $(\underline{a}) = (a_0, \ldots, a_d)$ of $(\underline{x}) = (x_0, \ldots, x_d)$. In particular (disjoint sequences), for every $i \leqslant d$, we have

$$\mathrm{D}(a_0, \ldots, a_{i-1}, x_0, \ldots, x_{i-1}, a_ix_i) = \mathrm{D}(a_0 + x_0, \ldots, a_{i-1} + x_{i-1}),$$

but also (complementary sequences) $1 \in \langle a_d, x_d \rangle$. This shows that a_d is invertible since $x_d \in \mathfrak{m}$. Let i be the smallest index such that a_i is invertible (here we use the hypothesis that $\mathfrak{m}$ is detachable).
We then get $a_0, \ldots, a_{i-1} \in \mathfrak{m}$, then

$$\mathrm{D}(x_0, \ldots, x_{i-1}, x_i) \subseteq \mathrm{D}(a_0 + x_0, \ldots, a_{i-1} + x_{i-1}) \subseteq \mathfrak{m},$$

and finally

$$\begin{aligned} \mathfrak{m} = \mathrm{D}(x_0, \ldots, x_{i-1}, x_i, x_{i+1}, \ldots, x_d) \subseteq \\ \mathrm{D}(\underbrace{a_0 + x_0, \ldots, a_{i-1} + x_{i-1}, x_{i+1}, \ldots, x_d}_{d \text{ elements}}) \subseteq \mathfrak{m}. \end{aligned}$$

□

Remark. For a generalization see Exercises XV-7 and XV-8. ■

2. Heitmann dimension and Bass' theorem

We will introduce a new dimension, which we will call the Heitmann dimension of a commutative ring. Its definition will be copied from the inductive definition of the Krull dimension, and we will denote it by Hdim. Beforehand, we introduce the dimension Jdim defined by Heitmann.

2.1. Definition and notation.

- If $\mathfrak{a}$ is an ideal of $\mathbf{A}$ we let $\mathrm{J}_{\mathbf{A}}(\mathfrak{a})$ be its *Jacobson radical*, i.e. the inverse image of $\mathrm{Rad}(\mathbf{A}/\mathfrak{a})$ by the canonical projection $\mathbf{A} \to \mathbf{A}/\mathfrak{a}$.
- If $\mathfrak{a} = \langle x_1, \dots, x_n \rangle$ we denote $\mathrm{J}_{\mathbf{A}}(\mathfrak{a})$ by $\mathrm{J}_{\mathbf{A}}(x_1, \dots, x_n)$. In particular, $\mathrm{J}_{\mathbf{A}}(0) = \mathrm{Rad}\,\mathbf{A}$.
- Let Heit $\mathbf{A}$ be the set of ideals $\mathrm{J}_{\mathbf{A}}(x_1, \dots, x_n)$. We call it the *Heitmann lattice* of the ring $\mathbf{A}$.
- We define Jdim $\mathbf{A}$ as equal to Kdim(Heit $\mathbf{A}$).

We therefore have $x \in \mathrm{J}_{\mathbf{A}}(\mathfrak{a})$ if and only if for every $y \in \mathbf{A}$, $1 + xy$ is invertible modulo $\mathfrak{a}$. In other words

$$x \in \mathrm{J}_{\mathbf{A}}(\mathfrak{a}) \iff 1 + x\mathbf{A} \subseteq (1+\mathfrak{a})^{\mathrm{sat}},$$

and $\mathrm{J}_{\mathbf{A}}(\mathfrak{a})$ is the largest ideal $\mathfrak{b}$ such that $1 + \mathfrak{b} \subseteq (1+\mathfrak{a})^{\mathrm{sat}}$.
We therefore have $\big(1 + \mathrm{J}_{\mathbf{A}}(\mathfrak{a})\big)^{\mathrm{sat}} = (1+\mathfrak{a})^{\mathrm{sat}}$ and $\mathrm{J}_{\mathbf{A}}\big(\mathrm{J}_{\mathbf{A}}(\mathfrak{a})\big) = \mathrm{J}_{\mathbf{A}}(\mathfrak{a})$.
In particular $\mathrm{J}_{\mathbf{A}}\big(\mathrm{J}_{\mathbf{A}}(0)\big) = \mathrm{J}_{\mathbf{A}}(0)$ and the ring $\mathbf{A}/\mathrm{Rad}\,\mathbf{A}$ has its Jacobson radical reduced to 0.

2.2. Lemma.

1. *For an arbitrary ideal* $\mathfrak{a}$ *we have* $\mathrm{J}_{\mathbf{A}}(\mathfrak{a}) = \mathrm{J}_{\mathbf{A}}\big(\mathrm{D}_{\mathbf{A}}(\mathfrak{a})\big) = \mathrm{J}_{\mathbf{A}}\big(\mathrm{J}_{\mathbf{A}}(\mathfrak{a})\big)$.
   Consequently, Heit $\mathbf{A}$ *is a quotient distributive lattice of* Zar $\mathbf{A}$*.*
2. *For* u*,* $v \in \mathbf{A}$ *we have*
   $$\mathrm{J}_{\mathbf{A}}(u,v) \;=\; \mathrm{J}_{\mathbf{A}}(u+v, uv) \;=\; \mathrm{J}_{\mathbf{A}}(u+v) \vee \mathrm{J}_{\mathbf{A}}(uv).$$
   In particular, if $uv \in \mathrm{J}_{\mathbf{A}}(0)$*, then* $\mathrm{J}_{\mathbf{A}}(u,v) = \mathrm{J}_{\mathbf{A}}(u+v)$*.*

D We have $\mathfrak{a} \subseteq \mathrm{D}_{\mathbf{A}}(\mathfrak{a}) \subseteq \mathrm{J}_{\mathbf{A}}(\mathfrak{a})$, therefore $\mathrm{J}_{\mathbf{A}}(\mathfrak{a}) = \mathrm{J}_{\mathbf{A}}\big(\mathrm{D}_{\mathbf{A}}(\mathfrak{a})\big) = \mathrm{J}_{\mathbf{A}}\big(\mathrm{J}_{\mathbf{A}}(\mathfrak{a})\big)$. The equality $\mathrm{D}_{\mathbf{A}}(u,v) = \mathrm{D}_{\mathbf{A}}(u+v, uv)$ therefore implies $\mathrm{J}_{\mathbf{A}}(u,v) = \mathrm{J}_{\mathbf{A}}(u+v, uv)$. □

Comment. The Jdim introduced by Heitmann in [101] corresponds to the following spectral space Jspec $\mathbf{A}$: it is the smallest spectral subspace of Spec $\mathbf{A}$ containing the set Max $\mathbf{A}$ of the maximal ideals of $\mathbf{A}$. This space can be described as the adherence of Max $\mathbf{A}$ in Spec $\mathbf{A}$ for the constructible topology. A topology having as its generator set of open sets the $\mathfrak{D}_{\mathbf{A}}(a)$'s and their complements $\mathfrak{V}_{\mathbf{A}}(a)$. Heitmann notices that the dimension used in Swan's theorem or in Serre's Splitting Off theorem, namely the dimension of Max $\mathbf{A}$, only works well in the case where this space is Noetherian. In addition, in this case, the dimension of Max $\mathbf{A}$ is that of a spectral space, the space $\mathsf{jspec}\,\mathbf{A}$ formed by the prime ideals which are intersections of maximal ideals. However, in the general case, the subspace $\mathsf{jspec}\,\mathbf{A}$ of $\mathsf{Spec}\,\mathbf{A}$ is no longer spectral, and so, according to a remark which he qualifies as philosophical, $\mathsf{jspec}\,\mathbf{A}$ must be replaced by the spectral space that naturally offers itself as a spare solution, namely $\mathsf{Jspec}\,\mathbf{A}$. Actually, $\mathsf{Jspec}\,\mathbf{A}$ is identified with the spectrum of the distributive lattice $\mathsf{Heit}\,\mathbf{A}$ (see [49, Theorem 2.11]), and the compact-open subspaces of $\mathsf{Jspec}\,\mathbf{A}$ form a quotient lattice of $\mathsf{Zar}\,\mathbf{A}$, canonically isomorphic to $\mathsf{Heit}\,\mathbf{A}$. In constructive mathematics, we therefore define $\mathsf{Jdim}\,\mathbf{A}$ as equal to $\mathsf{Kdim}(\mathsf{Heit}\,\mathbf{A})$. ■

The definition of the Heitmann dimension given below is quite natural, insofar as it mimics the constructive definition of the Krull dimension by replacing $\mathrm{D}_\mathbf{A}$ with $\mathrm{J}_\mathbf{A}$.

2.3. Definition. Let $\mathbf{A}$ be a commutative ring, $x \in \mathbf{A}$ and $\mathfrak{a}$ be a finitely generated ideal. The *Heitmann boundary of* $\mathfrak{a}$ *in* $\mathbf{A}$ is the quotient ring $\mathbf{A}_\mathrm{H}^\mathfrak{a} := \mathbf{A}/\mathcal{J}_\mathbf{A}^\mathrm{H}(\mathfrak{a})$ with

$$\mathcal{J}_\mathbf{A}^\mathrm{H}(\mathfrak{a}) := \mathfrak{a} + (\mathrm{J}_\mathbf{A}(0) : \mathfrak{a}).$$

This ideal is called the *Heitmann boundary ideal of* $\mathfrak{a}$ *in* $\mathbf{A}$.
We also let $\mathcal{J}_\mathbf{A}^\mathrm{H}(x) := \mathcal{J}_\mathbf{A}^\mathrm{H}(x\mathbf{A})$ and $\mathbf{A}_\mathrm{H}^x := \mathbf{A}/\mathcal{J}_\mathbf{A}^\mathrm{H}(x)$.

2.4. Definition. The *Heitmann dimension* of $\mathbf{A}$ is defined by induction as follows

- $\mathsf{Hdim}\,\mathbf{A} = -1$ if and only if $1_\mathbf{A} = 0_\mathbf{A}$.
- Let $\ell \geqslant 0$, we have the equivalence
  $$\mathsf{Hdim}\,\mathbf{A} \leqslant \ell \iff \text{for every } x \in \mathbf{A},\ \mathsf{Hdim}(\mathbf{A}_\mathrm{H}^x) \leqslant \ell - 1.$$

This dimension is less than or equal to the Jdim defined by Heitmann in [101], i.e. the Krull dimension of the distributive lattice $\mathsf{Heit}(\mathbf{A})$.

2.5. Fact.

1. *The Heitmann dimension can only decrease by passage to a quotient ring.*
2. *The Heitmann dimension is always less than or equal to the Krull dimension.*
3. *More precisely* $\mathsf{Hdim}\,\mathbf{A} \leqslant \mathsf{Kdim}\big(\mathbf{A}/\mathrm{J}_\mathbf{A}(0)\big) \leqslant \mathsf{Kdim}\,\mathbf{A}$.
4. *Finally,* $\mathsf{Hdim}\,\mathbf{A} \leqslant 0$ *if and only if* $\mathsf{Kdim}\big(\mathbf{A}/\mathrm{J}_\mathbf{A}(0)\big) \leqslant 0$ *(i.e.* $\mathbf{A}$ *is residually zero-dimensional).*

D *1.* By induction on $\mathsf{Hdim}\,\mathbf{A}$[2] by noticing that for every $x \in \mathbf{A}$, the ring $(\mathbf{A}/\mathfrak{a})_\mathrm{H}^x$ is a quotient of $\mathbf{A}_\mathrm{H}^x$.

2. By induction on $\mathsf{Kdim}\,\mathbf{A}$ (by using *1*) by noticing that $\mathbf{A}_\mathrm{H}^x$ is a quotient of $\mathbf{A}_\mathrm{K}^x$.

[2] Actually by induction on n such that $\mathsf{Hdim}\,\mathbf{A} \leqslant n$.

3 and *4*. Let $\mathbf{B} = \mathbf{A}/\mathrm{J}_{\mathbf{A}}(0)$. Then $\mathrm{J}_{\mathbf{B}}(0) = \langle 0 \rangle$, and we have $\mathbf{A}_{\mathrm{H}}^{x} \simeq \mathbf{B}_{\mathrm{H}}^{\overline{x}} = \mathbf{B}_{\mathrm{K}}^{\overline{x}}$ for all $x \in \mathbf{A}$. □

Bass' "stable range" theorem, 2

2.6. Theorem. (Bass' theorem, with the Heitmann dimension, without Noetherianity) *Let* $n \geqslant 0$. *If* $\mathsf{Hdim}\,\mathbf{A} < n$, *then* $\mathsf{Bdim}\,\mathbf{A} < n$.
Abbreviated to: $\mathsf{Bdim}\,\mathbf{A} \leqslant \mathsf{Hdim}\,\mathbf{A}$. *In particular if* $\mathsf{Hdim}\,\mathbf{A} < n$, *every stably free* $\mathbf{A}$*-module of rank* $\geqslant n$ *is free.*

D The same proof would give Theorem 1.4 by replacing the Heitmann boundary with the Krull boundary. Recall that $\mathsf{Bdim}\,\mathbf{A} < n$ means that for all $b_1, \ldots, b_n \in \mathbf{A}$, there exist some x_i's such that the following implication is satisfied:

$$\forall a \in \mathbf{A} \quad (1 \in \langle a, b_1, \ldots, b_n \rangle \;\Rightarrow\; 1 \in \langle b_1 + ax_1, \ldots, b_n + ax_n \rangle).$$

Recall that $1 \in \langle L \rangle$ is equivalent to $1 \in \mathrm{J}_{\mathbf{A}}(L)$ for every list L. We reason by induction on n.
When $n = 0$ the ring is trivial and $\mathrm{J}_{\mathbf{A}}(1) = \mathrm{J}_{\mathbf{A}}(\emptyset)$.
Suppose $n \geqslant 1$. Let $\mathfrak{j} = \mathcal{J}_{\mathbf{A}}^{\mathrm{H}}(b_n)$. The induction hypothesis gives $x_1, \ldots, x_{n-1} \in \mathbf{A}$ such that

$$1 \in \langle b_1 + x_1 a, \ldots, b_{n-1} + x_{n-1} a \rangle \quad \text{in} \quad \mathbf{A}/\mathfrak{j}. \tag{1}$$

Let $L = (b_1 + x_1 a, \ldots, b_{n-1} + x_{n-1} a)$. An arbitrary element of $\mathfrak{j}$ is written in the form $b_n y + x$ with $x b_n \in \mathrm{J}_{\mathbf{A}}(0)$. The membership (1) therefore means that there exists an x_n such that

$$x_n b_n \in \mathrm{J}_{\mathbf{A}}(0) \quad \text{and} \quad 1 \in \langle L, b_n, x_n \rangle\,.$$

A fortiori

$$1 \in \mathrm{J}_{\mathbf{A}}(L, b_n, x_n) = \mathrm{J}_{\mathbf{A}}(L, b_n) \vee \mathrm{J}_{\mathbf{A}}(x_n). \tag{2}$$

Note that by hypothesis $1 \in \langle a, b_1, \ldots, b_n \rangle = \langle L, b_n, a \rangle$. Therefore

$$1 \in \mathrm{J}_{\mathbf{A}}(L, b_n, a) = \mathrm{J}_{\mathbf{A}}(L, b_n) \vee \mathrm{J}_{\mathbf{A}}(a). \tag{3}$$

As $\mathrm{J}_{\mathbf{A}}(x_n a) = \mathrm{J}_{\mathbf{A}}(a) \wedge \mathrm{J}_{\mathbf{A}}(x_n)$, (2) and (3) give by distributivity

$$1 \in \mathrm{J}_{\mathbf{A}}(L, b_n) \vee \mathrm{J}_{\mathbf{A}}(x_n a) = \mathrm{J}_{\mathbf{A}}(L, b_n, x_n a).$$

Since $b_n\, x_n\, a \in \mathrm{J}_{\mathbf{A}}(0)$, Lemma 2.2 gives $\mathrm{J}_{\mathbf{A}}(b_n, x_n a) = \mathrm{J}_{\mathbf{A}}(b_n + x_n a)$, and so

$$1 \in \mathrm{J}_{\mathbf{A}}(L, b_n + x_n a) = \mathrm{J}_{\mathbf{A}}(L, b_n, x_n a),$$

as required. □

"Improved" variant of Kronecker's theorem

2.7. Lemma. *Let a, c_1, …, c_m, u, v, $w \in \mathbf{A}$ and $Z = (c_1, \dots, c_m)$.*

1. $a \in \mathrm{D}_{\mathbf{A}}(Z) \iff 1 \in \langle Z \rangle_{\mathbf{A}[a^{-1}]}$.
2. $\big(w \in \mathrm{Rad}(\mathbf{A}[a^{-1}])$ *and* $a \in \mathrm{D}_{\mathbf{A}}(Z, w)\big) \implies a \in \mathrm{D}_{\mathbf{A}}(Z)$.
3. $\big(uv \in \mathrm{Rad}(\mathbf{A}[a^{-1}])$ *and* $a \in \mathrm{D}_{\mathbf{A}}(Z, u, v)\big) \implies a \in \mathrm{D}_{\mathbf{A}}(Z, u+v)$.

D *1.* Immediate.

2. Suppose $a \in \mathrm{D}_{\mathbf{A}}(Z, w)$ and work in the ring $\mathbf{A}[a^{-1}]$.
We have $1 \in \langle Z \rangle_{\mathbf{A}[a^{-1}]} + \langle w \rangle_{\mathbf{A}[a^{-1}]}$, and as w is in $\mathrm{Rad}(\mathbf{A}[a^{-1}])$, this implies that $1 \in \langle Z \rangle_{\mathbf{A}[a^{-1}]}$, i.e. $a \in \mathrm{D}_{\mathbf{A}}(Z)$.

3. Results from item *2* because $\mathrm{D}_{\mathbf{A}}(Z, u, v) = \mathrm{D}_{\mathbf{A}}(Z, u{+}v, uv)$ (Lemma 1.1).□

Remark. We can ask ourselves if the ideal $\mathrm{Rad}\,\mathbf{A}[a^{-1}]$ is the best possible. The answer is yes. The implication of item *2* is satisfied (for every Z) by replacing $\mathrm{Rad}\,\mathbf{A}[a^{-1}]$ with $\mathfrak{J}$ if and only if $\mathfrak{J} \subseteq \mathrm{Rad}\,\mathbf{A}[a^{-1}]$. ■

2.8. Lemma.
Suppose that $\mathsf{Hdim}\,\mathbf{A}[1/a] < n$, $L \in \mathbf{A}^n$ *and* $\mathrm{D}_{\mathbf{A}}(b) \leqslant \mathrm{D}_{\mathbf{A}}(a) \leqslant \mathrm{D}_{\mathbf{A}}(b, L)$. *Then there exists an* $X \in \mathbf{A}^n$ *such that* $\mathrm{D}_{\mathbf{A}}(L + bX) = \mathrm{D}_{\mathbf{A}}(b, L)$, *which is equivalent to* $b \in \mathrm{D}_{\mathbf{A}}(L + bX)$, *or to* $a \in \mathrm{D}_{\mathbf{A}}(L + bX)$. *In addition, we can take* $X = aY$ *with* $Y \in \mathbf{A}^n$.

D *Preliminary remark.* If $\mathrm{D}_{\mathbf{A}}(L + bX) = \mathrm{D}_{\mathbf{A}}(b, L)$, we have $a \in \mathrm{D}_{\mathbf{A}}(L + bX)$ because $a \in \mathrm{D}_{\mathbf{A}}(b, L)$. Conversely, if $a \in \mathrm{D}_{\mathbf{A}}(L + bX)$, we have $b \in \mathrm{D}_{\mathbf{A}}(L + bX)$ (since $b \in \mathrm{D}_{\mathbf{A}}(a)$), so $\mathrm{D}_{\mathbf{A}}(L + bX) = \mathrm{D}_{\mathbf{A}}(b, L)$.

We reason by induction on n. The case $n = 0$ is trivial.
Let $L = (b_1, \dots, b_n)$ and we start by looking for $X \in \mathbf{A}^n$.
Let $\mathfrak{j} = \mathcal{J}^{\mathrm{H}}_{\mathbf{A}[1/a]}(b_n)$ and $\mathbf{A}' = \mathbf{A}/(\mathfrak{j} \cap \mathbf{A})$, where $\mathfrak{j} \cap \mathbf{A}$ stands for "the inverse image of $\mathfrak{j}$ in $\mathbf{A}$." We have an identification $\mathbf{A}[1/a]/\mathfrak{j} = \mathbf{A}'[1/a]$.
As $\mathsf{Hdim}\,\mathbf{A}'[1/a] < n - 1$, we can apply the induction hypothesis to $\mathbf{A}'$ and $(a, b, b_1, \dots, b_{n-1})$, by noticing that $b_n = 0$ in $\mathbf{A}'$. We then obtain x_1, …, $x_{n-1} \in \mathbf{A}$ such that, by letting $Z = (b_1 + bx_1, \dots, b_{n-1} + bx_{n-1})$, we have $\mathrm{D}(Z) = \mathrm{D}(b, b_1, \dots, b_{n-1})$ in $\mathbf{A}'$. By the preliminary remark, this last equality is equivalent to $a \in \mathrm{D}_{\mathbf{A}'}(Z)$, which, by Lemma 2.7 *1*, means that $1 \in \langle Z \rangle$ in $\mathbf{A}'[1/a]$, i.e. $1 \in \langle Z \rangle + \mathfrak{j}$ in $\mathbf{A}[1/a]$. By definition of the Heitmann boundary, this means that there exists an x_n, which we can choose in $\mathbf{A}$, such that $x_n b_n \in \mathrm{Rad}\,\mathbf{A}[1/a]$ and $1 \in \langle Z, b_n, x_n \rangle_{\mathbf{A}[1/a]}$.
We therefore have $a \in \mathrm{D}_{\mathbf{A}}(Z, b_n, x_n)$. But we also have $a \in \mathrm{D}_{\mathbf{A}}(Z, b_n, b)$, since

$$\langle Z, b_n, b \rangle = \langle b_1, , \dots, b_{n-1}, b_n, b \rangle \overset{\mathrm{def}}{=} \langle L, b \rangle,$$

and since $a \in \mathrm{D}_{\mathbf{A}}(L, b)$ by hypothesis. Recap: $a \in \mathrm{D}_{\mathbf{A}}(Z, b_n, x_n)$, $a \in \mathrm{D}_{\mathbf{A}}(Z, b_n, b)$ so $a \in \mathrm{D}_{\mathbf{A}}(Z, b_n, bx_n)$. The application of Lemma 2.7 *3* with

$u = b_n$, $v = bx_n$ provides $a \in \mathrm{D}_{\mathbf{A}}(Z, b_n + bx_n)$, i.e. $a \in \mathrm{D}_{\mathbf{A}}(L + bX)$ where $X = (x_1, \ldots, x_n)$.

Finally, if $b^p \in \langle a \rangle_{\mathbf{A}}$, we can apply the result with b^{p+1} instead of b since $\mathrm{D}_{\mathbf{A}}(b) = \mathrm{D}_{\mathbf{A}}(b^{p+1})$. Then $L + b^{p+1}X$ is re-expressed as $L + baY$. □

For $a \in \mathbf{A}$, we always have $\mathsf{Hdim}\,\mathbf{A}[1/a] \leqslant \mathsf{Kdim}\,\mathbf{A}[1/a] \leqslant \mathsf{Kdim}\,\mathbf{A}$. Consequently the following theorem improves Kronecker's theorem.

2.9. Theorem. (Kronecker's theorem, Heitmann dimension)

1. *Let $n \geqslant 0$. If a, b_1, …, $b_n \in \mathbf{A}$ and $\mathsf{Hdim}\,\mathbf{A}[a^{-1}] < n$, then there exist x_1, …, $x_n \in \mathbf{A}$ such that*

$$\mathrm{D}_{\mathbf{A}}(a, b_1, \ldots, b_n) = \mathrm{D}_{\mathbf{A}}(b_1 + ax_1, \ldots, b_n + ax_n).$$

2. *Consequently, if a_1, …, a_r, b_1, …, $b_n \in \mathbf{A}$ and $\mathsf{Hdim}\,\mathbf{A}[1/a_i] < n$ for $i \in [\![1..r]\!]$, then there exist y_1, …, $y_n \in \langle a_1, \ldots, a_r \rangle$ such that*

$$\mathrm{D}_{\mathbf{A}}(a_1, \ldots, a_r, b_1, \ldots, b_n) = \mathrm{D}_{\mathbf{A}}(b_1 + y_1, \ldots, b_n + y_n).$$

D *1.* Direct consequence of Lemma 2.8 by making $a = b$.

2. Deduced from *1* by induction on r:

$$\begin{array}{rcl} \mathfrak{a} & = & \mathrm{D}_{\mathbf{A}}(a_1, \ldots, a_r, b_1, \ldots, b_n) \quad = \quad \mathrm{D}_{\mathbf{A}}(a_1, \ldots, a_{r-1}, b_1, \ldots, b_n) \vee \mathrm{D}_{\mathbf{A}}(a_r) \\ & = & \mathfrak{b} \vee \mathrm{D}_{\mathbf{A}}(a_r), \quad \text{with} \\ \mathfrak{b} & = & \mathrm{D}_{\mathbf{A}}(b_1 + z_1, \ldots, b_n + z_n) \end{array}$$

where z_1, …, $z_n \in \langle a_1, \ldots, a_{r-1} \rangle$, so $\mathfrak{a} = \mathrm{D}_{\mathbf{A}}(a_r, b_1 + z_1, \ldots, b_n + z_n)$, and we once again apply the result. □

3. Serre's Splitting Off theorem, the Forster-Swan theorem, and Bass' cancellation theorem

In this section, we describe the matrix properties of a ring that allow us to make Serre's Splitting Off theorem and the Forster-Swan theorem (control of the number of generators of a finitely generated module in terms of the number of local generators) work.

The following sections consist in developing results that show that certain rings satisfy the matrix properties in question. The first rings that appeared (thanks to Serre and Forster) were the Noetherian rings with certain dimension properties (the Krull dimension for Forster and the dimension of the maximal spectrum for Serre and Swan). Later Heitmann showed how to get rid of the Noetherianity regarding the Krull dimension, and gave the guiding ideas to do the same for the dimension of the maximal spectrum. In addition Bass also introduced a generalization in which he would replace the Krull dimension by the maximum of the Krull dimensions for the rings associated with a partition of the Zariski spectrum in constructible subsets. Finally, Coquand brought a “definitive” light to these questions by generalizing the results and by treating them constructively thanks to two subjacent notions to the previous proofs: n-stability on the one hand and Heitmann dimension on the other. The purely matrix aspect of the problems to be solved has clearly been highlighted in a review paper by Eisenbud-Evans [74, (1973)]. The present section can be considered as a non-Noetherian and constructive approach to these works.

3.1. Definition. Let $\mathbf{A}$ be a ring and $n \geqslant 0$ be an integer.

1. We write $\mathsf{Sdim}\,\mathbf{A} < n$ if, for every matrix F of rank $\geqslant n$, there is a unimodular linear combination of the columns.
   In other words $1 = \mathcal{D}_n(F) \Rightarrow \exists X,\ 1 = \mathcal{D}_1(FX)$.
2. We write $\mathsf{Gdim}\,\mathbf{A} < n$ when the following property is satisfied. For every matrix $F = [\,C_0 \,|\, C_1 \,|\, \dots \,|\, C_p\,]$ (the C_i's are the columns, and let $G = [\,C_1 \,|\, \dots \,|\, C_p\,]$) such that $1 = \mathcal{D}_1(C_0) + \mathcal{D}_n(G)$, there is a linear combination $C_0 + \sum_{i=1}^{p} \alpha_i C_i$, which is unimodular.

In the acronym Sdim, S refers to “splitting” or to “Serre” and is justified by Theorem 3.4. Similarly, in Gdim, G refers to “generators” and is justified by Theorem 3.6.

The notations $\mathsf{Sdim}\,\mathbf{A} < n$ and $\mathsf{Gdim}\,\mathbf{A} < n$ are justified by the following obvious implications, for every $n \geqslant 0$,

$$\mathsf{Sdim}\,\mathbf{A} < n \Rightarrow \mathsf{Sdim}\,\mathbf{A} < n+1 \text{ and } \mathsf{Gdim}\,\mathbf{A} < n \Rightarrow \mathsf{Gdim}\,\mathbf{A} < n+1.$$

Note that $\mathcal{D}_n(F) \subseteq \mathcal{D}_1(C_0) + \mathcal{D}_n(G)$, and consequently the hypothesis for F in $\mathsf{Sdim}\,\mathbf{A} < n$ implies the hypothesis for F in $\mathsf{Gdim}\,\mathbf{A} < n$. Moreover the conclusion in $\mathsf{Gdim}\,\mathbf{A} < n$ is stronger. This gives the following item *2*.

3.2. Fact.

1. $\mathsf{Sdim}\,\mathbf{A} < 0 \iff \mathsf{Gdim}\,\mathbf{A} < 0 \iff$ *the ring* $\mathbf{A}$ *is trivial.*
2. *For all* $n \geqslant 0$, *we have* $\mathsf{Gdim}\,\mathbf{A} < n \implies \mathsf{Sdim}\,\mathbf{A} < n$.
   Abbreviated to $\mathsf{Sdim}\,\mathbf{A} \leqslant \mathsf{Gdim}\,\mathbf{A}$.
3. *If* $\mathbf{B} = \mathbf{A}/\mathfrak{a}$, *we have* $\mathsf{Sdim}\,\mathbf{B} \leqslant \mathsf{Sdim}\,\mathbf{A}$ *and* $\mathsf{Gdim}\,\mathbf{B} \leqslant \mathsf{Gdim}\,\mathbf{A}$.
4. *We have* $\mathsf{Sdim}\,\mathbf{A} = \mathsf{Sdim}\,\mathbf{A}/\mathrm{Rad}\,\mathbf{A}$ *and* $\mathsf{Gdim}\,\mathbf{A} = \mathsf{Gdim}\,\mathbf{A}/\mathrm{Rad}\,\mathbf{A}$.
5. *If* $\mathbf{A}$ *is n-stable (Section 4), then* $\mathsf{Gdim}\,\mathbf{A} < n$ *(Theorem 5.3).*
   Abbreviated to $\mathsf{Gdim}\,\mathbf{A} \leqslant \mathsf{Cdim}\,\mathbf{A}$.
6. *If* $\mathsf{Hdim}\,\mathbf{A} < n$, *then* $\mathsf{Gdim}\,\mathbf{A} < n$ *(Theorem 5.7).*
   Abbreviated to $\mathsf{Gdim}\,\mathbf{A} \leqslant \mathsf{Hdim}\,\mathbf{A}$.

D It suffices to prove items *3* and *4*. Item *4* is clear because an element of $\mathbf{A}$ is invertible in $\mathbf{A}$ if and only if it is invertible in $\mathbf{A}/(\mathrm{Rad}\,\mathbf{A})$.

3 for Sdim. Let $F \in \mathbf{A}^{m\times r}$ with $\mathcal{D}_n(F) = 1$ modulo $\mathfrak{a}$. If $n > \inf(m, r)$ we obtain $1 \in \mathfrak{a}$ and all is well. Otherwise, let $a \in \mathfrak{a}$ such that $1 - a \in \mathcal{D}_n(F)$.

Consider the matrix $H \in \mathbf{A}^{(m+n)\times r}$ obtained by superposing F and the matrix $a\mathrm{I}_n$ followed by $r-n$ null columns.
We have $1-a^n \in \mathcal{D}_n(F)$, so $1 \in \mathcal{D}_n(H)$. A linear combination of the columns of H is unimodular. The same linear combination of the columns of F is unimodular modulo $\mathfrak{a}$.

3 for Gdim. The same technique works, but here it suffices to consider the matrix $H \in \mathbf{A}^{(m+1)\times r}$ obtained by inserting the row $[\,a\ 0\ \cdots\ 0\,]$ underneath F. □

The proof of the following fact helps to justify the slightly surprising definition chosen for $\mathsf{Gdim}\,\mathbf{A} < n$.

3.3. Fact. *For all $n \geqslant 0$, we have* $\mathsf{Gdim}\,\mathbf{A} < n \Rightarrow \mathsf{Bdim}\,\mathbf{A} < n$.
Abbreviated to $\mathsf{Bdim}\,\mathbf{A} \leqslant \mathsf{Gdim}\,\mathbf{A}$.

D For example with $n=3$. Consider (a, b_1, b_2, b_3) with $1 = \langle a, b_1, b_2, b_3\rangle$. We want some x_i's such that $1 = \langle b_1 + ax_1, b_2 + ax_2, b_3 + ax_3\rangle$. Consider the matrix $F = \begin{bmatrix} b_1 & a & 0 & 0 \\ b_2 & 0 & a & 0 \\ b_3 & 0 & 0 & a \end{bmatrix} = [\,C_0 \mid G\,]$ with $G = a\mathrm{I}_3$. We have

$$1 = \mathcal{D}_1(C_0) + \mathcal{D}_3(G), \quad \text{i.e. } 1 = \langle b_1, b_2, b_3\rangle + \left\langle a^3 \right\rangle,$$

because $1 = \langle b_1, b_2, b_3\rangle + \langle a\rangle$. By applying the definition of $\mathsf{Gdim}\,\mathbf{A} < 3$ to F, we obtain a unimodular vector ${}^{\mathrm{t}}[\,b_1 + ax_1\ \ b_2 + ax_2\ \ b_3 + ax_3\,]$. □

Serre's Splitting Off theorem

The following version of Serre's theorem is relatively easy, the delicate part being to establish that $\mathsf{Sdim}\,\mathbf{A} < k$ for a ring $\mathbf{A}$. Modulo Theorems 5.3 and 5.7 we obtain the truly strong versions of the theorem.

3.4. Theorem. (Serre's Splitting Off theorem, with Sdim)
Let $k \geqslant 1$ and M be a projective $\mathbf{A}$-module of rank $\geqslant k$, or more generally isomorphic to the image of a matrix of rank $\geqslant k$.
Suppose that $\mathsf{Sdim}\,\mathbf{A} < k$. Then $M \simeq N \oplus \mathbf{A}$ for a certain module N isomorphic to the image of a matrix of rank $\geqslant k-1$.

D Let $F \in \mathbf{A}^{n\times m}$ be a matrix with $\mathcal{D}_k(F) = 1$. By definition, we have a vector $u = {}^{\mathrm{t}}[\,u_1 \cdots u_n\,] \in \operatorname{Im} F$ which is unimodular in $\mathbf{A}^n$. Therefore $\mathbf{A}u$ is a free submodule of rank 1 and a direct summand in $\mathbf{A}^n$, and a fortiori in M. More precisely, if $P \in \mathbb{AG}_n(\mathbf{A})$ is a projector of image $\mathbf{A}u$, we obtain $M = \mathbf{A}u \oplus N$ with

$$N = \operatorname{Ker}(P) \cap M = (\mathrm{I}_n - P)(M) = \operatorname{Im}\big((\mathrm{I}_n - P)\,F\big).$$

It remains to see that $(\mathrm{I}_n - P)\,F$ is of rank $\geqslant k-1$. Even if it entails localizing and making a change of basis, we can suppose that P is the standard projection $\mathrm{I}_{1,n}$. Then the matrix $G = (\mathrm{I}_n - P)\,F$ is the matrix F in which we have replaced its first row by 0, and it is clear that $\mathcal{D}_k(F) \subseteq \mathcal{D}_{k-1}(G)$. □

Thus, if M is the image of $F \in \mathbf{A}^{n\times m}$ of rank $\geqslant k$, we obtain a decomposition $M = N \oplus L$ where L is free of rank 1 as a direct summand in $\mathbf{A}^n$ and N isomorphic to the image of a matrix of rank $\geqslant k-1$. Now if F is of greater rank, we can iterate the procedure and we have the following corollary (with the correspondence $h \leftrightarrow k-1$).

3.5. Corollary. *Let $\mathbf{A}$ be a ring such that $\mathsf{Sdim}\,\mathbf{A} \leqslant h$, and M be a module isomorphic to the image of a matrix of rank $\geqslant h+s$. Then M contains as a direct summand a free submodule of rank s. More precisely, if M is the image of $F \in \mathbf{A}^{n\times m}$ of rank $\geqslant h+s$, we have $M = N \oplus L$ where L is free of rank s and a direct summand in $\mathbf{A}^n$, and N is the image of a matrix of rank $\geqslant h$.*

The Forster-Swan theorem

Recall that a finitely generated module M is said to be locally generated by r elements if $\mathcal{F}_r(M) = 1$. On this subject see the local number of generators lemma (Lemma IX-2.4).

The Forster-Swan theorem below was first established for the Krull dimension (Kdim instead of Gdim). The version presented here is relatively easy, and the delicate part is to establish that $\mathsf{Gdim}\,\mathbf{A} \leqslant \mathsf{Kdim}\,\mathbf{A}$ for every ring $\mathbf{A}$. Modulo Theorems 5.3 and 5.7 we obtain the known better versions of the theorem, under an entirely constructive form.

3.6. Theorem. (Forster-Swan theorem, with Gdim) *Let $k \geqslant 0$ and $r \geqslant 1$. If $\mathsf{Gdim}\,\mathbf{A} \leqslant k$, or even only if $\mathsf{Sdim}\,\mathbf{A} \leqslant k$ and $\mathsf{Bdim}\,\mathbf{A} \leqslant k+r$, and if a finitely generated $\mathbf{A}$-module M is locally generated by r elements, then it is generated by $k+r$ elements.*
In the first case, more precisely, if M is generated by $y_1, \ldots, y_{k+r+s}$, we can compute $z_1, \ldots, z_{k+r}$ in $\langle y_{k+r+1}, \ldots, y_{k+r+s}\rangle$ such that M is generated by $y_1 + z_1, \ldots, y_{k+r} + z_{k+r}$.

D Since M is finitely generated and $\mathcal{F}_r(M) = 1$, M is the quotient of a finitely presented module M' satisfying $\mathcal{F}_r(M') = 1$. We can therefore suppose that M is finitely presented.
Starting from a generator set with more than $k+r$ elements, we are going to replace it with a generator set of the stated form minus an element. Therefore let $(y_0, y_1, \ldots, y_p)$ be a generator set of M with $p \geqslant k+r$, and F be a presentation matrix of M for this system. Then by hypothesis $1 = \mathcal{F}_r(M) = \mathcal{D}_{p+1-r}(F)$, and since $p+1-r \geqslant k+1$ we have $1 = \mathcal{D}_{k+1}(F)$.

First case. Let L_0, …, L_p be the rows of F. We apply the definition of $\mathsf{Gdim}\,\mathbf{A} < k+1$ with the transposed matrix of F (which is of rank $\geqslant k+1$). We obtain some t_i's such that the row $L_0 + t_1L_1 + \cdots + t_pL_p$ is unimodular. Replacing the row L_0 with the row $L_0 + t_1L_1 + \cdots + t_pL_p$ amounts to the same as replacing the generator set $(y_0, y_1, \ldots, y_p)$ with

$$(y_0, y_1 - t_1y_0, \ldots, y_p - t_py_0) = (y_0, y'_1, \ldots, y'_p).$$

Since the new row L_0 is unimodular, a suitable linear combination of the columns is of the form ${}^{\mathrm{t}}[\,1\ y_1\ \cdots\ y_p\,]$. This means that we have $y_0 + y_1y'_1 + \cdots + y_py'_p = 0$ in M, and thus that $(y'_1, \ldots, y'_p)$ generates M.

Second case. We apply the definition of $\mathsf{Sdim}\,\mathbf{A} < k+1$ with the matrix F. We obtain a unimodular linear combination of columns, and we add this column in the first position in front of F. Then, by applying Fact V-4.9 with $\mathsf{Bdim}\,\mathbf{A} < k+r+1 \leqslant p+1$, by elementary row operations, we obtain a new presentation matrix of M (for another generator set) with the first column equal to ${}^{\mathrm{t}}[\,1\,0\,\cdots\,0\,]$. This means that the first element of the new generator set is null. □

Theorem 3.6 is obviously valid by replacing the ring $\mathbf{A}$ with the ring $\mathbf{A}/\mathrm{Ann}(M)$ or $\mathbf{A}/\mathcal{F}_0(M)$. We propose in Theorem 3.8 a slightly more subtle refinement.

3.7. Proposition. *Let $F = [\,C_0\,|\,C_1\,|\,\ldots\,|\,C_p\,] \in \mathbf{A}^{n\times(p+1)}$ (the C_i's are the columns) and $G = [\,C_1\,|\,\ldots\,|\,C_p\,]$, such that $F = [\,C_0\,|\,G\,]$.*
If $1 = \mathcal{D}_1(F)$ and if we have $\mathsf{Gdim}(\mathbf{A}/\mathcal{D}_{k+1}(F)) < k$ for $k \in \llbracket 1..q \rrbracket$, then there exist t_1, …, t_p such that the vector $C_0 + t_1C_1 + \cdots + t_pC_p$ is unimodular modulo $\mathcal{D}_{q+1}(F)$.

D First consider the ring $\mathbf{A}_2 = \mathbf{A}/\mathcal{D}_2(F)$. Since $\mathcal{D}_1(F) = 1$ and $\mathsf{Gdim}(\mathbf{A}_2) < 1$, we obtain some $t_{1,i}$'s and $C_{1,0} = C_0 + t_{1,1}C_1 + \cdots + t_{1,p}C_p$ such that $\mathcal{D}_1(C_{1,0}) = 1$ modulo $\mathcal{D}_2(F)$, i.e. $\mathcal{D}_1(C_{1,0}) + \mathcal{D}_2(G) = 1$. We change F into F_1 by replacing C_0 with $C_{1,0}$ without changing G. Note that we have $\mathcal{D}_i(F_1) = \mathcal{D}_i(F)$ for every i.
We then consider the ring $\mathbf{A}_3 = \mathbf{A}/\mathcal{D}_3(F_1)$ with $\mathsf{Gdim}(\mathbf{A}_3) < 2$.
Since $\mathcal{D}_1(C_{1,0}) + \mathcal{D}_2(G) = 1$, we obtain $C_{2,0} = C_{1,0} + t_{2,1}C_1 + \cdots + t_{2,p}C_p$ such that $\mathcal{D}_1(C_{2,0}) = 1$ modulo $\mathcal{D}_3(F)$, i.e. $\mathcal{D}_1(C_{2,0}) + \mathcal{D}_3(G) = 1$. We change F_1 into F_2 by replacing $C_{1,0}$ with $C_{2,0}$ without changing G. We once again have $\mathcal{D}_i(F_2) = \mathcal{D}_i(F)$ for every i.
We continue as above until we obtain a vector $C_{q,0}$ of the form $C_0 + t_1C_1 + \cdots + t_pC_p$ unimodular modulo $\mathcal{D}_{q+1}(F)$. □

3.8. Theorem. (Forster-Swan theorem, more general, with Gdim)
Let M be a finitely generated module over $\mathbf{A}$. Let $\mathfrak{f}_k = \mathcal{F}_k(M)$ be its Fitting ideals. Suppose that $1 \in \mathfrak{f}_m$ (i.e. M is locally generated by m elements) and that for $k \in \llbracket 0..m-1 \rrbracket$, we have $\mathsf{Gdim}(\mathbf{A}/\mathfrak{f}_k) < m-k$. Then M is generated by m elements. More precisely, if $M = \langle y_1, \dots, y_{m+s} \rangle$, we can compute some z_i's in $\langle y_{m+1}, \dots, y_{m+s} \rangle$ such that $M = \langle y_1 + z_1, \dots, y_m + z_m \rangle$.

D Since $\mathfrak{f}_0$ annihilates M, we can replace $\mathbf{A}$ with $\mathbf{A}/\mathfrak{f}_0$, or, which amounts to the same thing, suppose that $\mathfrak{f}_0 = \mathcal{F}_0(M) = 0$, which we do from now on. Starting with a generator set of M with more than m elements we are going to replace it by a generator set of the stated form minus an element. Therefore let $(y_0, y_1, \dots, y_p)$ be a generator set of M with $p \geqslant m$.

When the module is finitely presented we reason as for Theorem 3.6.
Let F be a presentation matrix of M for the considered generator set. We have $\mathfrak{f}_{k+1} = \mathcal{D}_{p-k}(F)$, and in particular $1 \in \mathfrak{f}_p = \mathcal{D}_1(F)$. The hypotheses of Proposition 3.7 are then satisfied with $q = p$ for the transposed matrix of F. If $L_0, \dots, L_p$ are the rows of F, we obtain some t_i's with $L_0 + t_1 L_1 + \cdots + t_p L_p$ unimodular modulo $\mathcal{D}_{p+1}(F) = \mathfrak{f}_0 = 0$. The remainder of the argument is as in Theorem 3.6.

The reasoning in the case where M is only assumed to be finitely generated consists in showing that M is the quotient of a finitely presented module which has a presentation matrix supporting with success the proof of Proposition 3.7. Let $\underline{y} = [\, y_0 \ \cdots \ y_p \,]$. Every syzygy between the y_i's is of the form $\underline{y}\, C = 0$ for some $C \in \mathbf{A}^{p+1}$.
The Fitting ideal $\mathfrak{f}_{p+1-i}$ of M is the ideal Δ_i, the sum of the determinantal ideals $\mathcal{D}_i(F)$, for $F \in \mathbf{A}^{(p+1) \times n}$ that satisfy $\underline{y}\, F = 0$, i.e. for the matrices that are "syzygy matrices for $(y_0, \dots, y_p)$."
By the hypotheses, we have $\Delta_1 = 1$ and $\mathsf{Gdim}(\mathbf{A}/\Delta_{k+1}) < k$ for $k \in \llbracket 1..p \rrbracket$. The fact that $\Delta_1 = 1$ is observed over a syzygy matrix F_1.
Consider the matrix ${}^{\mathrm{t}}F_1$ and the ring $\mathbf{A}_2 = \mathbf{A}/\Delta_2$. As $\mathsf{Gdim}(\mathbf{A}_2) < 1$, we obtain a linear combination $C_{1,0}$ of the columns of ${}^{\mathrm{t}}F_1$ unimodular modulo Δ_2, i.e. such that $1 = \mathcal{D}_1(C_{1,0}) + \Delta_2$. More precisely, we obtain $C_{1,0} = {}^{\mathrm{t}}F_1 X_1$ with $X_1 = {}^{\mathrm{t}}[\, 1 \ x_{1,1} \ \cdots \ x_{1,p} \,]$.
The equality $1 = \mathcal{D}_1(C_{1,0}) + \Delta_2$ provides an element $a \in \Delta_2$ obtained as a linear combination of a finite number of minors of order 2 of syzygy matrices, and so $a \in \mathcal{D}_2(F_2)$ for a syzygy matrix F_2. Then consider the matrix $F_2' = [\, F_1 \,|\, F_2 \,]$. For the transposed matrix of F_2' we first obtain that the column $C_2 = {}^{\mathrm{t}}F_2' X_1$ is unimodular. We replace the first column of ${}^{\mathrm{t}}F_2'$ by C_2, which gives a matrix ${}^{\mathrm{t}}F_2''$ suitable for the hypotheses of $\mathsf{Gdim}\, \mathbf{A}_3 < 2$ (where $\mathbf{A}_3 = \mathbf{A}/\Delta_3$), i.e. $1 = \mathcal{D}_1(C_2) + \mathcal{D}_2(F_2'')$. We ultimately obtain a linear combination $C_{2,0}$ of the columns of ${}^{\mathrm{t}}F_2'$ unimodular modulo Δ_3, i.e. such that $1 = \mathcal{D}_1(C_{2,0}) + \Delta_3$. More precisely, $C_{2,0} = {}^{\mathrm{t}}F_2' X_2$ with $X_2 = {}^{\mathrm{t}}[\, 1 \ x_{2,1} \ \cdots \ x_{2,p} \,]$. And so forth.

We ultimately obtain a syzygy matrix for $\underline{y}$,

$$F = [\,F_1 \,|\, \cdots \,|\, F_p\,]$$

and a vector $X_p = {}^{\mathrm{t}}[\,1\ x_{p,1}\ \cdots\ x_{p,p}\,]$ with the linear combination ${}^{\mathrm{t}}F\,X_p$ unimodular (since it is unimodular modulo $\Delta_{p+1} = \mathfrak{f}_0 = 0$).
The remainder of the argument is as in Theorem 3.6. □

Comment. Theorem 3.8 with Hdim or Kdim instead of Gdim has as an easy consequence in classical mathematics some much more abstract statements, which seem much more scholarly. For example the usual statement of the Forster-Swan theorem[3] (stated in the case where $\mathsf{Max}\,\mathbf{A}$ is Noetherian) uses the maximum,[4] for $\mathfrak{p} \in \mathsf{jspec}\,\mathbf{A}$ of $\mu_{\mathfrak{p}}(M) + \mathsf{Kdim}(\mathbf{A}/\mathfrak{p})$: here $\mu_{\mathfrak{p}}(M)$ is the minimum number of generators of $M_{\mathfrak{p}}$. This type of statement suggests that the prime ideals that are intersections of maximal ideals play an essential role in the theorem. In reality, it is not necessary to scare children with $\mathsf{jspec}\,\mathbf{A}$, because this abstract theorem is exactly equivalent (in the considered case, and in classical mathematics) to Theorem 3.8 for the Jdim, which in this envisaged case is equal to the Hdim. In addition, from a strictly practical point of view it is unclear how to access the quite mysterious maximum of the $\mu_{\mathfrak{p}}(M) + \mathsf{Kdim}(\mathbf{A}/\mathfrak{p})$. By contrast, the hypotheses of Theorem 3.8 are susceptible to a constructive proof, which in this case will lead to an algorithm making it possible to explicate the conclusion.

Bass' cancellation theorem

3.9. Definition. Given two modules M and L we say that *M is cancellative for L* if $M \oplus L \simeq N \oplus L$ implies $M \simeq N$.

3.10. Lemma. *Let M and L be two $\mathbf{A}$-modules. In the following statements we have 1 ⇔ 2 and 3 ⇒ 2.*

1. *M is cancellative for L.*
2. *For every decomposition $M \oplus L = M' \oplus L'$ with $L' \simeq L$, there exists an automorphism σ of $M \oplus L$ such that $\sigma(L') = L$.*
3. *For every decomposition $M \oplus L = M' \oplus L'$ with $L' \simeq L$, there exists an automorphism θ of $M \oplus L$ such that $\theta(L') \subseteq M$.*

D The equivalence of *1* and *2* is a game of photocopies.
1 ⇒ *2*. Suppose $M \oplus L = M' \oplus L'$. Since $L \xrightarrow{\sim} L'$, we obtain an isomorphism $M \oplus L \xrightarrow{\sim} M' \oplus L$, so $M \xrightarrow{\sim} M'$, and by performing the sum we obtain an isomorphism $M \oplus L \xrightarrow{\sim} M' \oplus L'$, i.e. an automorphism of $M \oplus L$

[3] Corollary 2.14 (page 108) in [Kunz] or Theorem 5.8 (page 36) in [Matsumura]. In addition, the authors replace $\mathbf{A}$ with $\mathbf{A}/\mathrm{Ann}(M)$, which costs nothing.

[4] Recall that $\mathsf{jspec}\,\mathbf{A}$ designates the subspace of $\mathsf{Spec}\,\mathbf{A}$ formed by the prime ideals which are intersections of maximal ideals.

which sends L to L'.
2 ⇒ *1*. Suppose $N \oplus L \xrightarrow{\sim} M \oplus L$. This isomorphism sends N to M' and L to L', such that $M \oplus L = M' \oplus L'$. Therefore there is an automorphism σ of $M \oplus L$ which sends L to L', and say M to M_1. Then,

$$N \simeq M' \simeq (M' \oplus L')/L' = (M \oplus L)/L' = (M_1 \oplus L')/L' \simeq M_1 \simeq M.$$

3 ⇒ *2*. Since $\theta(L')$ is a direct summand in $M \oplus L$, it is a direct summand in M, which we write as $M_1 \oplus \theta(L')$. Let λ be the automorphism of $M \oplus L$ which swaps L and $\theta(L')$ by fixing M_1. Then $\sigma = \lambda \circ \theta$ sends L' to L. □

Recall that an element x of an *arbitrary* module M is said to be unimodular when there exists a linear form $\lambda \in M^\star$ such that $\lambda(x) = 1$. It amounts to the same as saying that $\mathbf{A}x$ is free (of basis x) and a direct summand in M (Proposition II-5.1).

3.11. Theorem. (Bass' cancellation theorem, with Gdim)
Let M be a finitely generated projective $\mathbf{A}$-module of rank $\geqslant k$. If $\mathsf{Gdim}\,\mathbf{A} < k$, then M is cancellative for every finitely generated projective $\mathbf{A}$-module: if Q is finitely generated projective and $M \oplus Q \simeq N \oplus Q$, then $M \simeq N$.

D Suppose that we have shown that M is cancellative for $\mathbf{A}$.
Then, since $M \oplus \mathbf{A}^\ell$ also satisfies the hypothesis, we show by induction on ℓ that M is cancellative for $\mathbf{A}^{\ell+1}$. As a result M is cancellative for every direct summand in $\mathbf{A}^{\ell+1}$.
Finally, M is cancellative for $\mathbf{A}$ because it satisfies item *3* of Lemma 3.10 for $L = \mathbf{A}$. Indeed, suppose that $M = \operatorname{Im} F \subseteq \mathbf{A}^n$, where F is a projection matrix (of rank $\geqslant k$), and let L' be a direct summand in $M \oplus \mathbf{A}$, isomorphic to $\mathbf{A}$: $L' = \mathbf{A}(x, a)$ with (x, a) unimodular in $M \oplus \mathbf{A}$. Since every linear form over M extends to $\mathbf{A}^n$, there exists a form $\nu \in (\mathbf{A}^n)^\star$ such that $1 \in \langle \nu(x), a \rangle$. By Lemma 3.12 below, with $x = C_0$, there exists a $y \in M$ such that $x' = x + ay$ is unimodular in M. Consider a form $\mu \in M^\star$ such that $\mu(x') = 1$. We then define an automorphism θ of $M \oplus \mathbf{A}$ as follows

$$\theta = \begin{bmatrix} 1 & 0 \\ -a\mu & 1 \end{bmatrix} \begin{bmatrix} 1 & y \\ 0 & 1 \end{bmatrix} \; i.e. \; \begin{bmatrix} m \\ b \end{bmatrix} \mapsto \begin{bmatrix} m + by \\ \mu(x)b - a\mu(m) \end{bmatrix}.$$

Then $\theta(x, a) = (x', 0)$, so $\theta(L') \subseteq M$. The result follows by Lemma 3.10.□

In the following lemma, which ends the proof of Theorem 3.11, we use the notations of Proposition 3.7, the matrix $F = [\, C_0 \,|\, C_1 \,|\, \ldots \,|\, C_p \,]$ being that of the previous theorem.

3.12. Lemma. *If $\mathsf{Gdim}\,\mathbf{A} < k$ and $\mathcal{D}_k(F) = 1 = \mathrm{D}_{\mathbf{A}}(C_0) \vee \mathrm{D}_{\mathbf{A}}(a)$, then there exist $t_1, \ldots, t_p$ such that*

$$1 = \mathrm{D}_{\mathbf{A}}(C_0 + at_1C_1 + \cdots + at_pC_p).$$

D Consider the matrix $[\,C_0 \,|\, aC_1 \,|\, \dots \,|\, aC_p\,]$, obtained by replacing G by aG in F. As $\mathrm{D}_{\mathbf{A}}(C_0) \vee \mathcal{D}_k(G) = 1 = \mathrm{D}_{\mathbf{A}}(C_0) \vee \mathrm{D}_{\mathbf{A}}(a)$, we indeed have by distributivity $\mathrm{D}_{\mathbf{A}}(C_0) \vee \mathcal{D}_k(aG) = 1$. The result follows since $\mathsf{Gdim}\,\mathbf{A} < k$.□

A simple characteristic property for $\mathsf{Gdim}\,\mathrm{A} < n$

In order to prove $\mathsf{Gdim}\,\mathbf{A} < n$ for a ring $\mathbf{A}$ it suffices to verify the conclusion (in the definition of $\mathsf{Gdim}\,\mathbf{A} < n$) for particularly simple matrices. This is the subject of the following proposition.

3.13. Proposition. *For a ring $\mathbf{A}$ we have $\mathsf{Gdim}\,\mathbf{A} < n$ if and only if for every matrix $V \in \mathbb{M}_{n+1}(\mathbf{A})$ of the form*

$$V = \begin{bmatrix} b & c_1 & \cdots & \cdots & c_n \\ b_1 & a & 0 & \cdots & 0 \\ \vdots & 0 & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ b_n & 0 & \cdots & 0 & a \end{bmatrix} = [\,V_0 \mid V_1 \mid \dots \mid V_n\,],$$

and for every $d \in \mathbf{A}$ such that $1 = \langle b, a, d\rangle$, there exist x_i's $\in \mathbf{A}$ such that

$$1 = \mathcal{D}_1(V_0 + x_1V_1 + \cdots + x_nV_n) + \langle d\rangle\,.$$

Remark. Instead of using an element d subjected to the constraint $1 = \langle a, b, d\rangle$, we could have used a pair (u, v) not subjected to any constraint and replaced d by $1 + au + bv$ in the conclusion. In this form, it is particularly obvious that if the condition above is satisfied for the ring $\mathbf{A}$, it is satisfied for every quotient of $\mathbf{A}$. ■

D To show that the condition is necessary, we reason with the quotient ring $\mathbf{B} = \mathbf{A}/\langle d\rangle$ and we consider the matrix

$$F = V = [\,V_0 \mid V_1 \mid \dots \mid V_n\,].$$

With the notations of Definition 3.1 we have $p = n$, $F = [\,C_0 \mid G\,]$, and $C_i = V_i$ for $i \in [\![0..n]\!]$.
Since $1 = \langle b, a, d\rangle$ in $\mathbf{A}$, we have $1 = \langle b, a^n\rangle \subseteq \mathcal{D}_1(C_0) + \mathcal{D}_n(G)$ in $\mathbf{B}$, and the hypothesis of the definition is satisfied. Since $\mathsf{Gdim}\,\mathbf{B} < n$, we obtain x_i's in $\mathbf{A}$ such that

$$1 = \mathcal{D}_1(C_0 + x_1C_1 + \cdots + x_nC_n) \text{ in } \mathbf{B}.$$

Hence the desired conclusion in $\mathbf{A}$.

To prove the converse we proceed in two steps. First of all recall that if the condition is satisfied for the ring $\mathbf{A}$, it is satisfied for every quotient of $\mathbf{A}$. We will actually use this condition with $d = 0$ (the hypothesis over V then becomes of the same type as that which serves to define $\mathsf{Gdim} < n$), with the ring $\mathbf{A}$ and certain of its quotients.

First step: the case where the matrix F has $n+1$ columns, i.e. $p=n$. With $F \in \mathbf{A}^{m\times(n+1)}$, we have by hypothesis a linear form $\varphi_0 : \mathbf{A}^m \to \mathbf{A}$ and an n-multilinear alternating form $\psi : (\mathbf{A}^m)^n \to \mathbf{A}$ such that

$$1 = \varphi_0(C_0) + \psi(C_1, \ldots, C_n).$$

For $j \in [\![1..n]\!]$ let $\varphi_j : \mathbf{A}^m \to \mathbf{A}$ be the linear form

$$X \mapsto \psi(C_1, \ldots, C_{j-1}, X, C_j, \ldots, C_n).$$

By letting $a = \psi(C_1, \ldots, C_n)$, we then have

- $\varphi_1(C_1) = \cdots = \varphi_n(C_n) = a$,
- $\varphi_i(C_j) = 0$ if $1 \leqslant i \neq j \leqslant n$

Considering the matrix of the $\varphi_i(C_j)$'s, we obtain

$$V = [\,V_0 \mid \ldots \mid V_n\,] := \begin{bmatrix} \varphi_0(C_0) & \varphi_0(C_1) & \cdots & \cdots & \varphi_0(C_n) \\ \varphi_1(C_0) & a & 0 & \cdots & 0 \\ \vdots & 0 & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ \varphi_n(C_0) & 0 & \cdots & 0 & a \end{bmatrix},$$

that is $V = [\,\varphi(C_0) \mid \ldots \mid \varphi(C_n)\,]$ by letting $\varphi(Z) = \begin{bmatrix} \varphi_0(Z) \\ \vdots \\ \varphi_n(Z) \end{bmatrix}$.

We can apply the hypothesis with $d=0$. We find $x_1, \ldots, x_n \in \mathbf{A}$ such that the vector $V_0 + x_1V_1 + \cdots + x_nV_n$ is unimodular. This vector is equal to $\varphi(C_0 + x_1C_1 + \cdots + x_nC_n) = \varphi(C)$. Since this vector is unimodular and since φ is linear, the vector C is itself unimodular.

Second step: the general case.

As $1 = \mathcal{D}_1(C_0) + \mathcal{D}_n(G)$, we have a family $(\alpha_i)_{i\in[\![1..q]\!]}$ of subsets with n elements of $[\![1..p]\!]$ such that $1 = \mathcal{D}_1(C_0) + \sum_i \mathcal{D}_n(G_{\alpha_i})$, where G_{α_i} is the extracted matrix of G by uniquely considering the columns whose index is in α_i. Let $C_{0,0} = C_0$ and $J_\ell = \sum_{i>\ell} \mathcal{D}_n(G_{\alpha_i})$. We then apply the case of the first step successively with $\ell = 1, \ldots, q$ to obtain

$$1 = \mathcal{D}_1(C_{0,\ell}) = \mathcal{D}_1(C_{0,\ell-1}) + \mathcal{D}_n(G_{\alpha_\ell}) \text{ in } \mathbf{A}/J_\ell$$

and therefore $\mathcal{D}_1(C_{0,q}) = 1$ in $\mathbf{A}$.

Note that in this second step, we use the result of the first step with quotient rings of $\mathbf{A}$. □

4. Supports and n-stability

In Section 5 we will establish theorems regarding the elementary operations on matrices. They will have as corollaries some grand theorems due to Serre, Forster, Bass and Swan. We will give them in two similar but nevertheless different versions. We do not think that they can be reduced to a unique form.

The first version is based on the notion of n-stability. This version leads inter alia to a sophisticated result due to Bass in which a partition of the Zariski spectrum intervenes in a finite number of subsets which are all of small dimension (smaller than the Krull dimension of the ring). This result will be used in Chapter XVI to prove Bass' theorem (Theorem XVI-6.8) regarding the extended modules.

The second version uses the Heitmann dimension, introduced in Section 2, less than or equal to the Krull dimension, but for which we do not know of an analogue of Bass' sophisticated version.

Section 4 gives a few necessary preliminaries for the first version based on the n-stability.

Supports, dimension, stability

4.1. Definition. A *support* over a ring $\mathbf{A}$ in a distributive lattice $\mathbf{T}$ is a map $D : \mathbf{A} \to \mathbf{T}$, which satisfies the following axioms

- $D(0_{\mathbf{A}}) = 0_{\mathbf{T}}, \quad D(1_{\mathbf{A}}) = 1_{\mathbf{T}}$,
- $D(ab) = D(a) \wedge D(b)$,
- $D(a + b) \leqslant D(a) \vee D(b)$.

Let $D(x_1, \ldots, x_n) = D(x_1) \vee \cdots \vee D(x_n)$.

It is clear that $\mathrm{D}_{\mathbf{A}} : \mathbf{A} \to \mathsf{Zar}\,\mathbf{A}$ is a support, called the *Zariski support.* The following lemma shows that the Zariski support is the "free" support.

4.2. Lemma. *For every support D we have*

1. $D(a^m) = D(a)$ *for* $m \geqslant 1$, $D(ax) \leqslant D(x)$, $D(a, b) = D(a + b, ab)$.
2. $\langle x_1, \ldots, x_n\rangle = \langle y_1, \ldots, y_r\rangle$ *implies* $D(x_1, \ldots, x_n) = D(y_1, \ldots, y_r)$.
3. $\mathrm{D}_{\mathbf{A}}(y) \leqslant \mathrm{D}_{\mathbf{A}}(x_1, \ldots, x_n)$ *implies* $D(y) \leqslant D(x_1, \ldots, x_n)$.
4. *There exists a unique homomorphism θ of distributive lattices which makes the following diagram commute:*

$$\begin{tikzcd}
\mathbf{A} \arrow[d, "\mathrm{D}_{\mathbf{A}}"'] \arrow[dr, "D"] & & \textit{supports} \\
\mathsf{Zar}\,\mathbf{A} \arrow[r, dashed, "\theta\,!"'] & \mathbf{T} & \textit{homomorphisms of distributive lattices}
\end{tikzcd}$$

D The proof is left to the reader. □

Thus every support $D : \mathbf{A} \to \mathbf{T}$ such that $D(\mathbf{A})$ generates $\mathbf{T}$ as a distributive lattice is obtained by composing the Zariski support with a passage to the quotient $\mathsf{Zar}\,\mathbf{A} \to \mathsf{Zar}\,\mathbf{A}/\!\sim$ by an equivalence relation compatible with the lattice structure.

Denote $D(\mathfrak{a})$ by $D(x_1, \dots, x_n)$ if $\mathfrak{a} = \langle x_1, \dots, x_n \rangle$. We say that a vector $X \in \mathbf{A}^n$ is *D-unimodular* if $D(X) = 1$.

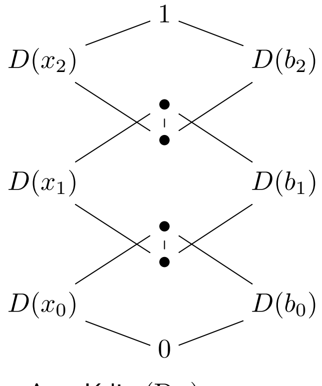
Dimension of a support, Kronecker's theorem

4.3. Definition. Given two sequences $(x_0, \dots, x_n)$ and $(b_0, \dots, b_n)$ in $\mathbf{A}$ and a support D over $\mathbf{A}$, we say that the two sequences are *D-complementary* if we have the following inequalities

$$\left.\begin{array}{rcl} D(b_0x_0) & = & D(0) \\ D(b_1x_1) & \leqslant & D(b_0, x_0) \\ \vdots & \vdots & \vdots \\ D(b_nx_n) & \leqslant & D(b_{n-1}, x_{n-1}) \\ D(1) & = & D(b_n, x_n) \end{array}\right\} \qquad (4)$$

The support D is said to be *of Krull dimension* $\leqslant n$ if every sequence $(x_0, \dots, x_n)$ in $\mathbf{A}$ admits a D-complementary sequence. Let $\mathsf{Kdim}(D) \leqslant n$.

For example for $n = 2$ the complementary sequences correspond to the following picture in $\mathbf{T}$.



Remark. Note that $\mathsf{Kdim}\,\mathbf{A} = \mathsf{Kdim}(\mathrm{D}_{\mathbf{A}})$. ■

The proof of the following lemma can be copied from that of Lemma 1.2 by replacing $\mathrm{D}_{\mathbf{A}}$ by D. Kronecker's theorem is then a direct consequence.

4.4. Lemma. *Let $\ell \geqslant 1$. If $(b_1, \dots, b_\ell)$ and $(x_1, \dots, x_\ell)$ are two D-complementary sequences in $\mathbf{A}$, then for every $a \in \mathbf{A}$ we have*

$$D(a, b_1, \dots, b_\ell) = D(b_1 + ax_1, \dots, b_\ell + ax_\ell),$$

i.e. $D(a) \leqslant D(b_1 + ax_1, \dots, b_\ell + ax_\ell)$.

4.5. Theorem. (Kronecker's theorem, for the supports)
If D is a support of Krull dimension $\leqslant n$, for every finitely generated ideal $\mathfrak{a}$ there exists an ideal $\mathfrak{b}$ generated by $n+1$ elements such that $D(\mathfrak{a}) = D(\mathfrak{b})$. Actually, for all $b_1, \ldots, b_{n+r}$ ($r \geqslant 2$), there exist $c_j \in \langle b_{n+2}, \ldots, b_{n+r}\rangle$ such that $D(b_1 + c_1, \ldots, b_{n+1} + c_{n+1}) = D(b_1, \ldots, b_{n+r})$.

Faithful supports

In this subsection we prove in particular that the Krull dimension of a ring (which we already know is equal to the dimension of its Zariski support) is equal to that of its Zariski lattice: here we keep the promise made in XIII-6.3.

4.6. Definition. A support $D : \mathbf{A} \to \mathbf{T}$ is said to be *faithful* if $\mathbf{T}$ is generated by the image of D and if, for every $a \in \mathbf{A}$ and $L \in \mathbf{A}^m$, the inequality $D(a) \leqslant D(L)$ implies the existence of a $b \in \langle L\rangle$ such that $D(a) \leqslant D(b)$.

For example the Zariski support $\mathrm{D}_{\mathbf{A}}$ is always faithful.

Let $D : \mathbf{A} \to \mathbf{T}$ be a support. If the image of $\mathbf{A}$ generates $\mathbf{T}$, since we have the equality $D(a_1) \wedge \cdots \wedge D(a_n) = D(a_1 \cdots a_n)$, every element of $\mathbf{T}$ can be written in the form $D(L)$ for a list L of elements of $\mathbf{A}$.

4.7. Lemma. *If D is faithful and $\mathsf{Kdim}\,\mathbf{T} < k$ then $\mathsf{Kdim}(D) < k$. In particular the Krull dimension of a ring is equal to that of its Zariski lattice.*

D Let $(a_1, \ldots, a_k)$ be a sequence in $\mathbf{A}$. We must show that it admits a D-complementary sequence.
Since $\mathsf{Kdim}\,\mathbf{T} < k$, the sequence $\big(D(a_1), \ldots, D(a_k)\big)$ has a complementary sequence $\big(D(L_1), \ldots, D(L_k)\big)$ in $\mathbf{T}$ with lists in $\mathbf{A}$ for L_i,

$$\begin{array}{rcl} D(a_1) \wedge D(L_1) & = & D(0) \\ D(a_2) \wedge D(L_2) & \leqslant & D(a_1, L_1) \\ \vdots & \vdots & \vdots \\ D(a_k) \wedge D(L_k) & \leqslant & D(a_{k-1}, L_{k-1}) \\ D(1) & = & D(a_k, L_k). \end{array}$$

Since D is faithful, there exists a c_k in $\langle a_k, L_k\rangle$ such that $D(1) \leqslant D(c_k)$, which gives $b_k \in \langle L_k\rangle$ such that $D(1) \leqslant D(a_k, b_k)$.
Note that we have

$$D(a_k b_k) = D(a_k) \wedge D(b_k) \leqslant D(a_k) \wedge D(L_k) \leqslant D(a_{k-1}, L_{k-1}).$$

Since D is faithful, we have $c_{k-1} \in \langle a_{k-1}, L_{k-1}\rangle$ with $D(a_k b_k) \leqslant D(c_{k-1})$, which gives $b_{k-1} \in \langle L_{k-1}\rangle$ such that $D(a_k b_k) \leqslant D(a_{k-1}, b_{k-1})$.
And so forth. Ultimately, we have constructed a sequence $(b_1, \ldots, b_k)$ which is D-complementary to $(a_1, \ldots, a_k)$. □

n-stable supports

We now abstract the property described in Lemma 4.4 for the complementary sequences in the following form.

4.8. Definition.

1. Let $n \geqslant 1$. A support $D : \mathbf{A} \to \mathbf{T}$ is said to be *n-stable* when, for all $a \in \mathbf{A}$ and $L \in \mathbf{A}^n$, there exists an $X \in \mathbf{A}^n$ such that $D(L, a) = D(L + aX)$, i.e. $D(a) \leqslant D(L + aX)$.
2. The ring $\mathbf{A}$ is said to be *n-stable* if its Zariski support $\mathrm{D}_{\mathbf{A}}$ is n-stable. We will write $\mathsf{Cdim}\,\mathbf{A} < n$ to say that $\mathbf{A}$ is n-stable.
3. The ring $\mathbf{A}$ is said to be 0-stable if it is trivial.

In the acronym Cdim, C alludes to “Coquand.”

Naturally, if $\mathsf{Kdim}(D) < n$ then D is n-stable. In particular, with the free support $\mathrm{D}_{\mathbf{A}}$, we obtain $\mathsf{Cdim}\,\mathbf{A} \leqslant \mathsf{Kdim}\,\mathbf{A}$. Moreover, Kronecker’s theorem applies (almost by definition) to every n-stable support.

The notation $\mathsf{Cdim}\,\mathbf{A} < n$ is justified by the fact that if D is n-stable, it is $(n+1)$-stable. Finally, item *3* in the definition was given for the sake of clarity, but it is not really necessary: by reading item *1* for $n = 0$, we obtain that for every $a \in \mathbf{A}$, $D(a) \leqslant D(0)$.

Examples.

1) A valuation ring, or more generally a ring $\mathbf{V}$ which satisfies “$a \mid b$ or $b \mid a$ for all a, b,” is 1-stable, even in infinite Krull dimension. For all (a, b) it suffices to find some x such that $\langle a, b\rangle = \langle b + xa\rangle$. If $a = qb$, we have $\langle a, b\rangle = \langle b\rangle$ and we take $x = 0$. If $b = qa$, we have $\langle a, b\rangle = \langle a\rangle$ and we take $x = 1 - q$.

2) A Bézout domain is 2-stable. More generally, a strict Bézout ring (see Section IV-7 on page 206 and Exercise IV-7) is 2-stable. More precisely, for a, b_1, $b_2 \in \mathbf{A}$, there exist x_1, x_2 such that $a \in \langle b_1 + x_1 a, b_2 + x_2 a\rangle$, i.e. $\langle a, b_1, b_2\rangle = \langle b_1 + x_1 a, b_2 + x_2 a\rangle$.
Indeed, by question *1.c* of the exercise, there exist comaximal u_1 and u_2 such that $u_1 b_1 + u_2 b_2 = 0$. We take x_1, x_2 such that $u_1 x_1 + u_2 x_2 = 1$ and we obtain the equality

$$a = u_1 b_1 + a + u_2 b_2 = u_1(b_1 + x_1 a) + u_2(b_2 + x_2 a). \qquad ■$$

4.9. Fact. *We always have* $\mathsf{Bdim}\,\mathbf{A} \leqslant \mathsf{Cdim}\,\mathbf{A}$.

D If $\mathbf{A}$ is n-stable, then $\mathsf{Bdim}\,\mathbf{A} < n$: indeed, we apply the definition with $(a, a_1, \ldots, a_n)$ in $\mathbf{A}$ satisfying $1 \in \langle a, a_1, \ldots, a_n\rangle$. □

4.10. Fact. *If D is n-stable, for every $a \in \mathbf{A}$ and $L \in \mathbf{A}^n$, there exists an $X \in \mathbf{A}^n$ such that $D(L, a) = D(L + a^2 X)$, i.e. $D(a) \leqslant D(L + a^2 X)$.*

Indeed, $D(a) = D(a^2)$ and $D(L, a) = D(L, a^2)$.

Constructions and patchings of supports

4.11. Definition.
The map $\mathrm{J}_{\mathbf{A}} : \mathbf{A} \to \mathsf{Heit}\,\mathbf{A}$ defines the *Heitmann support.*

Remark. A priori $\mathsf{Kdim}\,\mathrm{D}_{\mathbf{A}} = \mathsf{Kdim}\,\mathbf{A} \geqslant \mathsf{Kdim}\,\mathrm{J}_{\mathbf{A}} \geqslant \mathsf{Jdim}\,\mathbf{A}$. We lack examples that would show that the two inequalities can be strict. ■

4.12. Lemma. (Variant of the Gauss-Joyal lemma II-2.6)
If D is a support over $\mathbf{A}$, we obtain a support $D[X]$ over $\mathbf{A}[X]$ by letting

$$D[X](f) = D\big(\mathrm{c}(f)\big).$$

D Lemma II-2.6 gives $\mathrm{D}_{\mathbf{A}}\big(\mathrm{c}(fg)\big) = \mathrm{D}_{\mathbf{A}}\big(\mathrm{c}(f)\big) \wedge \mathrm{D}_{\mathbf{A}}\big(\mathrm{c}(g)\big)$. □

4.13. Lemma. (Support and quotient) *Let $D : \mathbf{A} \to \mathbf{T}$ be a support and $\mathfrak{a}$ be a finitely generated ideal of $\mathbf{A}$. We obtain a support*

$$D/\mathfrak{a} : \mathbf{A} \to \mathbf{T}/\mathfrak{a} \overset{\mathrm{def}}{=} \mathbf{T}/(D(\mathfrak{a}) = 0)$$

by composing D with the projection $\Pi_{D(\mathfrak{a})} : \mathbf{T} \to \mathbf{T}/(D(\mathfrak{a}) = 0)$.

1. $\mathrm{D}_{\mathbf{A}}/\mathfrak{a}$ *is canonically isomorphic to* $\mathrm{D}_{\mathbf{A}/\mathfrak{a}} \circ \mathsf{Zar}(\pi_{\mathfrak{a}})$*, where $\pi_{\mathfrak{a}}$ is the canonical map $\mathbf{A} \to \mathbf{A}/\mathfrak{a}$.*
2. *If D is faithful, then so is $D/\mathfrak{a}$.*
3. *If D is n-stable, then so is $D/\mathfrak{a}$.*
   In particular $\mathsf{Cdim}\,\mathbf{A}/\mathfrak{a} \leqslant \mathsf{Cdim}\,\mathbf{A}$.

D Recall that $\Pi_{D(\mathfrak{a})}(x) \leqslant \Pi_{D(\mathfrak{a})}(y) \iff x \vee D(\mathfrak{a}) \leqslant y \vee D(\mathfrak{a})$.
1. Results from Fact XI-4.5.
2. Let $D' = D/\mathfrak{a}$. Let $a \in \mathbf{A}$ and L be a vector such that $D'(a) \leqslant D'(L)$. We seek some $b \in \langle L \rangle$ such that $D'(a) \leqslant D'(b)$. By definition of D' we have $D(a) \leqslant D(L, \mathfrak{a})$, and since D is faithful, there exists a $c \in \langle L \rangle + \mathfrak{a}$ such that $D(a) \leqslant D(c)$, which gives some $b \in L$ such that $D(a) \leqslant D(b, \mathfrak{a})$, in other words $D'(a) \leqslant D'(b)$.
3. Let $a \in \mathbf{A}$ and $L \in \mathbf{A}^n$. We seek $X \in \mathbf{A}^n$ such that $D'(a) \leqslant D'(L + aX)$, i.e. $D(a) \vee D(\mathfrak{a}) \leqslant D(L + aX) \vee D(\mathfrak{a})$. However, we have some X which is suitable for D, that is $D(a) \leqslant D(L + aX)$, therefore it is suitable for D'.□

Dually we have the following lemma.

4.14. Lemma. (Support and localization) *Let $D : \mathbf{A} \to \mathbf{T}$ be a support and u be an element of $\mathbf{A}$. We obtain a support*

$$D[1/u] : \mathbf{A} \to \mathbf{T}[1/u] \overset{\mathrm{def}}{=} \mathbf{T}/(D(u) = 1)$$

by composing D with $j_{D(u)} : \mathbf{T} \to \mathbf{T}/(D(u) = 1)$.

1. $\mathrm{D}_{\mathbf{A}}[1/u]$ *is canonically isomorphic to* $\mathrm{D}_{\mathbf{A}[1/u]} \circ \mathsf{Zar}(\iota_u)$*, where ι_u is the canonical map $\mathbf{A} \to \mathbf{A}[1/u]$.*
2. *If D is faithful, then so is $D[1/u]$.*

3. If D is n-stable, then so is $D[1/u]$.
In particular $\mathsf{Cdim}\,\mathbf{A}[1/u] \leqslant \mathsf{Cdim}\,\mathbf{A}$.

D Recall that $j_{D(u)}(x) \leqslant j_{D(u)}(y) \iff x \wedge D(u) \leqslant y \wedge D(u)$.
1. Results from Fact XI-4.5.
2. Let $D' = D[1/u]$. Let $a \in \mathbf{A}$ and L be a vector such that $D'(a) \leqslant D'(L)$. By definition of D' we have $D(au) = D(a) \wedge D(u) \leqslant D(L)$. Since D is faithful, there exists a $b \in \langle L \rangle$ such that $D(au) \leqslant D(b)$, i.e. $D'(a) \leqslant D'(b)$.
3. As for Lemma 4.13 by replacing $D/\mathfrak{a}$ and $\vee$ by $D[1/u]$ and $\wedge$. □

4.15. Lemma.

1. *Let $D : \mathbf{A} \to \mathbf{T}$ be a support and $b \in \mathbf{A}$.*
   a. *D/b and $D[1/b]$ are n-stable if and only if D is n-stable.*
   b. *If D is faithful and if $\mathbf{T}/b$ and $\mathbf{T}[1/b]$ are of Krull dimension $< n$, then D is n-stable.*
2. *Let $\mathbf{A}$ be a ring and $b \in \mathbf{A}$. Then $\mathbf{A}/\langle b \rangle$ and $\mathbf{A}[1/b]$ are n-stable if and only if $\mathbf{A}$ is n-stable.*
   Abbreviated to: $\mathsf{Cdim}\,\mathbf{A} = \sup\big(\mathsf{Cdim}\,\mathbf{A}/\langle b \rangle, \mathsf{Cdim}\,\mathbf{A}[1/b]\big)$.

D It suffices to show the direct implication in item *1a.*
Let $a \in \mathbf{A}$ and $L \in \mathbf{A}^n$. Since D/b is n-stable, we have some $Y \in \mathbf{A}^n$ such that $D(a) \leqslant D(L + aY)$ in $\mathbf{T}/\big(D(b) = 0\big)$, i.e. in $\mathbf{T}$,

$$D(a) \leqslant D(b) \vee D(L + aY). \qquad (*)$$

Next we apply the n-stability of $D[1/b]$ with ab and $L + aY$ which provides some $Z \in \mathbf{A}^n$ such that $D(ab) \leqslant D(L + aY + abZ)$ in $\mathbf{T}/\big(D(b) = 1\big)$.
In $\mathbf{T}$, by letting $X = Y + bZ$, this is expressed as

$$D(ab) \wedge D(b) \leqslant D(L + aX), \quad \text{i.e.} \quad D(ab) \leqslant D(L + aX). \qquad (\#)$$

But we have $\langle b, L + aX \rangle = \langle b, L + aY \rangle$, therefore $D(b, L + aX) = D(b, L + aY)$. The inequalities $(*)$ and $(\#)$ are then expressed as

$$D(a) \leqslant D(b) \vee D(L + aX) \quad \text{and} \quad D(a) \wedge D(b) \leqslant D(L + aX).$$

This implies (by "cut," see page 656) that $D(a) \leqslant D(L + aX)$. □

Constructible partitions of the Zariski spectrum

A *constructible* subset of $\mathsf{Spec}\,\mathbf{A}$ is a Boolean combination of open sets of basis $\mathfrak{D}(a)$. In classical mathematics, if we equip the set $\mathsf{Spec}\,\mathbf{A}$ with the "constructible topology" having as its basis of open sets the constructible subsets, we obtain a spectral space, the *constructible spectrum of the ring* $\mathbf{A}$, which we can identify with $\mathsf{Spec}\,\mathbf{A}^\bullet$.

From a constructive point of view, we have seen that we can replace $\mathsf{Spec}\,\mathbf{A}$ (an object a little too ideal) by the lattice $\mathsf{Zar}\,\mathbf{A}$ (a concrete object), isomorphic in classical mathematics to the lattice of compact-open subspaces of

$\mathsf{Spec}\,\mathbf{A}$. When we pass from the Zariski topology to the constructible topology in classical mathematics, we pass from $\mathsf{Zar}\,\mathbf{A}$ to $\mathbb{B}\mathrm{o}(\mathsf{Zar}\,\mathbf{A}) \simeq \mathsf{Zar}(\mathbf{A}^\bullet)$ in constructive mathematics (for this last isomorphism, see Theorem XI-4.26).

Hyman Bass took interest in the partitions of the constructible spectrum. An elementary step of the construction of such a partition consists in the replacement of a ring $\mathbf{B}$ by the two rings $\mathbf{B}/\langle b\rangle$ and $\mathbf{B}[1/b]$, for an element b of $\mathbf{B}$. An important remark made by Bass is that these two rings can each have a strictly smaller Krull dimension than that of $\mathbf{B}$, whereas certain properties of the ring, to be satisfied in $\mathbf{B}$, only need to be satisfied in each of its two children. This is the case for the n-stability of the free support. In any case, this is the analysis that T. Coquand made from a few pages of [Bass].

In classical mathematics, from any covering of $\mathsf{Spec}\,\mathbf{A}$ by open sets of the constructible topology, we can extract a finite covering, which we can refine into a finite partition by some compact-open subspaces (i.e. some finite Boolean combinations of open sets with basis $\mathfrak{D}(a)$). These are a lot of high caliber abstractions, but the result is extremely concrete, and this is the result that interests us in practice.

We define in constructive mathematics a *constructible partition of the Zariski spectrum* by its dual version, which is a fundamental system of orthogonal idempotents in the Boolean algebra $\mathsf{Zar}\,\mathbf{A}^\bullet = \mathbb{B}\mathrm{o}(\mathsf{Zar}\,\mathbf{A})$.

In practice, an element of $\mathsf{Zar}\,\mathbf{A}^\bullet$ is given by a double list in the ring $\mathbf{A}$

$$(a_1, \ldots, a_\ell; u_1, \ldots, u_m) = (I; U)$$

that defines the following element of $\mathsf{Zar}\,\mathbf{A}^\bullet$

$\bigwedge_i \neg \mathrm{D}_{\mathbf{A}^\bullet}(a_i) \wedge \bigwedge_j \mathrm{D}_{\mathbf{A}^\bullet}(u_j) = \neg \mathrm{D}_{\mathbf{A}^\bullet}(a_1, \ldots, a_\ell) \wedge \mathrm{D}_{\mathbf{A}^\bullet}(u)$, where $u = \prod_j u_j$.

To this element $(I; U)$ is associated the ring $(\mathbf{A}/\langle I\rangle)[1/u]$.[5] A fundamental system of orthogonal idempotents of $\mathbb{B}\mathrm{o}(\mathsf{Zar}\,\mathbf{A})$ can then be obtained as a result of a tree construction which starts with the double list $(0; 1)$ and which authorizes the replacement of a list $(I; U)$ by two double lists $(I, a; U)$ and $(I; a, U)$ for some $a \in \mathbf{A}$.

The following crucial theorem is a corollary of item *2* of Lemma 4.15.

4.16. Theorem. *Consider a constructible partition of* $\mathsf{Spec}\,\mathbf{A}$*, described as above by a family* $(I_k; U_k)_{k \in \llbracket 1..m \rrbracket}$. *Let* $\mathfrak{a}_k$ *be the ideal* $\langle I_k\rangle$ *and* u_k *be the product of the elements of* U_k.

1. *If* $D : \mathbf{A} \to \mathbf{T}$ *is a support, and if all the* $(D/\mathfrak{a}_k)[1/u_k]$*'s are n-stable, then* D *is n-stable.*
2. *In particular, if each ring* $\mathbf{A}[1/u_k]/\mathfrak{a}_k$ *is n-stable (for example if its Krull dimension is* $< n$*), then* $\mathbf{A}$ *is n-stable.*

[5] In classical mathematics $\mathsf{Spec}(\mathbf{A}/\langle I\rangle)[1/u] = \bigcap_{a \in I} \mathfrak{V}(a) \cap \bigcap_{v \in U} \mathfrak{D}(v)$, where $\mathfrak{V}(a)$ designates the complement of $\mathfrak{D}(a)$.

Remarks.

1) The paradigmatic case of an n-stable ring is given in the previous theorem when each ring $\mathbf{A}[1/u_i]/\mathfrak{a}_i$ is of Krull dimension $< n$.

2) Every constructible partition of $\mathsf{Spec}\,\mathbf{A}$ can be refined in the partition described by the 2^n complementary pairs formed from a finite list $(a_1, \dots, a_n)$ in $\mathbf{A}$.

3) Analogous tree constructions appear in Chapter XV in the framework of the basic concrete local-global principle, but there are other rings, localized rings denoted by $\mathbf{A}_{\mathcal{S}(I;U)}$, that intervene then. ∎

5. Elementary column operations

In this section we establish analogous theorems in two different contexts. The first uses the stability of a support, the second uses the Heitmann dimension.

The reader can visualize most of the results of the chapter in the following picture, keeping in mind Theorems 3.4, 3.6, 3.8 and 3.11.

An arrow such that $\mathsf{Sdim} \longrightarrow \mathsf{Gdim}$ is added for $\mathsf{Sdim}\,\mathbf{A} \leqslant \mathsf{Gdim}\,\mathbf{A}$.

$$\begin{tikzcd}
\mathsf{Sdim} \arrow[dr, "\text{Fact 3.2 2}"] & & \mathsf{Hdim} \arrow[dr, "\text{Fact 2.5}"] & \\
& \mathsf{Gdim} \arrow[ur, "\text{Thm. 5.7}"] \arrow[dr, "\text{Thm. 5.3}"'] & & \mathsf{Kdim} \\
\mathsf{Bdim} \arrow[ur, "\text{Fact 3.3}"'] & & \mathsf{Cdim} \arrow[ur, "\text{Def. 4.8}"'] &
\end{tikzcd}$$

With the stability of a support

In this subsection, $D : \mathbf{A} \to \mathbf{T}$ is a fixed support

We fix the following notations, analogous to those used to define $\mathsf{Gdim}\,\mathbf{A} < n$ in Definition 3.1.

5.1. Notation. Let $F = [\,C_0 \,|\, C_1 \,|\, \dots \,|\, C_p\,]$ be a matrix in $\mathbf{A}^{m\times(p+1)}$ (the C_i's are the columns) and $G = [\,C_1 \,|\, \dots \,|\, C_p\,]$, such that $F = [\,C_0 \,|\, G\,]$.

Notice that for every n we have $\mathrm{D}_{\mathbf{A}}\big(C_0, \mathcal{D}_n(F)\big) = \mathrm{D}_{\mathbf{A}}\big(C_0, \mathcal{D}_n(G)\big)$, and a fortiori $D\big(C_0, \mathcal{D}_n(F)\big) = D\big(C_0, \mathcal{D}_n(G)\big)$.

5.2. Lemma. *Suppose that D is n-stable and take the notation 5.1 with $m = p = n$. Let $\delta = \det(G)$. There exist $x_1, \dots, x_n$ such that*

$$D(C_0, \delta) \leqslant D\big(C_0 + \delta(x_1C_1 + \cdots + x_nC_n)\big).$$

D It suffices to realize $D(\delta) \leqslant D\big(C_0 + \delta(x_1C_1 + \cdots + x_nC_n)\big)$, i.e.

$$D(\delta) \leqslant D(C_0 + \delta GX) \text{ for some } X \in \mathbf{A}^n.$$

Let $\widetilde{G}$ be the adjoint matrix of G and $L = \widetilde{G}C_0$. For any $X \in \mathbf{A}^n$, we have $\widetilde{G}(C_0 + \delta GX) = L + \delta^2 X$, so $\mathrm{D}_{\mathbf{A}}(L + \delta^2 X) \leqslant \mathrm{D}_{\mathbf{A}}(C_0 + \delta GX)$, and a fortiori $D(L + \delta^2 X) \leqslant D(C_0 + \delta GX)$. Since D is n-stable, by Fact 4.10, we have some $X \in \mathbf{A}^n$ such that $D(\delta) \leqslant D(L + \delta^2 X)$.
Therefore $D(\delta) \leqslant D(C_0 + \delta GX)$, as required. □

5.3. Theorem. (Coquand's theorem, 1: Forster-Swan and others with the n-stability) *We have* $\mathsf{Gdim}\,\mathbf{A} \leqslant \mathsf{Cdim}\,\mathbf{A}$. *Consequently, Serre's Splitting Off, Forster-Swan' and Bass' cancellation theorems (3.4, 3.6, 3.8, 3.11) apply with the* Cdim.

D We assume $\mathsf{Cdim}\,\mathbf{A} < n$ and we prove $\mathsf{Gdim}\,\mathbf{A} < n$. We use the characterization of $\mathsf{Gdim}\,\mathbf{A} < n$ given in Proposition 3.13. Lemma 5.2 with the support $D = \mathrm{D}_{\mathbf{A}/\langle d\rangle}$ tells us that the equivalent property described in 3.13 is satisfied if $\mathsf{Cdim}\,\mathbf{A}/\langle d\rangle < n$. We conclude by observing that $\mathsf{Cdim}\,\mathbf{A}/\langle d\rangle \leqslant \mathsf{Cdim}\,\mathbf{A}$. □

5.4. Theorem. (Coquand's theorem, 2: elementary column operations, support and n-stability) *With the notations 5.1, let $n \in [\![1..p]\!]$. If D is n-stable there exist $t_1, \dots, t_p \in \mathcal{D}_n(G)$ such that*

$$D\big(C_0, \mathcal{D}_n(G)\big) \leqslant D(C_0 + t_1C_1 + \cdots + t_pC_p).$$

The proof of this theorem as a consequence of Lemma 5.2 is analogous to the proof of the difficult implication in Proposition 3.13, in a slightly different context. The result is stronger because Proposition 3.13 is only interested in the special case given in Corollary 5.5, with in addition $D = \mathrm{D}_{\mathbf{A}}$.

D We need to find $t_1, \dots, t_p$ in $\mathcal{D}_n(G)$ such that, for every minor ν of order n of G, we have $D(C_0, \nu) \leqslant D(C_0 + t_1C_1 + \cdots + t_pC_p)$.
Actually it suffices to know how to realize

$$D(C_0, \delta) \leqslant D\big(C_0 + \delta(x_1C_1 + \cdots + x_pC_p)\big)$$

for *one* minor δ of order n of G, and as previously mentioned, for this $D(\delta) \leqslant D\big(C_0 + \delta(x_1C_1 + \cdots + x_pC_p)\big)$ is sufficient.
Indeed in this case, we replace C_0 by $C_0' = C_0 + \delta(x_1C_1 + \cdots + x_pC_p)$ in F (without changing G), and we can pass to another minor δ' of G for which we will obtain $x_1', \dots, x_p'$, satisfying

$$D(C_0, \delta, \delta') \leqslant D(C_0', \delta') \leqslant D\big(C_0' + \delta'(x_1'C_1 + \cdots + x_p'C_p)\big) = D(C_0''),$$

with $C_0'' = C_0 + t_1''C_1 + \cdots + t_p''C_p$ and so forth.
To realize the inequality

$$D(\delta) \leqslant D\big(C_0 + \delta(x_1C_1 + \cdots + x_pC_p)\big)$$

for some minor δ of order n of G, we use Lemma 5.2 with the extracted matrix Γ corresponding to the minor δ, and for C_0 we limit ourselves to the rows of Γ, which gives us a vector Γ_0. We obtain some $X \in \mathbf{A}^n$ such that

$$D(\delta) \leqslant D(\Gamma_0 + \delta\Gamma X) \leqslant D(C_0 + \delta GZ).$$

where $Z \in \mathbf{A}^p$ is obtained by completing X with 0's. □

Still with the notations 5.1, we obtain as a corollary the following result, which implies, when $D = \mathrm{D}_{\mathbf{A}}$, that $\mathsf{Gdim}\,\mathbf{A} \leqslant \mathsf{Cdim}\,\mathbf{A}$.

5.5. Corollary. *With the notations 5.1, let $n \in [\![1..p]\!]$.*
If D is n-stable and $1 = D\big(C_0, \mathcal{D}_n(G)\big)$, there exist $t_1, \ldots, t_p$ such that the vector $C_0 + t_1C_1 + \cdots + t_pC_p$ is D-unimodular.

With the Heitmann dimension

5.6. Lemma. *We consider a matrix of the form*

$$\begin{bmatrix} b_0 & c_1 & \cdots & \cdots & c_n \\ b_1 & a & 0 & \cdots & 0 \\ \vdots & 0 & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ b_n & 0 & \cdots & 0 & a \end{bmatrix},$$

for which we denote the columns by $V_0, V_1, \ldots, V_n$.
If $\mathsf{Hdim}\,\mathbf{A} < n$ *and* $1 = \mathrm{D}_{\mathbf{A}}(b_0, a)$, *then there exist $x_1, \ldots, x_n \in a\mathbf{A}$ such that* $1 = \mathrm{D}_{\mathbf{A}}(V_0 + x_1V_1 + \cdots + x_nV_n)$.

D The proof is by induction on n. For $n = 0$, it is clear.
If $n > 0$, let $\mathfrak{j} = \mathcal{I}^{\mathrm{H}}_{\mathbf{A}}(b_n)$. We have $b_n \in \mathfrak{j}$ and $\mathsf{Hdim}\,\mathbf{A}/\mathfrak{j} < n - 1$, therefore by induction hypothesis, we can find $y_1, \ldots, y_{n-1} \in \mathbf{A}$ such that

$$1 = \mathrm{D}(U_0 + ay_1U_1 + \cdots + ay_{n-1}U_{n-1}) \quad \text{in } \mathbf{A}/\mathfrak{j}, \tag{α}$$

where U_i designates the vector V_i minus its last coordinate.
Let $U_0' = U_0 + ay_1U_1 + \cdots + ay_{n-1}U_{n-1}$, we have $\mathrm{D}_{\mathbf{A}}(U_0', a) = \mathrm{D}_{\mathbf{A}}(U_0, a)$. The equality (α) means that there exists a y_n such that $b_ny_n \in \mathrm{J}_{\mathbf{A}}(0)$ and

$$1 = \mathrm{D}_{\mathbf{A}}(U_0') \vee \mathrm{D}_{\mathbf{A}}(b_n, y_n). \tag{β}$$

Let $V_0' = V_0 + ay_1V_1 + \cdots + ay_{n-1}V_{n-1} + ay_nV_n$. The lemma is proven if $1 \in \mathrm{D}_{\mathbf{A}}(V_0')$. Notice that V_0' minus its last coordinate is the vector $U_0' + a_ny_nU_n$ and that its last coordinate is $b_n + a^2y_n$, hence the tight game that comes with b_n, a, y_n. We have

$$\mathrm{D}_{\mathbf{A}}(U_0' + ay_nU_n) \vee \mathrm{D}_{\mathbf{A}}(a) = \mathrm{D}_{\mathbf{A}}(U_0', a) = \mathrm{D}_{\mathbf{A}}(U_0, a) \supseteq \mathrm{D}_{\mathbf{A}}(b_0, a) = 1, \quad (\gamma)$$

and, by (β),

$$\mathrm{D}_{\mathbf{A}}(U_0' + ay_nU_n) \vee \mathrm{D}_{\mathbf{A}}(b_n, y_n) = \mathrm{D}_{\mathbf{A}}(U_0') \vee \mathrm{D}_{\mathbf{A}}(b_n, y_n) = 1. \quad (\delta)$$

Next (γ) and (δ) imply

$$\mathrm{D}_{\mathbf{A}}(U_0' + ay_nU_n) \vee \mathrm{D}_{\mathbf{A}}(b_n, a^2y_n) = 1 = \mathrm{J}_{\mathbf{A}}(U_0' + ay_nU_n, b_n, a^2y_n), \quad (\eta)$$

and by Lemma 2.2, since $b_na^2y_n \in \mathrm{J}_{\mathbf{A}}(0)$,

$$1 = \mathrm{J}_{\mathbf{A}}(U_0' + ay_nU_n, b_n + a^2y_n),$$

i.e. $1 = \mathrm{D}_{\mathbf{A}}(V_0')$. □

5.7. Theorem. (Coquand's theorem, 3: Forster-Swan and others with the Heitmann dimension) *We have* $\mathsf{Gdim}\,\mathbf{A} \leqslant \mathsf{Hdim}\,\mathbf{A}$. *Consequently, Serre's Splitting Off, Forster-Swan' and Bass' cancellation theorems apply with the* Hdim *(Theorems 3.4, 3.6, 3.8, 3.11).*

D We use the characterization of $\mathsf{Gdim}\,\mathbf{A} < n$ given in Proposition 3.13. Lemma 5.6 tells us that the equivalent property described in 3.13 is satisfied if $\mathsf{Hdim}\,\mathbf{A}/\langle d\rangle < n$. We conclude by noticing that $\mathsf{Hdim}\,\mathbf{A}/\langle d\rangle \leqslant \mathsf{Hdim}\,\mathbf{A}$.□

Final remark. All the theorems of commutative algebra which we have proven in this chapter are ultimately brought back to theorems regarding matrices and their elementary operations. ■

Exercises and problems

Exercise 1. Explicate the computation that gives the proof of Theorem 1.3 in the case $n = 1$.

Exercise 2. *(A property of regular sequences)*
Let $(a_1, \dots, a_n)$ be a regular sequence of $\mathbf{A}$ and $\mathfrak{a} = \langle a_1, \dots, a_n\rangle$ ($n \geqslant 1$).
1. Show that $(\overline{a_1}, \dots, \overline{a_n})$ is an $(\mathbf{A}/\mathfrak{a})$-basis of $\mathfrak{a}\big/\mathfrak{a}^2$.
2. Deduce, when $1 \notin \mathfrak{a}$, that n is the minimum number of generators of the ideal $\mathfrak{a}$. For example, if $\mathbf{k}$ is a nontrivial ring and $\mathbf{A} = \mathbf{k}[X_1, \dots, X_m]$, then for $n \leqslant m$, the minimum number of generators of the ideal $\langle X_1, \dots, X_n\rangle$ is n.

Exercise 3. *(Number of generators of* $\mathfrak{a}/\mathfrak{a}^2$ *and of* $\mathfrak{a}$*)*
Let $\mathfrak{a}$ be a finitely generated ideal of $\mathbf{A}$ with $\mathfrak{a}/\mathfrak{a}^2 = \langle\overline{a_1}, \cdots, \overline{a_n}\rangle$.
1. Show that $\mathfrak{a}$ is generated by $n + 1$ elements.
2. Show that $\mathfrak{a}$ is locally generated by n elements in the following precise sense: there exists an $s \in \mathbf{A}$ such that over the two localized rings $\mathbf{A}_s$ and $\mathbf{A}_{1-s}$, $\mathfrak{a}$ is generated by n elements.
3. Deduce that if $\mathbf{A}$ is local-global (for example if $\mathbf{A}$ is residually zero-dimensional), then $\mathfrak{a}$ is generated by n elements.

Exercise 4. *1.* Let E be an $\mathbf{A}$-module and F be a $\mathbf{B}$-module. If E and F are generated by m elements, the same goes for the $(\mathbf{A}\times\mathbf{B})$-module $E\times F$.
2. Let $\mathfrak{a}\subseteq\mathbf{A}[X]$ be an ideal containing a separable polynomial $P=\prod_{i=1}^{s}(X-a_i)$. Let $\mathrm{ev}_{a_i}:\mathbf{A}[X]\twoheadrightarrow\mathbf{A}$ be the evaluation morphism that specializes X in a_i. Suppose that each $\mathfrak{a}_i:=\mathrm{ev}_{a_i}(\mathfrak{a})$ is generated by m elements. Show that $\mathfrak{a}$ is generated by $m+1$ elements.
3. Let $\mathbf{K}$ be a discrete field and $V\subset\mathbf{K}^n$ be a finite set. Show that the ideal

$$\mathfrak{a}(V)=\{\,f\in\mathbf{K}[X_1,\dots,X_n]\,|\,\forall\,w\in V,\ f(w)=0\,\}$$

is generated by n elements (note that this bound does not depend on $\#V$ and that the result is clear for $n=1$).

Exercise 5. *(The left cubic of $\mathbb{P}^3$, image of $\mathbb{P}^1$ under the Veronese embedding of degree 3)* The base ring $\mathbf{k}$ is arbitrary, except in the first question where it is a discrete field. We define the Veronese morphism $\psi:\mathbb{P}^1\to\mathbb{P}^3$ by

$$\psi:(u:v)\mapsto(x_0:x_1:x_2:x_3)\quad\text{with}\quad x_0=u^3,\ x_1=u^2v,\ x_2=uv^2,\ x_3=v^3.$$

1. Show that $\operatorname{Im}\psi=\mathcal{Z}(\mathfrak{a})$ where $\mathfrak{a}=\langle D_1,D_2,D_3\rangle=\mathcal{D}_2(M)$ with the matrix

$$M=\begin{bmatrix}X_0&X_1&X_2\\X_1&X_2&X_3\end{bmatrix},$$

$$D_1=X_1X_3-X_2^2,\ D_2=-X_0X_3+X_1X_2,\ D_3=X_0X_2-X_1^2.$$

2. Show that $\mathfrak{a}$ is the kernel of $\varphi:\mathbf{k}[X_0,X_1,X_2,X_3]\to\mathbf{k}[U,V]$, $X_i\mapsto U^{3-i}V^i$. In particular, if $\mathbf{k}$ is integral, $\mathfrak{a}$ is prime and if $\mathbf{k}$ is reduced, $\mathfrak{a}$ is radical. We will show that by letting

$$\mathfrak{a}^\bullet=\mathbf{A}\oplus\mathbf{A}X_1\oplus\mathbf{A}X_2\quad\text{with}\quad\mathbf{A}=\mathbf{k}[X_0,X_3],$$

we get $\mathbf{k}[X_0,X_1,X_2,X_3]=\mathfrak{a}+\mathfrak{a}^\bullet$ and $\operatorname{Ker}\varphi\cap\mathfrak{a}^\bullet=0$.
3. Show that $\mathfrak{a}$ cannot be generated by two generators.
4. Explicate a homogeneous polynomial F_3 of degree 3 such that $\mathrm{D}_{\mathbf{A}}(\mathfrak{a})=\mathrm{D}_{\mathbf{A}}(D_1,F_3)$. In particular, if $\mathbf{k}$ is reduced, $\mathfrak{a}=\mathrm{D}_{\mathbf{A}}(D_1,F_3)$.

Exercise 6. Show that if two sequences are disjoint (see page 810) they remain disjoint when we multiply one of the sequences by an element of the ring.

Exercise 7. *(Transitivity of the action of $\mathbb{GL}_2(\mathbf{k}[x,y])$ on the systems of two generators of $\langle x,y\rangle$)* The result of question *1* is due to Jean-Philippe Furter, of the Université de La Rochelle.
Let $\mathbf{k}$ be a ring, $\mathbf{A}=\mathbf{k}[x,y]$ and $p,\ q\in\mathbf{A}$ satisfying $\langle p,q\rangle=\langle x,y\rangle$.

1. Construct a matrix $A\in\mathbb{GL}_2(\mathbf{A})$ such that $A\begin{bmatrix}x\\y\end{bmatrix}=\begin{bmatrix}p\\q\end{bmatrix}$ and $\det(A)\in\mathbf{k}^\times$.

2. We write $p=\alpha x+\beta y+\dots$, $q=\gamma x+\delta y+\dots$ with $\alpha,\ \beta,\ \gamma,\ \delta\in\mathbf{k}$.

- *a.* Show that $\begin{bmatrix}\alpha&\beta\\\gamma&\delta\end{bmatrix}\in\mathbb{GL}_2(\mathbf{k})$.
- *b.* Let $G\subset\mathbb{GL}_2(\mathbf{A})$ be the intersection of $\mathbb{SL}_2(\mathbf{A})$ and of the kernel of the homomorphism "reduction modulo $\langle x,y\rangle$" $\mathbb{GL}_2(\mathbf{A})\to\mathbb{GL}_2(\mathbf{k})$. The subgroup G is distinguished in $\mathbb{GL}_2(\mathbf{A})$. The subgroup $G\,\mathbb{GL}_2(\mathbf{k})=\mathbb{GL}_2(\mathbf{k})\,G$ of $\mathbb{GL}_2(\mathbf{A})$ operates transitively on the systems of two generators of $\langle x,y\rangle$.

3. Let $p = x + \sum_{i+j=2} p_{ij}x^iy^j$, $q = y + \sum_{i+j=2} q_{ij}x^iy^j$. We have $\langle x, y\rangle = \langle p, q\rangle$ if and only if the following equations are satisfied

$$p_{20}p_{02} + p_{02}q_{11} + q_{02}^2 = p_{20}p_{11} + p_{02}q_{20} + p_{11}q_{11} - p_{20}q_{02} + q_{11}q_{02} = p_{20}^2 + p_{11}q_{20} + q_{20}q_{02} = 0$$

4. Generalize the result of the previous question.

Exercise 8. *(About Smith rings and* Sdim*)*
For the notions of a strict Bézout ring and a Smith ring, see Section IV-7 on page 206 and Exercises IV-7 and IV-8. Exercise IV-8 gives a direct solution of item *5.*

1. If $\mathbf{A}$ is a Smith ring, we have $\mathsf{Sdim}\,\mathbf{A} \leqslant 0$.
Deduce $\mathsf{Sdim}\,\mathbb{Z}$, $\mathsf{Bdim}\,\mathbb{Z}$, $\mathsf{Gdim}\,\mathbb{Z}$ and $\mathsf{Cdim}\,\mathbb{Z}$.

In questions *2* and *3*, the ring $\mathbf{A}$ is arbitrary.

2. Let $A \in \mathbb{M}_2(\mathbf{A})$ and $u \in \mathbf{A}^2$ be a unimodular vector. Show that $u \in \operatorname{Im} A$ if and only if there exists a $Q \in \mathbb{GL}_2(\mathbf{A})$ such that u is the first column of AQ.

3. Let $A \in \mathbb{M}_2(\mathbf{A})$ of rank $\geqslant 1$. Then A is equivalent to a diagonal matrix if and only if $\operatorname{Im} A$ contains a unimodular vector.

4. Let $\mathbf{A}$ be a strict Bézout ring. Show that $\mathsf{Sdim}\,\mathbf{A} \leqslant 0$ if and only if $\mathbf{A}$ is a Smith ring.

5. Deduce that a ring $\mathbf{A}$ is a Smith ring if and only if it is a strict Bézout ring and if for comaximal a, b, c the matrix $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$ has a unimodular vector in its image. This last condition can be expressed by the condition known as the Kaplansky condition: $1 \in \langle a, b, c\rangle \Rightarrow$ there exist p, q such that $1 \in \langle pa, pb + qc\rangle$.

Remark: we dispose of the elementary characterization: $\mathbf{A}$ is a strict Bézout ring if and only if for every a, $b \in \mathbf{A}$, there exist d and comaximal a', b' such that $a = da'$ and $b = db'$. If we add the Kaplansky condition above, we obtain an elementary characterization of Smith rings.

Some solutions, or sketches of solutions

Exercise 1. The given proof says this. Since $\mathsf{Kdim}\,\mathbf{A} \leqslant 0$, there exists some x_1 such that $b_1x_1 \in \mathrm{D}_{\mathbf{A}}(0)$ and $1 \in \mathrm{D}_{\mathbf{A}}(b_1, x_1)$. A fortiori $b_1ax_1 \in \mathrm{D}_{\mathbf{A}}(0)$ and $a \in \mathrm{D}_{\mathbf{A}}(b_1, ax_1)$. Lemma 1.1 tells us that $\mathrm{D}_{\mathbf{A}}(b_1, ax_1) = \mathrm{D}_{\mathbf{A}}(b_1 + ax_1)$, so $a \in \mathrm{D}_{\mathbf{A}}(b_1 + ax_1)$.

Exercise 2. *1.* Let $b_1, \ldots, b_n \in \mathbf{A}$ such that $\sum_i \overline{b_i}\overline{a_i} = 0$ in $\mathfrak{a}\big/\mathfrak{a}^2$. In other words $\sum_i b_ia_i = \sum_i c_ia_i$ with $c_i \in \mathfrak{a}$. By Lemma IV-2.4, there exists an alternating matrix $M \in \mathbb{M}_n(\mathbf{A})$ such that $[\,b_1 - c_1 \ \cdots \ b_n - c_n\,] = [\,a_1 \ \cdots \ a_n\,]M$. Hence $b_i - c_i \in \mathfrak{a}$, and so $b_i \in \mathfrak{a}$.

Same thing, presented more abstractly. We know that a presentation matrix of the $\mathbf{A}$-module $\mathfrak{a}$ for the generator set $(a_1, \ldots, a_n)$ is $R_{\underline{a}}$. By changing the base ring $\mathbf{A} \to \mathbf{A}/\mathfrak{a}$, this gives a null presentation matrix ($R_{\underline{a}}$ mod $\mathfrak{a}$) of the $\mathbf{A}/\mathfrak{a}$-module $\mathfrak{a}/\mathfrak{a}^2$ for $(\overline{a_1}, \ldots, \overline{a_n})$, which means that this system is a basis.

2. If $(y_1, \ldots, y_p)$ is a generator set of the ideal $\mathfrak{a}$, $(\overline{y_1}, \ldots, \overline{y_p})$ is a generator set of the free $(\mathbf{A}/\mathfrak{a})$-module $\mathfrak{a}/\mathfrak{a}^2$ of rank n. Therefore, if $p < n$, $\mathbf{A}/\mathfrak{a}$ is trivial.

Exercise 3. *1.* By letting $\mathfrak{b} = \langle a_1, \cdots, a_n \rangle$, the equality $\mathfrak{a}/\mathfrak{a}^2 = \langle \overline{a_1}, \cdots, \overline{a_n} \rangle$ means that $\mathfrak{a} = \mathfrak{b} + \mathfrak{a}^2$. We then have $(\mathfrak{a}/\mathfrak{b})^2 = (\mathfrak{a}^2 + \mathfrak{b})/\mathfrak{b} = \mathfrak{a}/\mathfrak{b}$, and the finitely generated ideal $\mathfrak{a}/\mathfrak{b}$ of $\mathbf{A}/\mathfrak{b}$ is idempotent, therefore generated by an idempotent. Therefore there exists some $e \in \mathfrak{a}$, idempotent modulo $\mathfrak{b}$, such that $\mathfrak{a} = \mathfrak{b} + \langle e \rangle$: $\mathfrak{a} = \langle a_1, \ldots, a_n, e \rangle$.

2. With the same notations we see that $(1-e)\mathfrak{a} \subseteq \mathfrak{b} + \left\langle e^2 - e \right\rangle \subseteq \mathfrak{b}$.
Therefore in $\mathbf{A}_{1-e}$, $(a_1, \ldots, a_n)$ generates $\mathfrak{a}$ whereas in $\mathbf{A}_e$, $1 \in \mathfrak{a}$.

Variant. We introduce $S = 1 + \mathfrak{a}$ and work on $\mathbf{A}_S$: $\mathfrak{a}\mathbf{A}_S \subseteq \mathrm{Rad}(\mathbf{A}_S)$ and so, by Nakayama, a generator set of $\mathfrak{a}_S \big/ \mathfrak{a}_S^2$ is also a generator set of $\mathfrak{a}_S$. We therefore have $\mathfrak{a}_S = \mathfrak{b}_S$, hence the existence of some $s \in S$ such that $s\mathfrak{a} \subseteq \mathfrak{b}$. In $\mathbf{A}_s$, $(a_1, \ldots, a_n)$ generates $\mathfrak{a}$, whereas in $\mathbf{A}_{1-s}$, $1 \in \mathfrak{a}$ ($s \in 1 + \mathfrak{a}$, so $1 - s \in \mathfrak{a}$).

Exercise 4. Item *1* is obvious, and we deduce *2* since $\mathfrak{a}/\langle P \rangle \simeq \mathfrak{a}_1 \times \cdots \times \mathfrak{a}_s$. We deduce *3* by induction on n. We observe that the Chinese remainder theorem used in item *2* is concretely realized by the interpolation à la Lagrange.
Note: see also Exercise III-2.

Exercise 5. *1.* ψ is homogeneous of degree 3. Let $p = (x_0 : x_1 : x_2 : x_3)$ in $\mathscr{Z}(\mathfrak{a})$. If $x_0 \neq 0$, we are brought back to $x_0 = 1$, so $(x_0, x_1, x_2, x_3) = (1, x_1, x_1^2, x_1^3) = \psi(1 : x_1)$. If $x_0 = 0$, then $x_1 = 0$, then $x_2 = 0$, so $p = \psi(0 : 1)$.

2. Let $\mathbf{k}[\underline{x}] = \mathbf{k}[\underline{X}]/\mathfrak{a}$ and $\overline{\mathbf{A}} = \mathbf{k}[x_0, x_3]$. Showing the equality $\mathbf{k}[\underline{X}] = \mathfrak{a} + \mathfrak{a}^\bullet$ amounts to showing that $\mathbf{k}[\underline{x}] = \overline{\mathbf{A}} + \overline{\mathbf{A}}x_1 + \overline{\mathbf{A}}x_2$. We have the relations $x_1^3 = x_0^2 x_3 \in \overline{\mathbf{A}}$, and $x_2^3 = x_0 x_3^2 \in \overline{\mathbf{A}}$, therefore $\overline{\mathbf{A}}[x_1, x_2]$ is the $\overline{\mathbf{A}}$-module generated by the $x_1^i x_2^j$'s for i, $j \in [\![0..2]\!]$. But we also have $x_1 x_2 = x_0 x_3$, $x_1^2 = x_0 x_2$, $x_2^2 = x_1 x_3$, which completes the proof of $\overline{\mathbf{A}}[x_1, x_2] = \overline{\mathbf{A}} + \overline{\mathbf{A}}x_1 + \overline{\mathbf{A}}x_2$.

Let $h = a + bX_1 + cX_2 \in \mathfrak{a}^\bullet$ satisfy $\varphi(h) = 0$ ($a, b, c \in \mathbf{A} = \mathbf{k}[X_0, X_3]$). We therefore have

$$a(U^3, V^3) + b(U^3, V^3)U^2V + c(U^3, V^3)UV^2 = 0.$$

By letting $p(T) = a(U^3, T)$, $q(T) = b(U^3, T)U^2$, $r(T) = c(U^3, T)U$, we obtain the equality $p(V^3) + q(V^3)V + r(V^3)V^2 = 0$, and an examination modulo 3 of the exponents in V of p, q, r provides $p = q = r = 0$. Hence $a = b = c = 0$, i.e. $h = 0$. Now, if $f \in \operatorname{Ker}\varphi$, by writing $f = g + h$ with $g \in \mathfrak{a}$, $h \in \mathfrak{a}^\bullet$, we obtain $h \in \operatorname{Ker}\varphi \cap \mathfrak{a}^\bullet = 0$, so $f = g \in \mathfrak{a}$.

3. Let $E = \mathfrak{a}/\langle \underline{X} \rangle \mathfrak{a}$. It is a $\mathbf{k}[\underline{X}]/\langle \underline{X} \rangle$-module generated by $d_i = \overline{D_i}$. In other words $E = \mathbf{k}d_1 + \mathbf{k}d_2 + \mathbf{k}d_3$. Moreover, d_1, d_2, d_3 are $\mathbf{k}$-linearly independent. Indeed, if $ad_1 + bd_2 + cd_3 = 0$, then $aD_1 + bD_2 + cD_3 \in \langle \underline{X} \rangle \mathfrak{a}$, which for homogeneity reasons gives $aD_1 + bD_2 + cD_3 = 0$, then $a = b = c = 0$. Therefore E is free of rank 3 over $\mathbf{k}$. If G is a generator set of $\mathfrak{a}$, then $\overline{G}$ is a generator set of the $\mathbf{k}$-module E, therefore $\#\overline{G} \geqslant 3$, a fortiori $\#G \geqslant 3$.

4. Let $F_3 = X_0D_2 + X_1D_3 = -X_0^2X_3 + 2X_0X_1X_2 - X_1^3 \in \langle D_2, D_3\rangle$. We have

$$D_2^2 = -(X_3F_3 + X_1^2D_1) \in \langle D_1, F_3\rangle\,, \quad D_3^2 = -(X_1F_3 + X_0^2D_1) \in \langle D_1, F_3\rangle\,,$$
$$D_2D_3 = X_0X_1D_1 + X_2F_3 \in \langle D_1, F_3\rangle \ \text{ then}$$
$$\langle D_1, D_2, D_3\rangle^2 \subseteq \langle D_1, F_3\rangle \subseteq \langle D_1, D_2, D_3\rangle\,, \text{ hence } \sqrt{\langle D_1, D_2, D_3\rangle} = \sqrt{\langle D_1, F_3\rangle}.$$

Exercise 7. *1.* Let us first notice that for $m_{ij} \in \mathbf{A} = \mathbf{k}[x, y]$, an equality

$$\begin{bmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

entails $m_{ij} \in \langle x, y\rangle$. Moreover, we will use the following identities for 2×2 matrices: $\det(A + B) = \det(A) + \det(B) + \mathrm{Tr}(\widetilde{A}B)$ and

$$\text{for } H = \begin{bmatrix} v \\ -u \end{bmatrix} [\,y \ \ -x\,], \quad \mathrm{Tr}(\widetilde{A}H) = [\,u\ v\,]\,A \begin{bmatrix} x \\ y \end{bmatrix}.$$

By hypothesis, we have A, $B \in \mathbb{M}_2(\mathbf{A})$ such that

$$A \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} p \\ q \end{bmatrix} \text{ and } B \begin{bmatrix} p \\ q \end{bmatrix} = \begin{bmatrix} x \\ y \end{bmatrix}$$

therefore $(BA - \mathrm{I}_2) \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$. Thus, modulo $\langle x, y\rangle = \langle p, q\rangle$, we have $BA \equiv \mathrm{I}_2$. Therefore $a = \det(A)(0, 0) \in \mathbf{k}^\times$ and we can express, with u, $v \in \mathbf{A}$, $\det(A) = a + up + vq$. Let $H = \begin{bmatrix} v \\ -u \end{bmatrix} [\,y \ \ -x\,]$. We have $H \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$, $\det(H) = 0$, and we change A to $A' = A - H$. Then $A' \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} p \\ q \end{bmatrix}$ and

$$\det(A') = \det(A) + \det(H) - \mathrm{Tr}(\widetilde{A}H) = a + up + vq - [\,u\ v\,] \begin{bmatrix} p \\ q \end{bmatrix} = a.$$

2. We decompose A into homogeneous components: $A = A_0 + A_1 + \ldots$, and we examine the equality $A \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} p \\ q \end{bmatrix}$.

The examination of the homogeneous component of degree 1 gives $A_0 = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$, and we know that $\det(A) = \det(A_0) \in \mathbf{k}^\times$.

We then can write $A_0(A_0^{-1}A) \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} p \\ q \end{bmatrix}$ with $A_0 \in \mathbb{GL}_2(\mathbf{k})$ and $A_0^{-1}A \in G$.

3. We write $A \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} p \\ q \end{bmatrix}$ with $A \in G$. For degree reasons, we obtain an equality $A = \mathrm{I}_2 + xB + yC$ with B, $C \in \mathbb{M}_2(\mathbf{k})$. We then have

$$\begin{bmatrix} p \\ q \end{bmatrix} = A \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x \\ y \end{bmatrix} + B \begin{bmatrix} x^2 \\ xy \end{bmatrix} + C \begin{bmatrix} xy \\ y^2 \end{bmatrix} = \begin{bmatrix} x + b_{11}x^2 + (c_{11} + b_{12})xy + c_{12}y^2 \\ y + b_{21}x^2 + (c_{21} + b_{22})xy + c_{22}y^2 \end{bmatrix} \qquad (\star)$$

Moreover, we notice that the coefficient of $\det(A)-1$ in x^iy^j is a homogeneous polynomial of degree $i+j$ in the coefficients of B and C

$$\det(A)-1 = \mathrm{Tr}(B)x + \mathrm{Tr}(C)y + \det(B)x^2 + \mathrm{Tr}(\widetilde{B}C)xy + \det(C)y^2.$$

If **k** was an algebraically closed field, we could give the following argument. The equality $\det(A)=1$ defines a projective subvariety $V \subset \mathbb{P}^{8-1}$ (2×4 coefficients for (B,C)); on the other hand $(\star)$ defines a morphism $V \to \mathbb{P}^{6-1}$ (6 for the coefficients of $p-x$, $q-y$). The image of this morphism is the set W defined by the equations of the statement.

The ring **k** being arbitrary, we carefully examine the equations $(\star)$; by using $\mathrm{Tr}(B)=\mathrm{Tr}(C)=0$, we can express B and C in terms of the coefficients of p and q

$$B = \begin{bmatrix} p_{20} & p_{11}+q_{02} \\ q_{20} & -p_{20} \end{bmatrix}, \qquad C = \begin{bmatrix} -q_{02} & p_{02} \\ p_{20}+q_{11} & q_{02} \end{bmatrix}.$$

We thus construct a section $s : W \to G$ of the map $(\star)$, and in fact the three equations of W appearing in the statement are, up to sign, $\det(C)$, $\mathrm{Tr}(\widetilde{B}C)$ and $\det(B)$.

Exercise 8. *1.* A "diagonal" rectangular matrix of rank $\geqslant 1$ has in its image a unimodular vector (this for every ring). Let A be a matrix of rank $\geqslant 1$, if **A** is a Smith ring, A is equivalent to a "diagonal" matrix D, therefore $\mathrm{Im}\,D$ contains a unimodular vector, and also $\mathrm{Im}\,A$.

We therefore have $\mathsf{Sdim}\,\mathbb{Z}=0$. Moreover, $\mathsf{Cdim}\,\mathbb{Z}\leqslant 1$ ($\mathbb{Z}$ is 2-stable because $\mathbb{Z}$ is a Bézout domain). Finally, $\mathsf{Bdim}\,\mathbb{Z}>0$ because $1\in\langle 2,5\rangle$ without finding some $x\in\mathbb{Z}$ such that $1\in\langle 2+5x\rangle$.
Recap: $\mathsf{Bdim}\,\mathbb{Z}=\mathsf{Gdim}\,\mathbb{Z}=\mathsf{Cdim}\,\mathbb{Z}=1$ but $\mathsf{Sdim}\,\mathbb{Z}=0$.

2. If $u=Av$, then v is unimodular. Therefore $v=Q\cdot e_1$ with $Q\in\mathbb{SL}_2(\mathbf{A})$ and u is the first column of AQ. The other direction is immediate.

3. Suppose that $\mathrm{Im}\,A$ contains a unimodular vector. By item *2*, we have $A\sim B$ with $B\cdot e_1$ unimodular. Therefore the space of rows of B contains a vector of the form $[\,1\ *\,]$. Item *2* for ${}^{\mathrm{t}}B$ gives

$${}^{\mathrm{t}}B \sim \begin{bmatrix} 1 & * \\ * & * \end{bmatrix} \sim \begin{bmatrix} 1 & 0 \\ 0 & * \end{bmatrix}, \text{ diagonal.}$$

Recap: A is equivalent to a diagonal matrix. The other direction is immediate.

4. Let **A** be a strict Bézout ring with $\mathsf{Sdim}\,\mathbf{A}\leqslant 0$. We show that every triangular matrix $M\in\mathbb{M}_2(\mathbf{A})$ is equivalent to a diagonal matrix.
We can write $M=dA$ with A of rank $\geqslant 1$ (because **A** is a strict Bézout ring). Since $\mathsf{Sdim}\,\mathbf{A}\leqslant 0$, $\mathrm{Im}\,A$ contains a unimodular vector therefore is equivalent to a diagonal matrix D. Ultimately $M\sim dD$.

5. Now easy.

Bibliographic comments

If we stick to the constructive aspect of the results, the whole chapter is essentially due to T. Coquand, with at times the help of the authors of the book that you are holding in your hands. This is a remarkable success for the constructive approach of the theory of the Krull dimension. Without this approach, it was simply unthinkable to obtain in a general constructive form the “grand” classical theorems proven here. In addition, this approach has guided the development of a new dimension, which we call Heitmann dimension, thanks to which the remarkable Heitmann non-Noetherian results were able to be improved further, namely the general non-Noetherian version of Serre’s Splitting Off theorem and of the Forster-Swan theorem.

Kronecker’s theorem is usually stated in the following form: an algebraic variety in $\mathbb{C}^n$ can always be defined by $n+1$ equations.
It was extended to the case of Noetherian rings by van der Waerden [197] in the following form: in a Noetherian ring of Krull dimension n, every ideal has the same nilradical as an ideal generated by at most $n+1$ elements.
Kronecker’s version was improved by various authors in the articles [182, Storch] and [75, Eisenbud&Evans] which showed that n equations generally suffice. A constructive proof of this last theorem is in [51, Coquand&al.].
Moreover, we still do not know whether every curve in the complex space of dimension 3 is an intersection of two surfaces or not (see [Kunz], Chapter 5).
Lemma 2.8 is Heitmann’s Corollary 2.2 [101], (for us, the Hdim replaces the Jdim) which leads to Theorem 2.9 (Heitmann’s improvement of Kronecker’s theorem).
The local Kronecker’s theorem 1.6 is due to Lionel Ducos [69].

Note regarding the “stable range.” Theorem 2.6 is due to Bass in the Noetherian case (with the dimension of the maximal spectrum, which in this case coincides with the Jdim and the Hdim) and to Heitmann in the non-Noetherian case with the Jdim. Theorem 1.4 is a non-Noetherian version, but with the Krull dimension, of Theorem 2.6.

Note regarding the Jdim. In [101] Heitmann introduces the Jdim for a not necessarily Noetherian ring as the correct substitute for the dimension of the maximal spectrum $\mathsf{Max}\,\mathbf{A}$. It is the dimension of $\mathsf{Jspec}\,\mathbf{A}$, the smallest spectral subspace of $\mathsf{Spec}\,\mathbf{A}$ containing $\mathsf{Max}\,\mathbf{A}$. He establishes Bass’ “stable range” theorem for this dimension. However, for the theorems by Serre and Forster-Swan, he has to use an ad hoc dimension, the upper bound of the $\mathsf{Jdim}(\mathbf{A}[1/x])$’s for $x \in \mathbf{A}$. As this ad hoc dimension is bounded above by the Krull dimension anyway, he is then able to obtain, in particular, a non-Noetherian version of the cited grand theorems for the Krull dimension.

Note regarding Serre’s theorem and the Forster-Swan theorem. Serre’s theorem is in [174, Serre]. The Forster-Swan theorem (Noetherian version)

is in [88, Forster] for the Krull dimension and in [187, Swan] for the dimension of the maximal spectrum. Non-Noetherian versions for the Krull dimension are due to Heitmann [100, 101]. Finally, the article by Eisenbud-Evans [74] has greatly helped to clarify matters regarding Forster, Swan and Serre's theorems.
Sections 3 and 5 (second part: Heitmann dimension) are inspired by the outline of [74, Eisenbud&Evans] and [101, Heitmann]. These sections give constructive versions of Serre's (Splitting Off), Forster-Swan's, and Bass' (cancellation) theorems. This improves (even without taking into account the constructive aspect of the proof) all the known theorems on the subject, by answering positively for the Heitmann dimension (and a fortiori for the Jdim) a question left open by Heitmann.

Note regarding the Hdim. The Heitmann dimension, denoted by Hdim, was introduced in [48] (see also [49]). Fundamentally it is the dimension that makes the proofs work in the article by Heitmann [101]. The fact that it is better a priori than the Jdim is not the core point. It is rather the fact that Serre's and Forster-Swan's theorems work with the Hdim, and so a fortiori with the Jdim, which gives the complete non-Noetherian version of these theorems, which had been conjectured by Heitmann.
In the case of a Noetherian ring, the Hdim, Heitmann's Jdim and the dimension of the maximal spectrum $\mathsf{Max}\,\mathbf{A}$ which intervenes in Serre's and Swan's [187] theorems are the same (refer to [49, 101]).

Note regarding n-stability. The notion of a support dates back to Joyal [116] and Español [77], who use it to give a constructive characterization of the Krull dimension of commutative rings. It is used systematically in the recent articles by T. Coquand. In Section 4 and in the first part of Section 5 the notion of an n-stable support is decisive. It was invented by T. Coquand [37] to update the constructive content of Bass' rhetoric on the finite partitions of $\mathsf{Spec}\,\mathbf{A}$ in [Bass].

The version of Bass' cancellation theorem for the Hdim was first proved by Lionel Ducos [68]. The proof that we give is based on [49] instead.

Regarding Exercise 7, Murthy, in [144], proved the following general result. Let $\mathbf{A} = \mathbf{k}[x_1, \dots, x_m]$ be a polynomial ring ($\mathbf{k}$ being a commutative ring) and $r \geqslant 1$ be fixed. Suppose, for every $n \in [\![1..r]\!]$, that every unimodular vector of $\mathbf{A}^n$ is completable and consider, for $n \leqslant \inf(r, m)$, the set of systems of r generators of the ideal $\langle x_1, \dots, x_n \rangle$ of $\mathbf{A}$, such as for example $(x_1, \dots, x_n, 0, \dots, 0)$ where there are $r - n$ zeros. Then the group $\mathbb{GL}_r(\mathbf{A})$ operates transitively on this set (Murthy's result is actually much more precise).

Chapter XV

The local-global principle

Contents

Introduction

In this chapter, we discuss a few important methods directly related to what is commonly called the local-global principle in commutative algebra.

In Section 2 we develop it in the form of concrete local-global principles. This is to say that certain properties are globally true as soon as they are locally true. Here the term locally is taken in the constructive sense: after localization at a finite number of comaximal monoids.

In Section 3, we establish the corresponding abstract local-global principles, by using, inevitably, non-constructive proofs: here locally is taken in the abstract sense, i.e. after localization at any prime ideal.

In Section 4, we explain the construction of "global" objects from objects of the same nature only defined locally.

Sections 5, 6 and 7 are devoted to the "dynamic and constructive decryption" of methods used in abstract algebra. Recall that in Section VII-2 we presented the general philosophy of this dynamic method.

In Section 5, we discuss the constructive decryption of abstract methods that fall within a general framework of the type "local-global principle." We give a general statement (but inevitably a little informal) for this, and we give simple examples, which could be treated more directly. The truly pertinent examples will come in Chapter XVI.

This dynamic method is a fundamental tool of constructive algebra. We could have written this work by starting with this preliminary explanation and by systematically using this decryption. We preferred to start by developing everything that could be directly developed, by establishing the concrete local-global principles that usually allow us to avoid using the dynamic decryption as such. In short, rather than highlighting the magic at work in classical algebra we preferred to first show a different kind of magic at work in constructive algebra under the general slogan: "why make things complicated when you can make them simple?"

In Section 6, we analyze the method of abstract algebra, which consists in "seeing what happens when we quotient by an arbitrary maximal ideal."

In Section 7, we analyze the method which consists in "seeing what happens when we localize at an arbitrary minimal prime ideal."

In Sections 8 and 9, we examine to what extent certain local-global principles remain valid when we replace in the statements the lists of comaximal elements by lists of depth $\geqslant 1$ or of depth $\geqslant 2$.

1. Comaximal monoids, coverings

We treat in Section 2 concrete versions of principles of the local-global type. For these concrete versions, the localization have to be done in a finite number of comaximal elements (or of comaximal monoids) of $\mathbf{A}$: *if the considered property is true after localization at a finite number of comaximal elements, then it is true.*

We introduce a generalization.

1.1. Definition. We say that *the monoids $S_1, \ldots, S_n$ of the ring $\mathbf{A}$ cover the monoid S* if S is contained in the saturated monoid of each S_i and if an ideal of $\mathbf{A}$ that intersects each of the S_i's always intersects S, in other words if we have

$$\forall s_1 \in S_1 \ \ldots \ \forall s_n \in S_n \ \ \exists\, a_1, \ldots, a_n \in \mathbf{A} \quad \textstyle\sum_{i=1}^n a_i s_i \in S.$$

Monoids are comaximal if they cover the monoid $\{1\}$.

In classical mathematics (with the axiom of the prime ideal)[1] we have the characterization given in the following lemma. For some monoid S, we denote by U_S the subset of $\mathsf{Spec}\,\mathbf{A}$ defined by

$$U_S = \{\, \mathfrak{p} \in \mathsf{Spec}\,\mathbf{A} \,|\, \mathfrak{p} \cap S = \emptyset \,\}\,.$$

If S is the monoid generated by the element s, we denote U_S by U_s. From a constructive point of view, $\mathsf{Spec}\,\mathbf{A}$ is a topological space known via its basis of open sets $U_s = \mathfrak{D}_{\mathbf{A}}(s)$ but whose points are often difficult to access.

Recall that we denote by S^{sat} the saturated monoid of the monoid S.

1.2. Lemma*.

1. *For every monoid S we have $S^{\mathrm{sat}} = \bigcap_{\mathfrak{p} \in U_S} (\mathbf{A} \setminus \mathfrak{p})$. Consequently for two monoids S and T, $S^{\mathrm{sat}} \subseteq T^{\mathrm{sat}} \Leftrightarrow U_T \subseteq U_S$.*
2. *$S_1, \ldots, S_n$ are comaximal if and only if $\mathsf{Spec}\,\mathbf{A} = \bigcup_i U_{S_i}$.*
3. *$S_1, \ldots, S_n$ cover the monoid S if and only if $U_S = \bigcup_i U_{S_i}$.*

D *1.* Results from the Krull lemma: if an ideal $\mathfrak{a}$ does not intersect a monoid S, there exists a prime ideal $\mathfrak{p}$ such that $\mathfrak{a} \subseteq \mathfrak{p}$ and $\mathfrak{p} \cap S = \emptyset$.

2. We can assume that $\mathbf{A}$ is not trivial. If the monoids are comaximal and if $\mathfrak{p}$ is a prime ideal not belonging to any of the U_{S_i}'s, there is in each S_i an element s_i of $\mathfrak{p}$, therefore by the definition of the comaximal monoids, $1 \in \mathfrak{p}$,

[1] The axiom of the prime ideal affirms that every strict ideal of a ring is contained in a prime ideal. This is a weakened version of the axiom of choice. In the classical set theory ZF, the axiom of choice is equivalent to the axiom of the maximal ideal, which states that every strict ideal of a ring is contained in a maximal ideal. This is a little stronger that the axiom of the prime ideal. The latter is equivalent to the fact that every consistent formal theory admits a model (this is the compactness theorem in classical logic). In classical set theory with the axiom of choice, the axiom of the prime ideal becomes a theorem and is called "Krull's lemma."

a contradiction. Conversely assume that $\mathsf{Spec}\,\mathbf{A} = \bigcup_i U_{S_i}$ and let $s_1 \in S_1$, $\ldots$, $s_n \in S_n$. If $\langle s_1, \ldots, s_n \rangle$ does not contain 1, it is contained in a prime ideal $\mathfrak{p}$. Therefore $\mathfrak{p}$ is in none of the U_{S_i}'s, a contradiction. □

The following lemma is a variation on the theme: *a covering of coverings is a covering.* It is also a generalization of Fact V-7.2. The corresponding computations are immediate. In classical mathematics it would be even faster via Lemma* 1.2.

1.3. Lemma. (Successive localizations lemma, 2)

1. (Associativity) *If the monoids S_1, $\ldots$, S_n of the ring $\mathbf{A}$ cover the monoid S and if each S_ℓ is covered by monoids $S_{\ell,1}, \ldots, S_{\ell,m_\ell}$, then the $S_{\ell,j}$'s cover S.*
2. (Transitivity)
   a. *Let S be a monoid of the ring $\mathbf{A}$ and $S_1, \ldots, S_n$ be monoids of the ring $\mathbf{A}_S$. For $\ell \in [\![1..n]\!]$ let V_ℓ be the monoid of $\mathbf{A}$ formed by the numerators of the elements of S_ℓ. Then the monoids $V_1, \ldots, V_n$ cover S if and only if the monoids S_1, $\ldots$, S_n are comaximal.*
   b. *More generally let $S_0, \ldots, S_n$ be monoids of the ring $\mathbf{A}_S$ and for $\ell = 0, \ldots, n$ let V_ℓ be the monoid of $\mathbf{A}$ formed by the numerators of elements of S_ℓ. Then the monoids $V_1, \ldots, V_n$ cover V_0 if and only if S_1, $\ldots$, S_n cover S_0 in $\mathbf{A}_S$.*

1.4. Definition and notation. Let U and I be subsets of the ring $\mathbf{A}$. Let $\mathcal{M}(U)$ be the monoid generated by U, and $\mathcal{S}(I,U)$ be the monoid

$$\mathcal{S}(I,U) = \langle I \rangle_{\mathbf{A}} + \mathcal{M}(U).$$

The pair $\mathfrak{q} = (I,U)$ is also called a *potential prime ideal*, and we write (by abuse) $\mathbf{A}_\mathfrak{q}$ for $\mathbf{A}_{\mathcal{S}(I,U)}$. Similarly we let

$$\mathcal{S}(a_1, \ldots, a_k; u_1, \ldots, u_\ell) = \langle a_1, \ldots, a_k \rangle_{\mathbf{A}} + \mathcal{M}(u_1, \ldots, u_\ell).$$

We say that such a monoid *admits a finite description.* The pair

$$(\{a_1, \ldots, a_k\}, \{u_1, \ldots, u_\ell\})$$

is called a *finite potential prime ideal.*

It is clear that for $u = u_1 \cdots u_\ell$, the monoids $\mathcal{S}(a_1, \ldots, a_k; u_1, \ldots, u_\ell)$ and $\mathcal{S}(a_1, \ldots, a_k; u)$ are equivalent, i.e. have the same saturated monoid.

Remark. The potential prime ideal $\mathfrak{q} = (I,U)$ is constructed for the following goal: *when we localize at $\mathcal{S}(I,U)$, we obtain $U \subseteq \mathbf{A}_\mathfrak{q}^\times$ and $I \subseteq \mathrm{Rad}(\mathbf{A}_\mathfrak{q})$.* Similarly, for every prime ideal $\mathfrak{p}$ such that $I \subseteq \mathfrak{p}$ and $U \subseteq \mathbf{A} \setminus \mathfrak{p}$, we have $U \subseteq \mathbf{A}_\mathfrak{p}^\times$ and $I \subseteq \mathrm{Rad}(\mathbf{A}_\mathfrak{p})$. The pair $\mathfrak{q} = (I,U)$ therefore represents partial information on such a prime ideal. It can be considered as an approximation of $\mathfrak{p}$. This explains the terminology of a potential prime ideal and the notation $\mathbf{A}_\mathfrak{q}$.

We can compare the approximations of $\mathfrak{p}$ by finite potential prime ideals with approximations of a real number by rational intervals. ■

1.5. Lemma. (Successive localizations lemma, 3)
Let U and I be subsets of the ring $\mathbf{A}$ and $a \in \mathbf{A}$, then the monoids

$$\mathcal{S}(I; U, a) \overset{\text{def}}{=} \mathcal{S}(I, U \cup \{a\}) \ \ \textit{and} \ \ \mathcal{S}(I, a; U) \overset{\text{def}}{=} \mathcal{S}(I \cup \{a\}, U)$$

cover the monoid $\mathcal{S}(I, U)$.
In particular, the monoids $S = \mathcal{M}(a) = \mathcal{S}(0; a)$ and $S' = \mathcal{S}(a; 1) = 1 + a\mathbf{A}$ are comaximal.

D Let $x \in \mathcal{S}(I; U, a)$, $y \in \mathcal{S}(I, a; U)$. We need to see that $\langle x, y \rangle$ meets $\langle I \rangle + \mathcal{M}(U)$, or that $\langle x, y \rangle + \langle I \rangle$ meets $\mathcal{M}(U)$.
We have $k \geqslant 0$, $u, v \in \mathcal{M}(U)$ and $z \in \mathbf{A}$ such that $x \in ua^k + \langle I \rangle$ and $y \in v - az + \langle I \rangle$. Modulo $\langle x, y \rangle + \langle I \rangle$, $ua^k \equiv 0$, $v \equiv az$ so $uv^k \equiv 0$, i.e. $uv^k \in \langle x, y \rangle + \langle I \rangle$ with $uv^k \in \mathcal{M}(U)$. □

Comment. The previous lemma is fundamental. It is the constructive counterpart of the following banal observation in classical mathematics: after localizing at a prime ideal every element is found to be either invertible or in the radical. When dealing with this type of argument in a classical proof, most of the time it can be interpreted constructively by means of this lemma. Its proof is very simple, in the image of the banality of the observation made in the classical proof. But here there is a true computation. We can in fact ask whether the classical proof avoids this computation. A detailed analysis shows that no: it is found in the proof of Lemma* 1.2. ■

The examples given in the following lemma are frequent.

1.6. Lemma. *Let $\mathbf{A}$ be a ring, U and I be subsets of $\mathbf{A}$, and $S = \mathcal{S}(I, U)$.*

1. *If $s_1, \ldots, s_n \in \mathbf{A}$ are comaximal elements, the monoids $\mathcal{M}(s_i)$ are comaximal. More generally, if $s_1, \ldots, s_n \in \mathbf{A}$ are comaximal elements in $\mathbf{A}_S$, the monoids $\mathcal{S}(I; U, s_i)$ cover the monoid S.*
2. *Let $s_1, \ldots, s_n \in \mathbf{A}$. The monoids*
$$S_1 = \mathcal{S}(0; s_1),\ S_2 = \mathcal{S}(s_1; s_2),\ S_3 = \mathcal{S}(s_1, s_2; s_3), \ldots,$$
$$S_n = \mathcal{S}(s_1, \ldots, s_{n-1}; s_n) \text{ and } S_{n+1} = \mathcal{S}(s_1, \ldots, s_n; 1)$$
are comaximal.
More generally, the monoids
$$V_1 = \mathcal{S}(I; U, s_1),\ V_2 = \mathcal{S}(I, s_1; U, s_2),\ V_3 = \mathcal{S}(I, s_1, s_2; U, s_3),\ \ldots,$$
$$V_n = \mathcal{S}(I, s_1, \ldots, s_{n-1}; U, s_n) \text{ and } V_{n+1} = \mathcal{S}(I, s_1, \ldots, s_n; U)$$
cover the monoid $S = \mathcal{S}(I, U)$.
3. *If S, S_1, …, $S_n \subseteq \mathbf{A}$ are comaximal monoids and if $a \in \mathbf{A}$, then the monoids $\mathcal{S}(I; U, a)$, $\mathcal{S}(I, a; U)$, S_1, …, S_n are comaximal.*

D Items *2* and *3* result immediately from Lemmas 1.3 and 1.5.
1. The first case results from the fact that for $k_1, \ldots, k_n \geqslant 1$, we have, for large enough k, $\langle s_1, \ldots, s_n \rangle^k \subseteq \langle s_1^{k_1}, \ldots, s_n^{k_n} \rangle$ (e.g. $k = \sum_i (k_i - 1) + 1$).

For the general case, let $t_1, \ldots, t_n$ with $t_i \in \mathcal{S}(I; U, s_i)$; we want to show that $\langle t_1, \ldots, t_n \rangle$ meets $S = \mathcal{S}(I, U)$. By definition, there is some $u_i \in \mathcal{M}(U)$ and $k_i \geqslant 0$ such that $t_i \in u_i s_i^{k_i} + \langle I \rangle$; by letting $u = u_1 \cdots u_n \in \mathcal{M}(u)$, we obtain $us_i^{k_i} \in \langle t_i \rangle + \langle I \rangle \subseteq \langle t_1, \ldots, t_n \rangle + \langle I \rangle$. Therefore for large enough k,

$$u \langle s_1, \ldots, s_n \rangle^k \subseteq u \langle s_1^{k_1}, \ldots, s_n^{k_n} \rangle \subseteq \langle t_1, \ldots, t_n \rangle + \langle I \rangle .$$

But as $s_1, \ldots, s_n$ are comaximal elements in $\mathbf{A}_S$, there is some $s \in S$ such that $s \in \langle s_1, \ldots, s_n \rangle$; therefore $us^k \in \langle t_1, \ldots, t_n \rangle + \langle I \rangle$, i.e. $\langle t_1, \ldots, t_n \rangle$ meets $us^k + \langle I \rangle \subseteq S$. □

2. A few concrete local-global principles

Linear systems

The following concrete local-global principle is a slight generalization of the local-global principle II-2.3 (basic concrete local-global principle), which only concerned item *4* below in the case of free modules of finite rank. Actually the essential result has already been given in the local-global principle II-6.7 (concrete local-global principle for modules). We give the proofs again to emphasize their great simplicity.

Let $M_1, \ldots, M_\ell, P$ be $\mathbf{A}$-modules. We say that a map $\Phi : M_1 \times \cdots \times M_\ell \to P$ is *homogeneous* if there exist integers $r_1, \ldots, r_\ell$ such that we identically have $\Phi(a_1 x_1, \ldots, a_\ell x_\ell) = a_1^{r_1} \cdots a_\ell^{r_\ell} \Phi(x_1, \ldots, x_\ell)$. In such a case, the map Φ "passes to the localizations": it can be naturally extended to a map

$$\Phi_S : S^{-1} M_1 \times \cdots \times S^{-1} M_\ell \to S^{-1} P$$

for any monoid S. The prototype of a homogeneous map is a map given by homogeneous polynomials in the coordinates when the modules are free of finite rank.

2.1. Concrete local-global principle. *Let $S_1, \ldots, S_n$ be comaximal monoids of $\mathbf{A}$, M, N, P be $\mathbf{A}$-modules, φ, ψ be linear maps from M to N, $\theta : N \to P$ be linear map, and x, y be elements of N. We write $\mathbf{A}_i$ for $\mathbf{A}_{S_i}$, M_i for M_{S_i}, etc. Then we have the following equivalences.*

1. *Concrete patching of the equalities*

$$x = y \quad \text{in} \quad N \quad \iff \quad \forall i \in \llbracket 1..n \rrbracket \;\; x/1 = y/1 \quad \text{in} \quad N_i.$$

2. *Concrete patching of the equalities of linear maps*

$$\varphi = \psi \quad \text{in} \quad \mathrm{L}_{\mathbf{A}}(M, N) \qquad \iff$$
$$\forall i \in \llbracket 1..n \rrbracket \;\; \varphi/1 = \psi/1 \quad \text{in} \quad \mathrm{L}_{\mathbf{A}_i}(M_i, N_i).$$

3. *Concrete patching of the regular elements*

$$x \textit{ is regular in } N \qquad \iff$$
$$\forall i \in \llbracket 1..n \rrbracket \;\; x/1 \textit{ is regular in } N_i.$$

4. *Concrete patching of the solutions of systems of linear equations*

$$x \in \operatorname{Im}\varphi \quad \iff \quad \forall i \in [\![1..n]\!] \;\; x/1 \in \operatorname{Im}\varphi_i.$$

5. *Concrete patching of the solutions of systems of linear equations under homogeneous conditions. Let (Φ_ℓ) be a finite family of homogeneous maps*

$$\Phi_\ell : \mathrm{L}_{\mathbf{A}}(M,N)\times N \to Q_\ell, \text{ or } \Phi_\ell : \mathrm{L}_{\mathbf{A}}(M,N) \to Q_\ell, \text{ or } \Phi_\ell : N \to Q_\ell.$$

Then

$$\big((\&_\ell\ \Phi_\ell(\varphi,y)=0) \;\Rightarrow\; y \in \operatorname{Im}\varphi\big) \qquad \iff$$
$$\forall i \in [\![1..n]\!] \;\; \big((\&_\ell\ \Phi_\ell(\varphi,y) =_{Q_{\ell,i}} 0) \;\Rightarrow\; y/1 \in \operatorname{Im}\varphi_i\big)\,.$$

where we have written $Q_{\ell,i}$ for $(Q_\ell)_{S_i}$.

6. *Concrete patching of the exact sequences. The sequence*

$$M \xrightarrow{\varphi} N \xrightarrow{\theta} P$$

is exact if and only if the sequences

$$M_i \xrightarrow{\varphi_{S_i}} N_i \xrightarrow{\theta_{S_i}} P_i$$

are exact for $i \in [\![1..n]\!]$.

7. *Concrete patching of direct summands in the finitely presented modules. Here M is a finitely generated submodule of a finitely presented module N.*

$$M \textit{ is a direct summand in } N \iff$$
$$\forall i \in [\![1..n]\!] \; M_i \textit{ is a direct summand in } N_i.$$

D The conditions are necessary because of Fact II-6.4. A direct verification is immediate anyway. Let us prove that the local conditions are sufficient.

1. Suppose that $x/1 = 0$ in each N_i. For suitable $s_i \in S_i$ we therefore have $s_i x = 0$ in N. As $\sum_{i=1}^n a_i s_i = 1$, we obtain $x = 0$ in N.

2. Immediate consequence of *1.*

3. Suppose that $x/1$ is regular in each N_i. Let $a \in \mathbf{A}$ with $ax = 0$ in $\mathbf{A}$, therefore also $ax/1 = 0$ in each N_i. We therefore have $a/1 = 0$ in each $\mathbf{A}_i$, so also in $\mathbf{A}$.

4. Suppose that the equation $\varphi(z) = x$ admits a solution z_i in each M_i. We can write $z_i = y_i/s_i$ with $y_i \in M$ and $s_i \in S_i$. We therefore have $u_i\varphi(y_i) = s_i u_i x$ in N with $u_i \in S_i$. As $\sum_{i=1}^n a_i s_i u_i = 1$, let $z = \sum_{i=1}^n a_i u_i y_i$. We obtain $\varphi(z) = x$ in N.

5. This is a simple variant of *4.* The homogeneity of the Φ_ℓ's intervenes so that the local property is well-defined, and so that it results from the global property.

6. This is a special case of the previous item.

7. Let $\rho : N \to N/M$ be the canonical projection. The module N/M is also a finitely presented module. The module M is a direct summand in N if and only if ρ is right-invertible. We can therefore conclude by the local-global principle IV-3.1. □

Remark. We can see that item *5*, a simple variant of item *4*, implies all the others as special cases. Moreover, item *4* results from item *1* with $y = 0$ by considering the module $\big(N/\varphi(M)\big)_{S_i} \simeq N_{S_i}/\varphi_{S_i}(M_{S_i})$. We could therefore have stated item *1* as the only basic principle and, from it, deduce items *2* to *6* as corollaries. Finally, item *7* also directly results from item *4* (see the proof of the local-global principle IV-3.1). ■

Finiteness properties for modules

The usual finiteness properties of modules have a local character. Most have already been proven, we summarize.

2.2. Concrete local-global principle. (Concrete patching of finiteness properties for modules) *Let S_1, …, S_n be comaximal monoids of $\mathbf{A}$ and M be an $\mathbf{A}$-module. Then we have the following equivalences.*

1. *M is finitely generated if and only if each of the M_{S_i}'s is an $\mathbf{A}_{S_i}$-finitely generated module.*
2. *M is finitely presented if and only if each of the M_{S_i}'s is an $\mathbf{A}_{S_i}$-finitely presented module.*
3. *M is flat if and only if each of the M_{S_i}'s is an $\mathbf{A}_{S_i}$-flat module.*
4. *M is finitely generated projective if and only if each of the M_{S_i}'s is an $\mathbf{A}_{S_i}$-finitely generated projective module.*
5. *M is projective of rank k if and only if each of the M_{S_i}'s is a projective $\mathbf{A}_{S_i}$-module of rank k.*
6. *M is coherent if and only if each of the M_{S_i}'s is an $\mathbf{A}_{S_i}$-coherent module.*
7. *M is Noetherian if and only if each of the M_{S_i}'s is a Noetherian $\mathbf{A}_{S_i}$-module.*

D *1.* See the local-global principle II-3.6.

2. See the local-global principle IV-4.13.

3. See the local-global principle VIII-1.7.

4. See the local-global principle V-2.4. We can also use the fact that a finitely presented module is projective if and only if it is flat (and apply items *2* and *3*).

5. Results from item *4* and from the fact that the polynomial rank can be locally computed (it is equal to X^k if and only if it is equal to X^k after localization at comaximal monoids).

6. See the local-global principle II-3.5.

7. We exhibit the proof for the Noetherianity constructively defined à la Richman-Seidenberg. Let us limit ourselves to the case of two comaximal localizations at S_1 and S_2. Consider a non-decreasing sequence $(M_k)_{k\in\mathbb{N}}$ of finitely generated submodules of M. It admits an infinite subsequence

$\big(M_{\sigma(k)}\big)_{k\in\mathbb{N}}$, where $\sigma(k) < \sigma(k+1)\,\forall\, k$, with $M_{\sigma(k)} = M_{\sigma(k)+1}$ after localization at S_1 for all k. Consider the infinite sequence $M_{\sigma(k)}$ seen in M_{S_2}. It admits two equal consecutive terms $M_{\sigma(k)}$ and $M_{\sigma(k+1)}$. So $M_{\sigma(k)}$ and $M_{\sigma(k)+1}$ are equal both in M_{S_1} and M_{S_2}. Therefore they are equal in M.□

Properties of commutative rings

We recall a few results already established regarding the local character of a few interesting properties for commutative rings, in the sense of the localization at comaximal monoids.

2.3. Concrete local-global principle. (Concrete patching of properties of commutative rings) *Let S_1, …, S_n be comaximal monoids and $\mathfrak{a}$ be an ideal of $\mathbf{A}$. Then we have the following equivalences.*

1. *$\mathbf{A}$ is coherent if and only if each $\mathbf{A}_{S_i}$ is coherent.*
2. *$\mathbf{A}$ is a pf-ring if and only if each $\mathbf{A}_{S_i}$ is a pf-ring.*
3. *$\mathbf{A}$ is a pp-ring if and only if each $\mathbf{A}_{S_i}$ is a pp-ring.*
4. *$\mathbf{A}$ is reduced if and only if each $\mathbf{A}_{S_i}$ is reduced.*
5. *The ideal $\mathfrak{a}$ is locally principal if and only if each $\mathfrak{a}_{S_i}$ is locally principal.*
6. *$\mathbf{A}$ is arithmetic if and only if each $\mathbf{A}_{S_i}$ is arithmetic.*
7. *$\mathbf{A}$ is a Prüfer ring if and only if each $\mathbf{A}_{S_i}$ is a Prüfer ring.*
8. *The ideal $\mathfrak{a}$ is integrally closed if and only if each $\mathfrak{a}_{S_i}$ is integrally closed.*
9. *$\mathbf{A}$ is normal if and only if each $\mathbf{A}_{S_i}$ is normal.*
10. *$\mathbf{A}$ is of Krull dimension $\leqslant k$ if and only if each $\mathbf{A}_{S_i}$ is of Krull dimension $\leqslant k$.*
11. *$\mathbf{A}$ is Noetherian if and only if each $\mathbf{A}_{S_i}$ is Noetherian.*

Moreover recall that for localizations at comaximal elements, the concrete local-global principle also applies for the notions of a Dedekind ring and of a strongly discrete Noetherian coherent ring (local-global principle XII-7.14).

Concrete local-global principles for algebras

Localization at the source

2.4. Concrete local-global principle. *Let S_1, …, S_n be comaximal monoids of a ring $\mathbf{k}$ and $\mathbf{A}$ be a $\mathbf{k}$-algebra. Then the following properties are equivalent.*

1. *$\mathbf{A}$ is finitely generated (resp. flat, faithfully flat, finitely presented, finite, integral, strictly finite, separable, strictly étale) over $\mathbf{k}$.*
2. *Each of the algebras $\mathbf{A}_{S_i}$ is finitely generated (resp. flat, faithfully flat, finitely presented, finite, integral, strictly finite, separable, strictly étale) over $\mathbf{k}_{S_i}$.*

Similarly if $\mathbf{A}$ *is strictly finite and if* $\lambda \in \mathbf{A}^\star$*, then* λ *is dualizing if and only if each of the forms* λ_{S_i} *is dualizing.*

D *1* ⇔ *2.* We introduce the faithfully flat $\mathbf{k}$-algebra $\prod_i \mathbf{k}_{S_i}$. It then suffices to apply Theorem VIII-6.8.

The question of the dualizing form (when $\mathbf{A}$ is strictly finite) is a question of isomorphism of modules and stems from the concrete local-global principles for modules (by taking into account Fact VI-6.11). □

Localization at the sink

There are also the local-global principles that correspond to properties said to be "local in $\mathbf{A}$." Here we need localizations at comaximal elements (comaximal monoids are not sufficient).

2.5. Concrete local-global principle.
Let $\mathbf{A}$ *be a* $\mathbf{k}$*-algebra and* s_1*, …,* s_m *be comaximal elements of* $\mathbf{A}$*. Then the following properties are equivalent.*

1. $\mathbf{A}$ *is finitely generated (resp. finitely presented, flat) over* $\mathbf{k}$*.*
2. *Each of the algebras* $\mathbf{A}_{s_i}$ *is finitely generated (resp. finitely presented, flat) over* $\mathbf{k}$*.*

D First of all if $\mathbf{A} = \mathbf{k}[x_1,\dots,x_n] = \mathbf{k}[X_1,\dots,X_n]/\mathfrak{a}$ and $s = S(\underline{x})$ (where $S \in \mathbf{k}[\underline{X}]$), then $\mathbf{A}_s = \mathbf{k}[x_1,\dots,x_n,t]$ with $t = 1/s$ in $\mathbf{A}_s$, which also gives

$$\mathbf{A}_s = \mathbf{k}[X_1,\dots,X_n,T]/(\mathfrak{a} + \langle TS(\underline{X}) - 1\rangle)\ .$$

Thus the property of being finitely generated or finitely presented is stable by localization at an element (but it is not stable for a localization at an arbitrary monoid).
Regarding the flatness, as $\mathbf{A}_s$ is flat over $\mathbf{A}$, if $\mathbf{A}$ is flat over $\mathbf{k}$, $\mathbf{A}_s$ is flat over $\mathbf{k}$ (Fact VIII-6.4).

Now suppose that $\sum_i s_i u_i = 1$ in $\mathbf{A}$.
First of all let us see what we obtain if each of the $\mathbf{k}$-algebras $\mathbf{A}_{s_i}$ is finitely generated. We can suppose that the generators are derived from elements of $\mathbf{A}$ (by considering the corresponding fraction of denominator 1). Let us make a single list $(x_1,\dots,x_n)$ with all these elements of $\mathbf{A}$. The reader will then observe by a small computation that $\mathbf{A}$ is generated by

$$(x_1,\dots,x_n,s_1,\dots,s_m,u_1,\dots,u_m) = (y_1,\dots,y_p),\ \text{with } p = n + 2m.$$

Now let us consider the case where all the algebras $\mathbf{A}_{s_i}$ are finitely presented. We consider some indeterminates Y_i corresponding to the list $(y_1,\dots,y_p)$ defined above. We write $s_i = S_i(\underline{x})$, $u_i = U_i(\underline{x})$ (polynomials in $\mathbf{k}[\underline{x}]$).
For the common generator set $(x_1,\dots,x_n)$ that we have just considered, and for each $i \in [\![1..m]\!]$, we have a corresponding polynomial system, say

F_i, in $\mathbf{k}[\underline{X}, Y_{n+i}, T_i]$, which allows us to define the isomorphism

$$\mathbf{k}[\underline{X}, Y_{n+i}, T_i]/\mathfrak{a}_i \to \mathbf{A}_{s_i},$$

with $\mathfrak{a}_i = \langle F_i, Y_{n+i} - S_i(\underline{X}), Y_{n+i}T_i - 1\rangle$. For each $f \in F_i$ there is an exponent k_f such that $s_i^{k_f} f(\underline{x}) = 0$ in $\mathbf{A}$. We can take all the k_f's equal, say, to k.

We then consider the following polynomial system in $\mathbf{k}[Y_1, \ldots, Y_p]$, with $Y_j = X_j$ for $j \in [\![1..n]\!]$. First of all we take all the $Y_{n+i}^k f(\underline{X})$'s for $f \in F_i$ and $i \in [\![1..m]\!]$.

Next we write the relations $Y_{n+i} - S_i(\underline{X})$'s and $Y_{n+m+i} - U_i(\underline{X})$'s for the indices $i \in [\![1..m]\!]$. Finally, we take the relation that corresponds to $\sum_i u_i s_i = 1$, i.e. $\sum_{i=1}^m Y_{n+i}Y_{n+m+i} - 1$.

The readers will do the computation to convince themselves that we indeed have a faultless description of the $\mathbf{k}$-algebra $\mathbf{A}$. The contrary would have been surprising, even immoral, since we have transcribed all that we could have known about the situation. The key was that this could have been expressed by a finite system of relations over a finite system of indeterminates. Actually we proceeded exactly as in the proof of the local-global principle IV-4.13 for the finitely presented modules.

Regarding the flatness, consider $(a_1, \ldots, a_n)$ in $\mathbf{k}$ and $(x_1, \ldots, x_n)$ in $\mathbf{A}$ such that $\sum_i x_i a_i = 0$. We want to show that $(x_1, \ldots, x_n)$ is an $\mathbf{A}$-linear combination of linear dependence relations in $\mathbf{k}$. We know that this is true after localization at each of the s_k's. We therefore have an exponent N such that for each k we have an equality

$$s_k^N(x_1, \ldots, x_n) = \sum_{j=1}^{p_j} b_{k,j}(x_{1,k,j}, \ldots, x_{n,k,j}),$$

$(x_{i,k,j} \in \mathbf{k}$, $b_{k,j} \in \mathbf{A})$ with $\sum_i x_{i,k,j} a_i = 0$. We finish by taking an $\mathbf{A}$-linear combination of the s_k^N's equal to 1. □

3. A few abstract local-global principles

An essential tool in classical algebra is the localization at (the complement of) a prime ideal. This tool is a priori difficult to use constructively because we do not know how to construct the prime ideals which intervene in the classical proofs, and whose existence relies on the axiom of choice. However, we observe that those prime ideals are generally used in proofs by contradiction, and this gives an explanation of the fact that the use of these "ideal" objects can be avoided and even interpreted constructively (see Section 5).

The abstract local-global principle in commutative algebra is an informal principle according to which certain properties regarding modules over commutative rings are true if and only if they are true after localization at any prime ideal.

We now recall a few cases where the abstract local-global principle applies in classical mathematics, by explaining the link with the corresponding concrete principles.

An abstract version of the concrete local-global principle 2.1 is the following.

3.1. Abstract local-global principle*. *Let φ, ψ be linear maps $M \to N$, θ be a linear map $N \to P$, and x, y be elements of N. Then we have the following equivalences.*

1. *Abstract patching of the equalities*
$$x = y \quad \text{in} \quad N \quad \iff \quad \forall \mathfrak{p} \in \mathsf{Spec}\,\mathbf{A} \;\; x/1 = y/1 \quad \text{in} \quad N_\mathfrak{p}.$$
2. *Abstract patching of the equalities of linear maps*
$$\varphi = \psi \quad \text{in} \quad \mathrm{L}_\mathbf{A}(M, N) \qquad \iff$$
$$\forall \mathfrak{p} \in \mathsf{Spec}\,\mathbf{A} \;\; \varphi/1 = \psi/1 \quad \text{in} \quad \mathrm{L}_{\mathbf{A}_\mathfrak{p}}(M_\mathfrak{p}, N_\mathfrak{p}).$$
3. *Abstract patching of the regular elements*
$$x \textit{ is regular in } N \qquad \iff$$
$$\forall \mathfrak{p} \in \mathsf{Spec}\,\mathbf{A} \quad x/1 \;\; \textit{is regular in } N_\mathfrak{p}.$$
4. *Abstract patching of the solutions of systems of linear equations*
$$x \in \operatorname{Im}\varphi \quad \iff \quad \forall \mathfrak{p} \in \mathsf{Spec}\,\mathbf{A} \;\; x/1 \in \operatorname{Im}\varphi_\mathfrak{p}.$$
5. *Abstract patching of the solutions of systems of linear equations under homogeneous conditions. Let (Φ_ℓ) be a finite family of homogeneous maps*
$$\Phi_\ell : \mathrm{L}_\mathbf{A}(M,N) \times N \to Q_\ell, \textit{ or } \Phi_\ell : \mathrm{L}_\mathbf{A}(M,N) \to Q_\ell, \textit{ or } \Phi_\ell : N \to Q_\ell.$$
Then
$$\big((\&_\ell\ \Phi_\ell(\varphi, y) = 0\big) \;\Rightarrow\; y \in \operatorname{Im}\varphi\big) \qquad \iff$$
$$\forall \mathfrak{p} \in \mathsf{Spec}\,\mathbf{A} \;\; \big((\&_\ell\ \Phi_\ell(\varphi, y) =_{Q_{\ell,\mathfrak{p}}} 0\big) \;\Rightarrow\; y/1 \in \operatorname{Im}\varphi_\mathfrak{p}\big),$$
where we have written $Q_{\ell,\mathfrak{p}}$ for $(Q_\ell)_\mathfrak{p}$.
6. *Abstract patching of the exact sequences. The sequence*
$$M \xrightarrow{\varphi} N \xrightarrow{\theta} P$$
is exact if and only if the sequence
$$M_\mathfrak{p} \xrightarrow{\varphi_\mathfrak{p}} N_\mathfrak{p} \xrightarrow{\theta_\mathfrak{p}} P_\mathfrak{p}$$
is exact for every $\mathfrak{p} \in \mathsf{Spec}\,\mathbf{A}$.
7. *Abstract patching of direct summands in finitely presented modules. Here M is a finitely generated submodule of a finitely presented module N.*
$$M \textit{ is a direct summand in } N \iff$$
$$\forall \mathfrak{p} \in \mathsf{Spec}\,\mathbf{A} \; M_\mathfrak{p} \textit{ is a direct summand in } N_\mathfrak{p}.$$

Proofs (nonconstructive). The conditions are necessary because of Fact II-6.4. A direct verification is actually immediate. For the converses, we assume without loss of generality that the ring $\mathbf{A}$ is nontrivial. It suffices to treat item *4* (see the remark on page 852). Actually we have already established item *6*, which implies item *4*, in the abstract local-global principle II-6.8 (page 63), but we think that it is usefull to give two distinct classical proofs (the second is the one given in Chapter II) and to compare their degree of effectivity.

First proof.
Suppose $x \notin \operatorname{Im}\varphi$, it amounts to the same as saying that $x \neq 0$ in $N/\varphi(M)$. Since for a prime ideal $\mathfrak{p}$ we have $\big(N/\varphi(M)\big)_\mathfrak{p} \simeq N_\mathfrak{p}/\varphi_\mathfrak{p}(M_\mathfrak{p})$, it suffices to prove item *1* with $y = 0$. We reason by contradiction by assuming $x \neq 0$ in N. In other words $\operatorname{Ann}_\mathbf{A}(x) \neq \langle 1 \rangle$, and there exists a $\mathfrak{p} \in \operatorname{\mathsf{Spec}} \mathbf{A}$ which contains $\operatorname{Ann}_\mathbf{A}(x)$. Then, since $\big(\operatorname{Ann}_\mathbf{A}(x)\big)_\mathfrak{p} = \operatorname{Ann}_{\mathbf{A}_\mathfrak{p}}(x/1)$, we obtain $x \neq_{N_\mathfrak{p}} 0$.

Second proof.
The property $x \in \operatorname{Im}\varphi$ is of finite character. We can therefore apply Fact* II-2.12 which says (in classical mathematics) that for a finite character property, the concrete local-global principle (localization at comaximal monoids) is equivalent to the abstract local-global principle (localization at all the maximal ideals). □

Comments.
1) It seems impossible that the second proof, which is too general, can ever be made into a constructive proof. The first proof is not "generally" constructive either, but there exist some cases where it is. For this it suffices to satisfy the following conditions, in the case of item *4*.

- The module N is finitely presented and the module M is finitely generated.
- The ring $\mathbf{A}$ is coherent and strongly discrete.
- For every strict finitely generated ideal $\mathfrak{a}$ of $\mathbf{A}$ we know how to construct a prime ideal $\mathfrak{p}$ containing $\mathfrak{a}$.

The last two conditions are satisfied when $\mathbf{A}$ is a finitely presented algebra over $\mathbb{Z}$ or over a "fully factorial" field (see [MRR]).

2) This allows us, for example, to give another constructive proof of the explicit matrix form theorem (Theorem X-1.7). As mentioned on page 543, it suffices to treat the generic case and to show certain equalities $r_i r_j = 0$ and $r_h u = 0$. As the ring $\mathbf{G}_n$ is a finitely presented algebra over $\mathbb{Z}$, we can show these equalities by applying the abstract patching of the equalities. We are therefore brought back to the case of a local ring obtained as a

localization of $\mathbf{G}_n$, and in this case the equalities are true since the module is free by applying the local freeness lemma.

3) In practice, we can understand the abstract local-global principle 3.1 in the following intuitive form: to prove a theorem of commutative algebra whose meaning is that a certain system of linear equations over a commutative ring $\mathbf{A}$ admits a solution, it suffices to treat the case where the ring is local. It is a principle of the same type as the Lefschetz principle: to prove a theorem of commutative algebra whose meaning is that a certain algebraic identity takes place, it suffices to treat the case where the ring is the complex number field (or any subring that suits us best, in fact). This remark is developed in Section 5.

4) In the article [10], Hyman Bass makes the following comment regarding a Noetherian version of the abstract local-global principle 3.1, item *7*.
The latter result, elementary as it is, seems to defy any proof which does not either use, or essentially reconstruct, the functor Ext^1.
This comment is surprising, in view of the perfectly trivial character of our proof of the corresponding concrete principle, which computes nothing that resembles an Ext^1. Actually, when the goal is to show that a short exact sequence splits, it seems that the efficient computational machinery of the Ext's is often useless, and that it can be short-circuited by a more elementary argument.

5) The abstract local-global principle above also works by uniquely using the localization at any maximal ideal, as seen in the abstract local-global principle II-6.8 (page 63). But this is not really useful because the localizations at the maximal ideals are the least extensive (among the localizations at the prime ideals). However, there are cases where the classical reasoning uniquely uses localizations at minimal prime ideals. They are more subtle proofs that are more difficult to decrypt constructively. We will elaborate on this in Section 7.

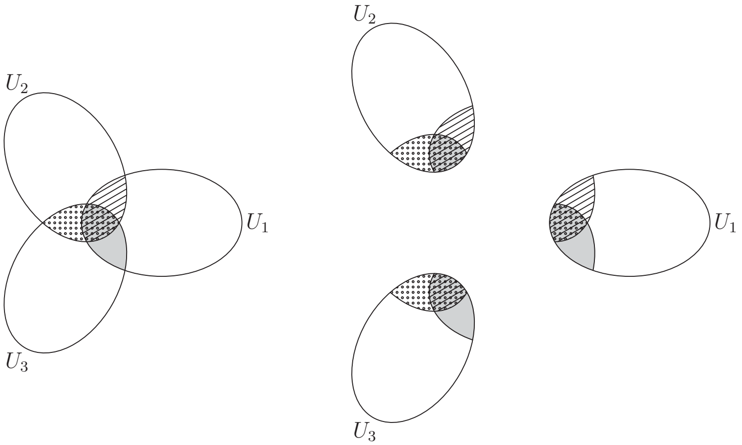
6) As mentioned on page 33, the abstract local-global principle for finitely generated modules does not work: just because a module is finitely generated after localization at every prime ideal does not mean it is necessarily finitely generated. The same would hold for the concrete patching principle of finitely presented modules or for that of coherent modules. This denotes a certain superiority of the concrete local-global principles over the abstract local-global principles. ■

4. Concrete patching of objects

Glue and scissors

Here we give a brief discussion regarding patching methods in differential geometry and their translations in commutative algebra.

First of all we examine the possibility of constructing a smooth manifold from local charts, i.e. by a patching of open sets U_i of $\mathbb{R}^n$ by means of diffeomorphisms (or isomorphisms) $\varphi_{ij} : U_{ij} \to U_{ji}$: U_{ij} is an open set of U_i and $\varphi_{ji} = \varphi_{ij}^{-1}$.



We will consider the simple case where the variety is obtained by only patching a finite number of open sets of $\mathbb{R}^n$.

In this case the condition to fulfil is that the morphisms of patchings must be *compatible between them three by three.* This precisely means the following. For each triple of distinct indices (i, j, k) we consider the open set $U_{ijk} = U_{ij} \cap U_{ik}$ (therefore with $U_{ijk} = U_{ikj}$). The compatibility means on the one hand that, for each (i, j, k), the restriction $\varphi_{ij}|_{U_{ijk}}$ establishes an isomorphism from U_{ijk} to U_{jik}, and on the other hand that if we compose the isomorphisms

$$U_{ijk} \xrightarrow{\varphi_{ij}|_{U_{ijk}}} U_{jik} \quad \text{and} \quad U_{jki} \xrightarrow{\varphi_{jk}|_{U_{jki}}} U_{kji}$$

we obtain the isomorphism $U_{ijk} \xrightarrow{\varphi_{ik}|_{U_{ijk}}} U_{kij}$: $\varphi_{ik}|_\bullet = \varphi_{jk}|_\bullet \circ \varphi_{ij}|_\bullet$.

If we try to do the same thing in commutative algebra, we will consider some rings $\mathbf{A}_i$ (corresponding to the rings $C^\infty(U_i)$) and some elements $f_{ij} \in \mathbf{A}_i$. The ring $C^\infty(U_{ij})$ would correspond to $\mathbf{A}_i[1/f_{ij}]$ and the patching morphism φ_{ij} to an isomorphism $\omega_{ij} : \mathbf{A}_i[1/f_{ij}] \to \mathbf{A}_j[1/f_{ji}]$. We will also have to formulate some three-by-three compatibility conditions. We then hope to construct a ring $\mathbf{A}$ and some elements $f_i \in \mathbf{A}$, such that $\mathbf{A}_i$ could be identified with $\mathbf{A}[1/f_i]$, f_{ij} with "f_j seen in $\mathbf{A}[1/f_i]$," and ω_{ij} with the identity between $\mathbf{A}[1/f_i][1/f_j]$ and $\mathbf{A}[1/f_j][1/f_i]$.

Unfortunately, this does not always work well. The ring $\mathbf{A}$ that is supposed to patch the $\mathbf{A}_i$'s does not always exist (however, if it exists it is well-determined, up to unique isomorphism).

The first example of this obvious failure of the patching is in projective space. The complex projective space $\mathbb{P}^n(\mathbb{C})$ is obtained by patching affine charts $\mathbb{C}^n$, but the corresponding rings of functions, isomorphic to $\mathbb{C}[X_1, \dots, X_n]$, do not patch together: there are no polynomial functions defined over $\mathbb{P}^n(\mathbb{C})$, besides the constants, and by localizing the ring $\mathbb{C}$ there is no chance of obtaining the ring $\mathbb{C}[X_1, \dots, X_n]$.

This illustrates the fact that algebraic geometry is much more rigid than C^∞ geometry.

This unpleasant phenomenon is at the origin of the creation of Grothendieck's schemes, which are the abstract objects formally obtained by patching rings along patching morphisms when the three-by-three compatibility conditions are satisfied, but whose patching no ring wants to perform.

Let us now consider the question of the patching of vector bundles when they are locally defined over a fixed smooth variety U, covered by a finite number of open sets U_i. Let $U_{ij} = U_i \cap U_j$. The vector bundle $\pi : W \to U$ that we want to construct, whose every fiber is isomorphic to a given vector space F, is known a priori only by its restrictions $\pi_i : W_i \to U_i$. In order to patch, we need patching diffeomorphisms $\psi_{ij} : W_{ij} \to W_{ji}$

where $W_{ij} = \pi_i^{-1}(U_{ij})$. These morphisms must first of all respect the structure of the vector space fiber by fiber. In addition, again, we need three-by-three compatibility conditions, analogous to those which we have defined in the first case.

Now if we pass to the analogous case in commutative algebra, we must start from a ring $\mathbf{A}$ with a system of comaximal elements $(f_1, \dots, f_\ell)$. Let $\mathbf{A}_i = \mathbf{A}[1/f_i]$ and $\mathbf{A}_{ij} = \mathbf{A}[1/f_i f_j]$. For each index i, we give the "module of the sections of the fiber $\pi_i : W_i \to U_i$," i.e. an $\mathbf{A}_i$-module M_i. The ψ_{ij}'s are now represented by isomorphisms of $\mathbf{A}_{ij}$-modules

$$\mathbf{A}_{ij} \otimes_{\mathbf{A}_i} M_i \xrightarrow{\theta_{ij}} \mathbf{A}_{ji} \otimes_{\mathbf{A}_j} M_j \xrightarrow{\sim} M_{ij} = M_{ji}.$$

We will see in the following subsections that this time everything goes well: if the three-by-three compatibility conditions are satisfied, we indeed have an $\mathbf{A}$-module M that "patches" the $\mathbf{A}_i$-modules M_i.

A simple case

4.1. Theorem. *Let* $\mathbf{A}$ *be an integral ring with quotient field* $\mathbf{K}$*,* N *be a torsion-free* $\mathbf{A}$*-module,* $S_1, \ldots, S_n$ *be comaximal monoids of* $\mathbf{A}$ *and for each* $i \in [\![1..n]\!]$ *let* M_i *be* $\mathbf{A}_{S_i}$*-submodule of* $S_i^{-1}N \subseteq \mathbf{K} \otimes_{\mathbf{A}} N$*. Suppose that for each* $i, j \in [\![1..n]\!]$ *we have* $S_j^{-1}M_i = S_i^{-1}M_j$ *(seen as* $\mathbf{A}$*-submodules of* $\mathbf{K} \otimes_{\mathbf{A}} N$*). Then we have the following results.*

1. *There exists a unique* $\mathbf{A}$*-submodule* M *of* N *such that we have* $S_i^{-1}M = M_i$ *for each* $i \in [\![1..n]\!]$*.*
2. *This submodule* M *is equal to the intersection of the* M_i*'s.*
3. *If the* M_i*'s are finitely generated (resp. finitely presented, coherent, finitely generated projective), the same goes for* M*.*

D *1* and *2*. Let $P = \bigcap_i M_i$. First of all $P \subseteq N$ because one element of the intersection is of the form

$$\frac{x_1}{s_1} = \cdots = \frac{x_n}{s_n} = \frac{\sum_i a_i x_i}{\sum_i a_i s_i} = \sum\nolimits_i a_i x_i \quad \text{if} \quad \sum\nolimits_i a_i s_i = 1 \ \text{ in } \mathbf{A}$$

(with $x_i \in N$, $s_i \in S_i$ for $i \in [\![1..n]\!]$).
Let us show that the module P satisfies the required conditions.
First of all $P \subseteq M_i$ so $S_i^{-1}P \subseteq M_i$ for each i. Conversely, let $x_1 \in M_1$ for example, we want to see that x_1 is in $S_1^{-1}P$.
Since $S_j^{-1}M_1 = S_1^{-1}M_j$, there exists a $u_{1,j} \in S_1$ such that $u_{1,j}x_1 \in M_j$. By letting $s_1 = \prod_{j \neq 1} u_{1,j}$, we indeed obtain $s_1 x_1 \in \bigcap_i M_i$.
Now let us prove the uniqueness.
Let Q be a module satisfying the required conditions. We have $Q \subseteq S_i^{-1}Q = M_i$ and thus $Q \subseteq P$. Then consider the sequence $Q \to P \to 0$. Since it is exact after localization at comaximal monoids, it is exact (local-global principle II-6.7), i.e. the inclusion homomorphism is surjective, so $Q = P$.

Finally, item *3* results from already established concrete local-global principles. □

If we do not assume that the ring is integral and the module is torsion-free, the previous theorem is a little more delicate. This will be the object of the local-global principle 4.4.

Patching of objects in modules

Let $\mathbf{A}$ be a commutative ring, $(S_i)_{i \in [\![1..n]\!]}$ be comaximal monoids of $\mathbf{A}$. Let $\mathbf{A}_i := \mathbf{A}_{S_i}$ and $\mathbf{A}_{ij} := \mathbf{A}_{S_i S_j}$ $(i \neq j)$ such that $\mathbf{A}_{ij} = \mathbf{A}_{ji}$. Let $\alpha_i : \mathbf{A} \to \mathbf{A}_i$ and $\alpha_{ij} : \mathbf{A}_i \to \mathbf{A}_{ij}$ be natural homomorphisms.

In the remainder, notations like $(M_{ij})_{i<j \in [\![1..n]\!]}$ and $(\varphi_{ij})_{i \neq j \in [\![1..n]\!]})$ mean that we have $M_{ij} = M_{ji}$ but (a priori) not $\varphi_{ij} = \varphi_{ji}$.

4.2. Concrete local-global principle. (Concrete patching of elements in a module, and of homomorphisms between modules)

1. *Let $(x_i)_{i\in[\![1..n]\!]}$ be an element of $\prod_{i\in[\![1..n]\!]}\mathbf{A}_i$. So that there exists some $x \in \mathbf{A}$ satisfying $\alpha_i(x) = x_i$ in each $\mathbf{A}_i$, it is sufficient and necessary for each $i < j$ we have $\alpha_{ij}(x_i) = \alpha_{ji}(x_j)$ in $\mathbf{A}_{ij}$. In addition, this x is then uniquely determined. In other terms the ring $\mathbf{A}$ (with the homomorphisms α_i) is the limit of the diagram*
$$\big((\mathbf{A}_i)_{i\in[\![1..n]\!]},(\mathbf{A}_{ij})_{i<j\in[\![1..n]\!]};(\alpha_{ij})_{i\neq j\in[\![1..n]\!]}\big)$$
$$\begin{tikzcd}
 & & \mathbf{A}_i \arrow[r, "\alpha_{ij}"] \arrow[ddr, "\alpha_{ik}"] & \mathbf{A}_{ij} \\
\mathbf{C} \arrow[r, dashed, "\psi!"'] \arrow[urr, "\psi_i"] \arrow[drr, "\psi_j"'] \arrow[ddrr, "\psi_k"'] & \mathbf{A} \arrow[ur, "\alpha_i"] \arrow[dr, "\alpha_j"] \arrow[ddr, "\alpha_k"'] & & \\
 & & \mathbf{A}_j \arrow[uur, "\alpha_{ji}"] \arrow[dr] & \mathbf{A}_{ik} \\
 & & \mathbf{A}_k \arrow[ur] \arrow[r, "\alpha_{kj}"'] & \mathbf{A}_{jk}
\end{tikzcd}$$

2. *Let M be an $\mathbf{A}$-module. Let $M_i := M_{S_i}$ and $M_{ij} := M_{S_iS_j}$ $(i \neq j)$ such that $M_{ij} = M_{ji}$. Let $\varphi_i : M \to M_i$ and $\varphi_{ij} : M_i \to M_{ij}$ be the natural linear maps. Then the $\mathbf{A}$-module M (with the linear maps $\varphi_i : M \to M_i$) is the limit of the diagram*
$$\big((M_i)_{i\in[\![1..n]\!]},(M_{ij})_{i<j\in[\![1..n]\!]};(\varphi_{ij})_{i\neq j\in[\![1..n]\!]}\big).$$

3. *Let N be another module, let $N_i := N_{S_i}$, $N_{ij} := N_{S_iS_j}$. For each $i \in [\![1..n]\!]$ let $\psi_i : M_i \to N_i$ be an $\mathbf{A}_i$-linear map. So that there exists an $\mathbf{A}$-linear map $\psi : M \to N$ satisfying $\psi_{S_i} = \psi_i$ for each i, it is sufficient and necessary, for each $i < j$, for the two linear maps $(S_j)^{-1}\psi_i$ and $(S_i)^{-1}\psi_j$ from M_{ij} to N_{ij} to be equal. In addition, the linear map ψ is then uniquely determined.*
$$\begin{tikzcd}
 & M_i \arrow[rrr, "\psi_i"] \arrow[ddr, "\varphi_{ij}"] & & & N_i \arrow[ddr, "\phi_{ij}"] & \\
M \arrow[ur, "\varphi_i"] \arrow[ddr, "\varphi_j"'] \arrow[rrr, dashed, "\psi!"] & & & N \arrow[ur, "\phi_i"] \arrow[ddr, "\phi_j"] & & \\
 & & M_{ij} \arrow[rrr, dashed] & & & N_{ij} \\
 & M_j \arrow[ur, "\varphi_{ji}"] \arrow[rrr, "\psi_j"] & & & N_j \arrow[ur, "\phi_{ji}"] &
\end{tikzcd}$$
In other terms the $\mathbf{A}$-module $\mathrm{L}_{\mathbf{A}}(M,N)$ is the limit of the diagram formed by the $\mathrm{L}_{\mathbf{A}_i}(M_i,N_i)$'s, the $\mathrm{L}_{\mathbf{A}_{ij}}(M_{ij},N_{ij})$'s and the natural linear maps.

D *1.* Special case of *2.*

2. Let $(x_i)_{i\in[\![1..n]\!]}$ be an element of $\prod_{i\in[\![1..n]\!]} M_i$. We need to show that for some $x \in M$ satisfying $\varphi_i(x) = x_i$ in each M_i to exist, it is sufficient and necessary that for each $i < j$ we have $\varphi_{ij}(x_i) = \varphi_{ji}(x_j)$ in M_{ij}. In addition, this x must be unique.

The condition is clearly necessary. Let us show that it is sufficient.

Let us show the existence of x. There exist s_i's in S_i and y_i's in M such that we have $x_i = y_i/s_i$ in each M_i. If $\mathbf{A}$ is integral, M torsion-free and each $s_i \neq 0$, we have in the module obtained by scalar extension to the quotient field

$$\frac{y_1}{s_1} = \frac{y_2}{s_2} = \cdots = \frac{y_n}{s_n} = \frac{\sum_i a_i y_i}{\sum_i a_i s_i} = \sum_i a_i y_i = x \in M,$$

with $\sum_i a_i s_i = 1$. In the general case we do just about the same thing. For each pair (i, j) with $i \neq j$, the fact that $x_i/1 = x_j/1$ in M_{ij} means that for certain $u_{ij} \in S_i$ and $u_{ji} \in S_j$ we have $s_j u_{ij} u_{ji} y_i = s_i u_{ij} u_{ji} y_j$. Let $u_i = \prod_{k\neq i} u_{ik} \in S_i$. We have $s_j u_i u_j y_i = s_i u_i u_j y_j$. Let (a_i) be elements of $\mathbf{A}$ such that $\sum_i a_i s_i u_i = 1$. Let $x = \sum a_i u_i y_i$. We need to show that $x/1 = x_i$ in M_i for each i. For example for $i = 1$, we write the following equalities in M

$$\begin{aligned} s_1 u_1 x \;&=\; s_1 u_1 \textstyle\sum_i a_i u_i y_i \;=\; \sum_i a_i s_1 u_1 u_i y_i \\ &=\; \textstyle\sum_i a_i s_i u_1 u_i y_1 \;=\; \big(\sum_i a_i s_i u_i\big) u_1 y_1 \;=\; u_1 y_1. \end{aligned}$$

Thus $s_1 u_1 x = u_1 y_1$ in M and $x = y_1/s_1$ in M_{S_1}.

Finally, the uniqueness of x results from the concrete patching principle of equalities.

3. The composites of the linear maps $M \to M_i \to N_i$ are compatible with the natural linear maps $N_i \to N_{ij}$. We conclude with the fact that N is the limit of the diagram of the N_i's and N_{ij}'s (item *2*). □

A delicate point (regarding item *3*). If M is a finitely presented $\mathbf{A}$-module or if $\mathbf{A}$ is integral and M finitely generated, the natural $\mathbf{A}_i$-linear maps $\mathrm{L}_{\mathbf{A}}(M, N)_{s_i} \to \mathrm{L}_{\mathbf{A}_i}(M_i, N_i)$ are isomorphisms (see Propositions V-9.3 and VIII-5.7).

In the general case, the notation ψ_{s_i} is made ambiguous because it can either represent an element of $\mathrm{L}_{\mathbf{A}_i}(M_i, N_i)$ or an element of $\mathrm{L}_{\mathbf{A}}(M, N)_{s_i}$, and the natural linear map $\mathrm{L}_{\mathbf{A}}(M, N)_{s_i} \to \mathrm{L}_{\mathbf{A}_i}(M_i, N_i)$ is a priori only injective if M is finitely generated. This ambiguity can be a source or error. Especially as $\mathrm{L}_{\mathbf{A}}(M, N)$ then appears as a limit of two essentially distinct diagrams: the one based on the $\mathrm{L}_{\mathbf{A}_i}(M_i, N_i)$'s (the most interesting of the two) and the one based on the $\mathrm{L}_{\mathbf{A}}(M, N)_{s_i}$'s. ■

An example of a patching of elements. Given that the determinants of endomorphisms of free modules are well-behaved under localization, given the theorem that affirms that the finitely generated projective modules are locally free (in the strong sense) and given the previous concrete local-global principle, we obtain the possibility of *defining* the determinant of an endomorphism of a finitely generated projective module by only using determinants of endomorphisms between free modules, after suitable comaximal localizations. In other words the following fact can be established independently of the theory of determinants developed in Chapters V and X.

Fact. *For an endomorphism φ of a finitely generated projective $\mathbf{A}$-module M, there exists a unique element $\det\varphi$ satisfying the following property: if $s \in \mathbf{A}$ is such that the module M_s is free, then $(\det\varphi)_s = \det(\varphi_s)$ in $\mathbf{A}_s$.* ■

Patching of modules

The patching principle 4.4 that follows specifies which conditions are needed in order for the limit of an analogous system of modules to fall within the framework indicated in the local-global principle 4.2.

4.3. Definition. Let S be a monoid of $\mathbf{A}$, M be an $\mathbf{A}$-module and N be an $\mathbf{A}_S$-module. An $\mathbf{A}$-linear map $\alpha : M \to N$ is called a *localization morphism at S* if it is a morphism of scalar extension from $\mathbf{A}$ to $\mathbf{A}_S$ for M (see page 196).

In other words, if $\alpha : M \to N$ is a localization morphism at S, and if $\beta_{M,S} : M \to M_S$ is the natural linear map, the unique $\mathbf{A}$-linear map $\varphi : M_S \to N$ such that $\varphi \circ \beta_{M,S} = \alpha$ is an isomorphism. A localization morphism at S can be characterized by the following conditions:

- $\forall x, x' \in M,\ \big(\alpha(x) = \alpha(x') \iff \exists s \in S,\ sx = sx'\big)$,
- $\forall y \in N,\ \exists x \in M,\ \exists s \in S,\ \ sy = \alpha(x)$.

4.4. Concrete local-global principle. (Concrete patching of modules) *Let S_1, …, S_n be comaximal monoids of $\mathbf{A}$.*
Let $\mathbf{A}_i = \mathbf{A}_{S_i}$, $\mathbf{A}_{ij} = \mathbf{A}_{S_iS_j}$ and $\mathbf{A}_{ijk} = \mathbf{A}_{S_iS_jS_k}$. We give in the category of $\mathbf{A}$-modules a commutative diagram $\mathfrak{D}$

$$\big((M_i)_{i\in I}, (M_{ij})_{i<j\in I}, (M_{ijk})_{i<j<k\in I}; (\varphi_{ij})_{i\neq j}, (\varphi_{ijk})_{i<j, i\neq k, j\neq k}\big)$$

as in the following figure.

$$\begin{tikzcd}
M_i \arrow[d, "\varphi_{ij}"'] \arrow[dr, "\varphi_{ik}"] & M_j \arrow[dl, "\varphi_{ji}"] \arrow[dr, "\varphi_{jk}"] & M_k \arrow[dl, "\varphi_{ki}"'] \arrow[d, "\varphi_{kj}"] \\
M_{ij} \arrow[dr, "\varphi_{ijk}"'] & M_{ik} \arrow[d, "\varphi_{ikj}"] & M_{jk} \arrow[dl, "\varphi_{jki}"] \\
& M_{ijk} &
\end{tikzcd}$$

Suppose that

- *For all i, j, k (with $i < j < k$), M_i is an $\mathbf{A}_i$-module, M_{ij} is an $\mathbf{A}_{ij}$-module and M_{ijk} is an $\mathbf{A}_{ijk}$-module. Recall that according to our notation conventions we let $M_{ji} = M_{ij}$, $M_{ijk} = M_{ikj} = \dots$*
- *For $i \neq j$, $\varphi_{ij} : M_i \to M_{ij}$ is a localization morphism at S_j (seen in $\mathbf{A}_i$).*
- *For $i \neq k$, $j \neq k$ and $i < j$, $\varphi_{ijk} : M_{ij} \to M_{ijk}$ is a localization morphism at S_k (seen in $\mathbf{A}_{ij}$).*

Then, by letting $\big(M, (\varphi_i)_{i\in[\![1..n]\!]}\big)$ be the limit of the diagram, each morphism $\varphi_i : M \to M_i$ is a localization morphism at S_i. In addition $\big(M, (\varphi_i)_{i\in[\![1..n]\!]}\big)$ is, up to unique isomorphism, the unique system that makes the diagram commutative and that makes each φ_i a localization morphism at S_i.

D The first item does not depend on the fact that the S_i's are comaximal. Indeed the construction of a limit of $\mathbf{A}$-modules for an arbitrary diagram is stable by flat scalar extension (because this is the kernel of a linear map between two products).

However, if we take as a scalar extension the localization morphism $\mathbf{A} \to \mathbf{A}_i$, the diagram can be simplified as follows

$$\begin{tikzcd}
M_i \arrow[d, "\varphi_{ij}"'] \arrow[dr, "\varphi_{ik}"] & \\
M_{ij} \arrow[dr, "\varphi_{ijk}"'] & M_{ik} \arrow[d, "\varphi_{ikj}"] \\
& M_{ijk}
\end{tikzcd}$$

and it trivially admits the limit M_i.

To prove the uniqueness, we reason without loss of generality with a system of comaximal elements $(s_1, \dots, s_n)$. Let $\big(N, (\psi_i)\big)$ be a competitor. Since M is the limit of the diagram, there is a unique $\mathbf{A}$-linear map $\lambda : N \to M$ such that $\psi_i = \varphi_i \circ \lambda$ for every i. Actually we have $\lambda(v) = \big(\psi_1(v), \dots, \psi_n(v)\big)$. Let us show that λ is injective. If $\lambda(v) = 0$ all the $\psi_i(v)$'s are null, and since ψ_i is a localization morphism at s_i, there exist exponents m_i such that $s_i^{m_i} v = 0$. Since the s_i's are comaximal, we have $v = 0$. As λ is injective we can assume $N \subseteq M$ and $\psi_i = \varphi_i|_N$. Let us show that $N = M$. Let $x \in M$. As ψ_i and φ_i are two localization morphisms at s_i, there is an exponent m_i such that $x s_i^{m_i} \in N$. Since the s_i's are comaximal, $x \in N$. □

Remark. To understand why the comaximality condition is really necessary for the uniqueness, let us examine the following "overly simple" example. With the ring $\mathbb{Z}$, and the unique element $s = 2$, let us take for M a free $\mathbb{Z}[1/2]$-module with basis (a) (where a is an arbitrary individual object). For clarity, let M' be the $\mathbb{Z}$-module M.

Also consider the free $\mathbb{Z}$-module N with basis (a). Consider two localization morphisms at $2^{\mathbb{N}}$, $\varphi : M' \to M$ and $\psi : N \to M$. They both send a to a. Thus M' and N are not isomorphic as $\mathbb{Z}$-modules and the uniqueness does not hold. If we had taken $s = 1$ we could have defined two distinct localization morphisms at 1, namely $\phi_1 : N \to N,\ a \mapsto a$, and $\phi_2 : N \to N,\ a \mapsto -a$, and the uniqueness would be guaranteed in the sense required in the statement. ∎

In practice, we often construct a module by taking some $\mathbf{A}_i$-modules M_i and by patching them via their localizations $M_{ij} = M_i[1/s_j]$. In this case the modules M_{ij} and M_{ji} are distinct, and we must give for each (i, j) an isomorphism of $\mathbf{A}_{ij}$-modules $\theta_{ij} : M_{ij} \to M_{ji}$. This gives the following variant, in which the modules M_{ijk} are not given in the hypothesis, but where we indicate the compatibility conditions that the θ_{ij}'s need to satisfy.

Concrete local-global principle 4.4 bis (Concrete patching of modules)
Let S_1, …, S_n be comaximal monoids of $\mathbf{A}$.
Let $\mathbf{A}_i = \mathbf{A}_{S_i}$, $\mathbf{A}_{ij} = \mathbf{A}_{S_iS_j}$ and $\mathbf{A}_{ijk} = \mathbf{A}_{S_iS_jS_k}$.
Assume we are given some $\mathbf{A}_i$-modules M_i and let

$$M_{j\ell} = M_j[1/s_\ell] \text{ and } M_{jk\ell} = M_j[1/s_ks_\ell] \text{ for all distinct } j, k, \ell \in [\![1..n]\!],$$

such that $M_{jk\ell} = M_{j\ell k}$, with the localization morphisms

$$\varphi_{j\ell} : M_j \to M_{j\ell} \text{ and } \varphi_{j\ell k} : M_{j\ell} \to M_{j\ell k}.$$

Also assume we are given some morphisms of $\mathbf{A}_{ij}$-modules $\theta_{ij} : M_{ij} \to M_{ji}$. Let $\theta^k_{ij} : M_{ijk} \to M_{jik}$ be the morphism of $\mathbf{A}_{ijk}$-modules obtained by localization at s_k from θ_{ij}. Finally, we suppose that the following compatibility relations are satisfied

- *$\theta_{ji} \circ \theta_{ij} = \mathrm{Id}_{M_{ij}}$ for $i \neq j \in [\![1..n]\!]$,*
- *for distinct i, j, k in $[\![1..n]\!]$, by circularly composing*

$$M_{ijk} \xrightarrow{\theta^k_{ij}} M_{jik} = M_{jki} \xrightarrow{\theta^i_{jk}} M_{kji} = M_{kij} \xrightarrow{\theta^j_{ki}} M_{ikj}$$

  we must obtain the identity.

Then, if $\big(M, (\varphi_i)_{i\in[\![1..n]\!]}\big)$ is the limit of the diagram

$$\big((M_i)_{i\in[\![1..n]\!]}), (M_{ij})_{i\neq j\in[\![1..n]\!]}; (\varphi_{ij})_{i\neq j}, (\theta_{ij})_{i\neq j}\big),$$

each morphism $\varphi_i : M \to M_i$ is a localization morphism at S_i.
In addition, $\big(M, (\varphi_i)_{i\in[\![1..n]\!]}\big)$ is, up to unique isomorphism, the unique system that makes the diagram commutative and that makes each φ_i a

localization morphism at S_i.

$$\begin{tikzcd}
& M_i \arrow[dl, "\varphi_{ij}"'] \arrow[dr, "\varphi_{ik}"] & & M_j \arrow[dll, "\varphi_{ji}"'] \arrow[dr, "\varphi_{jk}"] & & M_k \arrow[dll, "\varphi_{ki}"'] \arrow[d, "\varphi_{kj}"] \\
M_{ij} \arrow[r, shift left, "\theta_{ij}"] \arrow[ddr, "\varphi_{ijk}"'] & M_{ji} \arrow[l, shift left, "\theta_{ji}"] \arrow[drr, "\varphi_{jik}"] & M_{ik} \arrow[r, shift left, "\theta_{ik}"] \arrow[ddl, "\varphi_{ikj}"'] & M_{ki} \arrow[l, shift left, "\theta_{ki}"] \arrow[ddr, "\varphi_{kij}"] & M_{jk} \arrow[r, shift left, "\theta_{jk}"] \arrow[dl, "\varphi_{jki}"'] & M_{kj} \arrow[l, shift left, "\theta_{kj}"] \arrow[ddl, "\varphi_{kji}"] \\
& & & M_{jik} \arrow[dr, dashed, "\theta^i_{jk}"] & & \\
& M_{ijk} \arrow[urr, dashed, "\theta^k_{ij}"] & & & M_{kij} \arrow[lll, dashed, "\theta^j_{ki}"] &
\end{tikzcd}$$

D Note that the diagram above is commutative by construction, except eventually the bottom triangle in dotted lines, each time that it is possible to join two modules using two different paths: for example $\varphi_{ij} \circ \varphi_{ijk} = \varphi_{ik} \circ \varphi_{ikj}$ and $\theta^k_{ij} \circ \varphi_{ijk} = \varphi_{jik} \circ \theta_{ij}$.

Here we need to convince ourselves that the indicated compatibility conditions are exactly what is necessary and sufficient to be brought back to the situation described in the local-global principle 4.4.

For this, when $i < j < k$ we only keep M_{ij}, M_{ik}, M_{jk} and $M_{ijk} = M_{ikj}$. This forces us to replace

$$\begin{array}{rclcrcl}
\varphi_{ji} & : & M_j \to M_{ji} & \text{with} & \gamma_{ji} = \theta_{ji} \circ \varphi_{ji} & : & M_j \to M_{ij}, \\
\varphi_{ki} & : & M_k \to M_{ki} & \text{with} & \gamma_{ki} = \theta_{ki} \circ \varphi_{ki} & : & M_k \to M_{ik}, \\
\varphi_{kj} & : & M_k \to M_{kj} & \text{with} & \gamma_{kj} = \theta_{kj} \circ \varphi_{kj} & : & M_k \to M_{jk}, \\
\varphi_{jki} & : & M_{jk} \to M_{jik} & \text{with} & \gamma_{jki} = \theta^k_{ji} \circ \varphi_{jki} & : & M_{jk} \to M_{ijk}.
\end{array}$$

So far everything is taking place unhindered (in relation to the modules with two and three indices that we chose to preserve): the squares $(M_i, M_{ij}, M_{ijk}, M_{ik})$ and $(M_j, M_{ij}, M_{ijk}, M_{jk})$ are commutative and the arrows are localization morphisms.

It is only with the two localization morphisms $M_k \to M_{ijk}$ that we will see the problem.

$$\begin{tikzcd}
& M_i \arrow[dl, "\varphi_{ij}"'] \arrow[dr, "\varphi_{ik}"] & & M_j \arrow[dlll, "\gamma_{ji}"'] \arrow[dr, "\varphi_{jk}"] & & M_k \arrow[dlll, "\gamma_{ki}"'] \arrow[dl, "\gamma_{kj}"] \\
M_{ij} \arrow[dr, "\varphi_{ijk}"'] & & M_{ik} \arrow[dl, "\varphi_{ikj}"'] & & M_{jk} \arrow[dlll, "\gamma_{jki}"] & \\
& M_{ijk} & & & &
\end{tikzcd}$$

These two localization morphisms are now imposed, namely the one that passes through M_{ik}, which must be

$$\varphi_{ikj} \circ \gamma_{ki} = \varphi_{ikj} \circ \theta_{ki} \circ \varphi_{ki} = \theta^j_{ki} \circ \varphi_{kij} \circ \varphi_{ki},$$

and the one that passes through M_{jk}, which must be

$$\gamma_{jki} \circ \gamma_{kj} = \theta^k_{ji} \circ \varphi_{jki} \circ \theta_{kj} \circ \varphi_{kj} = \theta^k_{ji} \circ \theta^i_{kj} \circ \varphi_{kji} \circ \varphi_{kj}.$$

As $\varphi_{kij} \circ \varphi_{ki} = \varphi_{kji} \circ \varphi_{kj}$, the fusion is successful if $\theta^j_{ki} = \theta^k_{ji} \circ \theta^i_{kj}$. Actually the condition is also necessary because "every localization morphism is an epimorphism": if $\psi_1 \circ \varphi = \psi_2 \circ \varphi$ with φ being a localization morphism, then $\psi_1 = \psi_2$. □

Patching of homomorphisms between rings

4.5. Definition. Let S be a monoid of $\mathbf{A}$. A morphism $\alpha : \mathbf{A} \to \mathbf{B}$ is called a *localization morphism at S* if every morphism $\psi : \mathbf{A} \to \mathbf{C}$ such that $\psi(S) \subseteq \mathbf{C}^\times$ can be uniquely factored by α.

Remark. If $\alpha : \mathbf{A} \to \mathbf{B}$ is a localization homomorphism, and if $S = \alpha^{-1}(\mathbf{B}^\times)$, then $\mathbf{B}$ is canonically isomorphic to $\mathbf{A}_S$. Moreover, a localization morphism can also be characterized as follows

– $\forall x, x' \in \mathbf{A}\ (\alpha(x) = \alpha(x') \iff \exists s \in S\ sx = sx')$

– $\forall y \in \mathbf{B},\ \exists x \in \mathbf{A},\ \exists s \in S\ \ sy = \alpha(x)$. ■

In the theory of schemes developed by Grothendieck, the localization morphisms $\mathbf{A} \to \mathbf{A}[1/s]$ play a preponderant role.

We have already discussed at the beginning of this section (Section 4) the impossibility of patching rings in general, with the example of $\mathbb{P}^n(\mathbb{C})$, which leads to the definition of schemes.

The possibility of defining a category of schemes as "patchings of rings" ultimately relies on the following concrete patching principle for homomorphisms between rings. The proof of the principle is very simple. The important thing is that the morphism is uniquely defined using localizations and that the compatibility conditions are themselves described via more advanced localizations.

4.6. Concrete local-global principle. (Patching of morphisms of rings) *Let $\mathbf{A}$ and $\mathbf{B}$ be two rings, $s_1, \ldots, s_n$ be comaximal elements of $\mathbf{A}$ and $t_1, \ldots, t_n$ be comaximal elements of $\mathbf{B}$. Let*

$$\mathbf{A}_i = \mathbf{A}[1/s_i],\ \mathbf{A}_{ij} = \mathbf{A}[1/s_is_j],\ \mathbf{B}_i = \mathbf{B}[1/t_i] \text{ and } \mathbf{B}_{ij} = \mathbf{B}[1/t_it_j].$$

For each $i \in [\![1..n]\!]$, let $\varphi_i : \mathbf{A}_i \to \mathbf{B}_i$ be a homomorphism. Suppose that the following compatibility conditions are satisfied: for $i \neq j$ the two homomorphisms $\beta_{ij} \circ \varphi_i : \mathbf{A}_i \to \mathbf{B}_{ij}$ and $\beta_{ji} \circ \varphi_j : \mathbf{A}_j \to \mathbf{B}_{ij}$ can be factorized via $\mathbf{A}_{ij}$ and give the same homomorphism $\varphi_{ij} : \mathbf{A}_{ij} \to \mathbf{B}_{ij}$ (see *the diagram).*

$$\begin{tikzcd}
& \mathbf{A}_i \arrow[rrr, "\varphi_i"] \arrow[rd, "\alpha_{ij}"] & & & \mathbf{B}_i \arrow[rd, "\beta_{ij}"] & \\
\mathbf{A} \arrow[ru, dotted, "\alpha_i"] \arrow[rrr, dashed, "\varphi!"] \arrow[rdd, dotted, "\alpha_j"'] & & & \mathbf{B} \arrow[ru, dotted, "\beta_i"] \arrow[rdd, dotted, "\beta_j"] & & \\
& & \mathbf{A}_{ij} \arrow[rrr, dotted, "\varphi_{ij}"] & & & \mathbf{B}_{ij} \\
& \mathbf{A}_j \arrow[ru, "\alpha_{ji}"] \arrow[rrr, "\varphi_j"] & & & \mathbf{B}_j \arrow[ru, "\beta_{ji}"] &
\end{tikzcd}$$

Then there exists a unique homomorphism $\varphi : \mathbf{A} \to \mathbf{B}$ such that for each i, we have $\varphi_i \circ \alpha_i = \beta_i \circ \varphi$.

D The compatibility conditions are clearly necessary. Let us show that they are sufficient. By the local-global principle 4.2, $\mathbf{B}$ is the limit of the diagram of the $\mathbf{B}_i$'s, $\mathbf{B}_{ij}$'s and β_{ij}'s. The compatibility conditions imply that we also have the equalities

$$\beta_{ij} \circ (\varphi_i \circ \alpha_i) = \beta_{ji} \circ (\varphi_j \circ \alpha_j)$$

which are the conditions guaranteeing the existence and the uniqueness of φ. □

5. The basic constructive local-global machinery

Therefore localize at any prime ideal.
A classical mathematician

Recall that we presented in Section VII-2 the general philosophy of the dynamic method in constructive algebra.

We now indicate how several proofs using the local-global principle in abstract algebra can be decrypted into constructive proofs leading to the same results in an explicit form.

In Section 6 we will focus on the decryption of abstract proofs that use the quotients by all the maximal ideals and in Section 7 we will focus on the decryption of abstract proofs that use localizations at all the minimal prime ideals.

Decryption of classical proofs using localization at all primes

A typical argument of localization works as follows in classical mathematics. When the ring is local a certain property P is satisfied in virtue of a sufficiently concrete proof. When the ring is not local, the same property is still true (from a nonconstructive classical point of view) because it suffices to satisfy it locally. This in virtue of an abstract local-global principle.

We examine with some attention the first proof. We then see certain computations appear that are feasible in virtue of the following principle

$$\forall x \in \mathbf{A} \quad x \in \mathbf{A}^{\times} \ \vee \ x \in \mathrm{Rad}(\mathbf{A}),$$

a principle which is applied to elements x derived from the proof itself. In other words, the given classical proof in the local case provides us with a constructive proof under the hypothesis of a residually discrete local ring. Now here is our constructive dynamic decryption. In the case of an arbitrary ring, we repeat the same proof, by replacing each disjunction "x is invertible or x is in the radical" with the consideration of the two rings $\mathbf{A}_{\mathcal{S}(I,x;U)}$ and $\mathbf{A}_{\mathcal{S}(I;x,U)}$, where $\mathbf{A}_{\mathcal{S}(I,U)}$ is the "current" localization of the starting ring $\mathbf{A}$, at this point in the proof. When the initial proof is deployed thus, we will have constructed in the end a certain, finite because the proof is finite, number of localized rings $\mathbf{A}_{S_i}$, for which the property is true. From a constructive point of view, we obtain at least the "quasi-global" result, i.e. after localization at comaximal monoids, in virtue of Lemma 1.5. We then call upon a concrete local-global principle to conclude the result.

Our decryption of the classical proof is made possible by the fact that the property P is of finite character (see Section II-2 from page 26, and Section V-9): it is preserved by localization, and if it is true after localization at a monoid S_i, it is also true after localization at some $s_i \in S_i$.

The complete decryption therefore contains two essential ingredients. The first is the decryption of the given proof in the local case which allows us to obtain a quasi-global result. The second is the constructive proof of the concrete local-global principle corresponding to the abstract local-global principle used in classical mathematics. In all the examples that we have encountered, this constructive proof offers no difficulty because the proof found in the classical literature already gives the concrete argument, at least in a telegraphic form (except sometimes in Bourbaki, where the concrete arguments are skilfully hidden).

The general conclusion is that the classical proofs "by abstract local-global principle" are already constructive, if we bother to read them in detail. This is good news, other than the fact that this confirms that no supernatural miracles take place in mathematics.

The method indicated above therefore gives, as a corollary of Lemma 1.5, the following general decryption principle, which *allows us to automatically obtain a global constructive version (or at least quasi-global) of a theorem from its local version.*

Local-global machinery with prime ideals.

When we reread a constructive proof, given for the case of a residually discrete local ring, with an arbitrary ring $\mathbf{A}$*, such that at the start we consider it as* $\mathbf{A} = \mathbf{A}_{\mathcal{S}(0;1)}$ *and at each disjunction (for an element* a *that occurs during the computation in the local case)*

$$a \in \mathbf{A}^{\times} \ \vee \ a \in \mathrm{Rad}(\mathbf{A}),$$

we replace the "current" ring $\mathbf{A}_{\mathcal{S}(I,U)}$ *with the two rings* $\mathbf{A}_{\mathcal{S}(I;U,a)}$ *and* $\mathbf{A}_{\mathcal{S}(I,a;U)}$ *(in each of which the computation can be continued), at the end of the rereading we obtain a finite family of rings* $\mathbf{A}_{\mathcal{S}(I_j,U_j)}$ *with the comaximal monoids* $\mathcal{S}(I_j,U_j)$ *and finite* I_j*,* U_j*. In each of these rings, the computation has been successfully continued and has produced the desired result.*

Please take note that if "the current ring" is $\mathbf{A}' = \mathbf{A}_{\mathcal{S}(I;U)}$ and if the disjunction relates to

$$b \in \mathbf{A}'^{\times} \ \vee \ b \in \mathrm{Rad}(\mathbf{A}'),$$

with $b = a/(u+i)$, $a \in \mathbf{A}$, $u \in \mathcal{M}(U)$ and $i \in \langle I \rangle_{\mathbf{A}}$, then the localized rings $\mathbf{A}_{\mathcal{S}(I;U,a)}$ and $\mathbf{A}_{\mathcal{S}(I,a;U)}$ must be considered.

In what follows we will speak of the local-global machinery with prime ideals as we do of the "basic local-global machinery."

Examples of the basic local-global machinery

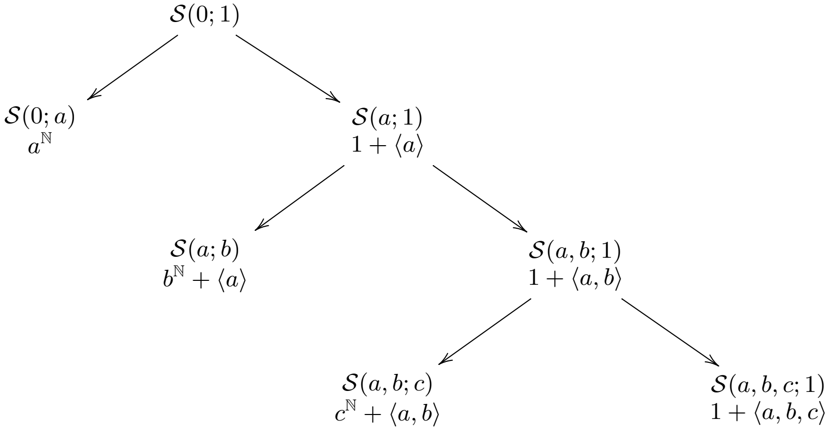
First example

We want to prove the following result.

5.1. Lemma. *Let* $f \in \mathbf{A}[X]$ *be a primitive polynomial and* $r \in \mathbf{A}$ *be a regular element with* $\mathsf{Kdim}\,\mathbf{A} \leqslant 1$*. Then the ideal* $\langle f, r\rangle$ *contains a monic polynomial.*

D We begin by proving the lemma in the case where $\mathbf{A}$ is a residually discrete local ring. We can write $f = f_1 + f_2$ with $f_1 \in (\mathrm{Rad}\,\mathbf{A})[X]$ and f_2 pseudomonic. Moreover, for every $e \in \mathrm{Rad}\,\mathbf{A}$ we have an equality $r^m(e^m(1+ye)+zr) = 0$, so r divides e^m. Consequently r divides a power of f_1, say with exponent N. We have ${f_2}^N = (f - f_1)^N \in \langle f, f_1^N\rangle \subseteq \langle f, r\rangle$. Then, f_2^N provides the monic polynomial required.

For an arbitrary ring we re-express the previous proof dynamically. For example if $f = aX^2 + bX + c$, we explicate the previous reasoning in the following form.



Either a is invertible, or it is in the radical. If a is invertible, then we take $f_2 = f$, $f_1 = 0$.

Otherwise, either b is invertible, or it is in the radical. If b is invertible, then we take $f_2 = bX + c$, $f_1 = aX^2$.

Otherwise, either c is invertible, or it is in the radical. If c is invertible, then we take $f_2 = c$, $f_1 = aX^2 + bX$. Otherwise $\langle 1\rangle = \langle a, b, c\rangle \in \operatorname{Rad}\mathbf{A}$ so the ring is trivial.

See above the graph of the tree of the successive localizations. The comaximal monoids are found at the leaves of the tree, the last one contains 0 and does not intervene in the computation.

Let us complete the proof by indicating how we construct a monic polynomial in the ideal $\langle f, r\rangle$ of $\mathbf{A}_{\mathcal{S}(I,U)}[X]$ from two monic polynomials g and h in the ideals $\langle f, r\rangle$ of $\mathbf{A}_{\mathcal{S}(I,y;U)}[X]$ and $\mathbf{A}_{\mathcal{S}(I;y,U)}[X]$. On the one hand we have

$$sg = sX^m + g_1 \text{ with } \deg g_1 < m,\ s \in \mathcal{S}(I, y; U) \text{ and } sg \in \langle f, r\rangle_{\mathbf{A}[X]}\,,$$

and on the other hand

$$th = tX^n + h_1 \text{ with } \deg h_1 < n,\ t \in \mathcal{S}(I; y, U) \text{ and } th \in \langle f, r\rangle_{\mathbf{A}[X]}\,.$$

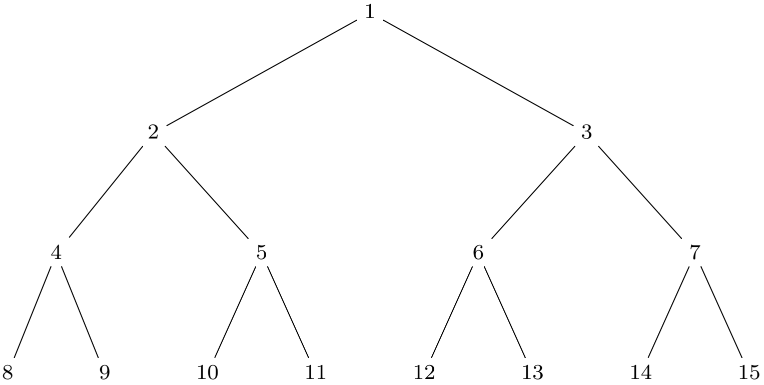
The polynomials $sX^n g$ and $tX^m h$ of formal degree $n + m$ have for formally leading coefficients s and t. By taking $us + vt \in \mathcal{S}(I, U)$, the work ends with $usX^n g + vtX^m h$. □

Second example: a quasi-global result obtained from a given proof for a local ring

Dynamic reread of the local freeness lemma. The dynamic rereading of “Azumaya’s proof” (page 494) of the local freeness lemma gives a new proof of the theorem which states that the finitely generated projective modules are locally free, with the following precise formulation.

If $F \in \mathbb{M}_n(\mathbf{A})$ is a projection matrix, there exist 2^n comaximal elements s_i such that over each $\mathbf{A}_{s_i}$, the matrix is similar to a standard projection matrix. More precisely, for each $k = 0, \dots, n$ there are $\binom{n}{k}$ localizations at which the matrix is similar to $\mathrm{I}_{k,n}$.

First recall (see the graph below) how the computation tree for a local ring with a matrix F in $\mathbb{M}_3(\mathbf{A})$ is presented.



At the point 1 the computation starts with the test "f_{11} or $1 - f_{11}$ is invertible" (note that the disjunction is generally not exclusive, and the test must only certify that one of the two possibilities takes place). If the test certifies that f_{11} is invertible, we follow the left branch, we go to 2 where we make a base change that allows us to reduce the matrix to the form $\begin{array}{|c|c|}\hline 1 & 0 \\ \hline 0 & G \\ \hline \end{array}$ with $G \in \mathbb{M}_2(\mathbf{A})$ and $G^2 = G$. If the test certifies that $1 - f_{11}$ is invertible, we follow the right branch, we go to 3 where we make a base change that allows us to reduce the matrix to the form $\begin{array}{|c|c|}\hline 0 & 0 \\ \hline 0 & H \\ \hline \end{array}$ with $H^2 = H$.

If we reach 2, we test the element g in position $(1, 1)$ in G. According to the result, we head towards 4 or 5 to make a base change that reduces us to one of the two forms $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & a \end{bmatrix}$ with $a^2 = a$, or $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & b \end{bmatrix}$ with $b^2 = b$.

If we reach 3, we test the element h in position $(1, 1)$ in H. According to the result, we head towards 6 or 7 to make a base change that reduces us to one of the two forms $\begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & c \end{bmatrix}$ with $c^2 = c$, or $\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & d \end{bmatrix}$ with $d^2 = d$.

In all cases, we finish with an invertibility test that certifies that the idempotent is equal to 1 or to 0, which gives one of the 8 possible diagonal projection matrices (with only 0's and 1's on the diagonal).

If we dynamically reread this computation with an arbitrary ring, we obtain the following comaximal localizations.

At the start at 1, we have the ring $\mathbf{A}_1 = \mathbf{A}$. At 2 and 3 we have the comaximal localizations $\mathbf{A}_2 = \mathbf{A}_1[1/f_{11}]$ and $\mathbf{A}_3 = \mathbf{A}_1[1/(1 - f_{11})]$. At 4 and 5 we have the following comaximal localizations of $\mathbf{A}_2$: $\mathbf{A}_4 = \mathbf{A}_2[1/g]$ and $\mathbf{A}_5 = \mathbf{A}_2[1/(1 - g)]$. At 6 and 7 we have the following comaximal localizations of $\mathbf{A}_3$: $\mathbf{A}_6 = \mathbf{A}_3[1/h]$ and $\mathbf{A}_7 = \mathbf{A}_3[1/(1 - h)]$.

We move on to the final level. At 8 and 9 we create the following comaximal localizations of $\mathbf{A}_4$: $\mathbf{A}_8 = \mathbf{A}_4[1/a]$ and $\mathbf{A}_9 = \mathbf{A}_4[1/(1 - a)]$. At 10 and 11 we create the following comaximal localizations of $\mathbf{A}_5$: $\mathbf{A}_{10} = \mathbf{A}_5[1/b]$ and $\mathbf{A}_{11} = \mathbf{A}_5[1/(1 - b)]$ etc.

Ultimately, by considering the denominators d_i ($i = 8, \ldots, 15$) of the fractions created in the different branches (for example d_{11} is the denominator in $\mathbf{A}$ of the fraction $1/f_{11}(1 - g)(1 - b)$, where $g \in \mathbf{A}_2$ and $b \in \mathbf{A}_5$), we obtain eight comaximal elements of $\mathbf{A}$, and for each of the localizations we obtain the corresponding reduced diagonal form of the starting matrix F.

In other words, the dynamic rereading of the proof given in the case of a local ring created eight comaximal elements, where the abstract classical proof would instruct us to localize at all the maximal ideals, which could take quite some time.

6. Quotienting by all the maximal ideals

A ring that has no maximal ideals is reduced to 0.
A classical mathematician

In the literature we find a certain number of proofs in which the author proves a result by considering "the passage to the quotient by an arbitrary maximal ideal." The analysis of these proofs shows that the result can be understood as the fact that a ring obtained from more or less complicated constructions is actually reduced to 0. For example, if we want to prove that an ideal $\mathfrak{a}$ of $\mathbf{A}$ contains 1, we reason by contradiction, we consider a maximal ideal $\mathfrak{m}$ that would contain $\mathfrak{a}$, and we find a contradiction by making a computation in the residual field $\mathbf{A}/\mathfrak{m}$.

This comes down to applying the quoted principle: a ring that has no maximal ideals is reduced to 0.

The idea of presenting the reasoning as a proof by contradiction is the result of an occupational bias. Proving that a ring is reduced to 0 is a fact of a concrete nature (we must prove that $1 = 0$ in the considered ring), and not a contradiction, and the computation performed in the field $\mathbf{A}/\mathfrak{m}$ only leads to a contradiction because one day we decided that, in a field, $1 = 0$ is prohibited. But the computation has nothing to do with such a prohibition. The computation in a field uses the fact that every element is null or invertible, but not the fact that this disjunction would be exclusive.

Consequently, the dynamic reread of the proof by contradiction in a constructive proof is possible according to the following method. Let us follow the computation that we are required to do as if the ring $\mathbf{A}/\mathfrak{a}$ were truly a field. Each time that the computation demands to know if an element x_i is null or invertible modulo $\mathfrak{a}$, let us bet on $x_i = 0$ and add it to $\mathfrak{a}$. After a while, we find that $1 = 0$ modulo the constructed ideal. Instead of losing courage in the face of such a contradiction, let us take a look at the good side of things. For example we have just observed that $1 \in \mathfrak{a} + \langle x_1, x_2, x_3 \rangle$. This is a positive fact and not a contradiction. We have actually just computed an inverse y_3 of x_3 in $\mathbf{A}$ modulo $\mathfrak{a} + \langle x_1, x_2 \rangle$. We can therefore examine the computation that the classical proof requires us to do when $x_1, x_2 \in \mathfrak{m}$ and x_3 is invertible modulo $\mathfrak{m}$. Except that we do not need $\mathfrak{m}$ since we have just established that x_3 is invertible modulo $\mathfrak{a} + \langle x_1, x_2 \rangle$.

Contrary to the strategy that corresponds to the localization at any prime ideal, we do not try to deploy all of the computation tree that seems to reveal itself to us. We only use quotients, and for this we systematically follow the "to be null" branch (modulo $\mathfrak{m}$) rather than the "to be invertible" branch. This creates more and more advanced successive quotients. When a so-called contradiction appears, i.e. when a computation reaches a certain result of positive nature, we backtrack by taking advantage of the information that we have just collected: an element has been certified invertible in the previous quotient.

For example, with a deployed tree of the type of that of page 873 and by taking as its general context the ring $\mathbf{A}/\mathfrak{a}$, if every time the right branch corresponds to $x = 0$ and the left one to an invertible x, it is necessary to start by following the path $1 \to 3 \to 7 \to 15$ and to consider the successive quotients. At 15 the computation gives us a positive result which allows us to backtrack to 7 to follow the branch $7 \to 14$. At 14 a positive result allows us to backtrack to point 3 (by the path $14 \to 7 \to 3$) by knowing that the element a_3 that produces the disjunction at this point is actually invertible. We can then follow the proposed computation for the branch $3 \to 6 \to 13$. At 13 the classical proof gives us a so-called contradiction, actually a positive result in the considered quotient at 6.

We will ultimately follow the path

$$1 \to 3 \to 7 \to 15 \to 7 \to 14 \to 3 \to 6 \to 13 \to 6 \to 12 \to 1 \to 2 \to 5 \to \\ 11 \to 5 \to 10 \to 2 \to 4 \to 9 \to 4 \to 8 \to 1.$$

We will uniquely compute in quotients of $\mathbf{A}/\mathfrak{a}$ and the final result is that $1 = 0$ in $\mathbf{A}/\mathfrak{a}$, i.e. $\mathfrak{a} = \mathbf{A}$, which was the pursued objective.

Note that during the first passage to the point 7, we work with the ring $\mathbf{A}_{1,3,7} = \mathbf{A}/(\mathfrak{a} + \langle a_1, a_3, a_7\rangle)$. Arriving at 15, we learn that this ring is trivial therefore that a_7 is invertible in $\mathbf{A}_{1,3} = \mathbf{A}/(\mathfrak{a} + \langle a_1, a_3\rangle)$. At 14, we learn that $\mathbf{A}_{1,3}$ is trivial, i.e. a_3 is invertible in the ring $\mathbf{A}_1 = \mathbf{A}/(\mathfrak{a} + \langle a_1\rangle)$. We therefore head for the point 6 with both the ring $\mathbf{A}_1$ and an inverse of a_3 in hand ... Thus in repeated passages to the same point we are not working with the same ring, because new information accumulates as we progress through the computations.

The argument of passage to the quotient by all the maximal ideals of $\mathbf{A}/\mathfrak{a}$ (assumed by contradiction non-reduced to 0), which seemed a little magical, is thus replaced by a very concrete computation, implicitly given by the classical proof. Let us summarize the previous discussion.

Local-global machinery with maximal ideals.
To reread a classical proof that proves by contradiction that a ring $\mathbf{A}$ *is trivial by assuming the contrary, then by considering a maximal ideal* $\mathfrak{m}$ *of this ring, by making a computation in the residual field and by finding the contradiction* $1 = 0$*, proceed as follows. First ensure that the proof becomes a constructive proof that* $1 = 0$ *under the additional hypothesis that* $\mathbf{A}$ *is a discrete field. Secondly, delete the additional hypothesis and follow step-by-step the previous proof by favoring the branch* $x = 0$ *each time that the disjunction "*$x = 0$ *or* x *is invertible" is required for the rest of the computation. Each time that we prove* $1 = 0$ *we have actually showed that in the previously constructed quotient ring, the last element to have undergone the test was invertible, which allows us to backtrack to this point to follow the branch "*x *is invertible" according to the proposed proof for the invertible case (which is now certified). If the considered proof is sufficiently uniform (experience shows that it is always the case), the computation obtained as a whole is finite and ends at the desired conclusion.*

Example.
The following crucial lemma was the only truly nonconstructive ingredient in the solution by Suslin of Serre's problem. We will expose this solution beginning on page 919 (see namely the proof of Theorem XVI-5.10). Here, we give the proof of the crucial lemma by Suslin in classical mathematics, then its constructive decryption.

6.1. Lemma. *Let $\mathbf{A}$ be a ring, n be an integer $\geqslant 2$ and $U = {}^{\mathrm{t}}[\,v_1 \ \cdots \ v_n\,]$ be a unimodular vector in $\mathbf{A}[X]^{n\times 1}$ with v_1 monic.*
Let $V = {}^{\mathrm{t}}[\,v_2 \ \cdots \ v_n\,]$. There exist matrices $E_1, \ldots, E_\ell \in \mathbb{E}_{n-1}(\mathbf{A}[X])$, such that, by letting w_i be the first coordinate of the vector E_iV, the ideal $\mathfrak{a}$ below contains 1

$$\mathfrak{a} = \langle \mathrm{Res}_X(v_1, w_1), \mathrm{Res}_X(v_1, w_2), \ldots, \mathrm{Res}_X(v_1, w_\ell)\rangle_{\mathbf{A}}\,.$$

D If $n = 2$, we have $u_1v_1 + u_2v_2 = 1$ and since v_1 is monic, $\mathrm{Res}(v_1, v_2) \in \mathbf{A}^\times$:

$$\mathrm{Res}(v_1, v_2)\mathrm{Res}(v_1, u_2) = \mathrm{Res}(v_1, u_2v_2) = \mathrm{Res}(v_1, u_2v_2 + u_1v_1) = \mathrm{Res}(v_1, 1) = 1.$$

If $n \geqslant 3$, let $d_1 = \deg v_1$. We suppose without loss of generality that the v_i's are formal polynomials of degrees $d_i < d_1$ $(i \geqslant 2)$. At the start we have some polynomials u_i such that $u_1v_1 + \cdots + u_nv_n = 1$.

Suslin's classical proof. We show that for every maximal ideal $\mathfrak{m}$, we can find a matrix $E_\mathfrak{m} \in \mathbb{E}_{n-1}(\mathbf{A}[X])$ such that, by letting $w_\mathfrak{m}$ be the first coordinate of $E_\mathfrak{m}V$, we have $1 \in \langle \mathrm{Res}_X(v_1, w_\mathfrak{m})\rangle$ modulo $\mathfrak{m}$. For this we work over the field $\mathbf{k} = \mathbf{A}/\mathfrak{m}$. By using the Euclidean algorithm, the gcd $w_\mathfrak{m}$ of the v_i's $(i \geqslant 2)$ is the first coordinate of a vector obtained by elementary manipulations over V. We lift the elementary matrix that was computed in $\mathbb{E}_{n-1}(\mathbf{k}[X])$ at a matrix $E_\mathfrak{m} \in \mathbb{E}_{n-1}(\mathbf{A}[X])$. Then, since v_1 and $w_\mathfrak{m}$ are coprime, the resultant $\mathrm{Res}_X(v_1, w_\mathfrak{m})$ is nonzero in the field $\mathbf{A}/\mathfrak{m}$.

Constructive proof (by decryption).
We perform a proof by induction on the smallest of the formal degrees d_i, which we denote by m (recall that $i \geqslant 2$). To fix the ideas suppose that it is d_2.
Basic step: if $m = -1$, $v_2 = 0$ and by an elementary transformation we put $u_3v_3 + \cdots + u_nv_n$ in position 2, which brings us to the case $n = 2$.
Inductive step: from $m - 1$ to m. Let a be the coefficient of v_2 of degree m and $\mathbf{B}$ be the ring $\mathbf{A}/\langle a\rangle$. In this ring the induction hypothesis is satisfied. Thus, we have matrices $E_1, \ldots, E_\ell \in \mathbb{E}_{n-1}(\mathbf{B}[X])$, such that, by letting $\widetilde{w_i}$ be the first coordinate of E_iV, we have the equality

$$\langle \mathrm{Res}_X(v_1, \widetilde{w_1}), \mathrm{Res}_X(v_1, \widetilde{w_2}), \ldots, \mathrm{Res}_X(v_1, \widetilde{w_\ell})\rangle_{\mathbf{B}} = \langle 1\rangle\,.$$

This means, by lifting the matrices in $\mathbb{E}_{n-1}(\mathbf{A}[X])$ without changing their name, and by letting w_i be the first coordinate of E_iV that we have

$$\langle a, \mathrm{Res}_X(v_1, w_1), \mathrm{Res}_X(v_1, w_2), \ldots, \mathrm{Res}_X(v_1, w_\ell)\rangle_{\mathbf{A}} = \langle 1\rangle\,.$$

Then consider $\mathfrak{b} = \langle \mathrm{Res}_X(v_1, w_1), \mathrm{Res}_X(v_1, w_2), \ldots, \mathrm{Res}_X(v_1, w_\ell)\rangle_{\mathbf{A}}$, and $\mathbf{C} = \mathbf{A}/\mathfrak{b}$. Since a is invertible in $\mathbf{C}$, we can by an elementary manipulation replace v_3 with a polynomial $v_3' = v_3 - qv_2$ with $\deg v_3' \leqslant m - 1$. We apply the induction hypothesis with the ring $\mathbf{C}$, we have elementary matrices E_1', $\ldots$, $E_q' \in \mathbb{E}_{n-1}(\mathbf{C}[X])$ that we lift in $\mathbb{E}_{n-1}(\mathbf{A}[X])$ without changing their name. If w_1', $\ldots$, w_q' are the corresponding polynomials (for each j, w_j' is the first coordinate of $E'_j V$), we obtain

$$1 \in \left\langle \mathrm{Res}_X(v_1, w_1), \dots, \mathrm{Res}_X(v_1, w_\ell), \mathrm{Res}_X(v_1, w'_1), \dots, \mathrm{Res}_X(v_1, w'_q) \right\rangle_{\mathbf{A}} .$$

□

Comment. Now let us see why this elegant proof is indeed a decryption of that of Suslin according to the method indicated beforehand. Let $a_2 = u_2 v_2 + \cdots + u_n v_n$.

When we want to treat the vector V over a discrete field by the Euclidean algorithm, we have to do divisions. One division depends on the degree of the dividend (the polynomial by which we divide). In the dynamic decryption, we therefore have tests to do on the coefficients of the dividend to determine its degree. If we choose to start with the division of v_3 by v_2, the indicated method therefore requires us to first consider the case where v_2 is identically null. Note that this corresponds to the basic step of the induction.

Let $\mathfrak{a}_1 = \left\langle (v_{2,i})_{i \in [\![0..d_2]\!]} \right\rangle$ be the ideal generated by the coefficients of v_2.

If v_2 is identically null, we have the resultant $r_1 = \mathrm{Res}(v_1, a_2) = \mathrm{Res}(v_1, w_1)$ (invertible) with w_1 which is of the first coordinate type of $E_1 V$ for an explicit matrix $E_1 \in \mathbb{E}_{n-1}$.

Naturally, this is only true modulo $\mathfrak{a}_1$, which gives $\mathfrak{a}_1 + \langle r_1 \rangle = \langle 1 \rangle$. Let $\mathfrak{a}_2 = \left\langle (v_{2,i})_{i \in [\![1..d_2]\!]} \right\rangle$. We have established that $\mathfrak{a}_2 + \langle r_1 \rangle + \langle v_{2,0} \rangle = \langle 1 \rangle$.

We now reason modulo $\mathfrak{b}_2 = \mathfrak{a}_2 + \langle r_1 \rangle$. Since $v_{2,0}$ is invertible and $v_2 = v_{2,0}$, we can reduce to 0 the vector v_3 by elementary manipulations then put in position 3 an element equal to a_2 modulo $\mathfrak{b}_2$, then bring it back to position 2. We therefore have a matrix $E_2 \in \mathbb{E}_{n-1}$ with w_2 being the first coordinate of $E_2 V$ and $\mathrm{Res}(v_1, w_2) = r_2$ is invertible in $\mathbf{A}/\mathfrak{b}_2$, i.e. $\mathfrak{a}_2 + \langle r_1 \rangle + \langle r_2 \rangle = \langle 1 \rangle$. Let $\mathfrak{a}_3 = \left\langle (v_{2,i})_{i \in [\![2..d_2]\!]} \right\rangle$. We have just established that $\mathfrak{a}_3 + \langle r_1, r_2 \rangle + \langle v_{2,1} \rangle = \langle 1 \rangle$.

We now reason modulo $\mathfrak{b}_3 = \mathfrak{a}_3 + \langle r_1, r_2 \rangle$. Since $v_{2,1}$ is invertible and $\mathfrak{a}_3 = 0$, we can reduce the vector v_3 to a constant by elementary manipulations (corresponding to the division of v_3 by v_2), then bring it in position 2. We find ourselves in the situation studied previously (where v_2 was reduced to a constant). We therefore know how to compute two new elementary matrices E_3 and E_4 such that, by letting w_3 and w_4 be their first coordinates, and $r_i = \mathrm{Res}(v_1, w_i)$, we obtain $\mathfrak{a}_3 + \langle r_1, r_2, r_3, r_4 \rangle = \langle 1 \rangle$.

Let $\mathfrak{a}_4 = \left\langle (v_{2,i})_{i \in [\![3..d_2]\!]} \right\rangle$. We have established that $\mathfrak{a}_4 + \langle r_1, r_2, r_3, r_4 \rangle + \langle v_{2,2} \rangle = \langle 1 \rangle$.

We now reason modulo $\mathfrak{b}_4 = \mathfrak{a}_4 + \langle r_1, r_2, r_3, r_4 \rangle$. Since $v_{2,2}$ is invertible and $\mathfrak{a}_4 = 0$, we can reduce the vector v_3 to the degree 1 by elementary manipulations (corresponding to the division of v_3 by v_2), then bring it in position 2. We find ourselves in the situation studied previously (where v_2

was of degree 1). $\ldots\ldots$ We obtain $\mathfrak{a}_4 + \langle r_1, r_2, \ldots, r_8 \rangle = \langle 1 \rangle$.
Let $\mathfrak{a}_5 = \big\langle (v_{2,i})_{i \in [\![4..d_2]\!]} \big\rangle$. We have established that $\mathfrak{a}_5 + \langle r_1, r_2, \ldots, r_8 \rangle + \langle v_{2,3} \rangle = \langle 1 \rangle$.

And so on and so forth $\ldots\ldots$

The important part of this is that the inverses of leading coefficients of successive v_2 that appear in the algorithm are always computed as elements of the ring and not by a localization procedure. Each time they are only invertible modulo a certain specified ideal, but it does not matter, the ideal grows by incorporating the authorized resultants but decreases by expelling intruders that are the coefficients of v_2. ■

7. Localizing at all the minimal prime ideals

A ring that has no minimal prime ideals is reduced to 0.
A classical mathematician

The readers are now called upon to convince themselves of the correctness of the following method, by replacing in the previous section addition by multiplication and passage to the quotient by localization.

Local-global machinery with minimal prime ideals.
To reread a classical proof that proves by contradiction that a ring **A** *is trivial by assuming the contrary, then by considering a minimal prime ideal of this ring, by making a computation in the localized ring (which is local and zero-dimensional, therefore a field in the reduced case) and by finding the contradiction* $1 = 0$*, proceed as follows.*
First ensure that the proof becomes a constructive proof of the equality $1 = 0$ *under the additional hypothesis that* **A** *is local and zero-dimensional.*
Secondly, delete the additional hypothesis and follow step-by-step the previous proof by favoring the "x is invertible" branch each time that the disjunction "x is nilpotent or x is invertible" is required for the rest of the computation. Each time that we prove $1 = 0$ *we actually have shown that in the previously constructed localized ring, the last element to be subjected to the test was nilpotent, which allows us to backtrack to this point to follow the "x is nilpotent" branch according to the proposed proof for the nilpotent case (which is now certified). If the considered proof is sufficiently uniform (experience shows that this is always the case), the computation obtained as a whole is finite and ends at the desired conclusion.*

Example. A quite spectacular example is given in the next chapter with the constructive decryption of an abstract proof of Traverso's theorem regarding seminormal rings.

8. Local-global principles in depth 1

Until now the different variants of the local-global principle were based on the families of comaximal elements, that is on the finite families that generate the ideal $\langle 1\rangle$. A weaker notion is sufficient for questions of regularity: these are the finite families that generate a faithful ideal, or more generally an E-regular ideal.

We say that they are families of depth $\geqslant 1$. In Section 9, we will examine what we call the families of depth $\geqslant 2$.

8.1. Definition.

1. A finite family $(a_1, \dots, a_n)$ of a ring $\mathbf{A}$ is called a *system of coregular elements* if the ideal $\langle a_1, \dots, a_n\rangle$ is faithful.[2]
   We also say that *the ideal* $\mathfrak{a}$*, or the list* $(a_1, \dots, a_n)$*, is of depth* $\geqslant 1$, and we express this in the form $\mathsf{Gr}_{\mathbf{A}}(a_1, \dots, a_n) \geqslant 1$.
2. Let E be an $\mathbf{A}$-module.
   - We say that an element $a \in \mathbf{A}$ is *E-regular* (or *regular for E*) if
   $$\forall x \in E,\ (ax = 0 \implies x = 0).$$
   - A finite family $(a_1, \dots, a_n)$ is said to be *once E-regular* if
   $$\forall x \in E,\ \big((a_1x = 0,\ \dots,\ a_nx = 0) \implies x = 0\big).$$
   We also say that the a_i's are *coregular for E*.
   We express this in the form $\mathsf{Gr}_{\mathbf{A}}(a_1, \dots, a_n, E) \geqslant 1$.
   - A finitely generated ideal $\mathfrak{a} \subseteq \mathbf{A}$ is said to be *E-regular* if some (every) generator set of $\mathfrak{a}$ is once E-regular. We also say that *the depth of E relative to $\mathfrak{a}$ is greater than or equal to* 1, and we express this in the form $\mathsf{Gr}_{\mathbf{A}}(\mathfrak{a}, E) \geqslant 1$.

Thus $\mathsf{Gr}_{\mathbf{A}}(\underline{a}) \geqslant 1$ means $\mathsf{Gr}_{\mathbf{A}}(\underline{a}, \mathbf{A}) \geqslant 1$. In what follows, we will often only give the statement with $\mathsf{Gr}_{\mathbf{A}}(\underline{a}, E) \geqslant 1$.

Remark. The notation $\mathsf{Gr}(\mathfrak{a}, E)$ comes from [Northcott]. In this wonderful book, Northcott defines the “true grade” à la Hochster as the better non-Noetherian substitute for the usual depth. ■

8.2. Fact.

- *The product of two E-regular finitely generated ideals is E-regular.*
- *If $\mathfrak{a} \subseteq \mathfrak{a}'$ with $\mathfrak{a}$ E-regular, then $\mathfrak{a}'$ is E-regular.*

[2] Not to be confused with the notion of a coregular sequence introduced by Bourbaki, as a dual notion of that of a regular sequence.

8.3. Lemma. ((a, b, ab) trick for depth 1)
Suppose that the ideals $\langle a, c_2, \ldots, c_n\rangle$ and $\langle b, c_2, \ldots, c_n\rangle$ are E-regular. Then the ideal $\langle ab, c_2, \ldots, c_n\rangle$ is E-regular.

D Let $x \in E$ such that $abx = c_2x = \cdots = c_nx = 0$.
Then $abx = c_2bx = \cdots = c_nbx = 0$, so $bx = 0$. So $bx = c_2x = \cdots = c_nx = 0$, therefore $x = 0$. □

We have the following immediate corollary.[3]

8.4. Lemma. *Let $\langle a_1, \ldots, a_n\rangle$ be an E-regular ideal and let $p_i \in \mathbb{N}$. Then the ideal $\left\langle a_1^{p_1}, \ldots, a_n^{p_n}\right\rangle$ is E-regular.*

We can compare the following local-global principle to items *1* and *3* of the local-global principle 2.1.

Note that the statement "$\mathfrak{b}$ is E-regular" is stable under localization when $\mathfrak{b}$ is finitely generated. This gives the implication in the direct sense for item *c* in the following local-global principle.

8.5. Concrete local-global principle. (Localizations in depth $\geqslant 1$)
Let b, a_1, $\ldots$, $a_n \in \mathbf{A}$, and $\mathfrak{b}$ be a finitely generated ideal. Let $\mathbf{A}_i = \mathbf{A}[1/a_i]$.

1. *Suppose that the a_i's are coregular.*
   - *a. We have $x = 0$ in $\mathbf{A}$ if and only if $x = 0$ in each $\mathbf{A}_i$.*
   - *b. The element b is regular if and only if it is regular in $\mathbf{A}_i$ for each i.*
   - *c. The ideal $\mathfrak{b}$ is faithful if and only if it is faithful in $\mathbf{A}_i$ for each i.*
2. *Let E be an $\mathbf{A}$-module and let $E_i = E[1/a_i]$.*
   Suppose that the ideal $\langle a_1, \ldots, a_n\rangle$ is E-regular.
   - *a. We have $x = 0$ in E if and only if $x = 0$ in each E_i.*
   - *b. The element b is E-regular if and only if it is E_i-regular for each i.*
   - *c. The ideal $\mathfrak{b}$ is E-regular if and only if it is E_i-regular for each i.*

D It suffices to treat item *2*.
a. If $x = 0$ in E_i there is an exponent k_i such that $a_i^{k_i}x = 0$ in E. We conclude by Lemma 8.4 (with the module $\mathbf{A}x$) that $x = 0$.

c. Suppose that $\mathfrak{b}$ is E_i-regular for each i, and $\mathfrak{b}\,x = 0$. Then $x = 0$ in each E_i, so $x = 0$ by item *a*. □

We often implicitly use the following lemma, which is a variant of Lemma V-7.2 stated for the systems of comaximal elements.

[3] We also could have noticed that for large enough q, the ideal $\langle a_1, \ldots, a_n\rangle^q$, which is E-regular, is contained in the ideal $\left\langle a_1^p, \ldots, a_n^p\right\rangle$.

8.6. Fact. (Lemma of successive coregular localizations)
If $\mathsf{Gr}_{\mathbf{A}}(s_1, \ldots, s_n, E) \geqslant 1$ *and if for each* i*, we have elements* $s_{i,1}$, $\ldots$, s_{i,k_i}*, coregular for* $E[1/s_i]$*, then the* $s_i s_{i,j}$*'s are coregular for* E*.*

D Let $\mathfrak{b}$ be the ideal generated by the $s_i s_{i,j}$'s. By item *2c* of the local-global principle 8.5, it suffices to prove that it is E-regular after localization at coregular elements for E. The s_i's are suitable. □

McCoy's theorem

As an application of the local-global principle 8.5, we give a new proof of McCoy's theorem (II-5.22 item *2*).

8.7. McCoy's theorem. *A matrix* $M \in \mathbf{A}^{m\times n}$ *is injective if and only if the determinantal ideal* $\mathcal{D}_n(M)$ *is faithful.*

D The implication "if" is simple. Let us show that if the matrix M is injective, the ideal $\mathcal{D}_n(M)$ is faithful. We perform an induction on the number of columns. Since M is injective, the coefficients of the first column (which represents the image of the first basis vector), generate a faithful ideal. By the local-global principle 8.5, it therefore suffices to prove that $\mathcal{D}_n(M)$ is faithful over the ring $\mathbf{A}_a = \mathbf{A}[1/a]$, where a is a coefficient of the first column.
Over this ring it is clear that the matrix M is equivalent to a matrix of the form $\begin{array}{|c|c|}\hline 1 & 0 \\ \hline 0 & N \\ \hline \end{array}$. In addition N is injective therefore by induction hypothesis the ideal $\mathcal{D}_{n-1}(N)$ is faithful over $\mathbf{A}_a$. Finally $\mathcal{D}_{\mathbf{A}_a,n-1}(N) = \mathcal{D}_{\mathbf{A}_a,n}(M)$.□

Remarks.
1) The proof also gives that if $m < n$ and M is injective, then the ring is trivial. Indeed at each step of the induction, when we replace M with N the difference $m - n$ remains constant. Therefore if $m < n$ we obtain "at the base step" an injective map from $\mathbf{A}^0$ in $\mathbf{A}^{n-m}$ which implies $1 = 0$ in $\mathbf{A}$. This is in accordance with the general statement of Theorem 8.7, because for $m < n$, $\mathcal{D}_n(M) = 0$, and if 0 is a regular element, the ring is trivial.

2) We often find in the literature McCoy's theorem stated as follows, in a contrapositive form (in appearance).
If the ideal is not faithful, the map is not injective.
Or more precisely.
If a nonzero element $x \in \mathbf{A}$ *annihilates* $\mathcal{D}_n(M)$*, there exists a nonzero column vector* $C \in \mathbf{A}^{m\times 1}$ *such that* $MC = 0$*.*
Unfortunately, this statement can only be proven with classical logic, and the existence of the vector C cannot result from a general algorithm. Here

is a counterexample, well-known by numerical analysts. If M is a matrix with real coefficients with $m < n$, we do not know how to produce a nonzero vector in its kernel so long as we do not know the rank of the matrix. For example for $m = 1$ and $n = 2$, we give two reals (a, b), and we look for a pair $(c, d) \neq (0, 0)$ such that $ac + bd = 0$. If the pair (a, b) is a priori indistinguishable from the pair $(0, 0)$, it is impossible to provide a suitable pair (c, d) so long as we have not established whether $|a| + |b|$ is null or not. Constructive variants of the contraposition are proposed in Exercises 11 and 12. ∎

9. Local-global principles in depth 2

9.1. Definition. Let $a_1, \ldots, a_n \in \mathbf{A}$ and E be an $\mathbf{A}$-module.

- The list $(\underline{a}) = (a_1, \ldots, a_n)$ is said to be *of depth* $\geqslant 2$ if it is of depth $\geqslant 1$ and if, for every list $(\underline{x}) = (x_1, \ldots, x_n)$ in $\mathbf{A}$ proportional[4] to $(\underline{a})$, there exists an $x \in \mathbf{A}$ such that $(\underline{x}) = x(\underline{a})$.
  We express this in the form $\mathsf{Gr}_{\mathbf{A}}(\underline{a}) \geqslant 2$ or $\mathsf{Gr}(\underline{a}) \geqslant 2$.
- The list $(\underline{a}) = (a_1, \ldots, a_n)$ is said to be *twice E-regular* if $\mathsf{Gr}_{\mathbf{A}}(\underline{a}, E) \geqslant 1$ and if, for every list $(\underline{x}) = (x_1, \ldots, x_n)$ in E proportional to $(\underline{a})$ there exists an $x \in E$ such that $(\underline{x}) = (\underline{a})x$.
  We express this in the form $\mathsf{Gr}_{\mathbf{A}}(a_1, \ldots, a_n, E) \geqslant 2$ or $\mathsf{Gr}(\underline{a}, E) \geqslant 2$.
  We also say[5] that *the depth of E relative to $(a_1, \ldots, a_n)$ is greater than or equal to 2.*

Examples. 1) In an integral ring a list (a, b) with $a, b \in \mathrm{Reg}(\mathbf{A})$ is of depth $\geqslant 2$ if and only if $\langle a \rangle \cap \langle b \rangle = \langle ab \rangle$, i.e. ab is the lcm of a and b in the sense of divisibility.
2) In a GCD-domain a list $(a_1, \ldots, a_n)$ is of depth $\geqslant 2$ if and only if 1 is the gcd of the list.
3) If $n = 1$ and the list is reduced to the single term a, $\mathsf{Gr}(a, E) \geqslant 2$ means that each $y \in E$ is of the form $y = ax$, i.e. $aE = E$. In particular $\mathsf{Gr}_{\mathbf{A}}(a) \geqslant 2$ means $a \in \mathbf{A}^{\times}$.
4) Every list of comaximal elements is of depth $\geqslant 2$ (by the basic local-global principle). ∎

It is clear that $\mathsf{Gr}(\underline{a}) \geqslant 2$ means $\mathsf{Gr}(\underline{a}, \mathbf{A}) \geqslant 2$. In the remainder this exempts us from duplicating the statements: we represent them with $\mathsf{Gr}(\underline{a}, E) \geqslant 2$ for an arbitrary module E whenever possible.

[4] Recall that this means that the determinants $\begin{vmatrix} a_i & a_j \\ x_i & x_j \end{vmatrix}$ are all null.

[5] Eisenbud speaks of the depth of $\mathfrak{a}$ over E, and Matsumura of the $\mathfrak{a}$-depth of E. The terminology adopted here is that of Bourbaki.

9.2. Proposition and definition.
Let $(\underline{a}) = (a_1, \ldots, a_n)$ *and* $(\underline{b}) = (b_1, \ldots, b_r)$ *in* $\mathbf{A}$ *and* E *be an* $\mathbf{A}$*-module. If* $\mathsf{Gr}_{\mathbf{A}}(\underline{a}, E) \geqslant 2$ *and* $\langle \underline{a} \rangle \subseteq \langle \underline{b} \rangle$*, then* $\mathsf{Gr}_{\mathbf{A}}(\underline{b}, E) \geqslant 2$.
Consequently, we say that a finitely generated ideal $\mathfrak{a}$ is twice E-regular *if every finite generator set of* $\mathfrak{a}$ *is twice* E*-regular (it suffices to verify it for a single one). We express this in the form* $\mathsf{Gr}_{\mathbf{A}}(\mathfrak{a}, E) \geqslant 2$.

D It suffices to prove the two following facts.

- If $\mathsf{Gr}(a_1, \ldots, a_n, E) \geqslant 2$, then $\mathsf{Gr}(a_1, \ldots, a_n, b, E) \geqslant 2$.
- If $a \in \langle a_1, \ldots, a_n \rangle$ and $\mathsf{Gr}(a_1, \ldots, a_n, a, E) \geqslant 2$, then $\mathsf{Gr}(a_1, \ldots, a_n, E) \geqslant 2$.

This indeed first shows that we can replace a generator set of a finitely generated ideal by another without changing “the depth $\geqslant 2$” and then that when we replace $\mathfrak{a}$ by a larger finitely generated ideal, the depth $\geqslant 2$ is preserved.
Let us consider the first item. We have a list $(x_1, \ldots, x_n, y)$ in E proportional to $(a_1, \ldots, a_n, b)$. We find some x (unique, in fact) such that $(\underline{x}) = (\underline{a})x$. We must show that $bx = y$. However, $a_i y = bx_i$ and $bx_i = ba_i x$ for $i \in [\![1..n]\!]$. Therefore $a_i(y - bx) = 0$ and we conclude that $y = bx$ because $\mathsf{Gr}(\underline{a}, E) \geqslant 1$. The second item is left to the reader. □

9.3. Lemma. ((a, b, ab) trick for depth 2)
Suppose that the lists $(a_1, \ldots, a_n, a)$ *and* $(a_1, \ldots, a_n, b)$ *are twice* E*-regular. Then the list* $(a_1, \ldots, a_n, ab)$ *is twice* E*-regular.*

D We already know that $(a_1, \ldots, a_n, ab)$ is once E-regular.
Let $(x_1, \ldots, x_n, y)$ be a list in E proportional to $(a_1, \ldots, a_n, ab)$. The list $(x_1 b, \ldots, x_n b, y)$ is proportional to $(a_1, \ldots, a_n, a)$. So there exists a $z \in E$ such that

$$x_1 b = a_1 z,\ \ldots,\ x_n b = a_n z,\ y = az$$

This implies the list $(x_1, \ldots, x_n, z)$ is proportional to $(a_1, \ldots, a_n, b)$. So there exists an $x \in E$ such that

$$x_1 = a_1 x,\ \ldots,\ x_n = a_n x,\ z = bx \ \text{ and a fortiori } y = abx$$

□

9.4. Concrete local-global principle. (For divisibility and integrally closed rings, localizations in depth 2) *Consider a family* $(\underline{s}) = (s_1, \ldots, s_n)$ *in* $\mathbf{A}$ *with* $\mathsf{Gr}_{\mathbf{A}}(\underline{s}, E) \geqslant 2$. *Let* $\mathbf{A}_i = \mathbf{A}[\frac{1}{s_i}]$ *and* $E_i = E[\frac{1}{s_i}]$.

1. *Let* $a \in \mathbf{A}$ *be a* E*-regular element and* $y \in E$. *Then* a *“divides” y in* E *if and only if* a *divides* y *after localization at each* s_i.
2. *Let* $(b_1, \ldots, b_m)$ *in* $\mathbf{A}$. *Then* $\mathsf{Gr}_{\mathbf{A}}(b_1, \ldots, b_m, E) \geqslant 2$ *if and only if* $\mathsf{Gr}_{\mathbf{A}_i}(b_1, \ldots, b_m, E_i) \geqslant 2$ *for each* i.
3. *Suppose that* $\mathbf{A}$ *is integral and* $\mathsf{Gr}_{\mathbf{A}}(\underline{s}) \geqslant 2$. *The ring* $\mathbf{A}$ *is integrally closed if and only if each ring* $\mathbf{A}_i$ *is integrally closed.*

D *1.* Suppose that a divides y after localization at s_i. We have $ax_i = u_iy$ in E for some $u_i = s_i^{n_i}$ and some $x_i \in E$. The list of the u_i's is twice E-regular (Lemma 9.3). We have $au_jx_i = u_iu_jy = au_ix_j$ and as a is E-regular, $u_jx_i = u_ix_j$. Therefore we have some $x \in E$ such that $x_i = u_ix$ for each i. This gives $u_iax = u_iy$ and as $\mathsf{Gr}(u_1, \dots, u_n, E) \geqslant 1$, we obtain $ax = y$.

2. Consider in $\mathbf{A}$ a sequence $(x_1, \dots, x_m)$ proportional to $(b_1, \dots, b_m)$. We seek some $x \in E$ such that $x_\ell = xc_\ell$ for every $\ell \in [\![1..m]\!]$. In each E_i we find some y_i such that $x_\ell = y_ic_\ell$ for every $\ell \in [\![1..m]\!]$. This means that we have some $u_i \in s_i^{\mathbb{N}}$ and some $z_i \in E$ such that $u_ix_\ell = z_ic_\ell$ in E for every $\ell \in [\![1..m]\!]$. It suffices to show that there exists some $z \in E$ such that $z_i = u_iz$ for each i, because then $u_i(x_\ell - zc_\ell) = 0$ for each i (and the u_i's are coregular for E). It therefore suffices to show that the z_i's form a family proportional to the u_i's, i.e. $u_iz_j = u_jz_i$ for all $i, j \in [\![1..n]\!]$. However, we know that the c_ℓ's are coregular for E (by the local-global principle 8.5). Therefore it suffices to show that we have the equalities $u_iz_jc_\ell = u_jz_ic_\ell$, but the two members are equal to $u_iu_jx_\ell$.

3. Let x and y in $\mathbf{A}$ with y integral over the ideal $x\mathbf{A}$. This remains true for each localized ring $\mathbf{A}_i$, which is integrally closed. Therefore x divides y in each $\mathbf{A}_i$. Therefore by item *1* with $E = \mathbf{A}$, x divides y in $\mathbf{A}$. □

9.5. Fact. (Successive localizations lemma, with depth 2)
If $\mathsf{Gr}_{\mathbf{A}}(s_1, \dots, s_n, E) \geqslant 2$ *and if for each* i *we have a list* $(s_{i,1}, \dots, s_{i,k_i})$ *in* $\mathbf{A}$ *which is twice* $E[1/s_i]$*-regular, then the system of the* $s_is_{i,j}$*'s is twice* E*-regular.*

D Applying 9.4 *2.*, it suffices to verify that the s_is_{ij}'s are twice E-regular after localization at elements that form a list twice E-regular. This works with the list of the s_i's. □

9.6. Lemma. *Let* $(\underline{a}) = (a_1, \dots, a_n)$ *and* $(\underline{b}) = (b_1, \dots, b_r)$ *in* $\mathbf{A}$ *and* E *be an* $\mathbf{A}$*-module. Let* $(\underline{a} \star \underline{b})$ *be the finite family of the* a_ib_j*'s.*
If $\mathsf{Gr}_{\mathbf{A}}(\underline{a}, E) \geqslant 2$ *and* $\mathsf{Gr}_{\mathbf{A}}(\underline{b}, E) \geqslant 2$ *then* $\mathsf{Gr}_{\mathbf{A}}(\underline{a} \star \underline{b}, E) \geqslant 2$.
In terms of finitely generated ideals:

- *if* $\mathsf{Gr}_{\mathbf{A}}(\mathfrak{a}, E) \geqslant 2$ *and* $\mathsf{Gr}_{\mathbf{A}}(\mathfrak{b}, E) \geqslant 2$ *then* $\mathsf{Gr}_{\mathbf{A}}(\mathfrak{a}\mathfrak{b}, E) \geqslant 2$.

D Applying 9.4 *2.*, it suffices to show that the family of a_ib_j's is twice E-regular after localization in each a_i. E.g., when localizing in a_1, the list of a_1b_j's generate the same ideal ideal as the b_j's, and this ideal is twice E-regular. □

Patchings in depth 2

The following definition allows us to simplify the writing of certain proofs a little.

9.7. Definition. *(System of monoids twice E-regular)*
A system $(S_1, \dots, S_n) = (\underline{S})$ of monoids of $\mathbf{A}$ is said to be *twice E-regular* if for all $s_1 \in S_1$, …, $s_n \in S_n$, we have $\mathsf{Gr}_{\mathbf{A}}(s_1, \dots, s_n, E) \geqslant 2$.

The most important case is the system of monoids $(s_1^{\mathbb{N}}, \dots, s_n^{\mathbb{N}})$ when $\mathsf{Gr}_{\mathbf{A}}(s_1, \dots, s_n, E) \geqslant 2$.

We now re-express the local-global principle 4.2 by replacing the hypothesis according to which the monoids are comaximal by a weaker hypothesis (system of monoids twice regular).

The context is the following. Consider a system of monoids $(\underline{S}) = (S_i)_{i \in \llbracket 1..n \rrbracket}$.
Let $\mathbf{A}_i := \mathbf{A}_{S_i}$ and $\mathbf{A}_{ij} := \mathbf{A}_{S_i S_j}$ $(i \neq j)$ such that $\mathbf{A}_{ij} = \mathbf{A}_{ji}$.
Let $\varphi_i : \mathbf{A} \to \mathbf{A}_i$ and $\varphi_{ij} : \mathbf{A}_i \to \mathbf{A}_{ij}$ be the natural homomorphisms.
In what follows notations like $(E_{ij})_{i<j \in \llbracket 1..n \rrbracket}$ and $(\varphi_{ij})_{i \neq j \in \llbracket 1..n \rrbracket})$ mean that we have $E_{ij} = E_{ji}$ but (a priori) not $\varphi_{ij} = \varphi_{ji}$.

9.8. Concrete local-global principle. (Concrete patching of elements of a module in depth 2) *Consider the context described above.*

1. *Suppose that $(\underline{S})$ is twice regular. Consider an element $(x_i)_{i \in \llbracket 1..n \rrbracket}$ of $\prod_{i \in \llbracket 1..n \rrbracket} \mathbf{A}_i$. So that there exists some $x \in \mathbf{A}$ satisfying $\varphi_i(x) = x_i$ in each $\mathbf{A}_i$, it is sufficient and necessary that for each $i < j$ we have $\varphi_{ij}(x_i) = \varphi_{ji}(x_j)$ in $\mathbf{A}_{ij}$. In addition, this x is then uniquely determined. In other terms the ring $\mathbf{A}$ (with the homomorphisms φ_i) is the limit of the diagram*
$$\big((\mathbf{A}_i)_{i \in \llbracket 1..n \rrbracket}, (\mathbf{A}_{ij})_{i<j \in \llbracket 1..n \rrbracket}; (\varphi_{ij})_{i \neq j \in \llbracket 1..n \rrbracket}\big).$$
2. *Let E be an $\mathbf{A}$-module. Suppose that $(\underline{S})$ is twice E-regular.
Let $E_i := E_{S_i}$ and $E_{ij} := E_{S_i S_j}$ $(i \neq j)$ such that $E_{ij} = E_{ji}$.
Let $\varphi_i : E \to E_i$ and $\varphi_{ij} : E_i \to E_{ij}$ be the natural linear maps. Then the pair $\big(E, (\varphi_i)_{i \in \llbracket 1..n \rrbracket}\big)$ gives the limit of the following diagram in the category of $\mathbf{A}$-modules*
$$\big((E_i)_{i \in \llbracket 1..n \rrbracket}, (E_{ij})_{i<j \in \llbracket 1..n \rrbracket}; (\varphi_{ij})_{i \neq j \in \llbracket 1..n \rrbracket}\big).$$

$$\begin{tikzcd}
 & & E_i \arrow[r, "\varphi_{ij}"] \arrow[rdd, "\varphi_{ik}"'] & E_{ij} \\
F \arrow[rru, "\psi_i"] \arrow[r, dashed, "\psi!"] \arrow[rrd, "\psi_j"'] \arrow[rrdd, "\psi_k"'] & E \arrow[ru, "\varphi_i"'] \arrow[rd, "\varphi_j"] \arrow[rdd, "\varphi_k"'] & & \\
 & & E_j \arrow[ruu, "\varphi_{ji}"'] \arrow[rd] & E_{ik} \\
 & & E_k \arrow[ru] \arrow[r, "\varphi_{kj}"'] & E_{jk}
\end{tikzcd}$$

D *1.* Special case of *2.*

2. Let $(x_i)_{i\in[\![1..n]\!]}$ be an element of $\prod_{i\in[\![1..n]\!]} E_i$. We must show the following equivalence: there exists an $x \in E$ satisfying $\varphi_i(x) = x_i$ in each E_i if and only if for each $i < j$ we have $\varphi_{ij}(x_i) = \varphi_{ji}(x_j)$ in E_{ij}. In addition, this x must be unique.

The condition is clearly necessary. Let us prove that it is sufficient.

Let us show the existence of x. Let us first note that there exist some s_i's in S_i and some y_i's in E such that we have $x_i = y_i/s_i$ in each E_i.

If $\mathbf{A}$ is integral, E is torsion-free and each $s_i \neq 0$, we have in the vector space obtained by scalar extension to the quotient field the equalities

$$\frac{y_1}{s_1} = \frac{y_2}{s_2} = \cdots = \frac{y_n}{s_n},$$

and given the hypothesis regarding the s_i's there exists some $x \in E$ such that $xs_i = y_i$ for each i.

In the general case we do just about the same thing.

For each pair (i, j) with $i \neq j$, the fact that $x_i/1 = x_j/1$ in E_{ij} means that for certain $u_{ij} \in S_i$ and $u_{ji} \in S_j$ we have $s_ju_{ij}u_{ji}y_i = s_iu_{ij}u_{ji}y_j$. For each i, let $u_i \in S_i$ be a common multiple of the u_{ik}'s (for $k \neq i$).

We then have $(s_ju_j)(u_iy_i) = (s_iu_i)(u_jy_j)$. Thus the vector of the u_iy_i's is proportional to the vector of the s_iu_i's. Since the system $(\underline{S})$ is twice E-regular, there exists some $x \in E$ such that $u_iy_i = s_iu_ix$ for every i, which gives the equalities $\varphi_i(x) = \frac{u_iy_i}{s_iu_i} = \frac{y_i}{s_i} = x_i$.

Finally, this x is unique because the S_i's are E-coregular. □

Now here is a variant of the local-global principle 4.4. This variant appears this time as a converse of the previous local-global principle.

9.9. Concrete local-global principle. (Concrete patching of modules in depth 2) *Let* $(\underline{S}) = (S_1, \ldots, S_n)$ *be a system of monoids of* $\mathbf{A}$. *Let* $\mathbf{A}_i = \mathbf{A}_{S_i}$, $\mathbf{A}_i = \mathbf{A}_{S_i}$, $\mathbf{A}_i{=}\mathbf{A}_{S_i}$, $\mathbf{A}_{ij}{=}\mathbf{A}_{S_iS_j}$ *and* $\mathbf{A}_{ijk}{=}\mathbf{A}_{S_iS_jS_k}$. *Suppose that a commutative diagram*

$$\big((E_i)_{i\in[\![1..n]\!]}\big), (E_{ij})_{i<j\in[\![1..n]\!]}, (E_{ijk})_{i<j<k\in[\![1..n]\!]}; (\varphi_{ij})_{i\neq j}, (\varphi_{ijk})_{i<j, i\neq k, j\neq k}\big)$$

(as in the figure below) is given in the category of $\mathbf{A}$*-modules with the following properties.*

- *For all i, j, k (with* $i < j < k$*),* E_i *is an* $\mathbf{A}_i$*-module,* E_{ij} *is an* $\mathbf{A}_{ij}$*-module and* E_{ijk} *is an* $\mathbf{A}_{ijk}$*-module. Recall that according to our conventions of notation we let* $E_{ji} = E_{ij}$, $E_{ijk} = E_{ikj} = \ldots$
- *For* $i \neq j$, $\varphi_{ij} : E_i \to E_{ij}$ *is a localization morphism at* S_j *(see in* $\mathbf{A}_i$*).*
- *For* $i \neq k$, $j \neq k$ *and* $i < j$, $\varphi_{ijk} : E_{ij} \to E_{ijk}$ *is a localization morphism at* S_k *(seen in* $\mathbf{A}_{ij}$*).*

$$\begin{tikzcd}
E_i \arrow[d, "\varphi_{ij}"'] \arrow[dr, "\varphi_{ik}"] & E_j \arrow[dl, "\varphi_{ji}"] \arrow[dr, "\varphi_{jk}"'] & E_k \arrow[dl, "\varphi_{ki}"'] \arrow[d, "\varphi_{kj}"] \\
E_{ij} \arrow[dr, "\varphi_{ijk}"'] & E_{ik} \arrow[d, "\varphi_{ikj}"] & E_{jk} \arrow[dl, "\varphi_{jki}"] \\
& E_{ijk} &
\end{tikzcd}$$

Then, if $\big(E,(\varphi_i)_{i\in[\![1..n]\!]}\big)$ is the limit of the diagram, we have the following results.

1. *Each morphism $\varphi_i : E \to E_i$ is a localization morphism at S_i.*
2. *The system $(\underline{S})$ is twice E-regular.*
3. *The system $\big(E,(\varphi_i)_{i\in[\![1..n]\!]}\big)$ is, up to unique isomorphism, the unique system $\big(F,(\psi_i)_{i\in[\![1..n]\!]}\big)$ with the $\psi_i \in \mathrm{L}_{\mathbf{A}}(F,E_i)$ satisfying the following items:*
   - *the diagram is commutative,*
   - *each ψ_i is a localization morphism at S_i,*
   - *the system $(\underline{S})$ is twice F-regular.*

D *1.* This property is valid with no hypothesis on the considered system of monoids (see the proof of the local-global principle 4.4).

2. Consider some $s_i \in S_i$ and a sequence $(\boldsymbol{x}_i)_{i\in[\![1..n]\!]}$ in E proportional to $(s_i)_{i\in[\![1..n]\!]}$. Let $\boldsymbol{x}_i = (x_{i1},\dots,x_{in})$. The proportionality of the two sequences means that $s_i x_{jk} = s_j x_{ik}$ in E_k for all i, j, k. Let $\boldsymbol{x} = (\frac{x_{ii}}{s_i})_{i\in[\![1..n]\!]}$. Next we prove that $s_i\boldsymbol{x} = \boldsymbol{x}_i$, i.e. $s_i\frac{x_{jj}}{s_j} = x_{ij}$ in each E_j. Indeed, this results from the equality of proportionality $s_i x_{jk} = s_j x_{ik}$ for $k = j$.

3. Since E is the limit of the diagram, there is a unique $\mathbf{A}$-linear map $\psi : F \to E$ such that $\psi_i = \varphi_i \circ \psi$ for all i.
Actually we have $\psi(y) = \big(\psi_1(y),\dots,\psi_n(y)\big)$.
Let us first show that ψ is injective. If $\psi(y) = 0$, all the $\psi_i(y)$'s are null, and since ψ_i is a localization morphism at S_i, there exist some $s_i \in S_i$ such that $s_i y = 0$. Since $(\underline{S})$ is an F-regular system, we have $y = 0$.
As ψ is injective we can suppose that $F \subseteq E$ and $\psi_i = \varphi_i|_F$.
In this case showing that ψ is bijective comes down to showing that $F = E$.
Let $\boldsymbol{x} \in E$. As ψ_i and φ_i are two localization morphisms at S_i, there are $u_i \in S_i$ such that $u_i\boldsymbol{x} \in F$. Since $(\underline{S})$ is twice F-regular, and since the sequence of the $u_i\boldsymbol{x}$'s is proportional to the sequence of the u_i's, there exists some $y \in F$ such that $u_i\boldsymbol{x} = u_i y$ for every i, so $y = \boldsymbol{x} \in F$. □

Exercises and problems

Exercise 1. Let $S_1, \ldots, S_n$, S be monoids of $\mathbf{A}$ such that S is contained in the saturated monoid of each S_i. The following properties are equivalent.

1. The S_i's cover S.

2. The S_i's are comaximal in $\mathbf{A}_S$.

Exercise 2. Let I be an ideal and U be a monoid of $\mathbf{A}$. Let $S = \mathcal{S}(I, U)$.

1. In $\mathbf{A}_S$, the monoid $\mathcal{S}(I; U, a)$ is equivalent to $\mathcal{S}(I; a) = I + a^{\mathbb{N}}$.

2. In $\mathbf{A}_S$, the monoid $\mathcal{S}(I, a; U)$ is equivalent to $\mathcal{S}(a; 1) = 1 + \langle a \rangle$.

Exercise 3. Give a proof of Lemma 1.5 based on the previous two exercises.

Exercise 4. Let $\mathbf{A}$ be a ring.

1. For $a_1, \ldots, a_n$ in $\mathbf{A}$, if $a_1 \cdots a_n \in \operatorname{Rad} \mathbf{A}$, the monoids $1 + \langle a_i \rangle$ are comaximal.

2. If $\mathfrak{a}_1, \ldots, \mathfrak{a}_\ell$ are ideals of $\mathbf{A}$, the monoids $1 + \mathfrak{a}_i$ cover the monoid $1 + \prod_i \mathfrak{a}_i$.

Exercise 5. *(In accordance with the definition of the prime ideals, if a product of factors is in a potential prime ideal, we can open branches of computation in each of which at least one of the factors is in the new potential prime ideal)*

We reuse the notations of Definition 1.4. Consider two subsets I and U of $\mathbf{A}$ and the corresponding monoid $\mathcal{S}(I, U)$. Let $a_1, \ldots, a_k \in \mathbf{A}$ for which we have

$$\prod_{i=1}^{k} a_i \in \langle I \rangle_{\mathbf{A}_{\mathcal{S}(I,U)}}.$$

1. Show that the monoids $\mathcal{S}(I \cup \{a_i\}, U)$ cover the monoid $\mathcal{S}(I, U)$.

2. If we have $a_i - a_j \in \mathcal{S}(I, U)$, then a_j is invertible in $\mathbf{A}_{\mathcal{S}(I \cup \{a_i\}, U)}$.

3. Suppose that for each $j \in [\![1..k]\!]$, we have an automorphism of $\mathbf{A}$ that fixes the monoid $\mathcal{S}(I, U)^{\mathrm{sat}}$ and that sends a_1 to a_j, and that each of the $\mathbf{A}_{\mathcal{S}(I \cup \{a_i\}, U)}$'s is trivial, then $\mathbf{A}_{\mathcal{S}(I,U)}$ is trivial.

Exercise 6. Let $S = (S_1, \ldots, S_n)$ be a family of monoids of $\mathbf{A}$.

1. Consider the family S' obtained from S by repeating each S_i a certain number of times (at least once)

$$S' = (S_1, S_1, \ldots, S_2, S_2, \ldots, S_n, S_n, \ldots)$$

Show that S is a family of comaximal monoids of $\mathbf{A}$ if and only if the same goes for S'.

2. Consider a second family $U = (U_1, \ldots, U_m)$ of monoids of $\mathbf{A}$. Suppose that for each $i \in [\![1..n]\!]$, there exists a $j \in [\![1..m]\!]$ such that $S_i \subseteq U_j$ and for each $j \in [\![1..m]\!]$ there exists an $i \in [\![1..n]\!]$ such that $U_j \supseteq S_i$. Show that if U is a family of comaximal monoids of $\mathbf{A}$, the same goes for S.

Exercise 7. *(Variation on the local Kronecker's theorem, page 811)*
To solve the exercise, we observe that the desired result is a "quasi-global" statement that we can obtain by rereading the proof of the local Kronecker's theorem. Let $x_0, \dots, x_d \in \mathbf{A}$ and $\mathfrak{a} = \mathrm{D}_{\mathbf{A}}(x_0, \dots, x_d)$. If $\mathsf{Kdim}\,\mathbf{A} \leqslant d$ and $\mathsf{Kdim}\,\mathbf{A}/\mathfrak{a} \leqslant 0$, there exist some elements $s_0, \dots, s_d \in \mathbf{A}$ and some ideals $\mathfrak{b}_0, \dots, \mathfrak{b}_d$, each generated by d elements, such that[6]

$$(s_0, \dots, s_d) \text{ is a f.s.o.i. of } \mathbf{A}/\mathfrak{a} \quad \text{and} \quad \forall i, \quad s_i\mathfrak{a} \subseteq \sqrt{\mathfrak{b}_i} \subseteq \mathfrak{a}$$

(locally, $\mathfrak{a}$ is maximal and radically generated by d elements).

Exercise 8. *(Second variation on the local Kronecker's theorem)*
Let $\mathbf{A}$ be a ring and $\mathfrak{a}$ be a finitely generated ideal. If $\mathsf{Kdim}\,\mathbf{A}/\mathfrak{a} \leqslant 0$ and $\mathsf{Kdim}\,\mathbf{A}_{1+\mathfrak{a}} \leqslant d$, there exist some elements $s_0, \dots, s_d \in \mathbf{A}$ and some ideals $\mathfrak{b}_0, \dots, \mathfrak{b}_d \subseteq \mathfrak{a}$, each generated by d elements, such that

$$(s_0, \dots, s_d) \text{ is a s.f.i.o. of } \mathbf{A}/\mathfrak{a} \quad \text{and} \quad \forall i, \quad s_i\mathfrak{a} \subseteq \sqrt{\mathfrak{b}_i}.$$

Exercise 9. Given the concrete patching principle of the modules (concrete local-global principle 4.4), and given the canonical isomorphism

$$\big(\mathrm{L}_{\mathbf{A}}(M, N)\big)_S \to \mathrm{L}_{\mathbf{A}_S}(M_S, N_S)$$

in the case of finitely presented modules (Proposition V-9.3), we have local characterizations for the determinant of a finitely generated projective module and that of a homomorphism between finitely generated projective modules (see Exercise X-19).

1. The module $\det(M)$ is characterized up to unique isomorphism by the following property: if $s \in \mathbf{A}$ is such that M_s is free, then $\det(M)_s \simeq \det(M_s)$, with compatible isomorphisms when we make a more advanced localization.[7]

2. If $\varphi\ : M \to N$ is a homomorphism of $\mathbf{A}$-finitely generated projective modules, the homomorphism $\det(\varphi)$ is characterized by the following property: if $s \in \mathbf{A}$ is such that M_s and N_s are free, then $\det(\varphi)_s = \det(\varphi_s)$ (modulo the canonical isomorphisms).

Exercise 10. Let $n \geqslant 3$, s_1, s_2 be two comaximal elements of $\mathbf{A}$. We propose to concretely patch two finitely generated projective modules P_1 and P_2 respectively defined over $\mathbf{A}_{s_1}$ and $\mathbf{A}_{s_2}$ which have isomorphic extensions to $\mathbf{A}_{s_1s_2}$. By using the enlargement lemma, we can suppose that they are images of projection matrices F_1 and F_2 over $\mathbf{A}_{s_1s_2}$ conjugated by means of a product of elementary matrices.

1. Let $E \in \mathbb{E}_n(\mathbf{A}_{s_1s_2})$. Show that there exists an $E_1 \in \mathbb{E}_n(\mathbf{A}_{s_1})$ and $E_2 \in \mathbb{E}_n(\mathbf{A}_{s_2})$ such that $E = E_1E_2$ over $\mathbf{A}_{s_1s_2}$.

2. Let $F_1 \in \mathbb{M}_n(\mathbf{A}_{s_1})$ and $F_2 \in \mathbb{M}_n(\mathbf{A}_{s_2})$ be two projection matrices over $\mathbf{A}_{s_1s_2}$ conjugated by means of a matrix $E \in \mathbb{E}_n(\mathbf{A}_{s_1s_2})$. What to do?

[6] f.s.o.i.: fundamental system of orthogonal idempotents.

[7] This precisely means: if $s'' = ss'$, then the isomorphism $(\det(M))_{s''} \simeq \det(M_{s''})$ is given by the localization of the isomorphism $(\det(M))_s \simeq \det(M_s)$.

Exercise 11. *(Contrapositive McCoy's theorem, distressing version)*
Let $\mathbf{A}$ be a nontrivial discrete ring and $M \in \mathbf{A}^{m\times n}$ be a matrix.

1. If $\mathcal{D}_n(M)$ is faithful, M is injective.
2. If we know an integer $k < n$ and some nonzero $x \in \mathbf{A}$, such that
$$x\mathcal{D}_{k+1}(M) = 0 \text{ and } \mathcal{D}_k(M) \text{ is faithful,}$$
then we can construct a nonzero vector in the kernel of M.

Exercise 12. *(Contrapositive McCoy's theorem, digestible version)*
Let $\mathbf{A}$ be a nontrivial discrete coherent ring and $M \in \mathbf{A}^{m\times n}$ be a matrix.

1. Either $\mathcal{D}_n(M)$ is faithful, and M is injective.
2. Or we can construct in the kernel of M a vector with at least a coordinate in $\mathbf{A}^*$.

Exercise 13. We notice that some definitions of depth 1 and of depth 2 are given in terms that do not make the additive structure of the considered ring intervene, but only its multiplicative structure, i.e. the monoid $(\mathbf{A}, \times, 1)$.

As the statement of Lemma 9.3 does not make use of the additive structure either, we can hope for a purely multiplicative proof of this lemma. The inspection of the proof given in the course shows that this is not the case. We therefore propose to the reader to find a proof of Lemma 9.3 which works for any monoid.

Problem 1. *(Avoiding the prime ideals)*
In this problem, we examine how to constructively decrypt a classical proof that uses as a basis tool "go see what happens in the fields $\mathrm{Frac}(\mathbf{A}/\mathfrak{p})$ for all the prime ideals $\mathfrak{p}$ of $\mathbf{A}$."

1. Let t be an indeterminate and a, b, c_1, ..., $c_n \in \mathbf{A}$ such that $(at+b, c_1, \ldots, c_n)$ is a unimodular vector over $\mathbf{A}[t, t^{-1}]$. We want to show that $ab \in \mathrm{D}_{\mathbf{A}}(c_1, \ldots, c_n)$. The following proof, typical in classical mathematics, uses **LEM** and the axiom of choice. If $ab \notin \mathrm{D}_{\mathbf{A}}(c_1, \ldots, c_n)$, there exists a prime ideal $\mathfrak{p}$ with $c_i \in \mathfrak{p}$ for $i \in [\![1..n]\!]$ and $ab \notin \mathfrak{p}$. Over the field $\mathbf{K} = \mathrm{Frac}(\mathbf{A}/\mathfrak{p})$, since $\overline{a}$ is nonzero, the equation $at + b = 0$ has a unique solution $t = -\overline{b}/\overline{a}$, which is nonzero because $\overline{b}$ is nonzero; we can then define a morphism $\varphi : \mathbf{A}[t, t^{-1}] \to \mathbf{K}$ by $t \mapsto -\overline{b}/\overline{a}$; φ transforms the unimodular vector $(at + b, c_1t, \ldots, c_nt)$ into the null vector of $\mathbf{K}^{n+1}$. A contradiction.
What do you think?

2. If $\mathbf{B}$ is a reduced ring describe the units of $\mathbf{B}[t, 1/t]$.
We will be able to show that if p, $q \in \mathbf{B}[t]$ satisfies $pq = t^m$ (with $p = \sum_k p_k t^k$ and $q = \sum_k q_k t^k$), then $1 \in \mathrm{c}(p)$, $1 \in \mathrm{c}(q)$ and
$$p_k p_\ell = q_k q_\ell = 0 \text{ if } k \neq \ell, \quad p_k q_\ell = 0 \text{ if } k + \ell \neq m, \quad p_i = q_i = 0 \text{ if } i > m.$$
Consequently, for $k \in [\![0..m]\!]$, $\langle p_k \rangle$ is generated by some idempotent e_k. We then have a fundamental system of orthogonal idempotents available $(e_0, \ldots, e_m)$ in $\mathbf{B}$ such that $\langle e_k \rangle = \langle p_k \rangle = \langle q_{m-k} \rangle$ for $k \in [\![0..m]\!]$ and
$$e_k p = e_k p_k t^k, \; e_k q = e_k q_{m-k} t^{m-k} \; \text{ and } \; e_k = e_k p_k q_{m-k}.$$

The result is clear when the ring is integral, so the reflex in classical mathematics is to use some prime ideals. A possible solution to constructively decrypt this reasoning is to use the formal Nullstellensatz (Theorem III-9.9).

Some solutions, or sketches of solutions

Exercise 1.
2 $\Rightarrow$ *1.* Let $s_1, \ldots, s_n$ with $s_i \in S_i$. We want b_i's $\in \mathbf{A}$ such that $b_1 s_1 + \cdots + b_n s_n \in S$. The fact that the S_i's are comaximal in $\mathbf{A}_S$ provides an $s \in S$ and some a_i's $\in \mathbf{A}$ such that $a_1 s_1 + \cdots + a_n s_n = s$ in $\mathbf{A}_S$; therefore there exists a $t \in S$ such that, in $\mathbf{A}$, $(ta_1)s_1 + \cdots + (ta_n)s_n = ts \in S$.

Exercise 2.
1. An element s of $\mathcal{S}(I; U, a)$ is of the form $x + ua^k$. We see that s divides the element $xu^{-1} + a^k \in \mathcal{S}(I; a)$ in $\mathbf{A}_S$.

2. An element s of $\mathcal{S}(I, a; U)$ is of the form $x + ya + u$. Let $x' = u^{-1}x$ and $y' = u^{-1}$. Then s divides in $\mathbf{A}_S$ the element $x' + y'a + 1$, which divides $1 + y''a$, where $y'' = (1 + x')^{-1}y'$.

Exercise 3. Let $S = \mathcal{S}(I, U)$, $S_1 = \mathcal{S}(I; U, a)$ and $S_2 = \mathcal{S}(I, a; U)$. We must prove that S_1 and S_2 are comaximal in $\mathbf{A}_S$. In $\mathbf{A}_S$, S_1 is equivalent to $I + a^{\mathbb{N}}$, and S_2 is equivalent to $1 + \langle a \rangle$. Let us use the following identity

$$y^k(x + a^k) + \left(\textstyle\sum_{j<k} y^j a^j\right)(1 - ya) = y^k(x + a^k) + 1 - y^k a^k = 1 + y^k x.$$

Applied to $x \in I$, it proves that $x + a^k$ and $1 - ya$ are comaximal in $\mathbf{A}_S$ (since $1 + y^k x \in 1 + I$ and since I is contained in the radical of $\mathbf{A}_S$).

Exercise 4. *1.* For $j \in [\![1..n]\!]$ let $b_j = 1 - a_j x_j$ in the monoid $1 + a_j\mathbf{A}$. Let $a = \prod_i a_i$. We must show that the ideal $\mathfrak{m} = \langle b_1, \ldots, b_n \rangle$ contains 1. However, modulo $\mathfrak{m}$ we have $1 = a_j x_j$, therefore $1 = a \prod_i x_i = ax$. Thus $1 - ax \in \mathfrak{m}$, but $1 - ax \in \mathbf{A}^{\times}$ because $a \in \operatorname{Rad} \mathbf{A}$.

2. It is clear that $S = 1 + \prod_i \mathfrak{a}_i \subseteq 1 + \mathfrak{a}_j = S_j$ for each j. We must therefore prove (Exercise 1) that the $1 + \mathfrak{a}_j$ given in $\mathbf{A}_S$ are comaximal. However, the product $\prod_i \mathfrak{a}_i$, seen in $\mathbf{A}_S$, is in $\operatorname{Rad} \mathbf{A}_S$. Therefore it suffices to apply item *1.*

Exercise 5. The hypothesis means that we have a $u \in \mathcal{M}(U)$ and a $j \in \langle I \rangle_{\mathbf{A}}$ such that $(u + j) \prod_{i=1}^k a_i \in \langle I \rangle_{\mathbf{A}}$, or $u \prod_{i=1}^k a_i \in \langle I \rangle_{\mathbf{A}}$.

1. First solution, by direct computation.

Consider $x_i \in S_i = \mathcal{S}(I \cup \{a_i\}, U)$ and look for a linear combination which is in $S = \mathcal{S}(I, U)$. For each i we write

$$x_i = u_i + j_i + a_i z_i \text{ with } u_i \in \mathcal{M}(U),\ j_i \in \langle I \rangle_{\mathbf{A}} \text{ and } z_i \in \mathbf{A}.$$

In the product

$$u \prod_{i=1}^k (x_i - (u_i + j_i)) = u \prod_{i=1}^k a_i z_i \in \langle I \rangle_{\mathbf{A}},$$

we re-express the left-hand side in the form

$$\sum_{i=1}^k c_i x_i \pm u \prod_{i=1}^k (u_i + j_i)$$

and we obtain, by moving $\pm u \prod_{i=1}^k (u_i + j_i)$ to the right-hand side, the desired membership $\sum_{i=1}^k c_i x_i \in \mathcal{S}(I, U)$.

Second solution, conceptual.
It is clear that $S \subseteq S_i$. It therefore suffices (Exercise 1) to show that the S_i's are comaximal in $\mathbf{A}_S$. In $\mathbf{A}_S$, (Exercise 2) the monoids S_i and $1 + \langle a_i \rangle$ have the same saturated monoid. It therefore suffices to see that the monoids $1 + \langle a_i \rangle$ are comaximal in $\mathbf{A}_S$. Moreover, we know that, seen in $\mathbf{A}_S$, I is contained in $\mathrm{Rad}(\mathbf{A}_S)$. We therefore apply item *1* of Exercise 4.

2. Clear since $a_j \in \mathcal{S}(I, U) + \langle a_i \rangle \subseteq \mathcal{S}(I \cup \{a_i\}, U)$.

3. If one of the $\mathbf{A}_{S_i}$'s is trivial, all of them are also trivial because they are pairwise isomorphic. Since the S_i's cover S, $\mathbf{A}_S$ is itself trivial.

Exercise 6. *1.* It suffices to show it for $S' = (S_1, S_1, S_2, \ldots, S_n)$.
Suppose that the family S is comaximal. Let s_1', $s_1'' \in S_1$, and $s_i \in S_i$ for $i \in [\![2..n]\!]$. The elements $s_1's_1''$, s_2, …, s_n are comaximal, and since $s_1's_1'' \in \langle s_1', s_1'' \rangle$, the same goes for s_1', s_1'', s_2, …, s_n. In the other direction, suppose that S' is comaximal and let $s_i \in S_i$ for $i \in [\![1..n]\!]$; then s_1, s_1, s_2, …, s_n are comaximal therefore the same goes for s_1, s_2, …, s_n.

2. By repeating some of the S_i's and the U_j's, we obtain two families S', U' of monoids of $\mathbf{A}$, indexed by the same interval $[\![1..p]\!]$ and satisfying $S_k' \subseteq U_k'$ for $k \in [\![1..p]\!]$. Since U is comaximal, the same goes for U' so for S' then for S.

Exercise 7. As $\mathsf{Kdim}\,\mathbf{A} \leqslant d$, there exists a sequence $(\underline{a}) = (a_0, \ldots, a_d)$ complementary to $(\underline{x}) = (x_0, \ldots, x_d)$. Therefore (disjoint sequences), for every $i \leqslant d$, we have

$$\mathrm{D}(a_0, \ldots, a_{i-1}, x_0, \ldots, x_{i-1}, a_i x_i) = \mathrm{D}(a_0 + x_0, \ldots, a_{i-1} + x_{i-1}).$$

As $\mathsf{Kdim}\,\mathbf{A}/\mathfrak{a} \leqslant 0$ and $\mathfrak{a} = \mathrm{D}_{\mathbf{A}}(\mathfrak{a})$, we also have $\mathbf{A} = \mathbf{A}a_i + (\mathfrak{a} : a_i)$ for all i. We then construct the triangle

$$\begin{aligned} & \mathbf{A} \\ = \; & \mathbf{A}a_0 + (\mathfrak{a} : a_0) \\ = \; & \mathbf{A}a_0 + (\mathfrak{a} : a_0)a_1 + (\mathfrak{a} : a_0)(\mathfrak{a} : a_1) \\ & \qquad \vdots \\ = \; & \mathbf{A}a_0 + (\mathfrak{a} : a_0)a_1 + \cdots + (\mathfrak{a} : a_0) \cdots (\mathfrak{a} : a_{d-1})a_d + (\mathfrak{a} : a_0) \cdots (\mathfrak{a} : a_d). \end{aligned}$$

Now, we write

$$1 = b_0 a_0 + b_1 a_1 + \cdots + b_d a_d + t$$

with $b_i \in (\mathfrak{a} : a_0) \cdots (\mathfrak{a} : a_{i-1})$ and $t \in (\mathfrak{a} : a_0) \cdots (\mathfrak{a} : a_d)$. For $i \leqslant d$, on the one hand we have

$$\begin{aligned} b_i \langle x_0, \ldots, x_{i-1} \rangle & \subseteq \mathrm{D}\big(b_i(a_0 + x_0), \ldots, b_i(a_{i-1} + x_{i-1})\big) \\ & \subseteq \mathrm{D}(b_i a_0, x_0, \ldots, b_i a_{i-1}, x_{i-1}) \subseteq \mathrm{D}(\mathfrak{a}) = \mathfrak{a}, \end{aligned}$$

and on the other hand

$$\begin{aligned} b_i a_i x_i & \in b_i \mathrm{D}(a_0 + x_0, \ldots, a_{i-1} + x_{i-1}) \\ & \subseteq \mathrm{D}\big(b_i(a_0 + x_0), \ldots, b_i(a_{i-1} + x_{i-1})\big) \subseteq \mathfrak{a}. \end{aligned}$$

Now let $s_i = b_i a_i$. Thus we reach

$$s_i \langle x_0, \ldots, x_{i-1}, x_i\rangle \subseteq \mathrm{D}\big(b_i(a_0 + x_0), \ldots, b_i(a_{i-1} + x_{i-1})\big) \subseteq \mathfrak{a},$$

then

$$\begin{aligned} & s_i \langle x_0, \ldots, x_{i-1}, x_i, x_{i+1}, \ldots, x_d\rangle \subseteq \\ & \mathrm{D}\big(\underbrace{b_i(a_0+x_0), \ldots, b_i(a_{i-1}+x_{i-1}), s_i x_{i+1}, \ldots, s_i x_d}_{\text{generate } \mathfrak{b}_i \text{ (def.)}}\big) \subseteq \mathfrak{a}. \end{aligned}$$

Therefore there exists an ideal $\mathfrak{b}_i$ generated by d elements satisfying

$$s_i\mathfrak{a} \subseteq \mathrm{D}(s_i\mathfrak{a}) \subseteq \mathrm{D}(\mathfrak{b}_i) \subseteq \mathfrak{a}.$$

We end the proof by using $1 \in \langle a_d, x_d\rangle$. We get

$$t \in t\,\langle a_d, x_d\rangle \subseteq \langle ta_d, x_d\rangle \subseteq \mathfrak{a},$$

so much so that the sum of the s_i's is equal to 1 mod $\mathfrak{a}$. Moreover, for $i > j$,

$$s_i s_j \in b_i a_j \mathbf{A} \subseteq \mathfrak{a},$$

which allows us to conclude that $(s_0, \ldots, s_d)$ is a fundamental system of orthogonal idempotents of $\mathbf{A}/\mathfrak{a}$.

Exercise 8. To begin with, Kronecker's theorem gives that $\sqrt{\mathfrak{a}}$ is radically generated by $d + 1$ elements. Next we apply the result of Exercise 7 to $\sqrt{\mathfrak{a}}$ in the localized ring $(1 + \mathfrak{a})^{-1}\mathbf{A}$. This provides some s_i's forming a fundamental system of orthogonal idempotents modulo $\sqrt{\mathfrak{a}}$ and some $\mathfrak{b}_i \subseteq \sqrt{\mathfrak{a}}$. Even if it entails taking multiples of powers of the s_i's, we can impose that $(s_0, \ldots, s_d)$ is a fundamental system of orthogonal idempotents of $\mathbf{A}/\mathfrak{a}$. Even if it entails taking powers of the generators of the $\mathfrak{b}_i$'s, we can impose $\mathfrak{b}_i \subseteq \mathfrak{a}$.

Exercise 10. *1.* [Lam06, page 208 Proposition 1.14].

2. We have $F_1E = EF_2$. We write $E = E_1E_2$, so $F_1E_1E_2 = E_1E_2F_2$ and

$$\widetilde{E_1}F_1E_1 =_{\mathbf{A}_{s_1s_2}} E_2F_2\widetilde{E_2}.$$

The matrix $\widetilde{E_1}F_1E_1$ (resp. $E_2F_2\widetilde{E_2}$) is a projection matrix over $\mathbf{A}_{s_1}$ (resp. over $\mathbf{A}_{s_2}$) because $\widetilde{E_1}E_1 = \mathrm{I}_n$ (resp. $\widetilde{E_2}E_2 = \mathrm{I}_n$). By the local-global principle of patching of the elements in a module (here $\mathbb{M}_n(\mathbf{A})$), there exists a unique matrix $F \in \mathbb{M}_n(\mathbf{A})$ which is equal to $\widetilde{E_1}F_1E_1$ over $\mathbf{A}_{s_1}$ and to $E_2F_2\widetilde{E_2}$ over $\mathbf{A}_{s_2}$. To prove that $F^2 = F$, it suffices to prove it over $\mathbf{A}_{s_1}$ and $\mathbf{A}_{s_2}$. Let $P = \mathrm{Im}\,F \subseteq \mathbf{A}^n$.
By construction, for $i = 1, 2$

$$P_{s_i} =_{\mathbf{A}^n_{s_i}} \mathrm{Im}\,F_{s_i} \simeq_{\mathbf{A}^n_{s_i}} \mathrm{Im}\,F_i \simeq_{\mathbf{A}^n_{s_i}} P_i.$$

Exercise 11. *(Contrapositive McCoy's theorem, distressing version)*

1. Already seen.

2. We have $x \neq 0$, $\mathcal{D}_k(M)$ is faithful and the ring is discrete, therefore there exists a minor μ of order k of M such that $x\mu \neq 0$. Suppose for example that μ is the north-west minor and let C_1, …, C_{k+1} be the first columns of M, let μ_i ($i \in [\![1..k]\!]$) be the suitably signed determinants of the matrices extracted on the rows $[\![1..k]\!]$ and the previous columns, except the column of index $i + 1$. Then the Cramer formulas give the equality $\sum_{i=1}^{k} x\mu_i C_i + x\mu C_{k+1} = 0$. As $x\mu \neq 0$, this gives a nonzero vector in the kernel of M.

Comment. In classical mathematics, if $\mathcal{D}_n(M)$ is not faithful, as $\mathcal{D}_0(M) = \langle 1 \rangle$ is faithful, there exists some $k < n$ such that $\mathcal{D}_k(M)$ is faithful and $\mathcal{D}_{k+1}(M)$ is not faithful. Still in classical mathematics, if $\mathcal{D}_{k+1}(M)$ is not faithful, there exists some $x \neq 0$ such that $x\mathcal{D}_{k+1}(M) = 0$. For these things to become explicit, we need for example to dispose of a test for the faithulness of the finitely generated ideals, in a very strong sense. ∎

Exercise 12. *(Contrapositive McCoy's theorem, digestible version)*
Since the determinantal ideals are finitely generated ideals, and the ring is coherent, their annihilators are also finitely generated ideals, and we can test the nullity of a finitely generated ideal because the ring is discrete. The hypotheses of Exercise 11 are therefore satisfied.
Note: The alternative "*1* or *2*" is exclusive because the ring is nonzero, this justifies the "either, ..., or" of the statement.

Problem 1. *1.* There is no miracle: a certificate for $ab \in \mathrm{D}_{\mathbf{A}}(c_1, \ldots, c_n)$ can be obtained from a certificate of unimodularity of $(at + b, c_1t, \ldots, c_nt)$ in $\mathbf{A}[t, t^{-1}]$.
By replacing $\mathbf{A}$ by $\mathbf{A}_1 = \mathbf{A}/\mathrm{D}_{\mathbf{A}}(c_1, \ldots, c_n)$, we are brought back to $\mathbf{A}$ being reduced and $c_i = 0$. The hypothesis is then $at + b$ is invertible in $\mathbf{A}[t, t^{-1}]$, and the result to be shown is $ab = 0$ (symmetric result in a, b just like the hypothesis).
We have $(at + b)g(t) = t^e$ for some $g \in \mathbf{A}[t]$ and some $e \in \mathbb{N}$, therefore the polynomial $at + b$ is primitive. To show $ab = 0$, it suffices to localize at a then at b. Over the localized ring at a, we take $t = -b/a$ in $(at+b)g(t) = t^e$, we obtain $(-b/a)^e = 0$. Thus, we have $b = 0$, then $ab = 0$. By symmetry, we obtain in $\mathbf{A}_b$, $a = 0$ so $ab = 0$.
Actually, if $ua + vb = 1$, the ring $\mathbf{A}_1$ is split in two by the idempotent ua. In the first component, $at + b = a$ with a invertible, in the second, $at + b = b$ with b invertible.

2. In classical mathematics: if we pass to the quotient by a prime ideal the result is clear. By continuity, the spectrum is partitioned into a finite number of open sets corresponding to the coveted fundamental system of orthogonal idempotents. A constructive proof is given in [199, Yengui]. The reader will also be able to draw from the proof of item *1.*
A method that we can systematically use consists in calling upon the formal Nullstellensatz (Theorem III-9.9).
In the current case, we note that the problem comes down to proving that the p_kp_ℓ's are null for $k \neq \ell$ and that the p_{m+r}'s null for $r > 0$. Once this is observed, since the p_k's are comaximal, we obtain a fundamental system of orthogonal idempotents $(e_0, \ldots, e_m)$ such that $e_kp = e_kp_kt^k$ for all k, from which the result follows.
The philosophy is the following: if we take all the coefficients of the problem as indeterminates over $\mathbb{Z}$, the hypothesis comes down to passing to the quotient by the radical $\mathfrak{a}$ of a finitely generated ideal, which represents the hypotheses. The goal is then to prove that the conclusions are also in $\mathfrak{a}$. For this it suffices to prove that it is indeed the case when we evaluate the problem in an arbitrary finite field. Here the indeterminates are p_0, ..., p_n, q_0, ..., q_n.

For $p = \sum_{k=0}^{n} p_k t^k$ and $q = \sum_{k=0}^{n} q_k t^k$; we define the polynomial

$$\sum r_j t^j \overset{\text{def}}{=} pq - t^m$$

(with all $r_j \in \mathbb{Z}[p_0, \ldots, p_n, q_0, \ldots, q_n]$) and the ideal $\mathfrak{a}$ is $\mathrm{D}(r_0, \ldots, r_{2n})$. We will show that the $p_k p_\ell$'s and $q_k q_\ell$'s are in $\mathfrak{a}$ if $k \neq \ell$, that the $p_k q_\ell$'s are in $\mathfrak{a}$ for $k + \ell \neq m$ and that the p_{m+r}'s and q_{m+r}'s are in $\mathfrak{a}$ for $r > 0$.
However, this directly results from item *2* in the formal Nullstellensatz (or then from item *4* in Corollary III-9.10).
In geometric terms: if $n \geqslant m$, the variety of the zeros of $pq - t^m$ over a field $\mathbf{K}$ is a space formed of $m + 1$ copies of $\mathbf{K}^\times$ isolated from one another; over a reduced ring the response is fundamentally the same, but the isolated components in the case of the fields here make a fundamental system of orthogonal idempotents appear.

Thus, the formal Nullstellensatz (Theorem III-9.9) provides a constructive method to decrypt the hidden algorithms in certain reasonings from classical mathematics, when the argument consists in seeing what happens in all the $\mathrm{Frac}(\mathbf{A}/\mathfrak{p})$'s for all the prime ideals of $\mathbf{A}$.

Bibliographic comments

The dynamic method as it is explained in the local-global machinery with prime ideals (Section 5) consists for the most part in flattening the computations implied by the *method of dynamic evaluation* given in [127, Lombardi], a successor of the dynamic method implemented in [54, Coste&al.] for proofs of the Nullstellensatz type, itself a successor of the dynamic evaluation à la D5 in Computer Algebra [58, Duval&al.]. With respect to what is proposed in [54, 127], the difference in the previous chapter is mainly that we have avoided the reference to formal logic.

In classical mathematics, we find the concrete patching principle of the finitely generated projective modules (item *4* of the local-global principle 2.2) for example in [Knight, Proposition 2.3.5 and Lemma 3.2.3] (with an almost entirely constructive proof) and in [Kunz, rule 1.14 of Chapter IV].

The constructive treatment of Suslin's lemma 6.1 is due to Ihsen Yengui [202], who gives the key to the local-global machinery with maximal ideals.

The local-global machinery with minimal prime ideals is due to Thierry Coquand [36, On seminormality].

Exercises 7 and 8 are due to Lionel Ducos [69].

The dynamic method was applied for the computation of "dynamic Gröbner bases" by Yengui in [200].

Chapter XVI

Extended projective modules

Contents

Introduction

In this chapter we constructively establish a few important results regarding the situations where the finitely generated projective modules over a polynomial ring are extended from the base ring.

We especially treat Traverso-Swan's theorem (Section 2), the patching à la Vaserstein-Quillen (Section 3), Horrocks' theorems (Section 4), Quillen-Suslin's theorem (Section 5), and in Section 6, Bass' theorem (Theorem 6.2) and the Lequain-Simis theorem (Theorem 6.16).

1. Extended modules

Given an algebra $\mathbf{A} \xrightarrow{\rho} \mathbf{B}$, the scalar extension from $\mathbf{A}$ to $\mathbf{B}$ transforms a module M over $\mathbf{A}$ into a module $\rho_\star(M) \simeq \mathbf{B} \otimes_\mathbf{A} M$ over $\mathbf{B}$. Recall that a $\mathbf{B}$-module isomorphic to such a module $\rho_\star(M)$ is said to be extended from $\mathbf{A}$. We also say that it comes from the $\mathbf{A}$-module M by scalar extension.

In the case of a finitely presented module, from the point of view of the presentation matrices, this corresponds to considering the matrix transformed by the homomorphism ρ.

A necessary condition for a finitely presented module to be extended is that its Fitting ideals are of the form $\rho(\mathfrak{a}_i)\mathbf{B}$ for finitely generated ideals $\mathfrak{a}_i$ of $\mathbf{A}$. This condition is realized for the finitely generated projective modules if and only if the idempotents of $\mathbf{B}$ are all images of idempotents of $\mathbf{A}$.

The problem of the extension

For the finitely generated projective modules, the following problem arises naturally given the morphism $\mathsf{GK}_0\, \rho : \mathsf{GK}_0\, \mathbf{A} \to \mathsf{GK}_0\, \mathbf{B}$.

Problem no. 1. Does every finitely generated projective module over $\mathbf{B}$ come from a finitely generated projective module over $\mathbf{A}$? Or yet again: is $\mathsf{GK}_0\, \rho$ surjective?

Recall that $\mathsf{GK}_0\, \mathbf{A}_{\mathrm{red}} = \mathsf{GK}_0\, \mathbf{A}$ and $\mathsf{GK}_0\, \mathbf{B}_{\mathrm{red}} = \mathsf{GK}_0\, \mathbf{B}$, such that the problem of the extension of the finitely generated projective modules can be narrowed down to the case of reduced rings. Moreover, if $\mathsf{H}_0\, \rho : \mathsf{H}_0\, \mathbf{A} \to \mathsf{H}_0\, \mathbf{B}$ is not surjective, the answer to problem no. 1 is negative "for the wrong reason" and the following problem is then more natural.

Problem no. 2. Does every projective module of constant rank over $\mathbf{B}$ come from a finitely generated projective module over $\mathbf{A}$?

For the finitely presented modules the natural generalization of the previous problem is then the following.

Problem no. 3. Does every finitely presented module over $\mathbf{B}$ whose Fitting ideals are extensions of finitely generated ideals of $\mathbf{A}$ come from a finitely presented module over $\mathbf{A}$?

The case of the polynomial rings

Let $\mathbf{B} = \mathbf{A}[X_1, \dots, X_r] = \mathbf{A}[\underline{X}]$. If $(\underline{a}) \in \mathbf{A}^r$ we denote by $\mathrm{ev}_{\underline{a}}$ the evaluation homomorphism at $\underline{a}$

$$\mathrm{ev}_{\underline{a}} : \mathbf{B} \to \mathbf{A},\ p \mapsto p(\underline{a}).$$

The two homomorphisms $\mathbf{A} \xrightarrow{j} \mathbf{B} \xrightarrow{\mathrm{ev}_{\underline{a}}} \mathbf{A}$ are composed according to the identity.

Most of what follows in this subsection could be written in the more general context of an $\mathbf{A}$-algebra $\mathbf{B}$ possessing a character (cf. Proposition IV-2.7). For polynomial rings we obtain the following results (with an obvious intuitive notation for $M(\underline{X})$).

1.1. Fact. *With* $\mathbf{B} = \mathbf{A}[\underline{X}]$.

1. *A* $\mathbf{B}$*-module* $M = M(\underline{X})$ *is extended from* $\mathbf{A}$ *if and only if it is isomorphic to* $M(\underline{0})$*.*
2. *In particular, if* M *is finitely presented with a presentation matrix* $G(\underline{X}) \in \mathbf{B}^{q \times m}$*, Lemma IV-1.1 implies that* M *is extended from* $\mathbf{A}$ *if and only if the matrices* $H(\underline{X})$ *and* $H(\underline{0})$*, where* H *is illustrated below, are equivalent over the ring* $\mathbf{B}$

$$H(\underline{X}) \ = \ \begin{array}{|c|c|c|c|c} \multicolumn{1}{c}{m} & \multicolumn{1}{c}{q} & \multicolumn{1}{c}{q} & \multicolumn{1}{c}{m} & \\ \hline G(\underline{X}) & 0 & 0 & 0 & q \\ \hline 0 & \mathrm{I}_q & 0 & 0 & q \\ \hline \end{array}$$

Remark. By Lemma IV-1.1 when the matrices $H(\underline{X})$ and $H(\underline{0})$ are equivalent, they are elementarily equivalent. ■

Regarding the finitely generated projective modules we obtain homomorphisms of semirings which are composed according to the identity

$$\mathsf{GK}_0\,\mathbf{A} \xrightarrow{\mathsf{GK}_0\,j} \mathsf{GK}_0\,\mathbf{A}[\underline{X}] \xrightarrow{\mathsf{GK}_0\,\mathrm{ev}_{\underline{a}}} \mathsf{GK}_0\,\mathbf{A}.$$

Consequently $\mathsf{GK}_0\,j$ is injective, and the phrase "every finitely generated projective module over $\mathbf{A}[\underline{X}]$ is extended from $\mathbf{A}$" means that $\mathsf{GK}_0\,j$ is an isomorphism, which we abbreviate to "$\mathsf{GK}_0\,\mathbf{A} = \mathsf{GK}_0\,\mathbf{A}[\underline{X}]$."

Similarly, for the Grothendieck rings

$$\mathsf{K}_0\,\mathbf{A} \xrightarrow{\mathsf{K}_0\,j} \mathsf{K}_0\,\mathbf{A}[\underline{X}] \xrightarrow{\mathsf{K}_0\,\mathrm{ev}_{\underline{a}}} \mathsf{K}_0\,\mathbf{A}, \quad \text{with} \quad \mathsf{K}_0(\mathrm{ev}_{\underline{a}}) \circ \mathsf{K}_0(j) = \mathrm{Id}_{\mathsf{K}_0\,\mathbf{A}}.$$

Moreover we have the following elementary results, in which each equality has the meaning that a natural morphism is an isomorphism.

1.2. Fact. *With* $\mathbf{B} = \mathbf{A}[\underline{X}]$.

1. $\mathrm{D}_{\mathbf{B}}(0) = \mathrm{D}_{\mathbf{A}}(0)\mathbf{B}$ *(a polynomial is nilpotent if and only if all its coefficients are nilpotent). In particular,* $\mathbf{B}_{\mathrm{red}} = \mathbf{A}_{\mathrm{red}}[\underline{X}]$.
2. *If* $\mathbf{A}$ *is reduced,* $\mathbf{B}^{\times} = \mathbf{A}^{\times}$. *More generally,* $\mathbf{B}^{\times} = \mathbf{A}^{\times} + \mathrm{D}_{\mathbf{A}}(0)\,\langle \underline{X} \rangle$.
3. $\mathbb{B}(\mathbf{A}) = \mathbb{B}(\mathbf{A}[\underline{X}])$ *and* $\mathsf{H}_0\,\mathbf{A} = \mathsf{H}_0\,\mathbf{A}[\underline{X}]$.
4. $\mathsf{GK}_0\,\mathbf{A} = \mathsf{GK}_0\,\mathbf{A}_{\mathrm{red}}$.
5. $\mathsf{GK}_0\,\mathbf{A} = \mathsf{GK}_0\,\mathbf{A}[\underline{X}] \iff \mathsf{GK}_0\,\mathbf{A}_{\mathrm{red}} = \mathsf{GK}_0\,\mathbf{A}_{\mathrm{red}}[\underline{X}]$.
6. $\mathsf{Pic}\,\mathbf{A} = \mathsf{Pic}\,\mathbf{B} \iff \mathsf{Pic}\,\mathbf{A}_{\mathrm{red}} = \mathsf{Pic}\,\mathbf{A}_{\mathrm{red}}[\underline{X}]$.

D *1* and *2*. See Lemma II-2.6.
3. We must show that every idempotent polynomial is constant. This is done (in a single variable) by induction on the formal degree of the polynomial.
4. This is Theorem X-5.10.
Items *5* and *6* result from items *1* and *4*. □

2. The Traverso-Swan's theorem, seminormal rings

This section is devoted to the study of the rings $\mathbf{A}$ for which the natural homomorphism from $\mathsf{Pic}\,\mathbf{A}$ to $\mathsf{Pic}\,\mathbf{A}[X_1, \ldots, X_r]$ is an isomorphism (i.e. the projective modules of constant rank 1 over $\mathbf{A}[X_1, \ldots, X_r]$ are all extended from $\mathbf{A}$). The answer is given by the Traverso-Swan-Coquand theorem ([191, 188, 36]):

Theorem (Traverso-Swan-Coquand)
The following properties are equivalent.

1. *The ring* $\mathbf{A}_{\mathrm{red}}$ *is seminormal (definition 2.5).*
2. *The natural homomorphism* $\mathsf{Pic}\,\mathbf{A} \xrightarrow{\mathsf{Pic}\,j} \mathsf{Pic}\,\mathbf{A}[X]$ *is an isomorphism.*
3. $\forall r \geqslant 1$, *the natural homomorphism* $\mathsf{Pic}\,\mathbf{A} \to \mathsf{Pic}\,\mathbf{A}[X_1, \ldots, X_r]$ *is an isomorphism.*
4. $\exists r \geqslant 1$, *the natural homomorphism* $\mathsf{Pic}\,\mathbf{A} \to \mathsf{Pic}\,\mathbf{A}[X_1, \ldots, X_r]$ *is an isomorphism.*

We will show *1* ⇒ *3* and *2* ⇒ *1*. As a corollary, $\mathbf{A}$ is seminormal if and only if $\mathbf{A}[X]$ is seminormal.

Preliminaries

First of all recall the following result (see Proposition V-2.11).

2.1. Lemma. *A projection matrix of rank* 1*,* P*, has a free image if and only if there exists a column vector* C *and a row vector* L *such that* $LC = 1$ *and* $CL = P$*. In addition,* C *and* L *are unique, up to the product by a unit, under the only condition that* $CL = P$*.*

Moreover recall that the natural morphism $\mathsf{Pic}\,\mathbf{A} \to \mathsf{Pic}\,\mathbf{A}[\underline{X}]$ is an isomorphism if and only if the natural morphism $\mathsf{Pic}\,\mathbf{A}_{\rm red} \to \mathsf{Pic}\,\mathbf{A}_{\rm red}[\underline{X}]$ is an isomorphism (Fact 1.2 *6*).

The two group homomorphisms

$$\mathsf{Pic}\,\mathbf{A} \xrightarrow{\mathsf{Pic}\,j} \mathsf{Pic}\,\mathbf{A}[\underline{X}] \xrightarrow{\mathsf{Pic}\,\mathrm{ev}_{\underline{0}}} \mathsf{Pic}\,\mathbf{A}$$

are composed according to the identity. The first is injective, the second surjective. They are isomorphisms if and only if the first is surjective, if and only if the second is injective.

This last property means: every idempotent square matrix $P(\underline{X})$ of rank 1 over $\mathbf{A}[\underline{X}]$ which satisfies "$\mathrm{Im}\,\big(P(\underline{0})\big)$ is free," satisfies "$\mathrm{Im}(P\big(\underline{X})\big)$ is free" in itself.

Actually, if $\mathrm{Im}\,\big(P(\underline{0})\big)$ is free, the matrix $\mathrm{Diag}(P(\underline{0}), 0_1)$ is similar to a standard projection matrix $\mathrm{I}_{1,n} = \mathrm{Diag}(1, 0_{n-1,n-1})$ (enlargement lemma V-2.10). Hence the following lemma.

2.2. Lemma. *The following properties are equivalent.*

1. *The natural homomorphism* $\mathsf{Pic}\,\mathbf{A} \to \mathsf{Pic}\,\mathbf{A}[\underline{X}]$ *is an isomorphism.*
2. *For every matrix* $M(\underline{X}) = (m_{i,j}) \in \mathbb{AG}_n(\mathbf{A}[\underline{X}])$ *such that* $M(\underline{0}) = \mathrm{I}_{1,n}$*, there exist* $f_1, \ldots, f_n, g_1, \ldots, g_n \in \mathbf{A}[\underline{X}]$ *such that* $m_{i,j} = f_i g_j$ *for all* i*,* j*.*

Note that the hypothesis $M(\underline{0}) = \mathrm{I}_{1,n}$ implies $\mathrm{rk}(M) = 1$ because the homomorphism $\mathsf{H}_0(\mathbf{A}[\underline{X}]) \to \mathsf{H}_0(\mathbf{A})$ is an isomorphism.

Convention. We abbreviate the statement "the natural morphism from $\mathsf{Pic}\,\mathbf{A}$ to $\mathsf{Pic}\,\mathbf{A}[\underline{X}]$ is an isomorphism" by writing: "$\mathsf{Pic}\,\mathbf{A} = \mathsf{Pic}\,\mathbf{A}[\underline{X}]$."

2.3. Lemma. *Let* $\mathbf{A} \subseteq \mathbf{B}$ *be reduced rings and* $f_1, \ldots, f_n, g_1, \ldots, g_n$ *be polynomials in* $\mathbf{B}[\underline{X}]$ *that satisfy the following properties*

$$(*) \qquad \begin{cases} f_1(\underline{0}) = g_1(\underline{0}) = 1, f_i(\underline{0}) = g_i(\underline{0}) = 0 \ \ (i = 2, \ldots, n), \\ m_{ij} \overset{\text{def}}{=} f_i g_j \in \mathbf{A}[\underline{X}] \ \ (i, j = 1, \ldots, n), \\ \sum_i f_i g_i = 1. \end{cases}$$

Under these hypotheses, the matrix $M := (m_{ij})$ *is a projection matrix of rank* 1*,* $M(\underline{0}) = \mathrm{I}_{1,n}$*, and the following properties are equivalent.*

1. *The module* $\operatorname{Im} M$ *is free over* $\mathbf{A}[\underline{X}]$*, i.e. extended from* $\mathbf{A}$*.*
2. *The* f_i*'s and the* g_i*'s are in* $\mathbf{A}[\underline{X}]$*.*
3. $f_1 \in \mathbf{A}[\underline{X}]$*.*

D *3* $\Rightarrow$ *2.* The g_j's are obtained from f_1 and from the m_{1j}'s by making divisions by non-decreasing powers, because the constant coefficient of f_1 is equal to 1. Similarly, we then obtain the f_i's from g_1 and from the m_{i1}'s. The converse implication is trivial.
2 $\Leftrightarrow$ *1.* By Lemma 2.1, the problem is to find suitable f_i's and g_j's from the matrix (m_{ij}). However, these f_i's and g_j's exist in $\mathbf{B}[\underline{X}]$, and the condition $f_1(\underline{0}) = 1$ forces their uniqueness because the rings are reduced (so the invertible elements in polynomial ring are constants). □

Lemmas 2.2 and 2.3 imply the following result.

2.4. Corollary. *Let* $\mathbf{A} \subseteq \mathbf{B}$ *be two reduced rings with* $\mathsf{Pic}\,\mathbf{B} = \mathsf{Pic}\,\mathbf{B}[\underline{X}]$*. The following properties are equivalent.*

1. $\mathsf{Pic}\,\mathbf{A} = \mathsf{Pic}\,\mathbf{A}[\underline{X}]$*.*
2. *If polynomials* $f_1, \ldots, f_n, g_1, \ldots, g_n$ *in* $\mathbf{B}[\underline{X}]$ *satisfy the conditions* $(*)$ *of Lemma 2.3, then the* f_i*'s and the* g_i*'s are in* $\mathbf{A}[\underline{X}]$*.*
3. *If polynomials* $f_1, \ldots, f_n, g_1, \ldots, g_n$ *in* $\mathbf{B}[\underline{X}]$ *satisfy the conditions* $(*)$*, then* $f_1 \in \mathbf{A}[\underline{X}]$*.*

Seminormal rings

An integral ring $\mathbf{A}$ is said to be *seminormal* if, each time that $b^2 = c^3 \neq 0$, the element $a = b/c$ of $\mathrm{Frac}(\mathbf{A})$ is actually in $\mathbf{A}$. In this case, $a^3 = b$ and $a^2 = c$.

2.5. Definition. An arbitrary ring $\mathbf{A}$ is said to be *seminormal* if each time that $b^2 = c^3$, there exists an $a \in \mathbf{A}$ such that $a^3 = b$ and $a^2 = c$.

2.6. Fact. *1. A seminormal ring is reduced.*
2. In a reduced ring, $x^2 = y^2$ *and* $x^3 = y^3$ *imply* $x = y$*.*

D *1.* If $b^2 = 0$, then $b^2 = 0^3$, hence $a \in \mathbf{A}$ with $a^3 = b$ and $a^2 = 0$, so $b = 0$.
2. In every ring, $(x - y)^3 = 4(x^3 - y^3) + 3(y^2 - x^2)(x + y)$. □

Consequently the element a in Definition 2.5 is always unique. In addition, $\mathrm{Ann}(b) = \mathrm{Ann}(c) = \mathrm{Ann}(a)$.

2.7. Fact. *Every normal ring is seminormal.*

D A ring is normal when every principal ideal is integrally closed. Such a ring is a pf-ring: if $uv = 0$, there exists an s such that $su = (1 - s)v = 0$ (Lemma XII-2.3). Let b and c such that $b^3 = c^2$, then c is integral over the ideal $\langle b \rangle$, hence some x such that $c = xb$, hence $b^3 = c^2 = x^2 b^2$

and $b^2(x^2-b)=0$. Therefore there exists an s such that $s(x^2-b)=0$ and $b^2(1-s)=0$. This gives $b(1-s)=0$, then $(sx)^2=s^2b=sb=b$. By letting $a=sx$, we get $a^2=b$, $a^3=bsx=bx=c$. □

The condition is necessary: Schanuel's example

2.8. Lemma. *If* $\mathbf{A}$ *is reduced and* $\mathsf{Pic}\,\mathbf{A}=\mathsf{Pic}\,\mathbf{A}[X]$*, then* $\mathbf{A}$ *is seminormal.*

D Let b, $c\in\mathbf{A}$ with $b^2=c^3$. Let $\mathbf{B}=\mathbf{A}[a]=\mathbf{A}+a\mathbf{A}$ be a reduced ring containing $\mathbf{A}$, with $a^3=b$, $a^2=c$.
Consider the polynomials f_i and g_j $(i,j=1,2)$ defined as follows

$$f_1=1+aX,\ f_2=g_2=cX^2 \text{ and } g_1=(1-aX)(1+cX^2).$$

We have $f_1g_1+f_2g_2=1$, $f_1(0)=g_1(0)=1$, $f_2(0)=g_2(0)=0$, and each product $m_{ij}=f_ig_j$ is in $\mathbf{A}[X]$. We apply Lemma 2.3: the image of the matrix (m_{ij}) is free if and only if $f_1\in\mathbf{A}[X]$, i.e. $a\in\mathbf{A}$. □

Note: For $\mathbf{B}$ we can take $\big(\mathbf{A}[T]/\langle T^2-c,T^3-b\rangle\big)_{\mathrm{red}}$. If a suitable element a is already present in $\mathbf{A}$, we obtain by uniquness $\mathbf{B}=\mathbf{A}$.

The case of integral rings

We first treat the GCD-domains, then the normal rings and finally the seminormal rings.

The case of a GCD-domain

Recall that a GCD-domain is an integral ring in which two arbitrary elements admit a greatest common divisor, i.e. an upper bound for the divisibility relation. Also recall that if $\mathbf{A}$ is a GCD-domain, the same goes for the polynomial ring $\mathbf{A}[\underline{X}]$.

2.9. Lemma. *If* $\mathbf{A}$ *is a GCD-domain, then* $\mathsf{Pic}\,\mathbf{A}=\{1\}$.

D We use the characterization given in Lemma 2.1.
Let $P=(m_{ij})$ be an idempotent matrix of rank 1. Since $\sum_i m_{ii}=1$, we can assume that $m_{1,1}$ is regular. Let f be the gcd of the elements of the first row. We write $m_{1j}=fg_j$ with the gcd of the g_j's equal to 1. The equality $m_{1,1}m_{ij}=m_{1j}m_{i1}$ gives, by simplifying by f, $g_1m_{ij}=m_{i1}g_j$. Thus, g_1 divides all the $m_{i1}g_j$'s, and so also divides their gcd m_{i1}. We write $m_{i1}=g_1f_i$. Since $g_1f_1=m_{1,1}=fg_1$, this gives $f_1=f$. Finally, $m_{1,1}m_{ij}=m_{1j}m_{i1}$ gives the equality $f_1g_1m_{ij}=f_1g_jg_1f_i$, then $m_{ij}=f_ig_j$. □

We then have the following corollary.

2.10. Proposition. *If* $\mathbf{A}$ *is a discrete field or a reduced zero-dimensional ring, then* $\mathsf{Pic}\,\mathbf{A} = \mathsf{Pic}\,\mathbf{A}[\underline{X}] = \{1\}$.

D Lemma 2.9 gives the result for the discrete fields. It then suffices to apply the elementary local-global machinery no. 2 (page 213). □

The case of a normal domain

2.11. Lemma. *If* $\mathbf{A}$ *is a normal domain, then* $\mathsf{Pic}\,\mathbf{A} = \mathsf{Pic}\,\mathbf{A}[\underline{X}]$.

D We use the characterization given in Corollary 2.4 *3*, with here $\mathbf{A} \subseteq \mathbf{K}$, the quotient field of $\mathbf{A}$. Let f_i and g_j, $(i, j \in [\![1..n]\!])$ be the suitable polynomials of $\mathbf{K}[\underline{X}]$. Then, since $f_1 g_1 = m_{1,1} \in \mathbf{A}[\underline{X}]$ and $g_1(\underline{0}) = 1$, given Kronecker's theorem III-3.3, the coefficients of f_1 are integral over the ring generated by the coefficients of $m_{1,1}$. Thus $f_1 \in \mathbf{A}[X]$. □

Remark. As for Proposition 2.10, we can extend the result of Lemma 2.11 to the case of a reduced ring $\mathbf{A}$ integrally closed in a reduced zero-dimensional ring $\mathbf{K} \supseteq \mathbf{A}$. ■

The case of a seminormal integral ring

2.12. Proposition. *If* $\mathbf{A}$ *is integral and seminormal, then* $\mathsf{Pic}\,\mathbf{A} = \mathsf{Pic}\,\mathbf{A}[\underline{X}]$.

Start of the proof. As in the proof of Lemma 2.11, we start with polynomials $f_1(\underline{X}), \ldots, f_n(\underline{X}), g_1(\underline{X}), \ldots, g_n(\underline{X})$ in $\mathbf{K}[\underline{X}]$ that satisfy the conditions $(*)$ of Lemma 2.3. We call $\mathbf{B}$ the subring of $\mathbf{K}$ generated by $\mathbf{A}$ and by the coefficients of the f_i's and the g_j's, or, what amounts to the same thing, generated by $\mathbf{A}$ and the coefficients of f_1. Then, given Kronecker's theorem, $\mathbf{B}$ is a finite extension of $\mathbf{A}$. Our goal is to show that $\mathbf{A} = \mathbf{B}$. Let $\mathfrak{a}$ be the conductor of $\mathbf{B}$ into $\mathbf{A}$, i.e. the set $\{\, x \in \mathbf{B} \,|\, x\mathbf{B} \subseteq \mathbf{A} \,\}$. It is both an ideal of $\mathbf{A}$ and $\mathbf{B}$. Our goal is now to show $\mathfrak{a} = \langle 1 \rangle$, i.e. $\mathbf{C} = \mathbf{A}/\mathfrak{a}$ is trivial. □

We start with two lemmas.

2.13. Lemma. *If* $\mathbf{A} \subseteq \mathbf{B}$, $\mathbf{A}$ *is seminormal and* $\mathbf{B}$ *is reduced, then the conductor* $\mathfrak{a}$ *of* $\mathbf{B}$ *into* $\mathbf{A}$ *is a radical ideal of* $\mathbf{B}$.

D We must show that if $u \in \mathbf{B}$ and $u^2 \in \mathfrak{a}$, then $u \in \mathfrak{a}$. So let $c \in \mathbf{B}$. We must show that $uc \in \mathbf{A}$. We know that u^2c^2 and $u^3c^3 = u^2(uc^3)$ are in $\mathbf{A}$ since $u^2 \in \mathfrak{a}$. Since $(u^3c^3)^2 = (u^2c^2)^3$, we have some $a \in \mathbf{A}$ such that $a^2 = (uc)^2$ and $a^3 = (uc)^3$. As $\mathbf{B}$ is reduced, we obtain $a = uc$, and so $uc \in \mathbf{A}$. □

Remark. The *seminormal closure* of a ring $\mathbf{A}$ in a reduced ring $\mathbf{B} \supseteq \mathbf{A}$ is obtained by starting from $\mathbf{A}$ and adding the elements x of $\mathbf{B}$ such that x^2 and x^3 are in the previously contructed ring. Note that by Fact 2.6, x is uniquely determined by the given x^2 and x^3. The proof of the previous lemma can then be interpreted as a proof of the following variant. ■

2.14. Lemma. *Let* $\mathbf{A} \subseteq \mathbf{B}$ *be reduced,* $\mathbf{A}_1$ *be the seminormal closure of* $\mathbf{A}$ *in* $\mathbf{B}$*, and* $\mathfrak{a}$ *be the conductor of* $\mathbf{B}$ *into* $\mathbf{A}_1$*. Then,* $\mathfrak{a}$ *is a radical ideal of* $\mathbf{B}$*.*

2.15. Lemma. *Let* $\mathbf{A} \subseteq \mathbf{B}$*,* $\mathbf{B} = \mathbf{A}[c_1, \ldots, c_q]$ *be reduced and finite over* $\mathbf{A}$ *and* $\mathfrak{a}$ *be the conductor of* $\mathbf{B}$ *into* $\mathbf{A}$*. Suppose that* $\mathfrak{a}$ *is a radical ideal, then it is equal to* $\{\, x \in \mathbf{A} \mid xc_1, \ldots, xc_q \in \mathbf{A} \,\}$*.*

D Indeed, if $xc_i \in \mathbf{A}$, then $x^\ell c_i^\ell \in \mathbf{A}$ for all ℓ, and so for some large enough N, $x^N y \in \mathbf{A}$ for all $y \in \mathbf{B}$, so x is in the nilradical of $\mathfrak{a}$ (if d is the upper bound of the degrees of the equations of integral dependence of the c_i's over $\mathbf{A}$, we can take $N = (d-1)q$). □

End of the proof of Proposition 2.12.
We first give it in classical mathematics. The natural classical reasoning would proceed by contradiction: the ring $\mathbf{C}$ is trivial because otherwise, it would have a minimal prime ideal and the localization at this minimal prime ideal would lead to a contradiction.
To avoid the nonconstructive character of the argument by contradiction, we localize at a maximal filter, recalling our definition "without negation" according to which a filter is maximal if and only if the localized ring is a zero-dimensional local ring. In other words we tolerate for the maximal filters of a ring not only the complements of the minimal prime ideals but also the filter generated by 0 which gives by localization the trivial ring. In classical mathematics a ring is then trivial if and only if its only maximal filter is the whole ring (in other words, the filter generated by 0).
Let us insist on the fact that it is only in the previous affirmation that the "classical" character of the argument is located. Because the proof of what follows is perfectly constructive: if S is a maximal filter of $\mathbf{C}$, then $0 \in S$ (so $S = \mathbf{C}$).
Consider the inclusion $\mathbf{C} = \mathbf{A}/\mathfrak{a} \subseteq \mathbf{B}/\mathfrak{a} = \mathbf{C}'$. Let S be a maximal filter of $\mathbf{C}$, and S_1 be the corresponding maximal filter of $\mathbf{A}$ (the inverse image of S by the canonical projection). Since S is a maximal filter, and since $\mathbf{C}$ is reduced, $S^{-1}\mathbf{C} = \mathbf{L}$ is a reduced zero-dimensional local ring, that is a discrete field, contained in the reduced ring $S^{-1}\mathbf{C}' = \mathbf{L}'$.
If x is an object defined over $\mathbf{B}$, let us denote by $\overline{x}$ what it becomes after the base change $\mathbf{B} \to \mathbf{L}'$. Since $\mathbf{L}$ is a discrete field, $\mathbf{L}[\underline{X}]$ is a GCD-domain, and the $\overline{f_i}$'s and $\overline{g_j}$'s are in $\mathbf{L}[\underline{X}]$. This means that there exists an $s \in S_1$ such that $sf_1 \in \mathbf{A}[X]$. By Lemma 2.15, this implies that $s \in \mathfrak{a}$. Thus $\overline{s} = 0$ and $\overline{s} \in S$. □

The proof given above for Proposition 2.12 is in fact quite simple. It is however not entirely constructive and it seems to only treat the integral case.

Constructive proof of Proposition 2.12.
We rewrite the proof given in classical mathematics by considering that the maximal filter S of $\mathbf{C}$ is a purely generic object which guides us in the constructive proof.
Imagine that the ring $\mathbf{C}$ is a discrete field, i.e. that we have already done the localization at a maximal filter.
Then, polynomials F_i and G_j of $\mathbf{C}[\underline{X}]$ satisfying $F_iG_j = \overline{m_{ij}}$ and $F_1(\underline{0}) = 1$ are computed from the $\overline{m_{ij}}$'s according to an algorithm that we deduce from the previously given constructive proofs for the case of discrete fields (Lemma 2.9). The uniqueness of the solution then forces the equality $F_1 = \overline{f_1}$, which shows that $\overline{f_1} \in \mathbf{C}[\underline{X}]$, and therefore that $\mathbf{C}$ is trivial.
This algorithm uses the disjunction "a is null or a is invertible," for the elements $a \in \mathbf{C}$ which are produced by the algorithm from the coefficients of the polynomials $\overline{m_{i,j}}$. As $\mathbf{C}$ is only a reduced ring, with neither a test for equality to 0 nor an invertibility test, the algorithm for discrete fields, if we execute it with $\mathbf{C}$, must be replaced by a tree in which we open two branches each time a question "is a null or invertible?" is asked by the algorithm.
Here we are, facing a gigantic, but finite, tree. Say that we have systematically placed the "a is invertible" branch on the left-hand side, and the "$a = 0$" branch on the right. Let us look at what happens in the extreme left branch.
We have successively inverted a_1, …, a_p and we have obtained an s that shows that the ring $\mathbf{C}[1/(a_1 \cdots a_p)]$ is trivial.
Conclusion: in the ring $\mathbf{C}$*, we have the equality* $a_1 \cdots a_p = 0$.
Let us take one step back up the tree.
In the ring $\mathbf{C}[1/(a_1 \cdots a_{p-1})]$, we know that $a_p = 0$.
The left branch should not have been opened. Let us take a look at the computation in the branch $a_p = 0$.
Let us follow from here the extreme left branch.
We have inverted a_1, …, a_{p-1}, then, say $b_1, \ldots, b_k$ (eventually, $k = 0$). We obtain an s that shows that the ring $\mathbf{C}[1/(a_1 \cdots a_{p-1}b_1 \cdots b_k)]$ is trivial.
Conclusion: in the ring $\mathbf{C}$*, we have the equality* $a_1 \cdots a_{p-1}b_1 \cdots b_k = 0$.
Let us take one step back up the tree. We know that $b_k = 0$ (or, if $k = 0$, $a_{p-1} = 0$) in the ring that was there just before the last branching; namely the ring $\mathbf{C}[1/(a_1 \cdots a_{p-1}b_1 \cdots b_{k-1})]$ (or, if $k = 0$, $\mathbf{C}[1/(a_1 \cdots a_{p-2})]$). The left branch should not have been opened. Let us look at the computation in the branch $b_k = 0$ (or, if $k = 0$, the branch $a_{p-1} = 0$)…
And so forth. When we follow the process all the way through, we find ourselves at the root of the tree with the ring $\mathbf{C} = \mathbf{C}[1/1]$, which is trivial.□

By using Lemma 2.14 instead of Lemma 2.13 we will obtain the following result, which is more precise than Proposition 2.12.

2.16. Proposition. *If $\mathbf{A}$ is an integral ring and P is a projective module of rank 1 over $\mathbf{A}[\underline{X}]$ such that $P(\underline{0})$ is free, there exist $c_1, \ldots, c_m$ in the quotient field of $\mathbf{A}$ such that*

1. *c_i^2 and c_i^3 are in $\mathbf{A}[(c_j)_{j<i}]$ for $i = 1, \ldots, m$,*
2. *P is free over $\mathbf{A}[(c_j)_{j\leqslant m}][X]$.*

Remark. Actually, only the quotient field of the subring generated by the coefficient present in a projection matrix, whose image is isomorphic to P, intervenes. ■

General case

2.17. Proposition. (Coquand) *Let $\mathbf{A} \subseteq \mathbf{K}$ with $\mathbf{K}$ reduced.*

1. *Given f and $g \in \mathbf{K}[\underline{X}]^n$ that satisfy the conditions $(*)$ of Lemma 2.3, we can construct $c_1, \ldots, c_m$ in $\mathbf{K}$ such that*
   - *c_i^2 and c_i^3 are in $\mathbf{A}[(c_j)_{j<i}]$ for $i \in [\![1..m]\!]$,*
   - *f and g have their coordinates in $\mathbf{A}[(c_k)_{k\in[\![1..m]\!]}][\underline{X}]$.*
2. *If $\mathsf{Pic}\,\mathbf{K} = \mathsf{Pic}\,\mathbf{K}[\underline{X}]$ and if P is a projective module of rank 1 over $\mathbf{A}[\underline{X}]$, there exist $c_1, \ldots, c_m$ in $\mathbf{K}$ such that*
   - *c_i^2 and c_i^3 are in $\mathbf{A}[(c_j)_{j<i}]$ for $i \in [\![1..m]\!]$,*
   - *$P \simeq P(\underline{0})$ over $\mathbf{A}[(c_k)_{k\in[\![1..m]\!]}][\underline{X}]$.*

D The proof of Proposition 2.12, or of its more precise variant 2.16, is in fact a proof of item *1* above. Item *2* is easily deduced. □

2.18. Theorem. (Traverso-Swan-Coquand)
If $\mathbf{A}$ is a seminormal ring, then $\mathsf{Pic}\,\mathbf{A} = \mathsf{Pic}\,\mathbf{A}[\underline{X}]$.

D We deduce it from the previous proposition by using the fact that there exists an overring $\mathbf{K}$ of $\mathbf{A}$ such that $\mathsf{Pic}\,\mathbf{K} = \mathsf{Pic}\,\mathbf{K}[\underline{X}]$. Indeed, every reduced ring is contained in a reduced zero-dimensional ring (Theorem XI-4.25 or XIII-7.8) $\mathbf{K}$, which satisfies $\mathsf{Pic}\,\mathbf{K} = \mathsf{Pic}\,\mathbf{K}[\underline{X}] = \{1\}$ (Proposition 2.10).□

A direct computation leading to the result

As is often the case when trying to implement on a machine a constructive theorem that has an elegant proof, we are led to finding certain shortcuts in the computations that give a definitively simpler solution. But this solution partially hides at least the thought process that developed the proof, if not the deep mechanism of the initial proof. See for example how Exercise X-3 trivializes the proof of the local structure theorem for finitely generated projective modules.

This is what happened with Proposition 2.17 which was finally realized by a quite elementary algorithm in [7, Barhoumi&Lombardi], based on the theory of the resultant ideal (see Section IV-10) and of the subresultant modules.

3. Patching à la Quillen-Vaserstein

In this section we present the so called Quillen patching. It is a deep result that could a priori seem a little too abstract (abusive usage of maximal ideals) but which happens to make a lot of constructive sense.

The proofs that we give are (for the most part) copied from [Kunz]. We have replaced the localization at any maximal ideal with the localization at comaximal monoids.

3.1. Lemma. *Let S be a monoid of the ring $\mathbf{A}$ and $P \in \mathbf{A}[X]$ be a polynomial such that $P =_{\mathbf{A}_S[X]} 0$ and $P(0) = 0$. Then, there exists an $s \in S$ such that $P(sX) = 0$.*

D The proof is left to the reader. □

Here is a slight variant.

3.2. Fact. *Let S be a monoid of the ring $\mathbf{A}$ and $P \in \mathbf{A}_S[X]$ be a polynomial such that $P(0) = 0$. Then, there exist $s \in S$ and $Q \in \mathbf{A}[X]$ such that $P(sX) =_{\mathbf{A}_S[X]} Q$.*

3.3. Lemma. *Let S be a monoid of the ring $\mathbf{A}$. Consider three matrices with coefficients in $\mathbf{A}[X]$, A_1, A_2, A_3 such that the product $A_1\,A_2$ has the same format as A_3. If $A_1\,A_2 =_{\mathbf{A}_S[X]} A_3$ and $A_1(0)\,A_2(0) = A_3(0)$, there exists an $s \in S$ such that $A_1(sX)\,A_2(sX) = A_3(sX)$.*

D Apply Lemma 3.1 to the coefficients of the matrix $A_1\,A_2 - A_3$. □

3.4. Lemma. *Let S be a monoid of the ring $\mathbf{A}$ and $C(X) \in \mathbb{GL}_p(\mathbf{A}_S[X])$. There exist $s \in S$ and $U(X,Y) \in \mathbb{GL}_p(\mathbf{A}[X,Y])$ such that $U(X,0) = \mathrm{I}_p$, and, over the ring $\mathbf{A}_S[X,Y]$, $U(X,Y) = C(X+sY)C(X)^{-1}$.*

D Let $E(X,Y) = C(X+Y)C(X)^{-1}$. Let $F(X,Y) = E(X,Y)^{-1}$. We have $E(X,0) = \mathrm{I}_p$, so $E(X,Y) = \mathrm{I}_p + E_1(X)Y + \cdots + E_k(X)Y^k$. For some $s_1 \in S$, the ${s_1}^j E_j$'s can be rewritten "without denominator." We thus obtain a matrix $E'(X,Y) \in \mathbb{M}_p(\mathbf{A}[X,Y])$ such that $E'(X,0) = \mathrm{I}_p$ and, over $\mathbf{A}_S[X,Y]$, $E'(X,Y) = E(X,s_1Y)$. We proceed similarly with F (and we can choose some common s_1). We then have $E'(X,Y)F'(X,Y) = \mathrm{I}_p$ in $\mathbb{M}_p(\mathbf{A}_S[X,Y])$ and $E'(X,0)F'(X,0) = \mathrm{I}_p$.
By applying Lemma 3.3 in which we replace X with Y and $\mathbf{A}$ with $\mathbf{A}[X]$, we obtain $s_2 \in S$ such that $E'(X,s_2Y)F'(X,s_2Y) = \mathrm{I}_p$.
Hence the desired result with $U = E'(X,s_2Y)$ and $s = s_1s_2$. □

3.5. Lemma. *Let S be a monoid of $\mathbf{A}$ and $G \in \mathbf{A}[X]^{q\times m}$. If $G(X)$ and $G(0)$ are equivalent over $\mathbf{A}_S[X]$, there exists an $s \in S$ such that $G(X + sY)$ and $G(X)$ are equivalent over $\mathbf{A}[X, Y]$.*

D Let $G = C\,G(0)\,D$ with $C \in \mathbb{GL}_q(\mathbf{A}_S[X])$ and $D \in \mathbb{GL}_m(\mathbf{A}_S[X])$. We therefore have

$$\begin{aligned} G(X+Y) &= C(X+Y)G(0)D(X+Y) \\ &= C(X+Y)C(X)^{-1}G(X)D(X)^{-1}D(X+Y). \end{aligned}$$

By applying Lemma 3.4, we obtain $s_1 \in S$, $U(X, Y) \in \mathbb{GL}_q(\mathbf{A}[X, Y])$ and $V(X, Y) \in \mathbb{GL}_m(\mathbf{A}[X, Y])$, such that

$$U(X, 0) = \mathrm{I}_q\,,\ \ V(X, 0) = \mathrm{I}_m\,,$$

and, over the ring $\mathbf{A}_S[X, Y]$,

$$U(X,Y) = C(X+s_1Y)C(X)^{-1} \text{ and } V(X,Y) = D(X)^{-1}D(X+s_1Y).$$

Therefore

$$G(X) = U(X, 0)G(X)V(X, 0),$$

and over the ring $\mathbf{A}_S[X, Y]$:

$$G(X+s_1Y) = U(X,Y)G(X)V(X,Y).$$

By applying Lemma 3.3 (as in Lemma 3.4), we obtain $s_2 \in S$ such that $G(X + s_1s_2Y) = U(X, s_2Y)G(X)V(X, s_2Y)$.
Hence the result with $s = s_1s_2$. □

3.6. Concrete local-global principle. (Vaserstein patching)
Let G be a matrix over $\mathbf{A}[X]$ and S_1, …, S_n be comaximal monoids of $\mathbf{A}$.

1. *The matrices $G(X)$ and $G(0)$ are equivalent over $\mathbf{A}[X]$ if and only if they are equivalent over $\mathbf{A}_{S_i}[X]$ for each i.*
2. *Same result for "the left-equivalence": two matrices M and N with the same format over a commutative ring are said to be* left-equivalent *if there exists an invertible square matrix H such that $H\,M = N$.*

D *1.* One sees easily that the set of $s \in \mathbf{A}$ such that the matrix $G(X+sY)$ is equivalent to $G(X)$ over $\mathbf{A}[X, Y]$ forms an ideal of $\mathbf{A}$. By applying Lemma 3.5, this ideal contains an element s_i in S_i for each i, so it contains 1, and $G(X + Y)$ is equivalent to $G(X)$. It remains to make $X = 0$.
2. In all the previous proofs, we can replace equivalence with left-equivalence. □

3.7. Concrete local-global principle. (Quillen patching)
Let M be a finitely presented module over $\mathbf{A}[X]$ and S_1, …, S_n be comaximal monoids of $\mathbf{A}$. Then, M is a module extended from $\mathbf{A}$ if and only if each M_{S_i} is extended from $\mathbf{A}_{S_i}$.

D This is a corollary of the previous theorem because the isomorphism between the modules $M(X)$ and $M(0)$ can be expressed by the equivalence of two matrices $H(X)$ and $H(0)$ constructed from a presentation matrix G of M (see Fact 1.1). □

Comment. The original formulation by Quillen, equivalent to the local-global principle 3.7 in classical mathematics, is the following: *if $M_{\mathfrak{m}}$ is extended from $\mathbf{A}_{\mathfrak{m}}$ after localization at every maximal ideal $\mathfrak{m}$, then M is extended from $\mathbf{A}$.* To constructively decipher a classical proof based on the Quillen patching in the original formulation, we will have to call upon the basic local-global machinery explained in Section XV-5. ■

A Roitman theorem

This subsection is devoted to the proof of the following theorem, which consists in a kind of converse of the Quillen patching theorem.

3.8. Theorem. (Roitman's theorem)
Let r be an integer $\geqslant 1$ and $\mathbf{A}[\underline{X}] = \mathbf{A}[X_1, \ldots, X_r]$. If every finitely generated projective $\mathbf{A}[\underline{X}]$-module is extended from $\mathbf{A}$, then every localization $\mathbf{A}_S$ of $\mathbf{A}$ satisfies the same property.

The univariate case

3.9. Lemma. *If every finitely generated projective $\mathbf{A}[X]$-module is extended from $\mathbf{A}$, then every localization $\mathbf{A}_S$ of $\mathbf{A}$ satisfies the same property.*

D *Special case: $\mathbf{A}_S$ is a residually discrete local ring.*
Let $\rho : \mathbf{A}[X] \to \mathbf{A}_S[X]$ be the natural morphism. Let $M \in \mathbb{AG}_n(\mathbf{A}_S[X])$. Since $\mathbf{A}_S$ is local, $M(0)$ is similar to a standard projector $\mathrm{I}_{k,n}$. We can therefore suppose without loss of generality that $M(0) = \mathrm{I}_{k,n}$, i.e. $M(X) = \mathrm{I}_{k,n} + M'(X)$ with $M'(X) \in \mathbb{M}_n(\mathbf{A}_S[X])$ and $M'(0) = 0$.
Let v be the "product of the denominators" in the coefficients of the entries of $M'(X)$. Since $M'(0) = 0$, we have a matrix $N' = N'(X) \in \mathbb{M}_n(\mathbf{A}[X])$ such that $M'(vX) =_{\mathbf{A}_S[X]} N'(X)^\rho$ and $N'(0) = 0$.
With $N(X) = \mathrm{I}_{k,n} + N'(X)$ we obtain $N(0) = \mathrm{I}_{k,n}$ and $M(vX) = N(X)^\rho$.
Since $M^2 =_{\mathbf{A}_S[X]} M$, we have some $s \in S$ such that $s(N^2 - N) = 0$.
As $(N^2 - N)(0) = 0$, we write $N^2 - N = XQ(X)$.
Now $sXQ(X) = 0$ implies $sQ(X) = 0$. A fortiori $sQ(sX) = 0$, so $N(sX)^2 = N(sX)$. However, the finitely generated projective modules over $\mathbf{A}[X]$ are extended from $\mathbf{A}$, therefore the projection matrix $N(sX)$ has a kernel and an image isomorphic to the kernel and to the image of $N(0) = \mathrm{I}_{k,n}$. Therefore

$N(sX)$ is similar to $\mathrm{I}_{k,n}$: there exists a $G = G(X) \in \mathbb{GL}_n(\mathbf{A}[X])$ such that

$$G^{-1}(X)N(sX)G(X) = \mathrm{I}_{k,n}.$$

By letting $H(X) = G(X)^\rho \in \mathbb{GL}_n(\mathbf{A}_S[X])$, we obtain over $\mathbf{A}_S[X]$ the equality

$$H^{-1}(X)M(svX)H(X) = \mathrm{I}_{k,n}$$

and therefore

$$H^{-1}(X/sv)M(X)H(X/sv) =_{\mathbf{A}_S[X]} \mathrm{I}_{k,n}$$

with $H(X/sv) \in \mathbb{GL}_n(\mathbf{A}_S[X])$.

General case. Let P be an arbitrary finitely generated projective $\mathbf{A}_S[X]$-module. Let $\mathbf{B} = \mathbf{A}_S$. As usual, $P(0)$ denotes the $\mathbf{B}$-module obtained by scalar extension via the morphism $\mathrm{ev}_0 : \mathbf{B}[X] \to \mathbf{B}$. We apply the basic local-global machinery (page 871) to the constructive proof that we have just given in the special case. We obtain comaximal monoids $V_1, \ldots, V_m$ of $\mathbf{B}$ with $P \simeq_{\mathbf{B}_{V_i}} P(0)$. We conclude with the Quillen patching: $P \simeq_{\mathbf{B}} P(0)$. □

Remark. To implement the algorithm corresponding to this proof. Actually the only particular property that we have used in the proof of the special case, it is that the finitely generated projective $\mathbf{A}_S$-modules are free. Therefore the implementation of the basic local-global machinery here is very elementary. It consists in constructing comaximal localizations for which the matrix $M(0)$ becomes similar to a standard projection matrix, and to get the algorithm given by the proof of the special case running in each of these localizations. Naturally, we end with the algorithm corresponding to the constructive proof of the Quillen patching. ■

The multivariate case

Proof of Roitman's theorem 3.8. We reason by induction on r. The case $r = 1$ has already been treated. Let us pass from $r \geqslant 1$ to $r + 1$. Consider a monoid S of a ring $\mathbf{A}$. Let $(X_1, \ldots, X_r) = (\underline{X})$.

We have $\mathbf{A}_S[\underline{X}, Y] = \mathbf{A}[\underline{X}, Y]_S = (\mathbf{A}[Y]_S)[\underline{X}]$. Let P be a finitely generated projective $\mathbf{A}_S[\underline{X}, Y]$-module. By the induction hypothesis applied with the ring $\mathbf{A}[Y]$, P is extended from $\mathbf{A}[Y]_S = \mathbf{A}_S[Y]$, that is, $P(\underline{X}, Y)$ is isomorphic to $P(\underline{0}, Y)$ as an $\mathbf{A}_S[\underline{X}, Y]$-module, and by the case $r = 1$ applied with the ring $\mathbf{A}$, $P(\underline{0}, Y)$ is extended from $\mathbf{A}_S$. □

A long-open question solved negatively

That question is the following.

If every finitely generated projective $\mathbf{A}[X]$*-module is extended from* $\mathbf{A}$*, is it always true that for any* r *every finitely generated projective* $\mathbf{A}[X_1, \ldots, X_r]$*-module is extended from* $\mathbf{A}$*?*

A negative response is given in [53, Cortiñas & al., (2011)].

A local-global principle à la Roitman

3.10. Concrete local-global principle. *Let n and $r > 0$. Consider the following property for a ring* $\mathbf{A}$. $\mathsf{P}_{n,r}(\mathbf{A})$: *every projective module of constant rank r over $\mathbf{A}[X_1, \ldots, X_n]$ is extended from* $\mathbf{A}$.
Let S_1, …, S_k be comaximal monoids of a ring $\mathbf{A}$. Then $\mathbf{A}$ satisfies the property $\mathsf{P}_{n,r}$ if and only if each of the $\mathbf{A}_{S_i}$'s satisfies it.
In particular $\mathbf{A}$ is seminormal if and only if each of the $\mathbf{A}_{S_i}$'s is seminormal.

D The condition is necessary by Roitman's theorem 3.8, whose proof remains valid if we limit ourselves to the projective modules of constant rank r.
The condition is sufficient by the Quillen patching 3.7. □

4. Horrocks' theorem

The following lemma is a special case of Proposition V-9.1 *4*.

4.1. Lemma. *Let S be a monoid of $\mathbf{A}$ and P, Q be finitely generated projective $\mathbf{A}$-modules such that $P_S \simeq Q_S$. Then, there exists an $s \in S$ such that $P_s \simeq Q_s$.*

4.2. Notation. Let $\mathbf{A}\langle X\rangle$ be the ring $S^{-1}\mathbf{A}[X]$, where S is the monoid of the monic polynomials of $\mathbf{A}[X]$.

4.3. Theorem. (Local Horrocks' theorem)
Let $\mathbf{A}$ be a residually discrete local ring and P be a finitely generated projective module over $\mathbf{A}[X]$. If P_S is free over $\mathbf{A}\langle X\rangle$, then P is free over $\mathbf{A}[X]$ (so extended from $\mathbf{A}$).

We use the proof by [146, Nashier & Nichols] which is almost constructive, as presented in [Lam06] or [Ischebeck & Rao].

We need a few preliminary results.

4.4. Lemma. *Let $\mathbf{A}$ be a ring, $\mathfrak{m} = \operatorname{Rad}\mathbf{A}$ and $S \subseteq \mathbf{A}[X]$ be the monoid of the monic polynomials. The monoids S and $1 + \mathfrak{m}[X]$ are comaximal.*

D Let $f(X) \in S$ and $g(X) \in 1 + \mathfrak{m}[X]$. The resultant $\operatorname{Res}_X(f, g)$ belongs to the ideal $\langle f, g\rangle$ of $\mathbf{A}[X]$. Since f is monic, the resultant is successfully subjected to the specialization $\mathbf{A} \to \mathbf{A}/\mathfrak{m}$. Therefore $\operatorname{Res}_X(f, g) \equiv \operatorname{Res}_X(f, 1) = 1 \bmod \mathfrak{m}$. □

4.5. Lemma. *Let $\mathbf{A} \subseteq \mathbf{B}$, $s \in \operatorname{Reg}(\mathbf{B})$, and P, Q be two finitely generated projective $\mathbf{B}$-modules with $sQ \subseteq P \subseteq Q$. If $\mathbf{B}$ and $\mathbf{B}/\langle s\rangle$ are (not necessarily finitely generated) projective $\mathbf{A}$-modules, then the same goes for the $\mathbf{A}$-module Q/P.*

D Since s is regular and since Q and P are submodules of a free module, the multiplication by s (denoted μ_s) is injective in P and in Q. We have the following exact sequences of **A**-modules.

$$\begin{array}{ccccccc} 0 \to & Q & \xrightarrow{\mu_s} & P & \longrightarrow & P/sQ & \to 0 \\ 0 \to & sQ/sP & \longrightarrow & P/sP & \longrightarrow & P/sQ & \to 0 \end{array}$$

The **A**-module P is projective by transitivity, the $\mathbf{B}/s\mathbf{B}$-module P/sP is projective, therefore by transitivity P/sP is a projective **A**-module. We can then apply Schanuel's lemma (Lemma V-2.7): $(P/sP) \oplus Q \simeq (sQ/sP) \oplus P$ as **A**-modules. Since Q is a projective **A**-module, the same goes for sQ/sP. But since μ_s is injective, sQ/sP is isomorphic to P/Q. □

4.6. Lemma. (Murthy & Pedrini, [145])
Let $\mathbf{A}$ *be a ring,* $\mathbf{B} = \mathbf{A}[X]$*,* S *be the monoid of the monic polynomials of* $\mathbf{A}[X]$*,* P*,* Q *be two finitely generated projective modules over* $\mathbf{B}$*, and* $f \in S$*.*

1. *If* $fQ \subseteq P \subseteq Q$*, then* P *and* Q *are stably isomorphic.*
2. *If* $P_S \simeq Q_S$*, then* P *and* Q *are stably isomorphic.*
3. *If in addition* P *and* Q *are of rank* 1*, then* $P \simeq Q$*.*

D *1.* Since f is monic, the **A**-algebra $\mathbf{B}/\langle f\rangle$ is a free **A**-module of rank $\deg f$. The $\mathbf{B}/\langle f\rangle$-module Q/fQ is finitely generated projective over **A**. By the previous lemma, the **A**-module $M = Q/P$ is projective, and it is finitely generated over $\mathbf{B}/\langle f\rangle$, so over **A**. Therefore $M[X]$ is a finitely generated projective **B**-module. We have two exact sequences (μ_X is multiplication by X)

$$\begin{array}{ccccccc} 0 \to & P & \longrightarrow & Q & \longrightarrow & M & \to 0, \\ 0 \to & M[X] & \xrightarrow{\mu_X} & M[X] & \longrightarrow & M & \to 0. \end{array}$$

By Schanuel's lemma (Lemma V-2.7) we have $P \oplus M[X] \simeq Q \oplus M[X]$ as **B**-modules. Since $M[X]$ is finitely generated projective over **B**, P and Q are stably isomorphic.

2. We know that $P_f \simeq Q_f$ for some $f \in S$.
By hypothesis, we have $F \in \mathbb{AG}_n(\mathbf{B})$ and $G \in \mathbb{AG}_n(\mathbf{B})$ with $P \simeq \operatorname{Im} F$, and $Q \simeq \operatorname{Im} G$. We know that $F' = \operatorname{Diag}(F, 0_m)$ and $G' = \operatorname{Diag}(G, 0_n)$ are conjugated over $\mathbf{B}_f$ (enlargement lemma V-2.10). This means that there exists a matrix $H \in \mathbb{M}_{m+n}(\mathbf{B})$ such that $HF' = G'H$ and $\det(H) = \delta$ divides a power of f. We then have $P_1 = \operatorname{Im}(HF') \subseteq \operatorname{Im} G'$. Then, by postmultiplying by $\widetilde{H}$, $(HF')\widetilde{H} = \delta G'$, which implies $\delta \operatorname{Im} G' \subseteq \operatorname{Im}(HF')$. Since H is injective, we have $P_1 \simeq P$, and moreover $\operatorname{Im} G' = Q_1 \simeq Q$. We can conclude with item *1* since $\delta Q_1 \subseteq P_1 \subseteq Q_1$.

3. The modules P and Q are of rank 1 and stably isomorphic, therefore isomorphic (Fact X-5.6). □

Proof of Theorem 4.3.
Notations: $\mathfrak{m} = \operatorname{Rad} \mathbf{A}$, $\mathbf{k} = \mathbf{A}/\mathfrak{m}$ (discrete field) $\mathbf{B} = \mathbf{A}[X]$, $n = \operatorname{rk}(P)$

($n \in \mathbb{N}$ since $\mathbf{B}$ is connected), $U = 1 + \mathfrak{m}[X]$, and $\overline{E}$ be the object E reduced modulo $\mathfrak{m}$.

1. We show by induction on n that we have an isomorphism $P \simeq P_1 \oplus \mathbf{B}^{n-1}$. For $n = 1$ it is trivial.

Little lemma (see the proof below)
There exist z, y_2, …, y_n, z_2, …, z_n in P such that $(z, y_2, \dots, y_n)$ is a basis of P_S over $\mathbf{B}_S$ and $(\overline{z}, \overline{z_2}, \dots, \overline{z_n})$ is a basis of $\overline{P}$ over $\overline{\mathbf{B}} = \mathbf{k}[X]$.

The $\mathbf{B}_U$-module P_U is free with basis $(z, \underline{z_2, \dots,} z_n)$: indeed, $\mathfrak{m} \subseteq \operatorname{Rad} \mathbf{B}_U$, and modulo $\mathfrak{m}$, $(\overline{z}, \overline{z_2}, \dots, \overline{z_n})$ generates $\overline{P} = \overline{P_U}$, so $(z, z_2, \dots, z_n)$ generates P_U by Nakayama's lemma. Finally, a finitely generated projective module of rank n generated by n elements is free.
Let $P' = P/\mathbf{B}z$. The two modules P'_U and P'_S are free. The monoids U and S are comaximal (Lemma 4.4), so P' is finitely generated projective over $\mathbf{B}$, hence $P \simeq P' \oplus \mathbf{B}z$. By induction hypothesis, $P' \simeq P_1 \oplus \mathbf{B}^{n-2}$, which gives $P \simeq P_1 \oplus \mathbf{B}^{n-1}$

2. The isomorphism $P \simeq P_1 \oplus \mathbf{B}^{n-1}$ with P_1 of rank 1 gives by localization that $(P_1)_S$ is stably free. We apply item *3* of Lemma 4.6: we obtain that P_1 is free. □

Proof of the little lemma. Let $(y_1, \dots, y_n)$ in P which is a $\mathbf{B}_S$-basis of P_S. There exists a basis $(\overline{z_1}, \overline{z_2}, \dots, \overline{z_n})$ of $\overline{P}$, with the z_i's in P such that $\overline{y_1} \in \mathbf{k}[X]\,\overline{z_2}$ (by dividing $\overline{y_1}$ by the gcd of its coefficients, we obtain a unimodular vector, and over a Bézout ring, every unimodular vector is completable). We look for z in the form $z_1 + X^r y_1$. It is clear that, for any r, $(\overline{z}, \overline{z_2}, \dots, \overline{z_n})$ is a basis of $\overline{P}$. Since $(y_1, \dots, y_n)$ is a $\mathbf{B}_S$-basis of P_S, there exists an $s \in S$ such that $sz_1 = \sum_{i=1}^{n} b_i y_i$, with the b_i's in $\mathbf{B}$.
Then, $sz = (b_1 + sX^r)y_1 + \sum_{i=2}^{n} b_i y_i$, and for large enough r, $b_1 + sX^r$ is a monic polynomial: $(z, y_2, \dots, y_n)$ is a $\mathbf{B}_S$-basis of P_S. □

We now give the global version.

4.7. Theorem. (Affine Horrocks' theorem)
Let S be the monoid of the monic polynomials of $\mathbf{A}[X]$ and P be a finitely generated projective module over $\mathbf{A}[X]$. If P_S is extended from $\mathbf{A}$, then P is extended from $\mathbf{A}$.

D We apply the basic local-global machinery (page 871) with the constructive proof of Theorem 4.3. We obtain a finite family of comaximal monoids of $\mathbf{A}$, $(U_i)_{i \in J}$, with each localized module P_{U_i} extended from $\mathbf{A}_{U_i}$. We conclude with the Quillen patching (concrete local-global principle 3.7). □

This important theorem can be completed by the following subtle result, which does not seem possible to extend to the finitely presented modules.

4.8. Theorem. (Bass)
Let P and Q be two finitely generated projective $\mathbf{A}$-modules. If they are isomorphic after scalar extension to $\mathbf{A}\langle X\rangle$, they are isomorphic.

D We reason with projection matrices and similarities between these matrices that correspond to isomorphisms between the image modules. Therefore implicitly, we systematically use the enlargement lemma V-2.10, without mentioning it.
We start with F and G in $\mathbb{AG}_n(\mathbf{A})$, conjugated over the ring $\mathbf{A}\langle X\rangle$. The finitely generated projective modules are $P \simeq \operatorname{Im} F$ and $Q \simeq \operatorname{Im} G$. We therefore have a matrix $H \in \mathbb{M}_n(\mathbf{A}[X])$, with $\det(H) \in S$ (monoid of the monic polynomials), and $HF = GH$.
By letting $Y = 1/X$, for large enough N, the matrix $Y^N H = H'$ is in $\mathbb{M}_n(\mathbf{A}[Y])$, with $\det(H') = Y^r\big(1 + Yg(Y)\big) = Y^r h(Y)$ where $h(0) = 1$, and obviously $H'F = GH'$. In other words, $F \sim G$ over the ring $\mathbf{A}[Y]_{Yh}$.
The elements Y and h are comaximal, so, by applying the patching theorem of the modules (concrete local-global principle XV-4.4), there exists some $\mathbf{A}[Y]$-module M such that M_Y is isomorphic to "P extended to $\mathbf{A}[Y]_Y$," and M_h is isomorphic to "Q extended to $\mathbf{A}[Y]_h$." And M is finitely generated projective since there are two comaximal localizations which are finitely generated projective modules. This provides a projection matrix E with coefficients in $\mathbf{A}[Y]$ such that $E \sim F$ over $\mathbf{A}[Y]_Y$ and $E \sim G$ over $\mathbf{A}[Y]_h$. Since Y is a monic polynomial, Horrocks' theorem tells us that $\operatorname{Im} E$ comes by scalar extension from a finitely generated projective $\mathbf{A}$-module M'. Consequently, for all a, $b \in \mathbf{A}$ the "evaluated" matrices $E(a)$ and $E(b)$ are conjugated over $\mathbf{A}$ (their images are both isomorphic to M').
Finally, $F \sim E(1)$ and $G \sim E(0)$ over $\mathbf{A}$, therefore $F \sim G$ over $\mathbf{A}$. □

Remark. For the mathematician who wishes to implement the algorithm subjacent to the previous proof, we suggest suggest using presentation matrices (whose cokernels are the modules) rather than projection matrices (whose images are the modules). This in particular avoids having to repetitively use an implementation of the enlargement lemma. ■

We finish this section with a corollary of Lemma 4.6. This theorem is to be compared with Theorem 5.4.

4.9. Theorem. (Concrete Quillen induction, stably free case)
Let $\mathcal{F}$ be a class of rings that satisfy the following properties.

1. *If $\mathbf{A} \in \mathcal{F}$, then $\mathbf{A}\langle X\rangle \in \mathcal{F}$.*
2. *If $\mathbf{A} \in \mathcal{F}$, every projective $\mathbf{A}$-module of constant rank is stably free.*

Then, for $\mathbf{A} \in \mathcal{F}$ and $r \in \mathbb{N}$, every projective $\mathbf{A}[X_1, \dots, X_r]$-module of constant rank is stably free.

D We proceed by induction on r, the case $r = 0$ being clear.
We pass from $r-1$ to r ($r \geqslant 1$). Let $\mathbf{A}$ be a ring in the class $\mathcal{F}$, and P be a projective module of constant rank over $\mathbf{A}[X_1, \ldots, X_r]$.
Let $\mathbf{B} = \mathbf{A}[(X_i)_{i<r}]$, $\mathbf{C} = \mathbf{A}[X_r]$, and V be the monoid of the monic polynomials of $\mathbf{A}[X_r]$. Thus $\mathbf{A}[X_1, \ldots, X_r] \simeq \mathbf{B}[X_r] \simeq \mathbf{C}[(X_i)_{i<r}]$.
The ring $\mathbf{A}\langle X_r \rangle = V^{-1}\mathbf{C}$ is in the class $\mathcal{F}$.
The $\mathbf{A}\langle X_r \rangle[(X_i)_{i<r}]$-module P_V, which is projective of constant rank, is stably free by induction hypothesis.
If S is the monoid of the monic polynomials of $\mathbf{B}[X_r]$, we have $V \subseteq S$, and so P_S is stably free over the ring $S^{-1}\mathbf{B}[X_r]$. By item *2* of Lemma 4.6, P is stably free. □

4.10. Corollary. *If $\mathbf{K}$ is a discrete field, every finitely generated projective module over $\mathbf{K}[X_1, \ldots, X_r]$ is stably free.*

D We apply the previous result with the class $\mathcal{F}$ of the discrete fields: if $\mathbf{K}$ is a discrete field, then $\mathbf{K}\langle X \rangle = \mathbf{K}(X)$ is also a discrete field. □

5. Solution to Serre's problem

In this section we present several constructive solutions to Serre's problem, in which $\mathbf{K}$ is a discrete field.

The finitely generated projective modules over $\mathbf{K}[X_1, \ldots, X_r]$ are free

À la Quillen

The solution by Quillen of Serre's problem is based on the Local Horrocks' theorem and on the following *Quillen induction* (see [Lam06]).

5.1. Abstract Quillen induction.
Let $\mathcal{F}$ be a class of rings that satisfies the following properties.

(Q1) *If $\mathbf{A} \in \mathcal{F}$, then $\mathbf{A}\langle X \rangle \in \mathcal{F}$.*

(Q2) *If $\mathbf{A} \in \mathcal{F}$, then $\mathbf{A}_\mathfrak{m} \in \mathcal{F}$ for every maximal ideal $\mathfrak{m}$ of $\mathbf{A}$.*

(Q3) *If $\mathbf{A} \in \mathcal{F}$ is local, every finitely generated projective $\mathbf{A}[X]$-module is extended from $\mathbf{A}$ (i.e. free).*

Then, for all $\mathbf{A} \in \mathcal{F}$ and all $r \geqslant 1$, every finitely generated projective module over $\mathbf{A}[X_1, \ldots, X_r]$ is extended from $\mathbf{A}$.

Actually, the properties (Q1), (Q2) and (Q3) are first used by Quillen to obtain the case $r = 1$, by using the Local Horrocks' theorem and the Quillen patching. The "proof by induction" part is based over the case $r = 1$, over (Q1) and over Horrocks' theorem (local or affine).

In what follows we isolate this proof by induction, which we qualify as a "concrete" Quillen induction. We replace (Q3) with a stronger version (q3) which is case $r = 1$.

In a posterior comment, we explain how we can actually somehow replace (q3) with (Q3) without losing the constructive character of the proof.

The proof by induction itself

5.2. Theorem. (Concrete Quillen induction)
Let $\mathcal{F}$ be a class of rings that satisfy the following properties.

(q1) *If* $\mathbf{A} \in \mathcal{F}$, *then* $\mathbf{A}\langle X\rangle \in \mathcal{F}$.

(q3) *If* $\mathbf{A} \in \mathcal{F}$, *every finitely generated projective* $\mathbf{A}[X]$*-module is extended from* $\mathbf{A}$.

Then, for all $\mathbf{A} \in \mathcal{F}$ *and all* $r \geqslant 1$, *every finitely generated projective module over* $\mathbf{A}[X_1, \dots, X_r]$ *is extended from* $\mathbf{A}$.

D Let us pass from $r \geqslant 1$ to $r + 1$. Consider a finitely generated projective $\mathbf{A}[X_1, \dots, X_r, Y]$-module $P = P(X_1, \dots, X_r, Y) = P(\underline{X}, Y)$. Let

- $P(\underline{X}, 0)$ be the $\mathbf{A}[\underline{X}]$-module obtained by the homomorphism $Y \mapsto 0$,
- $P(\underline{0}, Y)$ be the $\mathbf{A}[Y]$-module obtained by the homomorphism $\underline{X} \mapsto \underline{0}$,
- $P(\underline{0}, 0)$ be the $\mathbf{A}$-module obtained by the homomorphism $\underline{X}, Y \mapsto \underline{0}, 0$.

We must show that $P(\underline{X}, Y) \simeq P(\underline{0}, 0)$ over $\mathbf{A}[\underline{X}, Y]$.
We call S the monoid of the monic polynomials of $\mathbf{A}[Y]$, that is contained in the monoid S' of the monic polynomials of $\mathbf{A}[\underline{X}][Y]$. We then have

1. $P(\underline{X}, Y) \simeq P(\underline{0}, Y)$ over $\mathbf{A}\langle Y\rangle[\underline{X}] = \mathbf{A}[\underline{X}, Y]_S$ by induction hypothesis since $\mathbf{A}\langle Y\rangle \in \mathcal{F}$,
2. a fortiori $P(\underline{X}, Y) \simeq P(\underline{0}, Y)$ over $\mathbf{A}[\underline{X}]\langle Y\rangle = \mathbf{A}[\underline{X}, Y]_{S'}$,
3. $P(\underline{0}, Y) \simeq P(\underline{0}, 0)$ over $\mathbf{A}[Y]$ by the case $r = 1$,
4. $P(\underline{0}, 0) \simeq P(\underline{X}, 0)$ over $\mathbf{A}[\underline{X}]$ by induction hypothesis,
5. by combining 2, 3 and 4, we have $P(\underline{X}, Y) \simeq P(\underline{X}, 0)$ over $\mathbf{A}[\underline{X}]\langle Y\rangle$,
6. so, by the Affine Horrocks' theorem, $P(\underline{X}, Y) \simeq P(\underline{X}, 0)$ over $\mathbf{A}[\underline{X}, Y]$,
7. we combine this last isomorphism with the isomorphism between $P(\underline{X}, 0)$ and $P(\underline{0}, 0)$ over the ring $\mathbf{A}[\underline{X}]$ obtained by induction hypothesis.

□

5.3. Corollary. (Quillen-Suslin theorem, Quillen's proof)
If $\mathbf{K}$ is a discrete field (resp. a zero-dimensional ring), every finitely generated projective module over $\mathbf{K}[X_1,\dots,X_r]$ is free (resp. quasi-free).

D The concrete Quillen induction applies with the class $\mathcal{F}$ of discrete fields: note that $\mathbf{K}[X]$ is a Bézout domain, therefore the finitely generated projective modules over $\mathbf{K}[X]$ are free, and a fortiori extended. We pass to the reduced zero-dimensional rings by the elementary local-global machinery no. 2. Finally, for the zero-dimensional rings, we use the equality $\mathsf{GK}_0(\mathbf{A}) = \mathsf{GK}_0(\mathbf{A}_{\text{red}})$. □

Remarks. 1) Recall that a zero-dimensional ring is connected if and only if it is local. If $\mathbf{K}$ is such a ring, every finitely generated projective module over $\mathbf{K}[X_1,\dots,X_r]$ is free.
2) The concrete Quillen induction applies to the Bézout domain of Krull dimension $\leqslant 1$ (see Exercise 5) and more generally to the Prüfer rings of dimension $\leqslant 1$ (see Theorem 6.11). This generalizes the case of the Dedekind domains obtained by Quillen. For the case of regular Noetherian rings of Krull dimension $\leqslant 2$ (which we do not treat in this book), see [Lam06]. ■

(Q3) versus (q3)

The abstract Quillen induction (which does not provide any constructive results) presents the advantage of using a hypothesis (Q3) weaker than the hypothesis (q3) used in the concrete induction. We now explain how we can constructively recoup the situation, even for the hypothesis (Q3).

The free case.

In the case where the class $\mathcal{F}$ is such that the finitely generated projective modules are free, we observe that the hypothesis (q3) is actually useless. Indeed, let P be a finitely generated projective $\mathbf{A}[X]$-module and S be the monoid of the monic polynomials of $\mathbf{A}[X]$. Then, by (q1) the $\mathbf{A}\langle X\rangle$-module P_S is free, so extended from $\mathbf{A}$. But then, by the Affine Horrocks' theorem, the module P is extended from $\mathbf{A}$. In other words we have proved the following particularly simple version, for the free case.

5.4. Theorem. (Concrete Quillen induction, free case)
Let $\mathcal{F}$ be a class of rings that satisfies the following properties.

(q0) *If $\mathbf{A} \in \mathcal{F}$, every finitely generated projective $\mathbf{A}$-module is free.*

(q1) *If $\mathbf{A} \in \mathcal{F}$, then $\mathbf{A}\langle X\rangle \in \mathcal{F}$.*

Then, for all $\mathbf{A} \in \mathcal{F}$ and all $r \geqslant 1$, every finitely generated projective module over $\mathbf{A}[X_1,\dots,X_r]$ is free.

The general case.

We would have noticed that the property (Q2) does not intervene in the concrete Quillen induction: this hypothesis is rendered useless by the hypothesis (q3).

The property (Q2) however intervenes when we want to replace (q3) with (Q3), which is a hypothesis a priori weaker than (q3).

We think that this weakening of the hypothesis is always possible in practice, without losing the constructive character of the result. However, this is based on the basic local-global machinery (local-global machinery with prime ideals), and as the latter is a proof method and not strictly speaking a theorem, we were not able to formulate our concrete induction directly with (Q3), because we wanted a theorem in due form.

Let us move on to the explanation of the replacement of the strong hypothesis (q3) with the weak hypothesis (Q3).

We re-express the hypothesis (Q2) in the following more general form.

(q2) If $\mathbf{A} \in \mathcal{F}$ and S is a monoid of $\mathbf{A}$, then $\mathbf{A}_S \in \mathcal{F}$.

We suppose that (Q3) is satisfied in the following form: under the hypothesis that $\mathbf{A}$ is a residually discrete local ring in the class $\mathcal{F}$ we have a constructive proof of the fact that every finitely generated projective module P over $\mathbf{A}[X]$ is extended, which is translated into a computation algorithm (for the isomorphism between P and $P(0)$) based on the properties of the class $\mathcal{F}$ and on the disjunction

$$a \in \mathbf{A}^\times \quad \text{or} \quad a \in \operatorname{Rad}(\mathbf{A})$$

for the elements a that occur during the algorithm. Under these conditions the basic local-global machinery applies. Consequently for a finitely generated projective module P over $\mathbf{A}[X]$ for an arbitrary ring $\mathbf{A} \in \mathcal{F}$, the proof given in the local residually discrete case, followed step by step, provides us with comaximal monoids S_1, …, S_ℓ such that for each of them, the module P_{S_i} (over $\mathbf{A}_{S_i}[X]$) is extended from $\mathbf{A}_{S_i}$. Note that for this method to work, the considered class of rings must satisfy (q2), and that we can limit ourselves to the localizations at monoids $\mathcal{S}(a_1, \dots, a_n; b)$. It then only remains to apply the Quillen patching (concrete local-global principle 3.7) to obtain the desired result: the module P is extended from $\mathbf{A}$.

À la Suslin, Vaserstein or Rao

The solution by Suslin to Serre's conjecture consists in showing that every stably free module over $\mathbf{K}[X_1, \dots, X_r]$ is free (Serre had already proven that every finitely generated projective module over $\mathbf{K}[X_1, \dots, X_r]$ is stably free), in other words that the kernel of every surjective matrix is free, or that every unimodular vector is the first column of an invertible matrix (see Fact V-4.1 and Proposition V-4.6).

If $\mathcal{G}$ is a subgroup of $\mathbb{GL}_n(\mathbf{A})$ and A, $B \in \mathbf{A}^{n\times 1}$, we will write $A \overset{\mathcal{G}}{\sim} B$ to say that there exists a matrix $H \in \mathcal{G}$ such that $HA = B$. It is clear that this is an equivalence relation.

Recall that a unimodular vector $f \in \mathbf{A}^{n\times 1}$ is said to be completable if it is the first column vector of a matrix $G \in \mathbb{GL}_n(\mathbf{A})$. This amounts to saying that we have

$$f \overset{\mathbb{GL}_n(\mathbf{A})}{\sim} {}^{\mathrm{t}}[\,1\;0\;\cdots\;0\,].$$

The goal in this subsection is therefore to obtain a constructive proof of the following theorem.

5.5. Theorem. (Suslin)
Every unimodular vector f with coordinates in $\mathbf{K}[X_1,\ldots,X_r] = \mathbf{K}[\underline{X}]$ (where $\mathbf{K}$ is a discrete field) is completable.

We will give three distinct proofs, in chronological order.

First proof

Here we follow very closely Suslin's original proof. We only have to get rid of a nonconstructive usage of a generic maximal ideal, and have already done this work when we gave a constructive proof of Suslin's lemma (Lemma XV-6.1) in Chapter XV.

5.6. Fact. *Let M, $N \in \mathbb{M}_2(\mathbf{A})$. We have $\mathrm{Tr}(M)\,\mathrm{I}_2 = M + \widetilde{M}$ and*

$$\det(M+N) = \det(M) + \mathrm{Tr}(\widetilde{M}\,N) + \det(N).$$

D For the matrices in $\mathbb{M}_2(\mathbf{A})$, the map $M \mapsto \widetilde{M}$ is linear, so

$$\begin{aligned} \det(M+N)\,\mathrm{I}_2 \;=\; (\widetilde{M}+\widetilde{N})(M+N) &= \widetilde{M}M + (\widetilde{M}N + \widetilde{N}M) + \widetilde{N}N \\ &= \big(\det(M) + \mathrm{Tr}(\widetilde{M}\,N) + \det(N)\big)\,\mathrm{I}_2. \end{aligned}$$

□

5.7. Lemma. *Let $B \in \mathbb{M}_2(\mathbf{A})$, $H = H(X) \in \mathbb{M}_2(\mathbf{A}[X])$, $\mathbf{B}$ be an $\mathbf{A}$-algebra and $x \in \mathbf{B}$. Let $C(X) = B + XH$. Suppose $\det C = \det B = a$. By letting $S = \mathrm{I}_2 + x\widetilde{H}(ax)\,B$, we then have $S \in \mathbb{SL}_2(\mathbf{A})$ and $S\widetilde{B} = \widetilde{C}(ax)$.*

D Fact 5.6 gives $\det(C) = \det(B) + X\,(\mathrm{Tr}(\widetilde{H}\,B) + X\det H)$, and therefore

$$E(X) = \mathrm{Tr}(\widetilde{H}\,B) + X\det H = 0.$$

Let $H_1 = H(ax)$ and $C_1 = C(ax)$.
We have then $S\widetilde{B} = \widetilde{B} + x\widetilde{H_1}B\widetilde{B} = \widetilde{B} + ax\widetilde{H_1} = \widetilde{C_1}$ and

$$\begin{aligned} \det(S) &= 1 + x\,\mathrm{Tr}(\widetilde{H_1}B) + \det(x\widetilde{H_1}B) \\ &= 1 + x\,\mathrm{Tr}(\widetilde{H_1}B) + x^2a\det(H_1) = 1 + xE(ax) = 1. \end{aligned}$$

□

5.8. Lemma. (Suslin's lemma)
Let u, $v \in \mathbf{A}[X]$, $a \in \mathbf{A} \cap \langle u, v\rangle$, $\mathbf{B}$ be an $\mathbf{A}$-algebra and b, $b' \in \mathbf{B}$.
If $b \equiv b' \bmod a\mathbf{B}$, then $\begin{bmatrix} u(b) \\ v(b) \end{bmatrix} \overset{\mathbb{SL}_2(\mathbf{B})}{\sim} \begin{bmatrix} u(b') \\ v(b') \end{bmatrix}$.

D Let $p, q \in \mathbf{A}[X]$ such that $up + vq = a$ and $x \in \mathbf{B}$ such that $b' = b + ax$. Consider the matrix $M = \begin{bmatrix} p & q \\ -v & u \end{bmatrix} \in \mathbb{M}_2(\mathbf{A}[X])$. We apply Lemma 5.7 with the matrices $B = M(b)$ and $C(X) = M(b + X)$.
Note that the first column of $\widetilde{B}$ is $\begin{bmatrix} u(b) \\ v(b) \end{bmatrix}$ and that the first column of $\widetilde{C}(ax)$ is $\begin{bmatrix} u(b') \\ v(b') \end{bmatrix}$. □

5.9. Lemma. *Let $f \in \mathbf{A}[X]^{n \times 1}$, $\mathbf{B}$ be an $\mathbf{A}$-algebra and $\mathcal{G}$ be a subgroup of $\mathbb{GL}_n(\mathbf{B})$, then the set*

$$\mathfrak{a} = \left\{ a \in \mathbf{A} \mid \forall b,\, b' \in \mathbf{B}, \big((b \equiv b' \bmod a\mathbf{B}) \ \Rightarrow\ f(b) \overset{\mathcal{G}}{\sim} f(b')\big) \right\}$$

is an ideal of $\mathbf{A}$.

D The proof is left to the reader. □

5.10. Theorem. *Let $n \geqslant 2$, f be a unimodular vector of $\mathbf{A}[X]^{n \times 1}$ with f_1 monic, $\mathbf{B}$ be an $\mathbf{A}$-algebra, and $\mathcal{G} \subseteq \mathbb{GL}_n(\mathbf{B})$ be the subgroup generated by $\mathbb{E}_n(\mathbf{B})$ and $\mathbb{SL}_2(\mathbf{B})$.*[1] *Then, for all b, $b' \in \mathbf{B}$, we have $f(b) \overset{\mathcal{G}}{\sim} f(b')$.*

D It suffices to show that the ideal $\mathfrak{a}$ defined in Lemma 5.9 contains 1. For an elementary matrix $E = E(X) \in \mathbb{E}_{n-1}(\mathbf{A}[X])$, we consider the vector

$$\begin{bmatrix} g_2 \\ \vdots \\ g_n \end{bmatrix} = E \begin{bmatrix} f_2 \\ \vdots \\ f_n \end{bmatrix}.$$

We will show that the resultant $a = \mathrm{Res}_X(f_1, g_2)$, which is well-defined since f_1 is monic, is an element of $\mathfrak{a}$. We will therefore finish by invoking Suslin's lemma XV-6.1.
Let us therefore show that $a \in \mathfrak{a}$. We just use the fact that $a \in \langle f_1, g_2\rangle \cap \mathbf{A}$. We take b, $b' \in \mathbf{B}$ with $b \equiv b' \bmod a\mathbf{B}$. We want to reach $f(b) \overset{\mathcal{G}}{\sim} f(b')$. Note that for $i \geqslant 2$ we have

$$\begin{aligned} g_i(b') - g_i(b) \in \langle b' - b\rangle \subseteq \langle a\rangle \subseteq \langle f_1(b), g_2(b)\rangle\,, \\ \text{i.e.} \quad g_i(b') \in g_i(b) + \langle f_1(b), g_2(b)\rangle\,. \end{aligned} \tag{1}$$

[1] $\mathbb{SL}_2(\mathbf{B})$ is embedded in $\mathbb{GL}_n(\mathbf{B})$ by the injection $A \mapsto \mathrm{Diag}(A, \mathrm{I}_{n-2}$.

We then have a sequence of equivalences

$$\begin{bmatrix} f_1(b) \\ f_2(b) \\ f_3(b) \\ \vdots \\ f_n(b) \end{bmatrix} \overset{E(b)}{\sim} \begin{bmatrix} f_1(b) \\ g_2(b) \\ g_3(b) \\ \vdots \\ g_n(b) \end{bmatrix} \overset{\mathbb{E}_n(\mathbf{B})}{\sim} \begin{bmatrix} f_1(b) \\ g_2(b) \\ g_3(b') \\ \vdots \\ g_n(b') \end{bmatrix} \overset{\mathbb{SL}_2(\mathbf{B})}{\sim} \begin{bmatrix} f_1(b') \\ g_2(b') \\ g_3(b') \\ \vdots \\ g_n(b') \end{bmatrix} \overset{E(b')^{-1}}{\sim} \begin{bmatrix} f_1(b') \\ f_2(b') \\ f_3(b') \\ \vdots \\ f_n(b') \end{bmatrix}.$$

The second is given by Equation (1), the third by Lemma 5.8 applied to $u = f_1$ and $v = g_2$. □

5.11. Corollary. *Let $n \geqslant 2$, f be a unimodular vector of $\mathbf{A}[X]^{n\times 1}$ with f_1 monic and $\mathcal{G}$ be the subgroup of $\mathbb{GL}_n(\mathbf{A}[X])$ generated by $\mathbb{E}_n(\mathbf{A}[X])$ and $\mathbb{SL}_2(\mathbf{A}[X])$. Then $f \overset{\mathcal{G}}{\sim} f(0)$.*

D In Theorem 5.10, we take $\mathbf{B} = \mathbf{A}[X]$, $b = X$ and $b' = 0$. □

5.12. Corollary. *Let $\mathbf{K}$ be a discrete field, $n \geqslant 2$, f be a unimodular vector of $\mathbf{K}[\underline{X}]^{n\times 1}$, where $\mathbf{K}[\underline{X}] = \mathbf{K}[X_1, \ldots, X_r]$, and $\mathcal{G} \subseteq \mathbb{GL}_n(\mathbf{K}[\underline{X}])$ be the subgroup generated by $\mathbb{E}_n(\mathbf{K}[\underline{X}])$ and $\mathbb{SL}_2(\mathbf{K}[\underline{X}])$. Then $f \overset{\mathcal{G}}{\sim} {}^{\mathrm{t}}[\,1\ 0\ \cdots\ 0\,]$.*

D If $f_1 = 0$, we easily transform the vector f into ${}^{\mathrm{t}}[\,1\ 0\ \cdots\ 0\,]$ by elementary operations. Otherwise, a change of variables allows us to transform f_1 into a pseudomonic polynomial in X_r (Lemma VII-1.4). We can therefore assume that f_1 is monic in X_r, we apply Corollary 5.11 with the ring $\mathbf{A} = \mathbf{K}[X_1, \ldots, X_{r-1}]$, and we obtain $f \overset{\mathcal{G}}{\sim} f(X_1, \ldots, X_{r-1}, 0)$. We conclude by induction on r. □

We have indeed obtained Theorem 5.5, actually with an interesting precision over the group $\mathcal{G}$.

Second proof

We now closely follow a proof by Vaserstein [194] such as it is presented in [Lam06] but by using constructive arguments.

More generally we are interested in the possibility of finding in the equivalence class of a vector defined over $\mathbf{A}[X]$ a vector defined over $\mathbf{A}$, in a suitable sense.

We will use the following lemma.

5.13. Lemma. *Let $\mathbf{A}$ be a ring and $f(X) = {}^{\mathrm{t}}[\,f_1(X)\ \cdots\ f_n(X)\,]$ be a unimodular vector in $\mathbf{A}[X]^{n\times 1}$, with f_1 monic of degree $\geqslant 1$.*
Then, the ideal $\mathfrak{a} = \mathrm{c}(f_2) + \cdots + \mathrm{c}(f_n)$ contains 1.

D We have $1 = u_1 f_1$ in $\mathbf{A}/\mathfrak{a}$. This equality in the ring $(\mathbf{A}/\mathfrak{a})[X]$, with f_1 monic of degree $\geqslant 1$ implies that $\mathbf{A}/\mathfrak{a}$ is trivial (by induction on the formal degree of u_1). □

5.14. Theorem. (Little Horrocks' local theorem)
Let $n \geqslant 3$ be an integer, $\mathbf{A}$ be a residually discrete local ring and $f(X) = {}^{\mathrm{t}}[\, f_1(X) \ \cdots \ f_n(X)\,]$ be a unimodular vector in $\mathbf{A}[X]^{n\times 1}$, with f_1 monic. Then

$$f(X) = \begin{bmatrix} f_1 \\ \vdots \\ \vdots \\ f_n \end{bmatrix} \overset{\mathbb{E}_n(\mathbf{A}[X])}{\sim} \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \overset{\mathbb{E}_n(\mathbf{A})}{\sim} \begin{bmatrix} f_1(0) \\ \vdots \\ \vdots \\ f_n(0) \end{bmatrix}.$$

D Let d be the degree of f_1. By elementary row operations, we bring the polynomials $f_2, \ldots, f_n$ to being of degrees $< d$. Let $f_{i,j}$ be the coefficient of X^j in f_i. The vector ${}^{\mathrm{t}}[\, f_1(X) \ \cdots \ f_n(X)\,]$ remains unimodular. If $d = 0$, we are done. Otherwise given Lemma 5.13 and since the ring is local, one of the $f_{i,j}$'s for $i \in [\![2..n]\!]$ is a unit. Suppose for example that $f_{2,k}$ is invertible. We will see that we can find two polynomials v_1 and v_2 such that the polynomial $g_2 = v_1 f_1 + v_2 f_2$ is monic of degre $d-1$. If $k = d-1$, this works with $v_1 = 0$ and v_2 constant. If $k < d-1$, consider the following disjunction

$$f_{2,d-1} \in \mathbf{A}^{\times} \quad \text{or} \quad f_{2,d-1} \in \mathrm{Rad}(\mathbf{A}).$$

In the first case, we are reduced to $k = d-1$. In the second case the polynomial $q_2 = X f_2 - f_{2,d-1} f_1$ is of degree $\leqslant d-1$ and satisfies: $q_{2,k+1}$ is a unit. We have gained some ground: it now suffices to iterate the process. Now we therefore have $g_2 = v_1 f_1 + v_2 f_2$ of degree $d-1$ and monic. So we can divide f_3 by g_2 and we obtain $g_3 = f_3 - g_2 q$ of degree $< d-1$ ($q \in \mathbf{A}$), so the polynomial

$$h_1 = g_2 + g_3 = f_3 + g_2(1-q) = f_3 + (1-q)v_1 f_1 + (1-q)v_2 f_2$$

is monic of degree $d-1$. Thus, by an elementary row operation we were able to replace ${}^{\mathrm{t}}[\, f_1 \ f_2 \ f_3\,]$ with ${}^{\mathrm{t}}[\, f_1 \ f_2 \ h_1\,]$, with h_1 monic of degree $d-1$. We can therefore by a sequence of elementary row operations bring the vector ${}^{\mathrm{t}}[\, f_1(X) \ \ldots \ f_n(X)\,]$, with f_1 monic of degree d, to

$${}^{\mathrm{t}}[\, h_1(X) \ \ldots \ h_n(X)\,] \text{ with } h_1 \text{ monic of degree } d-1.$$

We obtain the desired result by induction on d. □

Terminology. We consider a system of formal polynomials (f_i) with $\deg f_i = d_i$. We then call the "head ideal of the system (f_i)" the ideal of the formally leading coefficients of the f_i's.

5.15. Theorem. (Little Horrocks' global theorem)
Let $n \geqslant 2$ be an integer, $\mathbf{A}$ be a ring and $f \in \mathbf{A}[X]^{n\times 1}$ be a unimodular vector. Suppose that the head ideal of the f_i's contains 1. *Then*

$$f(X) = \begin{bmatrix} f_1 \\ \vdots \\ f_n \end{bmatrix} \overset{\mathbb{GL}_n(\mathbf{A}[X])}{\sim} \begin{bmatrix} f_1(0) \\ \vdots \\ f_n(0) \end{bmatrix} = f(0).$$

D The case $n = 2$ is an exception: if $u_1 f_1 + u_2 f_2 = 1$, the equality

$$\begin{bmatrix} u_1 & u_2 \\ -f_2 & f_1 \end{bmatrix} \begin{bmatrix} f_1 \\ f_2 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

gives the required matrix, in $\mathbb{SL}_2(\mathbf{A}[X])$.
For $n \geqslant 3$, we apply the basic local-global machinery (page 871) with the constructive proof of Theorem 5.14. We obtain a finite family of comaximal monoids, $(S_i)_{i\in J}$ in $\mathbf{A}$, such that for each i we have $f(X) \overset{\mathbb{E}_n(\mathbf{A}_{S_i}[X])}{\sim} f(0)$. We conclude with the Vaserstein patching for the equivalences of matrices on the left-hand side (item *2* of the local-global principle 3.6). □

Conclusion. We have just obtained a (slightly weaker) variant of Corollary 5.11, and this gives the proof of Suslin's theorem 5.5 in the same way as in the first solution.

Comment. The little Horrocks' global theorem can also be obtained as a consequence of the "grand" Horrocks' global theorem 4.7. Let $P = \operatorname{Ker} {}^{\mathrm{t}}f(X)$. By localizing at f_1, P becomes free. The Affine Horrocks' theorem tells us that P is free, which means that $f(X) \sim {}^{\mathrm{t}}[\,1\;0\;\cdots\;0\,]$ over $\mathbb{GL}_n(\mathbf{A}[X])$. ■

Third proof

We now closely follow a proof by Rao. This time we will not need any induction on the number of variables to reach Suslin's theorem.

5.16. Lemma. *We consider a vector $x = (x_1, \ldots, x_n) \in \mathbf{A}^n$ and $s \in \mathbf{A}$. If x is unimodular over $\mathbf{A}/\langle s\rangle$ and over $\mathbf{A}[1/s]$, it is unimodular.*

D Let $\mathfrak{a} = \langle x_1, \ldots, x_n\rangle$. We have $s^r \in \mathfrak{a}$ (for a certain r) and $1 - as \in \mathfrak{a}$ (for a certain a). We write $1 = a^r s^r + (1 - as)(1 + as + \cdots) \in \mathfrak{a}$. □

5.17. Lemma. *Let $n \geqslant 2$ be an integer, $\mathbf{A}$ be a ring, and f be a unimodular vector in $\mathbf{A}[X]^{n\times 1}$: $f = {}^{\mathrm{t}}[\,f_1(X)\;\cdots\;f_n(X)\,]$. For each f_i of formal degree d_i, let $f_i^\star$ be the* formal reciprocal polynomial $X^{d_i} f_i(1/X)$. *Let $f^\star(X) = {}^{\mathrm{t}}[\,f_1^\star(X),\;\cdots\;f_n^\star(X)\,]$. If $f^\star(0)$ is unimodular, the same goes for $f^\star$.*

D By Lemma 5.16, it suffices to prove that $f^\star(0)$ is unimodular (it is true by hypothesis) and that $f^\star$ is unimodular over $\mathbf{A}[X, 1/X]$, which comes from the equality $\sum_i u_i(1/X)X^{-d_i} f_i^\star = 1$ (where $\sum_i u_i f_i = 1$ in $\mathbf{A}[X]$). □

5.18. Theorem. (Rao's theorem, [158])
Let $n \geqslant 2$ be an integer, $\mathbf{A}$ be a ring, and $f = {}^{\mathrm{t}}[\, f_1(X) \; \cdots \; f_n(X) \,]$ be a unimodular vector in $\mathbf{A}[X]^{n\times 1}$, with 1 in the head ideal of the f_i's. Then

$$f \overset{\mathbb{GL}_n(\mathbf{A}[X])}{\sim} f(0) \overset{\mathbb{GL}_n(\mathbf{A})}{\sim} f^\star(0) \overset{\mathbb{GL}_n(\mathbf{A}[X])}{\sim} f^\star.$$

If in addition one of the f_i's is monic, we have $f \overset{\mathbb{GL}_n(\mathbf{A}[X])}{\sim} {}^{\mathrm{t}}[\, 1 \; 0 \; \cdots \; 0 \,]$.

D Since $f \sim f(0)$ by the little Horrocks' global theorem, we deduce that $f \sim f(1)$. In addition, $f^\star(0)$ is unimodular therefore $f^\star$ is unimodular (by Lemma 5.17). Moreover, 1 is in the head ideal of the $f_i^\star$'s, which allows us to apply to $f^\star$ the little Horrocks' global theorem.
We conclude: $f \sim f(0) \sim f(1) = f^\star(1) \sim f^\star$. □

Comment. The same result is valid by replacing $\mathbb{GL}_n$ by $\mathbb{E}_n$, but the proof is strictly more delicate (see Theorem XVII-4.7). ■

Conclusion. We then obtain Suslin's theorem 5.5 (page 920) as follows. We take for $\mathbf{A}$ the ring $\mathbf{K}[X_1, \ldots, X_{r-1}]$ and we make a change of variables that renders pseudomonic one of the polynomials.
Thus,

- on the one hand, the solution is much more "efficient" than in the first two proofs since there is no longer an induction on the number of variables,
- and on the other hand, the theorem is much more general.

6. Projective modules extended from valuation or arithmetic rings

Recall that a valuation ring is a reduced ring in which we have, for all a, b, a divides b or b divides a. It is a normal, local ring without zerodivisors.

We begin with a useful result regarding valuation rings and the Krull dimension (we can also refer back to Exercise XII-3).

6.1. Lemma. *If $\mathbf{A}$ is a valuation ring, then so is $\mathbf{A}(X)$. If $\mathbf{A}$ is a valuation ring of finite Krull dimension, then $\mathbf{A}(X)$ has the same Krull dimension.*

D If $\mathbf{A}$ is a valuation ring, every $f \in \mathbf{A}[X]$ is expressible in the form $f = ag$ with $a \in \mathbf{A}$ and $g \in \mathbf{A}[X]$ which admits a coefficient equal to 1. In particular, g is invertible in $\mathbf{A}(X)$. If $F_1 = a_1g_1/u_1$ and $F_2 = a_2g_2/u_2$ are two arbitrary elements of $\mathbf{A}(X)$ (with $a_i \in \mathbf{A}$ and g_i, u_i primitive in $\mathbf{A}[X]$), then F_1 divides F_2 in $\mathbf{A}(X)$ if and only if a_1 divides a_2 in $\mathbf{A}$. Therefore "the divisibility is identical in $\mathbf{A}$ and $\mathbf{A}(X)$" and $\mathbf{A}(X)$ is a valuation ring. In addition, since the finitely generated ideals are principal, the canonical homomorphism $\mathsf{Zar}\,\mathbf{A} \to \mathsf{Zar}\,\mathbf{A}(X)$ is an isomorphism of distributive lattices (note: these are totally ordered sets), which implies that the Krull dimension is the same. □

The univariate case

This subsection is devoted in the most part to a constructive proof of the following Bass' theorem.

6.2. Theorem. *If $\mathbf{V}$ is a valuation ring of finite Krull dimension, every finitely generated projective $\mathbf{V}[X]$-module is free.*

We will actually prove slightly stronger variants: we can get rid off the hypothesis on the Krull dimension, and we have a version for arithmetic rings.

We start with a simple example.

A simple example

6.3. Proposition. *Every finitely generated projective module over $\mathbb{Z}[X]$ is free.*

D Let M be a finitely generated projective $\mathbb{Z}[X]$-module. First of all note that if M is of rank 1, it is free because $\mathbb{Z}[X]$ is a GCD-domain (Lemma 2.9). Now suppose that M is of rank $r > 1$. If we extend the scalars to $\mathbb{Q}[X]$, the module becomes free. Therefore there exists an integer $d > 0$ such that M becomes free over $\mathbb{Z}[1/d][X]$. If $d = 1$, nothing needs to be done. Otherwise, let $p_1, \ldots, p_k$ be the prime factors of d.

The monoids $d^{\mathbb{N}}$, $1 + p_1\mathbb{Z}$, …, $1 + p_k\mathbb{Z}$ are comaximal (see the fundamental example on page 22). It therefore suffices to show that the modules $M_{1+p_i\mathbb{Z}}$ are free (therefore extended), because then the Quillen patching implies that M is extended from $\mathbb{Z}$, therefore free.

Let p be any of the p_i's. Since $\mathbb{Z}_{1+p\mathbb{Z}}[X]$ is 2-stable (lemma below), by applying Serre's Splitting Off theorem (Theorem XIV-3.4), we obtain an isomorphism $M_{1+p\mathbb{Z}} \simeq \mathbb{Z}_{1+p\mathbb{Z}}[X]^{r-1} \oplus N$, with N being a projective $\mathbb{Z}_{1+p\mathbb{Z}}[X]$-module of constant rank 1. By the initial remark (which applies by replacing $\mathbb{Z}$ by $\mathbb{Z}_{1+p\mathbb{Z}}$), N is free, so M is free. □

6.4. Lemma. *The ring $\mathbb{Z}_{1+p\mathbb{Z}}[X]$ is 2-stable.*

D Consider the partition of $\mathsf{Spec}(\mathbb{Z}_{1+p\mathbb{Z}}[X])$ attached to $\{p\}$: more precisely, the ring $\mathbb{Z}_{1+p\mathbb{Z}}[X]$ is replaced by the two rings

$$\mathbb{Z}_{1+p\mathbb{Z}}[X][1/p] \simeq \mathbb{Q}[X] \text{ and } (\mathbb{Z}_{1+p\mathbb{Z}}[X])/\langle p\rangle \simeq \mathbb{F}_p[X],$$

which are of Krull dimension 1. Theorem XIV-4.16 then tells us that $\mathbb{Z}_{1+p\mathbb{Z}}[X]$ is 2-stable. □

Remark. Actually the use of prime factors of d, although intuitively natural, introduce an unnecessary complication. Indeed, the monoids $d^{\mathbb{N}}$ and $1 + d\mathbb{Z}$ being comaximal, it suffices to prove that $M_{1+d\mathbb{Z}}$ is free. As $\mathbb{Z}_{1+d\mathbb{Z}}[X]$ is a GCD-domain, the previous reasoning applies if we know how to show that $\mathbb{Z}_{1+d\mathbb{Z}}[X]$ is 2-stable. The proof of Lemma 6.4 works by replacing p by d, because $\mathbb{Z}_{1+d\mathbb{Z}}[X][1/d] \simeq \mathbb{Q}[X]$ and $\mathbb{Z}_{1+d\mathbb{Z}}[X]/\langle d\rangle \simeq (\mathbb{Z}/\langle d\rangle)[X]$, which are of Krull dimension 1 ($\mathbb{Z}/\langle d\rangle$ is zero-dimensional). ■

A more elaborate example

Given the previous remark we leave the proof of the following generalization to the reader.

6.5. Proposition. *Let $\mathbf{A}$ be an integral ring of Krull dimension $\leqslant 1$, d be an element of $\mathrm{Reg}(\mathbf{A})$, and M be a finitely generated projective $\mathbf{A}[X]$-module.*

1. $\mathbf{A}_{1+d\mathbf{A}}[1/d] = \mathrm{Frac}\,\mathbf{A}$ *is zero-dimensional.*
2. $\mathbf{A}_{1+d\mathbf{A}}/\langle d\rangle \simeq \mathbf{A}/\langle d\rangle$ *is zero-dimensional.*
3. $\mathbf{A}_{1+d\mathbf{A}}[X]$ *is 2-stable.*
4. *a. If $\mathbf{A}$ is a Bézout ring, M is free.*
   b. If $\mathbf{A}$ is seminormal, M is extended from $\mathbf{A}$.

An example in finite Krull dimension > 0

Let $\mathbf{V}$ be an integral ring with some elements $a_1, \ldots, a_k$. Suppose

$$\mathrm{D}_{\mathbf{V}}(a_1) \leqslant \mathrm{D}_{\mathbf{V}}(a_2) \leqslant \cdots \leqslant \mathrm{D}_{\mathbf{V}}(a_k).$$

The partition in constructible subsets of $\mathsf{Spec}\,\mathbf{V}$ associated with this family contains only $k+1$ elements

$$\mathrm{D}_{\mathbf{V}}(a_1),\ \mathrm{D}_{\mathbf{V}}(a_2) \setminus \mathrm{D}_{\mathbf{V}}(a_1),\ \ldots,\ \mathrm{D}_{\mathbf{V}}(a_k) \setminus \mathrm{D}_{\mathbf{V}}(a_{k-1}),\ \mathrm{D}_{\mathbf{V}}(1) \setminus \mathrm{D}_{\mathbf{V}}(a_k),$$

that correspond to the rings

$$\mathbf{V}[1/a_1],\ (\mathbf{V}/\langle a_1\rangle)[1/a_2],\ \ldots,\ (\mathbf{V}/\langle a_{k-1}\rangle)[1/a_k] \text{ and } \mathbf{V}/\langle a_k\rangle\,.$$

Now suppose that these rings are all *zero-dimensional*. Then, we similarly have a partition into $k+1$ constructible subsets of $\mathsf{Spec}\,\mathbf{V}[X]$ and the corresponding rings

$$\mathbf{V}[1/a_1][X],\ (\mathbf{V}/\langle a_1\rangle)[1/a_2][X],\ \ldots,\ (\mathbf{V}/\langle a_{k-1}\rangle)[1/a_k][X] \text{ and } (\mathbf{V}/\langle a_k\rangle)[X]$$

are all of Krull dimension $\leqslant 1$. Theorem XIV-4.16 then tells us that $\mathbf{V}[X]$ is 2-stable. Therefore if M is a projective $\mathbf{V}[X]$-module of constant rank r, by Serre's Splitting Off theorem, we obtain $M \simeq \mathbf{V}[X]^{r-1} \oplus N$, with N of constant rank 1.

If $\mathbf{V}$ is in addition a seminormal ring (resp. a GCD-domain), then N is extended from $\mathbf{V}$ (resp. then N is free), so M is extended from $\mathbf{V}$ (resp. M is free).

The result "$\mathbf{V}[X]$ is 2-stable" is satisfied when $\mathbf{V}$ is a valuation domain of Krull dimension k for which we have a precise sufficient knowledge of the valuation group. In classical mathematics (with **LEM** but without using the prime ideals or the axiom of choice) we therefore already obtain the desired Bass' theorem for valuation domains of finite Krull dimension.

However, the result is not of an algorithmic nature if we do not know how to compute some suitable elements a_i.

This difficulty will be bypassed dynamically.

Constructive proof of Bass' theorem

We need to establish the following theorem.

6.6. Theorem. *If $\mathbf{V}$ is a valuation ring, $\mathbf{V}[X]$ is 2-stable.*

We start with the following lemma (the proof of the theorem is postponed until page 929).

6.7. Lemma. *Let $\mathbf{V}$ be a valuation ring and $\mathbf{V}'$ be the valuation subring of $\mathbf{V}$ generated by a finite family of elements of $\mathbf{V}$. Then, $\mathbf{V}'[X]$ is 2-stable.*

D Let $\mathbf{V}_1$ be the subring of $\mathbf{V}$ generated by the finite family. We define

$$\mathbf{V}' = \{\, c/b \,|\, c, b \in \mathbf{V}_1,\ \text{regular } b \text{ divides } c \text{ in } \mathbf{V} \,\} \subseteq \mathrm{Frac}(\mathbf{V}_1).$$

It is easily seen that $\mathbf{V}'$ is a valuation domain. Moreover, since $\mathsf{Kdim}\,\mathbf{V}_1 \leqslant m$ for some m (see Lemma XIII-5.3), we have also $\mathsf{Kdim}\,\mathbf{V}' \leqslant m$. Indeed, consider a sequence $(z_1, \ldots, z_{m+1})$ in $\mathbf{V}'$, write $z_i = x_i/b$ with a common denominator b, and introduce a complementary sequence of $(x_1, \ldots, x_{m+1})$ in $\mathbf{V}_1$. A fortiori it is complementary in $\mathbf{V}'$.
Let ℓ_1, ℓ_2 and a in $\mathbf{W} = \mathbf{V}'[X]$. Let $L = (\ell_1, \ell_2)$ and $Q = (q_1, q_2)$. We are searching for q_1, $q_2 \in \mathbf{W}$ that satisfy $\mathrm{D}_{\mathbf{W}}(a, L) = \mathrm{D}_{\mathbf{W}}(L + aQ)$. If $\mathbf{V}'$ were a discrete field, we would have an algorithm to compute Q from L. By executing this algorithm, we would use the test "$y = 0$ or y invertible?" for some elements $y \in \mathbf{V}_1$ that occur during the computation (indeed, in the case where $\mathbf{V}'$ is a discrete field, some y/z in $\mathbf{V}'$ is null if y is null, invertible if y is invertible, z having been already certified as invertible).
We can transform the algorithm dynamically by replacing each test "$y = 0$ or y invertible?" by the splitting of "the current ring $\mathbf{A}$," which gives the

two rings $\mathbf{A}[1/y]$ and $\mathbf{A}/\mathrm{D}_{\mathbf{A}}(y)$.
At the beginning $\mathbf{A} = \mathbf{V}'$. As in $\mathbf{V}'$ the elements are comparable with respect to divisibility, all the introduced rings can be brought back to the standard form $\mathbf{V}'/\mathrm{D}_{\mathbf{V}'}(y_i)\,[1/y_{i-1}]$ ($i \in [\![2..k]\!]$) for a finite family $(y_i)_{i\in[\![1..k]\!]}$ of $\mathbf{V}_1$, with y_{i-1} dividing y_i in $\mathbf{V}'$ for $i \in [\![2..k]\!]$.
Here we might have the impression of having succeeded insofar as we could say that: we now apply Lemma XIV-4.15.
However, by reading the proof of this lemma, we see that during a splitting $\mathbf{B} \mapsto (\mathbf{B}[1/b], \mathbf{B}/\langle b\rangle)$, first the given L and a produce some Q for $\mathbf{B}/\langle b\rangle$, then $L + aQ$ and ab produce some R for $\mathbf{B}[1/b]$, the final result being that $Q + bR$ suits for L and a in $\mathbf{B}$.
Thus the dynamic of our transformed algorithm must be more carefully controlled.[2] What saves us is that in our dynamic use of Lemma XIV-4.15, the computations that start with L and a remain entirely in $\mathbf{V}' \subseteq \mathrm{Frac}(\mathbf{V}_1)$. Consequently, we can be certain not to fall into an infinite loop where the number of rings $\mathbf{V}'/\mathrm{D}_{\mathbf{V}'}(y_i)\,[1/y_{i-1}]$ would increase indefinitely, which would prevent the algorithm from halting. Indeed, if $k > m$ (where $\mathsf{Kdim}\,\mathbf{V}' \leqslant m$), the sequence $(y_1, \ldots, y_k)$ is singular, and since $\mathrm{D}_{\mathbf{V}'}(y_{i-1}) \leqslant \mathrm{D}_{\mathbf{V}'}(y_i)$ and $\mathsf{Zar}\,\mathbf{V}'$ is totally ordered, Lemma XIII-8.3 tells us that one of the following three situations occurs

- $\mathrm{D}_{\mathbf{V}'}(y_1) = 0$, in which case the ring $\mathbf{V}'/\mathrm{D}_{\mathbf{V}'}(y_2)\,[1/y_1]$ is trivial and the list is shortened by deleting y_1,
- $\mathrm{D}_{\mathbf{V}'}(y_{m+1}) = 1$, in which case the ring $\mathbf{V}'/\mathrm{D}_{\mathbf{V}'}(y_{m+1})\,[1/y_m]$ is trivial and the list is shortened by deleting y_{m+1},
- for some $i \in [\![2, m+1]\!]$, we have the equality $\mathrm{D}_{\mathbf{V}'}(y_{i-1}) = \mathrm{D}_{\mathbf{V}'}(y_i)$, in which case the ring $\mathbf{V}'/\mathrm{D}_{\mathbf{V}'}(y_i)\,[1/y_{i-1}]$ is trivial and the list is shortened by deleting y_i.

□

Remark. Thus, once $\mathbf{V}_1$ is fixed, the ring $\mathbf{V}'$ behaves, with regard to the 2-stability of $\mathbf{V}'[X]$ as the ring of finite Krull dimension "> 0 but entirely controlled" which was given in the previous subsection: the sequence of the y_i's, limited to m terms, behaves like the sequence of the a_i's of the previous subsection, except that the y_i's are produced dynamically as the algorithm executes whereas the a_i's were given at the start. ■

Proof of Theorem 6.6. Let ℓ_1, ℓ_2 and a in $\mathbf{V}[X]$. We search for $q_1, q_2 \in \mathbf{V}[X]$ satisfying $\mathrm{D}_{\mathbf{V}[X]}(a, L) = \mathrm{D}_{\mathbf{V}[X]}(L + aQ)$ (with $L = (\ell_1, \ell_2)$ and $Q = (q_1, q_2)$). We apply Lemma 6.7 with the finite family constituted by the coefficients of ℓ_1, ℓ_2 and a. We find q_1, q_2 in $\mathbf{V}'[X] \subseteq \mathbf{V}[X]$. □

[2] Otherwise, the lemma could actually be proven without any hypothesis on $\mathbf{V}$.

6.8. Theorem. (Bass-Simis-Vasconcelos) *If* $\mathbf{V}$ *is a valuation ring, every finitely generated projective* $\mathbf{V}[X]$*-module is free.*

D Let M be a finitely generated projective module over $\mathbf{V}[X]$. Since $\mathbf{V}[X]$ is connected, M has a constant rank $r \in \mathbb{N}$. Since $\mathbf{V}[X]$ is 2-stable, Serre's Splitting Off theorem gives us that $M \simeq \mathbf{V}[X]^{r-1} \oplus N$, where N is a projective $\mathbf{V}[X]$-module of constant rank 1. It remains to show that $N \simeq \mathbf{V}[X]$. If $\mathbf{V}$ is integral we finish like this: since $\mathbf{V}[X]$ is a GCD-domain, $N \simeq \mathbf{V}[X]$. In general we can say: $\mathbf{V}$ is normal, therefore every projective module of constant rank 1 over $\mathbf{V}[X]$ is extended from $\mathbf{V}$. However, $\mathbf{V}$ is local, in conclusion N is free over $\mathbf{V}[X]$. □

The case of arithmetic rings

6.9. Theorem. (Bass-Simis-Vasconcelos) *If* $\mathbf{A}$ *is an arithmetic ring, every finitely generated projective* $\mathbf{A}[X]$*-module is extended from* $\mathbf{A}$*.*

D First of all, since $\mathsf{GK}_0(\mathbf{A}) = \mathsf{GK}_0(\mathbf{A}_{\mathrm{red}})$ and $\mathbf{A}[X]_{\mathrm{red}} = \mathbf{A}_{\mathrm{red}}[X]$, it suffices to prove the theorem in the reduced case, i.e. for the Prüfer rings. Consider a finitely generated projective $\mathbf{A}[X]$-module M.
In classical mathematics we would apply the Quillen abstract patching theorem: a finitely generated projective module over $\mathbf{A}[X]$ is extended because it is extended if we localize at an arbitrary prime ideal of $\mathbf{A}$ (the ring becomes a valuation ring).
In constructive mathematics, we rewrite the constructive proof given in the local case (for Theorem 6.8) by applying the basic local-global machinery. More precisely, suppose that in the local case (i.e. for a valuation ring) we use the disjunction "a divides b or b divides a." Since we are dealing with a Prüfer ring, we know u, v, s, t such that $s + t = 1$, $sa = ub$ and $tb = va$. If $\mathbf{B}$ is the "current" ring, we consider the two comaximal localizations $\mathbf{B}[1/s]$ and $\mathbf{B}[1/t]$. In the first, a divides b, and in the second, b divides a.
Ultimately we obtain a finite family (S_i) of comaximal monoids of $\mathbf{A}$ such that after localization at any of the S_i's, the module M becomes free, therefore extended. We conclude with the Quillen patching (concrete local-global principle 3.7). □

Remarks. 1) We did not need to assume that the valuation ring was residually discrete to make the constructive proof of Theorems 6.6, 6.8 and 6.9 work. This is especially translated by the fact that in the last proof, the comaximal monoids are based on the disjunction (in a local ring) "s or $1 - s$ is invertible" and are directly given by comaximal elements.

2) In this type of passage from the local to the global, to make sure that the algorithm halts, we have to make sure that the version given in the local case is "uniform," meaning that its execution is done in a number of

steps that is bounded by a function of the discrete parameters of the input: the size of the matrix and the degrees of its coefficients. This is indeed the case here, modulo the proof of Lemma XIII-5.3. Note that the fact that the algorithm in the local case does not use any tests of equality to 0 greatly simplifies life and helps us to appreciate the validity of its dynamic implementation in the passage from the local to the global. ∎

The multivariate case

This subsection is devoted to the constructive proof of the following Lequain-Simis theorem.

Theorem (Lequain-Simis) *If* $\mathbf{A}$ *is an arithmetic ring, every finitely generated projective module over* $\mathbf{A}[X_1, \ldots, X_r]$ *is extended from* $\mathbf{A}$.

A dynamic comparison between the rings $\mathbf{A}(X)$ and $\mathbf{A}\langle X\rangle$

In the following theorem, we prove that for a ring $\mathbf{A}$ of dimension at most d, the ring $\mathbf{A}\langle X\rangle$ dynamically behaves like the ring $\mathbf{A}(X)$ or like a localization of a ring $\mathbf{A}_S[X]$ for a monoid S of $\mathbf{A}$ with $\mathsf{Kdim}\,\mathbf{A}_S \leqslant d-1$.

6.10. Theorem. (Dynamic comparison of $\mathbf{A}(X)$ with $\mathbf{A}\langle X\rangle$)
Let $\mathbf{A}$ *be a ring,* $f = \sum_{j=0}^{m} a_j X^j \in \mathbf{A}[X]$ *be a primitive polynomial, and, for* $j \in [\![1..m]\!]$, $S_j = \mathcal{S}^{\mathrm{K}}_{\mathbf{A}}(a_j) = a_j^{\mathbb{N}}(1 + a_j\mathbf{A})$ *be the Krull boundary monoid of* a_j *in* $\mathbf{A}$. *Then, the monoids* $f^{\mathbb{N}}$, S_1, …, S_m *are comaximal in* $\mathbf{A}\langle X\rangle$. *In particular, if* $\mathsf{Kdim}\,\mathbf{A}$ *and* $d \geqslant 0$, *each ring* $\mathbf{A}\langle X\rangle_{S_j}$ *is a localization of a ring* $\mathbf{A}_{S_j}[X]$ *with* $\mathsf{Kdim}\,\mathbf{A}_{S_j} \leqslant d-1$.

D For $x_1, \ldots, x_m \in \mathbf{A}$ and $n, d_1, \ldots, d_m \in \mathbb{N}$, we must show that the following elements of $\mathbf{A}[X]$

$$f^n,\ a_m^{d_m}(1 - a_m x_m),\ \ldots,\ a_1^{d_1}(1 - a_1 x_1),$$

generate an ideal of $\mathbf{A}[X]$ that contains a monic polynomial. We reason by induction on m; it is obvious for $m = 0$ because $a_m = a_0$ is invertible.
For $m \geqslant 1$ and $j \in [\![1..m-1]\!]$, let

$$a = a_m,\ \ x = x_m,\ \ d = d_m \ \text{ and } \ a'_j = a_j^{d_j}(1 - a_j x_j).$$

Consider the quotient $\mathbf{B} = \mathbf{A}/\big\langle a^d(1 - ax)\big\rangle$; we must show that the family

$$\mathcal{F} = (f^n,\ a'_{m-1},\ \ldots,\ a'_1)$$

generates an ideal of $\mathbf{B}[X]$ which contains a monic polynomial.
Since $a^d(1 - ax) = 0$, $e = a^d x^d$ is an idempotent and $\langle e\rangle = \big\langle a^d\big\rangle$.
Let $\mathbf{B}_e \simeq \mathbf{B}/\langle 1 - e\rangle$ and $\mathbf{B}_{1-e} \simeq \mathbf{B}/\langle e\rangle$. It suffices to show that $\langle\mathcal{F}\rangle_{\mathbf{B}_e[X]}$ and $\langle\mathcal{F}\rangle_{\mathbf{B}_{1-e}[X]}$ contain a monic polynomial.
In $\mathbf{B}_e[X]$, it is immediate because a is invertible. In $\mathbf{B}_{1-e}[X]$, we have $a^d = 0$. Let $f = aX^m + r$ with $r = \sum_{j=0}^{m-1} a_j X^j$. In $\mathbf{B}$, for every exponent δ,

the elements of $(a^\delta, a_{m-1}, \dots, a_1, a_0)$ are comaximal. For $\delta = d$, we deduce that in $\mathbf{B}_{1-e}[X]$, the polynomial r is primitive. Since $r = f - aX^m$ and $a^d = 0$, we have $r^d \in \langle f \rangle$ so $r^{dn} \in \langle f^n \rangle$.

We apply the induction hypothesis to the polynomial $r \in \mathbf{B}_{1-e}[X]$ of (formal) degree $m-1$: the ideal $\left\langle r^{dn}, a'_{m-1}, \cdots, a'_1 \right\rangle$ of $\mathbf{B}_{1-e}[X]$ contains a monic polynomial; therefore the same holds for the ideal $\left\langle f^n, a'_{m-1}, \cdots, a'_1 \right\rangle$. □

Remark. The previous theorem seems to have fallen from the sky as if by magic. Actually it is the result of a slightly complicated story. In the article [76], the following theorem was proved by starting with the special case of a residually discrete local ring, then by generalizing to an arbitrary ring by means of the basic local-global machinery.

Theorem. *Let* $\mathbf{A}$ *be a ring such that* $\mathsf{Kdim}\,\mathbf{A} \leqslant d \in \mathbb{N}$. *Let* $f \in \mathbf{A}[X]$ *be a primitive polynomial. There exist comaximal monoids* $V_1, \dots, V_\ell$ *of* $\mathbf{A}\langle X \rangle$ *such that for each* $i \in [\![1..\ell]\!]$, *either* f *is invertible in* $\mathbf{A}\langle X \rangle_{V_i}$, *or* $\mathbf{A}\langle X \rangle_{V_i}$ *is a localization of an* $\mathbf{A}_{S_i}[X]$ *with* $\mathsf{Kdim}\,\mathbf{A}_{S_i} < d$.

By explicating the algorithm contained in the proof of this theorem, we have obtained Theorem 6.10. ■

Dynamic machinery with $\mathbf{A}\langle X \rangle$ and $\mathbf{A}(X)$

The previous theorem allows us to implement a dynamic machinery of a new type.

Suppose that we have established a theorem for the valuation rings of Krull dimension $\leqslant n$. We want the same theorem for the rings $\mathbf{A}\langle X \rangle$ when $\mathbf{A}$ is a valuation ring of Krull dimension $\leqslant n$.

Suppose also that the property to be proven is stable by localization and that it comes from a concrete local-global principle.

We perform a proof by induction on the Krull dimension. When the Krull dimension is null, $\mathbf{A}$ is a discrete field and we have $\mathbf{A}\langle X \rangle = \mathbf{A}(X)$, which is also a discrete field, therefore the theorem applies.

Let us look at the passage from the dimension k to the dimension $k+1$ $(k < n)$. Notice that $\mathbf{A}(X)$ is a valuation ring with the same Krull dimension as $\mathbf{A}$ (Lemma 6.1). We assume that $\mathsf{Kdim}\,\mathbf{A} \leqslant k+1$. We have a constructive proof of the theorem for the valuation rings of Krull dimension $\leqslant n$, in particular it works for $\mathbf{A}(X)$. We try to make this proof (i.e. this algorithm) work with $\mathbf{A}\langle X \rangle$ instead of $\mathbf{A}(X)$. This proof uses the fact that in $\mathbf{A}(X)$ the primitive polynomials of $\mathbf{A}[X]$ are invertible. Each time that the initial proof uses the inverse of such a polynomial f, we call upon Theorem 6.10, which replaces the "current" ring by comaximal localizations. In the first localization the polynomial f has been inverted, and the proof can be continued as if $\mathbf{A}\langle X \rangle$ were $\mathbf{A}(X)$. In each of the other localizations we have replaced $\mathbf{A}\langle X\rangle$ by a localization of a ring $\mathbf{A}_{S_i}[X]$ with $\mathsf{Kdim}\,\mathbf{A}_{S_i} \leqslant k$, and, *if we are lucky*, the induction hypothesis allows us to conclude.

Ultimately we have proven the theorem for comaximal localizations of $\mathbf{A}\langle X\rangle$. Since the conclusion stems from a concrete local-global principle, we have proven the theorem for $\mathbf{A}\langle X\rangle$.

Application to the theorem of Maroscia and Brewer & Costa

The dynamic machinery explained in the previous subsection applies for the first of the following results.

(i) *If* $\mathbf{A}$ *is a valuation ring with* $\mathsf{Kdim}\,\mathbf{A} \leqslant 1$*, then* $\mathbf{A}\langle X\rangle$ *is a Prüfer ring with* $\mathsf{Kdim}\,\mathbf{A}\langle X\rangle \leqslant 1$*.*
Indeed, it suffices to prove the conclusion locally (here, after localization of $\mathbf{A}\langle X\rangle$ at comaximal monoids). However, Theorem 6.10 allows us to split the ring $\mathbf{A}\langle X\rangle$ into components that behave (for the computation to be done) either like $\mathbf{A}(X)$, or like a localized ring of a $\mathbf{K}[X]$ where $\mathbf{K}$ is reduced zero-dimensional. In the two cases we obtain a Prüfer ring of Krull dimension $\leqslant 1$.

(ii) *If* $\mathbf{A}$ *is a Prüfer ring with* $\mathsf{Kdim}\,\mathbf{A} \leqslant 1$*, then so is* $\mathbf{A}\langle X\rangle$*.*
Indeed, it suffices to prove the conclusion locally (here, after localization of $\mathbf{A}$ at comaximal monoids). We apply the local-global machinery of arithmetic rings to the proof of item (i): the ring $\mathbf{A}$ is subjected to comaximal localizations, in each of which it behaves like a valuation ring.

As a consequence we obtain a special version of the Lequain-Simis theorem by using the concrete Quillen induction (Theorem 5.2).

6.11. Theorem. (Maroscia, Brewer & Costa)
If $\mathbf{A}$ *is an arithmetic ring with* $\mathsf{Kdim}\,\mathbf{A} \leqslant 1$*, every finitely generated projective module over* $\mathbf{A}[X_1, \ldots, X_r]$ *is extended from* $\mathbf{A}$*.*

D Since $\mathbf{A}_{\mathrm{red}}[\underline{X}] = \mathbf{A}[\underline{X}]_{\mathrm{red}}$ and $\mathsf{GK}_0(\mathbf{B}) = \mathsf{GK}_0(\mathbf{B}_{\mathrm{red}})$, it suffices to treat the reduced case, i.e. the case of the Prüfer rings.

Let us verify that the class of Prüfer rings of Krull dimension $\leqslant 1$ satisfies the hypotheses of Theorem 5.2. The first condition is item (ii) above that we have just proven.

The second condition is that the finitely generated projective modules over $\mathbf{A}[X]$ are extended from $\mathbf{A}$. This is the Bass-Simis-Vasconcelos theorem.□

The Lequain-Simis induction

For the purpose of generalizing the Quillen-Suslin theorem to Prüfer domains, and observing that this class of rings is not stable under the passage from $\mathbf{A}$ to $\mathbf{A}\langle X\rangle$, Lequain and Simis [126] have found a skillful way to bypass the difficulty by proving a new induction theorem "à la Quillen," suitably modified.

6.12. Abstract Lequain-Simis induction.
Let $\mathcal{F}$ be a class of rings that satisfy the following properties.

(LS1) *If $\mathbf{A} \in \mathcal{F}$, every nonmaximal prime ideal $\mathfrak{p}$ of $\mathbf{A}$ has a finite height.*[3]

(LS2) *If $\mathbf{A} \in \mathcal{F}$, then $\mathbf{A}[X]_{\mathfrak{p}[X]} \in \mathcal{F}$ for every prime ideal $\mathfrak{p}$ of $\mathbf{A}$.*

(LS3) *If $\mathbf{A} \in \mathcal{F}$, then $\mathbf{A}_{\mathfrak{p}} \in \mathcal{F}$ for every prime ideal $\mathfrak{p}$ of $\mathbf{A}$.*

(LS4) *If $\mathbf{A} \in \mathcal{F}$ is local, every finitely generated projective module over $\mathbf{A}[X]$ is free.*

Then, for all $\mathbf{A} \in \mathcal{F}$ and all $r \geqslant 1$, every finitely generated projective module over $\mathbf{A}[X_1, \dots, X_r]$ is extended from $\mathbf{A}$.

Here note that if $\mathbf{A}$ is local with $\operatorname{Rad}\mathbf{A} = \mathfrak{m}$, then $\mathbf{A}(X) = \mathbf{A}[X]_{\mathfrak{m}[X]}$.

We propose a "constructive variation" on the theme of the Lequain-Simis induction. This is an important application of our dynamic comparison between $\mathbf{A}(X)$ and $\mathbf{A}\langle X\rangle$. This constructive induction "à la Lequain-Simis" is due to I. Yengui.

6.13. Theorem. (Yengui induction)
Let $\mathcal{F}$ be a class of commutative rings of finite Krull dimension (not necessarily bounded) which satisfies the following properties.

(ls1) *If $\mathbf{A} \in \mathcal{F}$, then $\mathbf{A}(X) \in \mathcal{F}$.*

(ls2) *If $\mathbf{A} \in \mathcal{F}$, then $\mathbf{A}_S \in \mathcal{F}$ for every monoid S of $\mathbf{A}$.*

(ls3) *If $\mathbf{A} \in \mathcal{F}$, then every finitely generated projective $\mathbf{A}[X]$-module is extended from $\mathbf{A}$.*

Then, for all $\mathbf{A} \in \mathcal{F}$ and all $r \geqslant 1$, every finitely generated projective module over $\mathbf{A}[X_1, \dots, X_r]$ is extended from $\mathbf{A}$.

Note: (ls1) replaces (LS2), (ls2) replaces (LS3) and (ls3) replaces (LS4).

D Due to Fact 1.2 *5*, we limit ourselves to the case of reduced rings. We reason by double induction on the number r of variables and over the Krull dimension d of $\mathbf{A}$.
The basic step for $r = 1$ (arbitrary d) is given by (ls3), and for $d = 0$ (with arbitrary r) it is the Quillen-Suslin theorem.
We suppose that the result is proven in r variables for the rings in $\mathcal{F}$. We consider the case of $r + 1$ variables and we perform an induction proof on (an upper bound d of) the Krull dimension of a ring $\mathbf{A} \in \mathcal{F}$.
Therefore let $\mathbf{A}$ be a ring of Krull dimension $\leqslant d + 1$. Let P be a finitely generated projective module over $\mathbf{A}[X_1, \dots, X_r, Y] = \mathbf{A}[\underline{X}, Y]$. Let $G = G(\underline{X}, Y)$ be a presentation matrix of P with coefficients in $\mathbf{A}[\underline{X}, Y]$. Let $H(\underline{X}, Y)$ be the matrix constructed from G as in Fact 1.1.
By using the induction hypothesis for r and (ls1), we obtain that the

[3] I.e., $\mathsf{Kdim}(\mathbf{A}_{\mathfrak{p}}) < \infty$.

matrices $H(\underline{X},Y)$ and $H(\underline{0},Y)$ are elementarily equivalent over $\mathbf{A}(Y)[\underline{X}]$. This means that there exist matrices Q_1, R_1 over $\mathbf{A}[\underline{X},Y]$ such that

$$Q_1H(\underline{X},Y) = H(\underline{0},Y)R_1$$
$$\text{with} \quad \det(Q_1) \text{ and } \det(R_1) \text{ primitive in } \mathbf{A}[Y].$$

We now show that $H(\underline{X},Y)$ and $H(\underline{0},Y)$ are equivalent over $\mathbf{A}\langle Y\rangle[\underline{X}]$. By the Vaserstein patching it suffices to show that they are equivalent over $\mathbf{A}\langle Y\rangle_{S_i}[\underline{X}]$ for comaximal monoids S_i of $\mathbf{A}\langle Y\rangle$.

We consider the primitive polynomial $f = \det(Q_1)\det(R_1) \in \mathbf{A}[Y]$, and we apply Theorem 6.10. If f is of formal degree m, we obtain monoids $(S_i)_{i\in[\![1..m]\!]}$ of $\mathbf{A}$ such that the monoids $V = f^{\mathbb{N}}$ and $(S_i)_{i\in[\![1..m]\!]}$ are comaximal in $\mathbf{A}\langle Y\rangle$. In addition, $\mathsf{Kdim}\,\mathbf{A}_{S_i} \leqslant d$ for $i \in [\![1..m]\!]$.

For the ring localized at V, $\det(Q_1)$ and $\det(R_1)$ are invertible in $\mathbf{A}\langle Y\rangle_V$. This implies that $H(\underline{X},Y)$ and $H(\underline{0},Y)$ are equivalent over $\mathbf{A}\langle Y\rangle_V[\underline{X}]$.

For a localized ring at S_i ($i \in [\![1..m]\!]$), by induction hypothesis over d and by using (ls2), $H(\underline{X},Y)$ and $H(\underline{0},0)$ are equivalent over $\mathbf{A}_{S_i}[\underline{X},Y]$. A fortiori $H(\underline{X},Y)$ and $H(\underline{0},Y)$ are equivalent over $\mathbf{A}_{S_i}[\underline{X},Y]$, therefore also over $\mathbf{A}\langle Y\rangle_{S_i}[\underline{X}]$, which is a localization of $\mathbf{A}_{S_i}[Y][\underline{X}] = \mathbf{A}_{S_i}[\underline{X},Y]$.

Thus, we have fulfilled the contract and we obtain invertible matrices Q and R over $\mathbf{A}\langle Y\rangle[\underline{X}] \subseteq \mathbf{A}[\underline{X}]\langle Y\rangle$ such that

$$Q\,H(\underline{X},Y) = H(\underline{0},Y)\,R.$$

Moreover, we know by (ls3) that $H(\underline{0},0)$ and $H(\underline{0},Y)$ are equivalent over $\mathbf{A}[Y] \subseteq \mathbf{A}[\underline{X}]\langle Y\rangle$, and by induction hypothesis over r that $H(\underline{0},0)$ and $H(\underline{X},0)$ are equivalent over $\mathbf{A}[\underline{X}] \subseteq \mathbf{A}[\underline{X}]\langle Y\rangle$. In conclusion $H(\underline{X},0)$ and $H(\underline{X},Y)$ are equivalent over $\mathbf{A}[\underline{X}]\langle Y\rangle$. Therefore by the Affine Horrocks' theorem, P is extended from $\mathbf{A}[\underline{X}]$.

Finally, by induction hypothesis over r, $P(\underline{X},0)$ is extended from $\mathbf{A}$. □

Remark. We have asked in (ls2) that the class $\mathcal{F}$ is stable under localization for any monoid. Actually in the proof only localizations at Krull boundary monoids intervene, or by inversion of a unique element (all this in an iterative way). ■

Lequain-Simis in finite dimension

6.14. Corollary.
If $\mathbf{A}$ is an arithmetic ring of finite Krull dimension, every finitely generated projective module over $\mathbf{A}[X_1,\dots,X_r]$ is extended from $\mathbf{A}$.

D We show that the class of arithmetic rings of finite Krull dimension satisfies the concrete Lequain-Simis induction. The condition (ls1) is given by Exercise XII-3, (ls3) by the Bass-Simis-Vasconcelos theorem, and (ls2) is clear. □

Local Lequain-Simis without the dimension hypothesis

6.15. Corollary. *If* $\mathbf{V}$ *is a valuation ring, every finitely generated projective module over* $\mathbf{V}[X_1, \ldots, X_r]$ *is extended from* $\mathbf{V}$ *(i.e. free).*

D Let M be a finitely generated projective module over $\mathbf{V}[X_1, \ldots, X_r]$. We must show that M is free. Let $F = (f_{ij}) \in \mathbb{AG}_q(\mathbf{V}[X_1, \ldots, X_r])$ be a matrix whose image is isomorphic to the module M. Let $\mathbf{V}_1$ be the subring of $\mathbf{V}$ generated by the coefficients of the polynomials f_{ij} and $\mathbf{V}'$ be the valuation subring of $\mathbf{V}$ generated by $\mathbf{V}_1$. Item *4* of Theorem XIII-8.20 tells us that every ring between $\mathbf{V}_1$ and $\operatorname{Frac}\mathbf{V}_1$, in particular $\mathbf{V}'$, is of finite Krull dimension. We apply Corollary 6.14. □

General Lequain-Simis theorem

6.16. Theorem. (Lequain-Simis) *If* $\mathbf{A}$ *is an arithmetic ring, every finitely generated projective module over* $\mathbf{A}[X_1, \ldots, X_r]$ *is extended from* $\mathbf{A}$.

D This results from Corollary 6.14 (the local case) with the same proof as as the proof which deduces Theorem 6.9 from Theorem 6.8. □

Conclusion: a few conjectures

The solution to Serre's problem has naturally led to a few conjectures about possibles generalizations.

We will cite the two most famous ones and refer to [Lam06, chap.V,VIII] for detailed information on the subject.

The first, and the strongest, is the *Hermite rings conjecture*, that can be stated in two equivalent forms, one local and another global, given the Quillen patching principle. Recall that a ring is called a “Hermite ring” when the stably free finitely generated modules are free, which amounts to saying that the unimodular vectors are completable.

(H) If $\mathbf{A}$ is a Hermite ring, then so is $\mathbf{A}[X]$.

(H') If $\mathbf{A}$ is a residually discrete local ring, then $\mathbf{A}[X]$ is a Hermite ring.

Bass' “stable-range” gives a first approach of the problem (see Proposition V-4.4, Corollary V-4.9 and Theorem V-4.10). Special cases are treated for example in [168, Roitman] and [203, 204, Yengui], which treats the $n = 1$ case of the following conjecture: over a ring $\mathbf{A}$ of Krull dimension $\leqslant 1$, the stably free $\mathbf{A}[X_1, \ldots, X_n]$-modules are free.

The second is the *Bass-Quillen conjecture.*

A coherent ring is called a *regular ring* if every finitely presented module admits a finite projective resolution (for the definition and an example of a finite projective resolution, see Problem X-8). For the Bass-Quillen conjecture there are also two equivalent versions, a local one and a global one.

(BQ) If $\mathbf{A}$ is a regular coherent Noetherian ring,[4] then the finitely generated projective modules over $\mathbf{A}[X_1, \dots, X_n]$ are extended from $\mathbf{A}$.

(BQ') If $\mathbf{A}$ is a regular coherent Noetherian residually discrete local ring,[5] then the finitely generated projective modules over $\mathbf{A}[X_1, \dots, X_n]$ are free.

Actually, since $\mathbf{A}$ regular Noetherian implies $\mathbf{A}[X]$ regular Noetherian, it would suffice to prove the $n = 1$ case. Partial results have been obtained. For example, the conjecture is proven in Krull dimension $\leqslant 2$, for arbitrary n (but at the moment we do not dispose of a constructive proof). We can a priori also consider a non-Noetherian version for the regular coherent rings of fixed Krull dimension $\leqslant k$.

Exercises and problems

Exercise 1. Let $\mathfrak{A}$ be an ideal of $\mathbf{A}[X]$ containing a monic polynomial and $\mathfrak{a}$ be an ideal of $\mathbf{A}$. Then $\mathbf{A} \cap (\mathfrak{A} + \mathfrak{a}[X])$ is contained in $\mathrm{D}_{\mathbf{A}}\big((\mathbf{A} \cap \mathfrak{A}) + \mathfrak{a}\big)$. In particular, if $1 \in \mathfrak{A} + \mathfrak{a}[X]$, then $1 \in (\mathbf{A} \cap \mathfrak{A}) + \mathfrak{a}$.

Exercise 2. *(Top-Bottom lemma)* Let $\mathbf{A}$ be a ring and $\mathfrak{m} = \mathrm{Rad}\,\mathbf{A}$.

1. Let $S \subseteq \mathbf{A}[X]$ be the monoid of the monic polynomials. The monoids S and $1 + \mathfrak{m}[X]$ are comaximal.
2. Let $U \subseteq \mathbf{A}[X]$ be the monoid $\big\{\, X^n + \sum_{k<n} a_k X^k \,|\, n \in \mathbb{N}, a_k \in \mathfrak{m}\ (k < n) \,\big\}$. The monoids U and $1 + \mathfrak{m} + X\mathbf{A}[X]$ are comaximal.

Exercise 3. The goal of the exercise is to show a result similar to the Vaserstein patching (local-global principle 3.6) in which we replace $\mathbb{GL}_n$ by $\mathbb{SL}_n$.

1. Let $\mathbf{B}$ be a ring and S be monoid of $\mathbf{B}$.
   a. Let $P \in \mathbf{B}[Y]$ such that $P(0) = 0$ and $P = 0$ in $\mathbf{B}_S[Y]$. Show that there exists an $s \in S$ such that $P(sY) = 0$.
   b. Let $H \in \mathbb{M}_n(\mathbf{B}[Y])$ such that $H(0) \in \mathbb{SL}_n(\mathbf{B})$ and $H \in \mathbb{SL}_n(\mathbf{B}_S[Y])$. Show that there exists an $s \in S$ such that $H(sY) \in \mathbb{SL}_n(\mathbf{B}[Y])$.
2. Prove Lemma 3.4 by replacing $\mathbb{GL}$ by $\mathbb{SL}$.
3. Prove the local-global principle 3.6 by replacing $\mathbb{GL}$ by $\mathbb{SL}$.

[4] Naturally, in classical mathematics the hypothesis “coherent” is superfluous.

[5] Naturally, in classical mathematics the hypotheses “coherent” and “residually discrete” are superfluous.

Exercise 4. Let $\mathbf{A}$ be a residually discrete local ring and $\mathfrak{b} \subseteq \mathbf{A}[X]$ be an invertible ideal containing a monic polynomial. We want to show that $\mathfrak{b}$ is a principal ideal.

This constitutes a special case of the Local Horrocks' theorem (Theorem 4.3): indeed, on the one hand $\mathfrak{b}$ is a projective $\mathbf{A}[X]$-module, and on the other hand, if $f \in \mathfrak{b}$ is a monic polynomial, then by localizing at f, $\mathfrak{b}_f = \mathbf{A}[X]_f$, and so, by the Local Horrocks' theorem, $\mathfrak{b}$ is a free $\mathbf{A}[X]$-module. This exercise gives a proof independent from the current one. In the special case studied here, we add the assumption that $\mathfrak{b}$ is generated by a monic polynomial.

Let $\mathbf{A}$ be a ring, let $\mathfrak{m} = \operatorname{Rad}\mathbf{A}$ and $\mathbf{k} = \mathbf{A}/\mathfrak{m}$. Let $\mathfrak{b} \subseteq \mathbf{A}[X]$ be an ideal containing a monic polynomial. Let $\overline{a}$ be the reduction of a modulo $\mathfrak{m}$.

1. Prove that every monic polynomial of $\overline{\mathfrak{b}} \subseteq \mathbf{k}[X]$ can be lifted to a monic polynomial of $\mathfrak{b}$.

Now suppose that $\mathbf{A}$ is residually discrete and local.

2. Show the existence of a monic polynomial $f \in \mathfrak{b}$ such that $\overline{\mathfrak{b}} = \langle \overline{f} \rangle$ in $\mathbf{k}[X]$ and so $\mathfrak{b} = \langle f \rangle + \mathfrak{b} \cap \mathfrak{m}[X]$.

Now suppose that the ideal $\mathfrak{b}$ is invertible.

3. Show that $\mathfrak{b} \cap \mathfrak{m}[X] = \mathfrak{b}\mathfrak{m}[X]$.

4. Consider the ring $\mathbf{A}[X]/\langle f \rangle$. Show that $\mathfrak{m}(\mathfrak{b}/\langle f \rangle) = \mathfrak{b}/\langle f \rangle$.
Deduce that $\mathfrak{b} = \langle f \rangle$.

We propose a generalization.

5. Does the proof work with a residually zero-dimensional ring $\mathbf{A}$?

Exercise 5. *(Brewer & Costa theorem: the case of Bézout domains of dimension* $\leqslant 1$*)* See also Exercise XII-3 and Theorem 6.11.

Let $\mathcal{F}$ be the class of Bézout domains of dimension $\leqslant 1$, and $\mathbf{A} \in \mathcal{F}$.

1. Show that $\mathsf{Kdim}\,\mathbf{A}\langle X \rangle \leqslant 1$ (use Exercise XIII-9).

2. Deduce that $\mathbf{A}\langle X \rangle$ is a Bézout ring.

3. The class $\mathcal{F}$ satisfies the hypotheses of Theorem 5.4 (concrete Quillen induction, free case). Thus, every finitely generated projective $\mathbf{A}[X_1, \dots, X_r]$-module is free.

Exercise 6. *(Local-global principle for seminormal rings)*
We give a direct proof of principle 3.10 in the special case of seminormal pf-rings.

1. In a pf-ring, if $xc = b$ and $b^2 = c^3$, then there exists a z such that $zc = b$ and $z^2 = c$, so $z^3 = b$.

2. Let S_1, …, S_n be comaximal monoids of a ring $\mathbf{A}$. Suppose that each of the $\mathbf{A}_{S_i}$'s is a seminormal pf-ring. Show that $\mathbf{A}$ is a seminormal pf-ring.

Exercise 7. *(Rings satisfying some of the conditions of the section "An example in finite Krull dimension > 0" page 927)*
Let $a_1, \ldots, a_k \in \mathbf{A}$, $a_0 = 0$, $a_{k+1} = 1$. Let $\mathbf{A}_1, \ldots, \mathbf{A}_{k+1}$ be the following rings

$$\mathbf{A}_i = \big(\mathbf{A}/\langle a_{i-1}\rangle\big)[1/a_i] \quad \text{for } i \in [\![1..k+1]\!].$$

We will show that if each $\mathbf{A}_i$ is zero-dimensional, then $\mathsf{Kdim}\,\mathbf{A} \leqslant k$. The same result holds with $\mathbf{A}_i = \big(\mathbf{A}/\mathrm{D}_{\mathbf{A}}(a_{i-1})\big)[1/a_i]$.

1. Let $a \in \mathbf{A}$. If $\mathsf{Kdim}\,\mathbf{A}[1/a] \leqslant n$ and $\mathsf{Kdim}\,\mathbf{A}/\langle a\rangle \leqslant m$, then $\mathsf{Kdim}\,\mathbf{A} \leqslant n+m+1$.

2. Deduce the stated result.

Some solutions, or sketches of solutions

Exercise 1. Let $\mathbf{B} = \mathbf{A}/\mathbf{A} \cap \mathfrak{A}$, $\mathbf{B}' = \mathbf{A}[X]/\mathfrak{A}$, $\mathfrak{b} = \overline{\mathfrak{a}}$, $\mathfrak{b}' = \mathfrak{b}\,\mathbf{B}'$.
The ring $\mathbf{B}'$ is an integral extension of $\mathbf{B}$. We apply the Lying Over (VI-3.12).
Another solution. Let $f \in \mathfrak{A}$ be monic. Let $a \in \mathbf{A} \cap (\mathfrak{A}+\mathfrak{a}[X])$, there exists a $g \in \mathfrak{A}$ such that $g \equiv a \bmod \mathfrak{a}$. Then $\mathrm{Res}(f,g) \equiv \mathrm{Res}(f,a) \bmod \mathfrak{a}$. But $\mathrm{Res}(f,a) = a^{\deg f}$ and $\mathrm{Res}(f,g) \in \mathfrak{A} \cap \mathbf{A}$.

Exercise 2. Use the resultant.

Exercise 3. *1b.* Let $P(Y) = 1 - \det\big(H(Y)\big)$. We apply item *1a.*

2. Lemma 3.4 provides us with a matrix $U(X,Y) \in \mathbb{GL}_r(\mathbf{A}[X,Y])$ such that

$$U(X,0) = \mathrm{I}_r \text{ and, over } \mathbf{A}_S[X,Y],\ U(X,Y) = C(X+sY)C(X)^{-1}.$$

By item *1*, there exists a $t \in S$ such that $U(X,tY) \in \mathbb{SL}_r(\mathbf{A}[X,Y])$.
Let $V(X,Y) = U(X,tY)$ and we replace s by st.

3. Lemma 3.5 is successfully subjected to the replacement of $\mathbb{GL}$ (implicit in the word "equivalent") by $\mathbb{SL}$. Likewise for the Vaserstein patching.

Exercise 4. *1.* We first show the following result: if we have g, $f \in \mathfrak{b}$ with $\overline{g}$ monic of degree r and f monic of degree $r+1$, then $\overline{g}$ can be lifted to a monic polynomial of $\mathfrak{b}$ (of degree r). We write $g = aX^{r+\delta} + \ldots$, with $\delta \in \mathbb{N}$ and we show by induction on δ that $\overline{g}$ can be lifted to a monic polynomial in $\mathfrak{b}$. If $\delta = 0$, we have $a \equiv 1 \bmod \mathfrak{m}$ (because $\overline{g}$ is monic), so a is invertible and the monic polynomial $a^{-1}g \in \mathfrak{b}$ lifts $\overline{g}$. If $\delta \geqslant 1$, we have $a \in \mathfrak{m}$ (because $\overline{g}$ is monic), and we consider $h = g - aX^{\delta-1}f \in \mathfrak{b}$. It is of the form $bX^{r+\delta-1} + \ldots$, and it satisfies $\overline{h} = \overline{g}$. We apply the induction hypothesis.
It then suffices to show that for all $g \in \mathfrak{b}$ such that $\overline{g}$ is monic of degree r, the ideal $\mathfrak{b}$ contains a monic polynomial of degree $r+1$. By hypothesis, $\mathfrak{b}$ contains a monic polynomial f. If $\deg(f) \leqslant r+1$, then the result is clear. If $n = \deg(f) > r+1$, then the polynomial $X^{n-(r+1)}\overline{g}$ is monic of degree $n-1$, and by the first step, $\mathfrak{b}$ contains a monic polynomial of degree $n-1$. We conclude by induction on $n-r$.

2. The ideal $\overline{\mathfrak{b}}$ is a finitely generated ideal of $\mathbf{k}[X]$, therefore $\overline{\mathfrak{b}}$ is principal. As $\mathfrak{b}$ contains a monic polynomial we can take the monic generator $\overline{h}$ and we lift it to a monic polynomial of $\mathfrak{b}$ by the previous question.

3. Let f be monic in $\mathfrak{b}$, and $\mathfrak{b}_1$ be the ideal that satisfies $\mathfrak{b}\mathfrak{b}_1 = \langle f\rangle$.
We consider $\mathfrak{b}' = \mathfrak{b}_1(\mathfrak{b} \cap \mathfrak{m}[X])/f$ (it is an ideal of $\mathbf{A}[X]$). Then $\mathfrak{b}\mathfrak{b}' = \mathfrak{b} \cap \mathfrak{m}[X]$.

We have $f\mathfrak{b}' \subseteq \mathfrak{m}[X]$ and f is monic so $\overline{\mathfrak{b}'} = 0$, i.e. $\mathfrak{b}' \subseteq \mathfrak{m}[X]$. By multiplying by $\mathfrak{b}$, we obtain $\mathfrak{b} \cap \mathfrak{m}[X] \subseteq \mathfrak{b}\mathfrak{m}[X]$, so $\mathfrak{b} \cap \mathfrak{m}[X] = \mathfrak{b}\mathfrak{m}[X]$.

4. We have

$$\mathfrak{m}(\mathfrak{b}/\langle f\rangle) = \mathfrak{c}/\langle f\rangle \text{ with } \mathfrak{c} = \mathfrak{m}\mathfrak{b} + \langle f\rangle = \mathfrak{m}[X]\mathfrak{b} + \langle f\rangle = \mathfrak{m}[X] \cap \mathfrak{b} + \langle f\rangle = \mathfrak{b}.$$

The $\mathbf{A}[X]/\langle f\rangle$-module $\mathfrak{b}/\langle f\rangle$ is finitely generated and as f is monic, $\mathbf{A}[X]/\langle f\rangle$ is a finitely generated $\mathbf{A}$-module. We deduce that $\mathfrak{b}/\langle f\rangle$ is a finitely generated $\mathbf{A}$-module. By Nakayama's lemma we obtain $\mathfrak{b}/\langle f\rangle = 0$, i.e. $\mathfrak{b} = \langle f\rangle$.

Exercise 5. *1.* We must show that for f, $g \in \mathbf{A}[X]$, we have $1 \in \mathcal{I}^{\mathrm{K}}_{\mathbf{A}\langle X\rangle}(f, g)$. Since $\mathbf{A}$ is a Bézout domain, every polynomial of $\mathbf{A}[X]$ is the product of an element of $\mathbf{A}$ by a primitive polynomial. By Exercise XIII-9, it suffices to show that $1 \in \mathcal{I}^{\mathrm{K}}_{\mathbf{A}\langle X\rangle}(f, g)$, either when f or g is primitive, or when f and g are constants a, b. In the latter case, since $\mathsf{Kdim}\,\mathbf{A} \leqslant 1$, this stems from $1 \in \mathcal{I}^{\mathrm{K}}_{\mathbf{A}}(a, b) \subseteq \mathcal{I}^{\mathrm{K}}_{\mathbf{A}\langle X\rangle}(a, b)$. Therefore suppose that f or g is primitive, for example f. It suffices to show that $1 \in \mathcal{I}^{\mathrm{K}}_{\mathbf{A}\langle X\rangle}(f, g)$ after localization at comaximal monoids. However, Theorem 6.10 provides boundary monoids S_j in $\mathbf{A}$ such that $f^{\mathbb{N}}$ and the S_j's are comaximal in $\mathbf{A}\langle X\rangle$. For the localization at $f^{\mathbb{N}}$, it is clear that $1 \in \mathcal{I}^{\mathrm{K}}(f, g)$.
As for $S_j^{-1}\mathbf{A}\langle X\rangle$, it is a localization of $\mathbf{A}_{S_j}[X]$ with $\mathbf{A}_{S_j}$ zero-dimensional, which gives $\mathsf{Kdim}\,\mathbf{A}_{S_j}[X] \leqslant 1$. Therefore $1 \in \mathcal{I}^{\mathrm{K}}(f, g)$ in $\mathbf{A}_{S_j}[X]$, and a fortiori in the localized ring $S_j^{-1}\mathbf{A}\langle X\rangle$.

2. The ring $\mathbf{A}[X]$ is a GCD-domain, so the same holds for its localized ring $\mathbf{A}\langle X\rangle$. As $\mathsf{Kdim}\,\mathbf{A}\langle X\rangle \leqslant 1$, Theorem XI-3.12 tells us that $\mathbf{A}\langle X\rangle$ is a Bézout ring.

3. We have proven the property (q1) and we already know that the property (q0) is satisfied (Theorem X-5.4).

Exercise 6. *1.* We have $x^2c^2 = b^2 = c^3$, so $c^2(x^2 - c) = 0$, therefore $c(x^2 - c) = 0$. Then let s, t such that $s + t = 1$, $sc = 0$ and $t(x^2 - c) = 0$. Let $z = tx$.
We have $tc = c$, $z^2 = t^2c = c$ and $zc = xtc = xc = b$.

2. Suppose that each of the $\mathbf{A}_{S_i}$'s is a seminormal pf-ring. Therefore $\mathbf{A}$ is a pf-ring.
Let b, $c \in \mathbf{A}$ with $b^2 = c^3$. If the $\mathbf{A}_{S_i}$'s are seminormal, there exist $x_i \in \mathbf{A}_{S_i}$ such that $x_i^2 = c$ and $x_i^3 = b$, and so $x_ic = b$. This implies that there exists an $x \in \mathbf{A}$ such that $xc = b$. We conclude by item *1.*

Note: There are seminormal rings that are not pf-rings: for example $\mathbf{k}[x, y]$ with $xy = 0$ where $\mathbf{k}$ is a discrete field.

Exercise 7.
1. Let $(\underline{x}) = (x_0, \ldots, x_n)$, $(\underline{y}) = (y_0, \ldots, y_m)$ be $n + m + 2$ elements of $\mathbf{A}$. By considering the iterated boundary monoid of $(\underline{y})$ in $\mathbf{A}/\langle a\rangle$, we obtain that $\mathcal{S}^{\mathrm{K}}_{\mathbf{A}}(\underline{y})$ contains a multiple of a, say ba. By considering the iterated boundary ideal of $(\underline{x})$ in $\mathbf{A}[1/a]$, we obtain that $\mathcal{I}^{\mathrm{K}}_{\mathbf{A}}(\underline{x})$ contains a power of a, say a^e.
Then $(ba)^e \in \mathcal{I}^{\mathrm{K}}_{\mathbf{A}}(\underline{x}) \cap \mathcal{S}^{\mathrm{K}}_{\mathbf{A}}(\underline{y})$, so $1 \in \mathcal{I}^{\mathrm{K}}_{\mathbf{A}}(\underline{x}, \underline{y})$ by Fact XIII-2.9, item *1.*

2. By using the previous question, we show by induction on $i \in [\![0..k + 1]\!]$ that we have $\mathsf{Kdim}\,\mathbf{A}[1/a_i] \leqslant i - 1$; for $i = k + 1$, we obtain $\mathsf{Kdim}\,\mathbf{A} \leqslant k$.

Bibliographic comments

Carlo Traverso proved the theorem that bears his name in [191], for a reduced Noetherian ring $\mathbf{A}$ (with an additional restriction). For the integral case without the Noetherian hypothesis we can refer back to [155, Querré], [23, Brewer&Costa] and [93, Gilmer&Heitmann]. The most general case is given by [188, Swan].

Traverso-Swan's theorem over the seminormal rings has been decrypted from the constructive point of view by Coquand in [36]. The decryption began with the elementary proof of Proposition 2.12 as it is given here. This proof is a (quite spectacular) simplification of the existing proofs in the literature. It was then necessary to bypass the argument of the consideration of a minimal prime ideal to obtain a complete constructive proof of the result. It is remarkable that, at the same time, the case of a non-integral ring could have been treated effortlessly, in contrast to what happens in Swan's proof in [188]. For a detailed explanation of [36] see [132, Lombardi&Quitté]. For a "simple" algorithm that realizes the theorem in the univariate case, see [7, Barhoumi&Lombardi]. A direct proof, in the same spirit, for the implication "seminormal ring $\mathbf{A}$ implies seminormal ring $\mathbf{A}[X]$" is found in [6, Barhoumi].

Roitman's theorem 3.8 is found in [167].

As for the history of the resolution of Serre's problem over polynomial rings, the reader can refer to Chapter III of Lam's book [Lam06] as well as the presentation by Ferrand to Bourbaki [84].

The original proofs of Quillen-Suslin's theorem (solution to Serre's problem) are found in [156, Quillen] and [183, Suslin]. Horrocks' theorems have their source in [108, Horrocks].

The "Quillen patching" that appears in [156] is often called the Quillen local-global principle. A remarkable overview of the applications of this principle and of its extensions is found in [9, Basu&al.]. Also read [160, Rao&Selby].

The ring $\mathbf{A}\langle X\rangle$ played a great role in the solution of Serre's problem by Quillen and in its successive generalizations (the theorems of Maroscia and Brewer&Costa, and of Lequain&Simis). The ring $\mathbf{A}(X)$ proved to be an efficient tool for several results of commutative algebra. Refer to the article [95, Glaz] for a considerably comprehensive bibliography regarding these two rings.

Lam's book [Lam06] (which follows [Lam]) is a gold mine regarding the extended projective modules. It contains especially several proofs of Horrocks' theorems (local and affine), with all the details and all the necessary references, at least from a classical mathematics' point of view.

The Affine Horrocks' theorem (Theorem 4.7) was constructively proven, first (for a slightly weaker variant) in the article [131, Lombardi&Quitté], then in [133, Lombardi,Quitté&Yengui]. The version given on page 914 reuses the latter article by specifying all the details. It is based on the books by Kunz and Lam.

Theorem 6.8 by Bass-Simis-Vasconcelos ([Bass, 175]) was decrypted from a constructive point of view by Coquand in [37].

Regarding the theorem of Maroscia and Brewer&Costa (Theorem 6.11), see the original articles [22, 137]. A constructive proof can be found in [133]. This theorem is a slight antecessor of the theorem of Lequain&Simis. The latter was mostly decrypted from a constructive point of view by I. Yengui [8, 76].

Many algorithms for Quillen-Suslin's theorem (the field case) have been proposed in Computer Algebra, generally based on the proof by Suslin.

Quillen-Suslin's theorem has been studied from the point of view of its algorithmic complexity in [86, Fitchas&Galligo] and [27, Caniglia&al.] (for efficient algorithms, but that seem yet to be implemented).

A new, simple and efficient algorithm for SuslinÍs theorem (complete a unimodular vector containing a monic polynomial) is given in [134, Lombardi&Yengui] and improved in [142, Mnif&Yengui].

Chapter XVII

Suslin's stability theorem, the field case

Contents

Introduction

In this chapter, we give an entirely constructive treatment of Suslin's stability theorem for the case of discrete fields.

1. The elementary group

Transvections

Regarding the elementary group $\mathbb{E}_n(\mathbf{A})$, recall that it is generated by the elementary matrices $\mathrm{E}_{i,j}^{(n)}(a) = \mathrm{E}_{i,j}(a)$.

If we let $(e_{ij})_{1 \leqslant i,j \leqslant n}$ be the canonical basis of $\mathbb{M}_n(\mathbf{A})$, we have

$$\mathrm{E}_{i,j}(a) = \mathrm{I}_n + a e_{ij}, \quad \mathrm{E}_{i,j}(a)\, e_k = \begin{cases} e_k & \text{if } k \neq j \\ e_j + a e_i & \text{if } k = j \end{cases} \qquad (i \neq j),$$

with for example

$$\mathrm{E}_{2,3}(a) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & a & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

For fixed i (resp. for fixed j) the matrices $\mathrm{E}_{i,j}(\bullet)$ commute, and form a subgroup of $\mathbb{E}_n(\mathbf{A})$ isomorphic to $(\mathbf{A}^{n-1}, +)$. For example

$$\mathrm{E}_{2,1}(a) \cdot \mathrm{E}_{2,3}(b) \cdot \mathrm{E}_{2,4}(c) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ a & 1 & b & c \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

and

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ a & 1 & b & c \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 & 0 \\ a' & 1 & b' & c' \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ a+a' & 1 & b+b' & c+c' \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

More generally let P be a finitely generated projective $\mathbf{A}$-module. We will say that a pair $(\lambda, w) \in P^\star \times P$ is *unimodular* if $\lambda(w) = 1$. In this case w is a unimodular element of P, λ is a unimodular element of $P^\star$ and the $\mathbf{A}$-linear map $\theta_P(\lambda \otimes w) : P \to P$ defined by $x \mapsto \lambda(x)w$ is the projection over $L = \mathbf{A}w$ parallel to $K = \operatorname{Ker} \lambda$, represented over $K \times L$ by the matrix

$$\begin{bmatrix} 0_{K \to K} & 0_{L \to K} \\ 0_{K \to L} & 1_{L \to L} \end{bmatrix} = \begin{bmatrix} 0_{K \to K} & 0 \\ 0 & \mathrm{Id}_L \end{bmatrix}.$$

If $u \in K$, the $\mathbf{A}$-linear map $\tau_{\lambda,u} := \mathrm{Id}_P + \theta_P(\lambda \otimes u)$, $x \mapsto x + \lambda(x)u$ is called a *transvection*, it is represented over $K \times L$ by the matrix

$$\begin{bmatrix} 1_{K \to K} & (\lambda \otimes u)|_L \\ 0_{K \to L} & 1_{L \to L} \end{bmatrix} = \begin{bmatrix} \mathrm{Id}_K & (\lambda \otimes u)|_L \\ 0 & \mathrm{Id}_L \end{bmatrix}.$$

For example, if $P = \mathbf{A}^n$, an elementary matrix defines a transvection.

Let $\mathbb{GL}(P)$ be the group of linear automorphisms of P and $\mathbb{SL}(P)$ be the subgroup of endomorphisms of determinant 1. The subgroup of $\mathbb{SL}(P)$

generated by the transvections will be denoted by $\widetilde{\mathbb{E}}(P)$. The affine map

$$u \mapsto \tau_{\lambda,u},\ \operatorname{Ker}\lambda \to \operatorname{End}_{\mathbf{A}}(P)$$

provides a homomorphism of the group $(\operatorname{Ker}\lambda, +)$ in the group $\widetilde{\mathbb{E}}(P)$.

In the case where $P = \mathbf{A}^n$, if λ is a coordinate form, we find that the matrix of the transvection is a product of elementary matrices. For example, with the vector $u = {}^{\mathrm{t}}[\,u_1\,u_2\,u_3\,0\,]$:

$$\begin{bmatrix} \mathrm{I}_3 & u' \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & u_1 \\ 0 & 1 & 0 & u_2 \\ 0 & 0 & 1 & u_3 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \prod_{i=1}^{3} \mathrm{E}_{i,4}(u_i).$$

However, note that a priori $\mathbb{E}_n(\mathbf{A})$ is only *contained in* $\widetilde{\mathbb{E}}(\mathbf{A}^n)$. This shows that the elementary group is a priori deprived of clear geometric meaning. As a crucial point, $\mathbb{E}_n(\mathbf{A})$ is a priori not stable under $\mathbb{GL}_n(\mathbf{A})$-conjugation.

Special matrices

We now only speak of the groups $\mathbb{E}_n(\mathbf{A})$.

Let $u = \begin{bmatrix} u_1 \\ \vdots \\ u_n \end{bmatrix} \in \mathbf{A}^{n\times 1}$ and $v = \begin{bmatrix} v_1 & \cdots & v_n \end{bmatrix} \in \mathbf{A}^{1\times n}$ to which we associate the matrix $\mathrm{I}_n + uv \in \mathbb{M}_n(\mathbf{A})$. We will provide results specifying the membership of this matrix to the elementary group $\mathbb{E}_n(\mathbf{A})$.

Since $\det(\mathrm{I}_n + uv) = 1 + \operatorname{tr}(uv) = 1 + vu$, it is imperative to demand the equality $vu \overset{\text{def}}{=} v_1u_1 + \cdots + v_nu_n = 0$. In this case, we have $(\mathrm{I}_n + uv)(\mathrm{I}_n - uv) = \mathrm{I}_n$.

The transvections admit for matrices the matrices of this type, with v being unimodular. In addition, the set of these matrices $\mathrm{I}_n + uv$ (with $vu = 0$) is a stable set under $\mathbb{GL}_n(\mathbf{A})$-conjugation.

For example, for $A \in \mathbb{GL}_n(\mathbf{A})$, we obtain $A\,\mathrm{E}_{ij}(a)\,A^{-1} = \mathrm{I}_n + auv$, where u is the column i of A and v is the row j of A^{-1}.

Take care, however, that if we do not assume that v is unimodular these matrices do not in general represent transvections. If neither u nor v is unimodular the matrix does not even a priori represent an element of $\widetilde{\mathbb{E}}(\mathbf{A}^n)$.

1.1. Lemma. *Suppose $u \in \mathbf{A}^{n\times 1}$, $v \in \mathbf{A}^{1\times n}$ and $vu = 0$.*
Then $\begin{bmatrix} \mathrm{I}_n + uv & 0 \\ 0 & 1 \end{bmatrix} \in \mathbb{E}_{n+1}(\mathbf{A})$.

D We have a sequence of elementary operations on the right-hand side (the first uses the equality $vu = 0$)

$$\begin{bmatrix} \mathrm{I}_n + uv & 0 \\ 0 & 1 \end{bmatrix} \xrightarrow{\alpha} \begin{bmatrix} \mathrm{I}_n + uv & -u \\ 0 & 1 \end{bmatrix} \xrightarrow{\beta}$$

$$\begin{bmatrix} \mathrm{I}_n & -u \\ v & 1 \end{bmatrix} \xrightarrow{\gamma} \begin{bmatrix} \mathrm{I}_n & 0 \\ v & 1 \end{bmatrix} \xrightarrow{\delta} \begin{bmatrix} \mathrm{I}_n & 0 \\ 0 & 1 \end{bmatrix}.$$

This implies $\left[\begin{array}{cc} \mathrm{I}_n + uv & 0 \\ 0 & 1 \end{array}\right] = \delta^{-1}\gamma^{-1}\beta^{-1}\alpha^{-1}$, i.e.

$$\left[\begin{array}{cc} \mathrm{I}_n + uv & 0 \\ 0 & 1 \end{array}\right] = \left[\begin{array}{cc} \mathrm{I}_n & 0 \\ v & 1 \end{array}\right] \cdot \left[\begin{array}{cc} \mathrm{I}_n & -u \\ 0 & 1 \end{array}\right] \cdot \left[\begin{array}{cc} \mathrm{I}_n & 0 \\ -v & 1 \end{array}\right] \cdot \left[\begin{array}{cc} \mathrm{I}_n & u \\ 0 & 1 \end{array}\right]. \quad \square$$

A column vector u is said to be *special* if at least one of its coordinates is null. If $vu = 0$ and if u is special we say that $\mathrm{I}_n + uv$ is a *special matrix.*

1.2. Corollary. *Let $u \in \mathbf{A}^{n\times 1}$ and $v \in \mathbf{A}^{1\times n}$ satisfy $vu = 0$. If u is special, then $\mathrm{I}_n + uv \in \mathbb{E}_n(\mathbf{A})$. In other words every special matrix is in $\mathbb{E}_n(\mathbf{A})$.*

D We can assume that $n \geqslant 2$ and $u_n = 0$. Let $u = \left[\begin{array}{c} \mathring{u} \\ 0 \end{array}\right]$, $v = \left[\begin{array}{cc} \mathring{v} & v_n \end{array}\right]$, with $\mathring{u} \in \mathbf{A}^{(n-1)\times 1}$ and $\mathring{v} \in \mathbf{A}^{1\times(n-1)}$. Then

$$\mathrm{I}_n + uv = \left[\begin{array}{cc} \mathrm{I}_{n-1} + \mathring{u}\,\mathring{v} & v_n\mathring{u} \\ 0 & 1 \end{array}\right] = \left[\begin{array}{cc} \mathrm{I}_{n-1} & v_n\mathring{u} \\ 0 & 1 \end{array}\right] \left[\begin{array}{cc} \mathrm{I}_{n-1} + \mathring{u}\,\mathring{v} & 0 \\ 0 & 1 \end{array}\right].$$

Since $\mathring{v}\,\mathring{u} = vu = 0$, Lemma 1.1 applies and $\mathrm{I}_n + uv \in \mathbb{E}_n(\mathbf{A})$. □

The special matrices are easily "lifted" from a localized ring $\mathbf{A}_S$ to $\mathbf{A}$ itself. More precisely, we obtain the following.

1.3. Fact. *Let $S \subseteq \mathbf{A}$ be a monoid, $u \in \mathbf{A}_S^{n\times 1}$, $v \in \mathbf{A}_S^{1\times n}$ with $vu = 0$ and u be special. Then there exist $s \in S$, $\widetilde{u} \in \mathbf{A}^{n\times 1}$, $\widetilde{v} \in \mathbf{A}^{1\times n}$ with $\widetilde{v}\widetilde{u} = 0$, $\widetilde{u}$ special and $u = \widetilde{u}/s$, $v = \widetilde{v}/s$ over $\mathbf{A}_S$.*

D By definition, $u = u'/s_1$, $v = v'/s_1$ with $s_1 \in S$, $u' \in \mathbf{A}^{n\times 1}$ and $v' \in \mathbf{A}^{1\times n}$. The equality $vu = 0$ provides some $s_2 \in S$ such that $s_2v'u' = 0$, and $u_i = 0$ provides some $s_3 \in S$ such that $s_3u'_i = 0$. Then $s = s_1s_2s_3$, $\widetilde{u} = s_2s_3u'$ and $\widetilde{v} = s_2s_3v'$ fulfill the required conditions. □

1.4. Theorem. *If $n \geqslant 3$, then $\widetilde{\mathbb{E}}(\mathbf{A}^n) = \mathbb{E}_n(\mathbf{A})$. In particular, $\mathbb{E}_n(\mathbf{A})$ is stable under $\mathbb{GL}_n(\mathbf{A})$-conjugation.*

Precisions: *Let $u \in \mathbf{A}^{n\times 1}$, $v \in \mathbf{A}^{1\times n}$ with $vu = 0$ and v unimodular. Then, we can write u in the form $u = u'_1 + u'_2 + \cdots + u'_N$, with $vu'_k = 0$ and each u'_k has at most two nonzero components. The matrix $\mathrm{I}_n + uv$ is then expressible as a product of special matrices*

$$\mathrm{I}_n + uv = (\mathrm{I}_n + u'_1v)\ (\mathrm{I}_n + u'_2v)\ \cdots\ (\mathrm{I}_n + u'_Nv)$$

and consequently, it belongs to $\mathbb{E}_n(\mathbf{A})$.

D The canonical basis of $\mathbf{A}^n$ is denoted $(e_1, \dots, e_n)$. We have $a_1, \dots, a_n$ in $\mathbf{A}$ such that $a_1v_1 + \cdots + a_nv_n = 1$.
For $i \leqslant j$, let us define $a_{ij} \in \mathbf{A}$ by $a_{ij} = u_ia_j - u_ja_i$. Then

$$u = \sum\nolimits_{i<j} a_{ij}(v_je_i - v_ie_j) = \sum\nolimits_{i\leqslant j} a_{ij}(v_je_i - v_ie_j).$$

Indeed, for fixed k, the coefficient of e_k in the right-hand sum is

$$\begin{aligned}\sum_{j\geqslant k} a_{kj}v_j - \sum_{i<k} a_{ik}v_i &= \sum_{j\geqslant k}(u_ka_j - u_ja_k)v_j - \sum_{i<k}(u_ia_k - u_ka_i)v_i \\ &= u_k\sum\nolimits_{j=1}^{n} a_jv_j - a_k\sum\nolimits_{j=1}^{n} u_jv_j \;=\; u_k.\end{aligned}$$

For $i < j$, we then define $u'_{ij} \in \mathbf{A}^{n\times 1}$ by $u'_{ij} = a_{ij}(v_je_i - v_ie_j)$. It is clear that u'_{ij} has at most two nonzero components and that $vu'_{ij} = 0$. □

2. The Mennicke symbol

2.1. Lemma. *Let a, b be comaximal elements in $\mathbf{A}$. Then the equivalence class in $\mathbb{SL}_3(\mathbf{A})/\mathbb{E}_3(\mathbf{A})$ of the matrix $\begin{bmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{bmatrix}$ does not depend on the choice of c and d satisfying $1 = ad - bc$.*
We denote by $\{a, b\}$ the element of $\mathbb{SL}_3(\mathbf{A})/\mathbb{E}_3(\mathbf{A})$ obtained thus. We call it the Mennicke symbol *of (a, b).*

D Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, $A' = \begin{bmatrix} a & b \\ c' & d' \end{bmatrix}$ with $ad - bc = ad' - bc' = 1$. Then

$$AA'^{-1} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} d' & -b \\ -c' & a \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ cd' - c'd & 1 \end{bmatrix},$$

and $\begin{bmatrix} A & 0_{2,1} \\ 0_{1,2} & 1 \end{bmatrix}\begin{bmatrix} A' & 0_{2,1} \\ 0_{1,2} & 1 \end{bmatrix}^{-1} = \begin{bmatrix} AA'^{-1} & 0_{2,1} \\ 0_{1,2} & 1 \end{bmatrix}$ is in $\mathbb{E}_3(\mathbf{A})$. □

2.2. Proposition. *The Mennicke symbol satisfies the following properties.*

1. *If $a \in \mathbf{A}^\times$, then $\{a, b\} = 1$ for all $b \in \mathbf{A}$.*
2. *If $\langle 1\rangle = \langle a, b\rangle = \langle a', b\rangle$ then $1 \in \langle aa', b\rangle$ and $\{aa', b\} = \{a, b\}\{a', b\}$.*
3. *If $1 \in \langle a, b\rangle$, then $\{a, b\} = \{b, a\} = \{a + tb, b\}$ for all $t \in \mathbf{A}$.*

D *1.* The matrix $\begin{bmatrix} a & b \\ 0 & a^{-1} \end{bmatrix}$ is a member of $\mathbb{E}_2(\mathbf{A})$.

2. We have

$$\begin{bmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{bmatrix} \overset{\mathbb{E}_3(\mathbf{A})}{\sim} \begin{bmatrix} a & 0 & b \\ 0 & 1 & 0 \\ c & 0 & d \end{bmatrix},$$

and

$$\begin{bmatrix} a' & b & 0 \\ c' & d' & 0 \\ 0 & 0 & 1 \end{bmatrix} \overset{\mathbb{E}_3(\mathbf{A})}{\sim} \begin{bmatrix} a' & 0 & -b \\ c' & 0 & -d' \\ 0 & 1 & 0 \end{bmatrix} \overset{\mathbb{E}_3(\mathbf{A})}{\sim} \begin{bmatrix} a' & 0 & -b \\ c' & 0 & -d' \\ 0 & 1 & a \end{bmatrix}.$$

The product $\{a, b\}\{a', b\}$ is represented by the product of the matrices on the right-hand side, i.e. by

$$\begin{bmatrix} aa' & b & 0 \\ c' & 0 & -d' \\ ca' & d & 1 \end{bmatrix} \overset{\mathbb{E}_3(\mathbf{A})}{\sim} \begin{bmatrix} aa' & b & 0 \\ * & * & 0 \\ ca' & d & 1 \end{bmatrix} \overset{\mathbb{E}_3(\mathbf{A})}{\sim} \begin{bmatrix} aa' & b & 0 \\ * & * & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

and therefore $\{a, b\}\{a', b\} = \{aa', b\}$.

3. If $ad - bc = 1$, then $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \overset{\mathbb{E}_2(\mathbf{A})}{\sim} \begin{bmatrix} -b & a \\ -d & c \end{bmatrix}$, and so

$$\{a, b\} = \{-b, a\} = \{-1, a\}\{b, a\} = \{b, a\}.$$

Finally, $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \overset{\mathbb{E}_2(\mathbf{A})}{\sim} \begin{bmatrix} a + tb & b \\ c + td & d \end{bmatrix}$, so $\{a, b\} = \{a + tb, b\}$. □

2.3. Lemma. (Local version)
Let $\mathbf{A}$ *be a residually discrete local ring and* f, $g \in \mathbf{A}[X]$ *be comaximal with* f *monic. Then we have*

$$\{f, g\} = \{f(0), g(0)\} = 1.$$

D Let $af + bg = 1$. First note that we can divide b by f and that we then obtain an equality $a_1 f + b_1 g = 1$ with $\deg(b_1) < \deg(f)$, and so, since f is monic, $\deg(a_1) < \deg(g)$. Therefore assume without loss of generality that $\deg(b) < \deg(f)$ and $\deg(a) < \deg(g)$.

Let r be the remainder of the Euclidean division of g by f. Then $\{f, g\} = \{f, r\}$. In particular, if $\deg(f) = 0$ we are done. Otherwise, we can assume $\deg(g) < \deg(f)$ and we reason by induction on $\deg(f)$. Since $\mathbf{A}$ is local and residually discrete, $g(0) \in \mathbf{A}^\times$ or $g(0) \in \mathfrak{m} = \operatorname{Rad} \mathbf{A}$.

First of all suppose that $g(0)$ is invertible. Then

$$\{f, g\} = \{f - g(0)^{-1} f(0) g, g\},$$

so that we can assume that $f(0) = 0$ and $f = X f_1$. Then

$$\{X f_1, g\} = \{X, g\}\{f_1, g\} = \{X, g(0)\}\{f_1, g\} = \{f_1, g\}$$

and the proof ends by induction since f_1 is monic.

Now suppose that $g(0)$ is in $\mathfrak{m}$. As $a(0)f(0) + b(0)g(0) = 1$, we have $a(0)f(0) \in 1 + \mathfrak{m} \subseteq \mathbf{A}^\times$, and so $a(0) \in \mathbf{A}^\times$. However,

$$\begin{bmatrix} f & g & 0 \\ -b & a & 0 \\ 0 & 0 & 1 \end{bmatrix} \equiv \begin{bmatrix} f - b & g + a & 0 \\ -b & a & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \text{mod } \mathbb{E}_3(\mathbf{A}[X]),$$

so

$$\{f, g\} = \{f - b, g + a\},$$

with $f - b$ monic, $\deg(f - b) = \deg(f)$, $\deg(g + a) < \deg(f)$ and $(g + a)(0)$ in $\mathfrak{m} + \mathbf{A}^\times = \mathbf{A}^\times$. We are therefore brought back to the previous case. □

Our basic local-global machinery (page 871) applied to the previous local proof, gives the following quasi-global lemma.

2.4. Lemma. (Quasi-global version)
Let $\mathbf{A}$ be a ring and f, g be elements of $\mathbf{A}[X]$ comaximal with f monic. Then, there exists in $\mathbf{A}$ a system of comaximal elements (s_i) such that in each localized ring $\mathbf{A}[1/s_i]$, we have the following equality of the Mennicke symbols

$$\{f, g\} = \{f(0), g(0)\} = 1.$$

3. Unimodular polynomial vectors

3.1. Notation. If $\mathfrak{b}$ is an ideal of $\mathbf{B}$, let $\mathbb{GL}_n(\mathbf{B}, \mathfrak{b})$ be the subgroup of $\mathbb{GL}_n(\mathbf{B})$ that is the kernel of the natural morphism $\mathbb{GL}_n(\mathbf{B}) \to \mathbb{GL}_n(\mathbf{B}/\mathfrak{b})$. We adopt an analogous notation for $\mathbb{SL}_n$.
Be careful for the group $\mathbb{E}_n$! Let $\mathbb{E}_n(\mathbf{B}, \mathfrak{b})$ be the normal subgroup generated by the $\mathrm{E}_{ij}(b)$'s with $b \in \mathfrak{b}$.

The group $\mathbb{E}_n(\mathbf{B}, \mathfrak{b})$ is a subgroup of the kernel of $\mathbb{E}_n(\mathbf{B}) \to \mathbb{E}_n(\mathbf{B}/\mathfrak{b})$, and in general, it is a strict subgroup. However, in the case where $\mathbf{B} = \mathbf{A}[X]$ and $\mathfrak{b} = \langle X \rangle$, the two groups coincide. This result is given by the following lemma.

3.2. Lemma. *The group $\mathbb{E}_n(\mathbf{A}[X], \langle X \rangle)$ is the kernel of the canonical homomorphism $\mathbb{E}_n(\mathbf{A}[X]) \to \mathbb{E}_n(\mathbf{A}[X]/\langle X \rangle) = \mathbb{E}_n(\mathbf{A})$. It is generated by the matrices of the type $\gamma\, \mathrm{E}_{ij}(Xg)\, \gamma^{-1}$ with $\gamma \in \mathbb{E}_n(\mathbf{A})$ and $g \in \mathbf{A}[X]$.*

D Let H be this kernel. We will use the following decomposition, valid in every group, of a product $\alpha_1\beta_1\alpha_2\beta_2 \cdots \alpha_m\beta_m$, for example with $m = 3$

$$\left(\alpha_1\beta_1\alpha_1^{-1}\right)\left((\alpha_1\alpha_2)\beta_2(\alpha_1\alpha_2)^{-1}\right)\left((\alpha_1\alpha_2\alpha_3)\beta_3(\alpha_1\alpha_2\alpha_3)^{-1}\right)(\alpha_1\alpha_2\alpha_3).$$

Therefore let $E = E(X) \in H$, $E = \prod_{i=1}^m \mathrm{E}_{i_k,j_k}(f_k)$ with $f_k \in \mathbf{A}[X]$.
We write $f_k = c_k + Xg_k$ with $c_k = f_k(0) \in \mathbf{A}$ and

$$\mathrm{E}_{i_k,j_k}(f_k) = \alpha_k\beta_k, \quad \text{with} \quad \alpha_k = \mathrm{E}_{i_k,j_k}(c_k), \quad \beta_k = \mathrm{E}_{i_k,j_k}(Xg_k).$$

We finish by applying the decomposition given above and by using the equality $\alpha_1 \cdots \alpha_m = E(0) = \mathrm{I}_n$. □

3.3. Proposition. *Let $n \geqslant 3$, $s \in \mathbf{A}$ and $E = E(X) \in \mathbb{E}_n(\mathbf{A}_s[X], \langle X\rangle)$. There exist $k \in \mathbb{N}$ and $E' = E'(X) \in \mathbb{E}_n(\mathbf{A}[X], \langle X\rangle)$ satisfying $E'(X) = E(s^k X)$ over $\mathbf{A}_s[X]$.*

D We can suppose $E = \gamma \mathrm{E}_{ij}(Xg)\gamma^{-1}$ with $\gamma \in \mathbb{E}_n(\mathbf{A}_s)$ and $g \in \mathbf{A}_s[X]$. Letting $u \in \mathbf{A}_s^{n\times 1}$ be the column i of γ and $v \in \mathbf{A}_s^{1\times n}$ be the row j of γ^{-1}, we have

$$E(X) = \gamma \mathrm{E}_{ij}(Xg)\gamma^{-1} = \mathrm{I}_n + (Xg)uv, \quad vu = 0, \quad v \text{ unimodular.}$$

Theorem 1.4 allows us to write $u = u'_1 + u'_2 + \cdots + u'_N$ with $vu'_k = 0$ and $u'_k \in \mathbf{A}_s^{n\times 1}$ has at most two nonzero components. We therefore have

$$E(X) = (\mathrm{I}_n + (Xg)u'_1 v)\ (\mathrm{I}_n + (Xg)u'_2 v)\ \cdots\ (\mathrm{I}_n + (Xg)u'_N v).$$

By using an analogous method to Fact 1.3, we easily prove that there exist $k \in \mathbb{N}$, $\widetilde{g} \in \mathbf{A}[X]$, $\widetilde{u}_k \in \mathbf{A}^{n\times 1}$ and $\widetilde{v} \in \mathbf{A}^{1\times n}$ such that we have over $\mathbf{A}_s$ the equalities $g = \widetilde{g}/s^k$, $u'_k = \widetilde{u}_k/s^k$, $v = \widetilde{v}/s^k$, $\widetilde{v}\widetilde{u}_k = 0$, and $\widetilde{u}_k$ has at most two nonzero components. Then let

$$E'(X) = (\mathrm{I}_n + (X\widetilde{g})\widetilde{u}_1\widetilde{v})\ (\mathrm{I}_n + (X\widetilde{g})\widetilde{u}_2\widetilde{v})\ \cdots\ (\mathrm{I}_n + (X\widetilde{g})\widetilde{u}_N\widetilde{v}).$$

By Corollary 1.2, each $\mathrm{I}_n + (X\widetilde{g})\widetilde{u}_k\widetilde{v}$ belongs to $\mathbb{E}_n(\mathbf{A}[X])$. We therefore have $E'(X) \in \mathbb{E}_n(\mathbf{A}[X])$, $E'(0) = \mathrm{I}_n$ and $E'(s^{3k}X) = E(X)$ over $\mathbf{A}_s[X]$. □

3.4. Lemma. *Let $n \geqslant 3$ be an integer, $s \in \mathbf{A}$ and $E = E(X) \in \mathbb{E}_n(\mathbf{A}_s[X])$. There exists an integer $k \geqslant 0$ such that for all a, $b \in \mathbf{A}$ congruent modulo s^k, the matrix $E^{-1}(aX)E(bX)$ is in the image of the natural homomorphism*

$$\mathbb{E}_n(\mathbf{A}[X], \langle X\rangle) \longrightarrow \mathbb{E}_n(\mathbf{A}_s[X], \langle X\rangle).$$

Note: in short, but less precisely, if a and b are sufficiently "close", the coefficients of the matrix $E^{-1}(aX)\,E(bX)$ have no more denominator.

D We introduce two new indeterminates T, U and let

$$E'(X,T,U) = E^{-1}\big((T+U)X\big)\,E(TX).$$

We have $E'(X,T,0) = \mathrm{I}_n$. We apply Proposition 3.3 with $F = E'$ by taking $\mathbf{A}[X,T]$ instead of $\mathbf{A}$ and U instead of X: there exist a matrix G in $\mathbb{E}_n(\mathbf{A}[X,T,U], \langle U\rangle)$ and an integer $k \geqslant 0$ such that

$$E'(X,T,s^kU) = G(X,T,U) \ \text{ in } \ \mathbb{E}_n(\mathbf{A}_s[X,T,U], \langle U\rangle).$$

Therefore $G(X,T,U) = E^{-1}\big((T+s^kU)X\big)\,E(TX)$ over $\mathbf{A}_s$, and if $b = a + s^k c$, then

$$E^{-1}(aX)\,E(bX) = G(X,a,c) \ \text{ over } \ \mathbf{A}_s.$$

We have $G(0,T,U) = \mathrm{I}_n$ over $\mathbf{A}_s$, but not necessarily over $\mathbf{A}$. Let

$$H(X,T,U) = G^{-1}(0,T,U)\,G(X,T,U).$$

We then have $H(0,T,U) = \mathrm{I}_n$ over $\mathbf{A}$ and $H(X,T,U) = G(X,T,U)$ over $\mathbf{A}_s$.

We therefore obtain

$$E^{-1}(aX)\,E(bX) = H(X,a,c) \quad\text{in}\quad \mathbb{E}_n(\mathbf{A}_s[X],\langle X\rangle),$$

with $H(X,a,c) \in \mathbb{E}_n(\mathbf{A}[X],\langle X\rangle)$. □

3.5. Lemma. *Let $n \geqslant 3$ be an integer, $s \in \mathbf{A}$ and*

$$E = E(X) \in \mathbb{GL}_n(\mathbf{A}[X]) \cap \mathbb{E}_n(\mathbf{A}_s[X]).$$

There exists an integer $k \geqslant 0$ such that for all $a, b \in \mathbf{A}$ congruent modulo s^k, the matrix $E^{-1}(aX)E(bX)$ is in $\mathbb{E}_n(\mathbf{A}[X],\langle X\rangle)$.

D The proof is left to the reader. □

3.6. Lemma. *Let $n \geqslant 3$, s, t be comaximal in $\mathbf{A}$ and*

$$E \in \mathbb{GL}_n(\mathbf{A}[X],\langle X\rangle) \cap \mathbb{E}_n(\mathbf{A}_s[X]) \cap \mathbb{E}_n(\mathbf{A}_t[X]).$$

Then $E \in \mathbb{E}_n(\mathbf{A}[X])$.

D By Lemma 3.5, there exists some k such that for all a, $b \in \mathbf{A}$ congruent modulo s^k, or modulo t^k, the matrix $E^{-1}(aX)E(bX)$ is in $\mathbb{E}_n(\mathbf{A}[X],\langle X\rangle)$.
Let $c \in \mathbf{A}$ such that $c \equiv 0 \bmod s^k$ and $c \equiv 1 \bmod t^k$.
Then we write $E = E^{-1}(0\cdot X)\,E(c\cdot X)\,E^{-1}(c\cdot X)\,E(1\cdot X)$. □

4. Suslin's and Rao's local-global principles

Now we prove [Gupta & Murthy, Lemma I 5.9 (page 26)].

4.1. Theorem. *Let $n \geqslant 3$ and $A = A(X) \in \mathbb{GL}_n(\mathbf{A}[X])$.*

1. *If $A(0) = \mathrm{I}_n$, then $\mathfrak{a} = \{\, s \in \mathbf{A} \mid A \in \mathbb{E}_n(\mathbf{A}_s[X]) \,\}$ is an ideal of $\mathbf{A}$.*
2. *The set $\mathfrak{a} = \left\{\, s \in \mathbf{A} \;\middle|\; A(X) \overset{\mathbb{E}_n(\mathbf{A}_s[X])}{\sim} A(0) \,\right\}$ is an ideal of $\mathbf{A}$.*

D The two formulations are equivalent; we prove the second from the first by considering $A(X)A(0)^{-1}$.
1. It is clear that $s \in \mathfrak{a} \Rightarrow as \in \mathfrak{a}$ for all $a \in \mathbf{A}$. Now let s, t in $\mathfrak{a}$. We must show that $s + t \in \mathfrak{a}$, or that $1 \in \mathfrak{a}\mathbf{A}_{s+t}$. In short, we suppose that s and $t = 1 - s$ are in $\mathfrak{a}$, and we must show that $1 \in \mathfrak{a}$.
By definition, we have $A \in \mathbb{E}_n(\mathbf{A}_s[X])$ and $A \in \mathbb{E}_n(\mathbf{A}_t[X])$; by Lemma 3.6, we have $A \in \mathbb{E}_n(\mathbf{A}[X])$, i.e. $1 \in \mathfrak{a}$. □

This lemma could have been written in the form of the following concrete local-global principle (very nearly [Gupta & Murthy, Lemma I 5.8]).

4.2. Concrete local-global principle. (For the elementary group)
Let $n \geqslant 3$, $S_1, \ldots, S_k$ be comaximal monoids of $\mathbf{A}$ and $A \in \mathbb{GL}_n(\mathbf{A}[X])$, with $A(0) = \mathrm{I}_n$. Then

$$A \in \mathbb{E}_n(\mathbf{A}[X]) \quad\iff\quad \textit{for } i \in [\![1..k]\!],\quad A \in \mathbb{E}_n(\mathbf{A}_{S_i}[X]).$$

The following theorem re-expresses [Gupta & Murthy, corollary II 3.8].

4.3. Theorem. (Global version of Lemma 2.3)
Let $n \geqslant 3$, and f, $g \in \mathbf{A}[X]$ be comaximal, with f monic. Then, we have the following equality of Mennicke symbols: $\{f, g\} = \{f(0), g(0)\}$.

D Let $af - bg = 1$. Let $B = \begin{bmatrix} f & g & 0 \\ b & a & 0 \\ 0 & 0 & 1 \end{bmatrix}$.
The equality $\{f, g\} = \{f(0), g(0)\}$ means $A = BB(0)^{-1} \in \mathbb{E}_3(\mathbf{A}[X])$. We obviously have $A(0) = \mathrm{I}_3$. The concrete local-global principle 4.2 tells us that it suffices to prove the assertion after localization at comaximal elements (s_i), and Lemma 2.4 has constructed such a family. □

4.4. Corollary. (Triviality of the Mennicke symbol over $\mathbf{K}[\underline{X}]$)
Let $\mathbf{K}$ be a discrete field, and f, $g \in \mathbf{K}[\underline{X}]$ be comaximal. Then $\{f, g\} = 1$.

D We reason by induction on the number r of variables in $\underline{X}$.
The case $r = 0$, i.e. $\mathbf{K}[\underline{X}] = \mathbf{K}$ stems from $\mathbb{E}_3(\mathbf{K}) = \mathbb{SL}_3(\mathbf{K})$ ($\mathbf{K}$ is a discrete field). For $r \geqslant 1$, we suppose without loss of generality that f is nonzero. A change of variables allows us to transform f into a pseudomonic polynomial in X_r (Lemma VII-1.4), say $f = ah$ with $a \in \mathbf{K}^*$ and h monic in X_r. Then, by letting $h_0 = h(X_1, \ldots, X_{r-1}, 0)$ and $g_0 = g(X_1, \ldots, X_{r-1}, 0)$, which are in $\mathbf{K}[X_1, \ldots, X_{r-1}]$, we have $\{f, g\} = \{h, g\} = \{h_0, g_0\}$. □

At the end of this section the results are proved in the case of an integral ring. They are actually true for an arbitrary ring. For the general case, we must refer back to [157, 158, 159].

4.5. Theorem. *Let $n \geqslant 3$, $\mathbf{A}$ be an integral ring and $f(X)$ be a unimodular vector in $\mathbf{A}[X]^n$.
Then the set $\mathfrak{a} = \left\{\, s \in \mathbf{A} \mid f(X) \overset{\mathbb{E}_n(\mathbf{A}_s[X])}{\sim} f(0) \,\right\}$ is an ideal.*

We express the same thing in the following concrete local-global principle.

4.6. Concrete Rao local-global principle. *Let $n \geqslant 3$, $\mathbf{A}$ be an integral ring, $f(X)$ be unimodular vector in $\mathbf{A}[X]^n$, and S_1, …, S_k be comaximal monoids of $\mathbf{A}$. The following properties are equivalent.*

1. $f(X) \overset{\mathbb{E}_n(\mathbf{A}[X])}{\sim} f(0)$.
2. $f(X) \overset{\mathbb{E}_n(\mathbf{A}_{S_i}[X])}{\sim} f(0)$ *for each i.*

Proof of Theorem 4.5.
We must show that the set

$$\mathfrak{a} = \left\{\, s \in \mathbf{A} \mid f(X) \overset{\mathbb{E}_n(\mathbf{A}_s[X])}{\sim} f(0) \,\right\}$$

is an ideal. Since all the computations in $\mathbf{A}_s$ are valid in $\mathbf{A}_{sa}$, we have: $s \in \mathfrak{a}$ implies $as \in \mathfrak{a}$. Now let s_1 and s_2 be in $\mathfrak{a}$. We must show $s_1 + s_2 \in \mathfrak{a}$, or $1 \in \mathfrak{a}\mathbf{A}_{s_1+s_2}$. In short, we suppose that s_1 and $s_2 = 1 - s_1$ are in $\mathfrak{a}$, and we

must show $1 \in \mathfrak{a}$.
By definition, for $i = 1, 2$, we have a matrix $E_i = E_i(X) \in \mathbb{E}_n(\mathbf{A}_{s_i}[X])$ such that $E_i f(X) = f(0)$. We have $E_i(0)f(0) = f(0)$. Therefore, even if it entails replacing E_i by $E_i^{-1}(0)E_i$, we can assume that $E_i(0) = \mathrm{I}_n$.
We introduce $E = E_1E_2^{-1} \in \mathbb{E}_n(\mathbf{A}_{s_1s_2}[X], \langle X\rangle)$, which gives an integer $k \geqslant 0$ satisfying the conclusion of Lemma 3.4 for the matrix E and for the two localizations $\mathbf{A}_{s_1} \to \mathbf{A}_{s_1s_2}$ and $\mathbf{A}_{s_2} \to \mathbf{A}_{s_1s_2}$.
Let $c \in \mathbf{A}$ with $c \equiv 1 \bmod s_1^k$ and $c \equiv 0 \bmod s_2^k$. We therefore have two matrices $E_1' \in \mathbb{E}_n(\mathbf{A}_{s_1}[X], \langle X\rangle)$, $E_2' \in \mathbb{E}_n(\mathbf{A}_{s_2}[X], \langle X\rangle)$ that satisfy

- $E^{-1}(cX)E(X) = E_2'$ over $\mathbf{A}_{s_1s_2}$ (since $c \equiv 1 \bmod s_1^k$),
- $E(cX) = E(cX)E(0 \cdot X) = E_1'$ over $\mathbf{A}_{s_1s_2}$ (since $c \equiv 0 \bmod s_2^k$).

We obtain $E = E_1'E_2' = E_1E_2^{-1}$ over $\mathbf{A}_{s_1s_2}$, and ${E_1'}^{-1}E_1 = E_2'E_2$ over $\mathbf{A}_{s_1s_2}$. Since ${E_1'}^{-1}E_1 = F_1$ is defined over $\mathbf{A}_{s_1}$, that $E_2'E_2 = F_2$ is defined over $\mathbf{A}_{s_2}$, that they are equal over $\mathbf{A}_{s_1s_2}$, and that s_1 and s_2 are comaximal, there exists a unique matrix $F \in \mathbb{M}_n(\mathbf{A}[X])$ which gives F_1 over $\mathbf{A}_{s_1}$ and F_2 over $\mathbf{A}_{s_2}$. Once again we must prove that $F \in \mathbb{E}_n(\mathbf{A}[X])$ and $Ff = f(0)$. The first item results from Lemma 3.6. To satisfy $Ff = f(0)$, we will assume that $\mathbf{A}$ is integral, which legitimizes the following equalities over $\mathbf{A}$

$$Ff = {E_1'}^{-1}E_1f = {E_1'}^{-1}f(0) = E^{-1}(cX)f(0) = E_2(cX)E_1^{-1}(cX)f(0) = E_2(cX)f(cX) = f(0).$$

□

Note: In this proof the last verification is the only place where we need to assume that the ring is integral.

4.7. Theorem. *Let $n \geqslant 3$, $\mathbf{A}$ be a ring and $f = {}^{\mathrm{t}}\big(f_1(X), \dots, f_n(X)\big)$ be a unimodular vector in $\mathbf{A}[X]^n$, with 1 in the head ideal of the f_i's. Then*

$$f \overset{\mathbb{E}_n(\mathbf{A}[X])}{\sim} f(0) \overset{\mathbb{E}_n(\mathbf{A})}{\sim} f^\star(0) \overset{\mathbb{E}_n(\mathbf{A}[X])}{\sim} f^\star.$$

If one of the f_i's is monic, we have $f \overset{\mathbb{E}_n(\mathbf{A}[X])}{\sim} {}^{\mathrm{t}}[\,1\ 0\ \cdots\ 0\,]$.

D The little Horrocks' local theorem (Theorem XVI-5.14) and Rao's local-global principle gives the first equivalence. Next we copy the proof of Rao's theorem (Theorem XVI-5.18) by replacing $\mathbb{GL}_n$ by $\mathbb{E}_n$. □

4.8. Corollary. (Transitivity of $\mathbb{E}_n$ for $n \geqslant 3$)
If $\mathbf{K}$ is a discrete field and $\mathbf{K}[\underline{X}] = \mathbf{K}[X_1, \dots, X_r]$, then $\mathbb{E}_n(\mathbf{K}[\underline{X}])$ acts transitively over the set of unimodular vectors of $\mathbf{K}[\underline{X}]^n$ for $n \geqslant 3$.

D We reason by induction on r. The case $r = 0$ stems from the fact that $\mathbf{K}$ is a discrete field.
Let $r \geqslant 1$ and $f = {}^{\mathrm{t}}[\,f_1(\underline{X})\ \cdots\ f_n(\underline{X})\,]$ be a unimodular vector of $\mathbf{K}[\underline{X}]^n$. Let $\mathbf{A} = \mathbf{K}[X_1, \dots, X_{r-1}]$. One of the f_i's is nonzero and a change of

variables allows for the transformation into a pseudomonic polynomial in X_r (Lemma VII-1.4). With f_i monic in X_r, we apply Theorem 4.7 to obtain

$$f \overset{\mathbb{E}_n(\mathbf{K}[\underline{X}])}{\sim} f(X_1, \dots, X_{r-1}, 0).$$

This last vector is a unimodular vector of $\mathbf{A}^n$. We apply the induction hypothesis. □

Finally, the proof that Theorem 4.3 implies Suslin's stability theorem is simple and constructive, as in [Gupta & Murthy].

4.9. Theorem. (Suslin's stability theorem, case of discrete fields)
Let $\mathbf{K}$ be a discrete field. For $n \geqslant 3$, we have $\mathbb{SL}_n(\mathbf{K}[\underline{X}]) = \mathbb{E}_n(\mathbf{K}[\underline{X}])$.

D Let us prove the following preliminary result.
For $A \in \mathbb{GL}_n(\mathbf{K}[\underline{X}])$, there exist P, $Q \in \mathbb{E}_n(\mathbf{K}[\underline{X}])$ such that

$$P\,A\,Q \in \mathbb{GL}_2(\mathbf{K}[\underline{X}]) \subseteq \mathbb{GL}_n(\mathbf{K}[\underline{X}]).$$[1]

Indeed, let us consider the last row of A. It is a unimodular vector, therefore (Corollary 4.8), there exists a $Q_n \in \mathbb{E}_n(\mathbf{K}[\underline{X}])$ such that the last row of $A\,Q_n$ is $[\,0\ \cdots\ 0\ 1\,]$. Hence $P_n \in \mathbb{E}_n(\mathbf{K}[\underline{X}])$ such that the last column of $P_n(A\,Q_n)$ is ${}^{\mathrm{t}}[\,0\ \cdots\ 0\ 1\,]$, i.e. $P_n\,A\,Q_n \in \mathbb{GL}_{n-1}(\mathbf{K}[\underline{X}])$.
By iterating, we find matrices P, $Q \in \mathbb{E}_n(\mathbf{K}[\underline{X}])$ of the form

$$P = P_3 \cdots P_n, \ \ Q = Q_n \cdots Q_3,$$

such that $P\,A\,Q \in \mathbb{GL}_2(\mathbf{K}[\underline{X}])$.
If in addition $A \in \mathbb{SL}_n(\mathbf{K}[\underline{X}])$, we obtain $P\,A\,Q \in \mathbb{SL}_2(\mathbf{K}[\underline{X}]) \hookrightarrow \mathbb{SL}_3(\mathbf{K}[\underline{X}])$. We can then consider its image in $\mathbb{SL}_3(\mathbf{K}[\underline{X}])/\mathbb{E}_3(\mathbf{K}[\underline{X}])$.
As the corresponding Mennicke symbol equals 1 (Corollary 4.4), we obtain $P\,A\,Q \in \mathbb{E}_3(\mathbf{K}[\underline{X}])$, and ultimately $A \in \mathbb{E}_n(\mathbf{K}[\underline{X}])$. □

Exercises and problems

Exercise 1. Let $U \in \mathbf{A}^{n\times m}$ and $V \in \mathbf{A}^{m\times n}$.

1. Prove, for $N \in \mathbb{M}_n(\mathbf{A})$, that

$$(\mathrm{I}_m - VNU)(\mathrm{I}_m + VU) = \mathrm{I}_m + V\big(\mathrm{I}_n - N(\mathrm{I}_n + UV)\big)U.$$

Deduce that if $\mathrm{I}_n + UV$ is invertible with inverse N, then $\mathrm{I}_m + VU$ is invertible with inverse $\mathrm{I}_m - VNU$.

2. Deduce that $\mathrm{I}_n + UV$ is invertible if and only if $\mathrm{I}_m + VU$ is invertible, and establish symmetrical formulas for their inverses.

3. Show that $\det(\mathrm{I}_n + VU) = \det(\mathrm{I}_m + UV)$ in all cases.

[1] The inclusion $\mathbb{GL}_r \hookrightarrow \mathbb{GL}_n$ is defined as usual by $B \mapsto \mathrm{Diag}(B, \mathrm{I}_{n-r})$.

4. Suppose that $\mathrm{I}_m + VU$ is invertible. Show the following membership, due to Vaserstein.

$$\begin{bmatrix} \mathrm{I}_n + UV & 0 \\ 0 & (\mathrm{I}_m + VU)^{-1} \end{bmatrix} \in \mathbb{E}_{n+m}(\mathbf{A}).$$

What happens when $VU = 0$?

Exercise 2. With the notations of Lemma 2.1, prove that the matrix $A'^{-1}A$ is of the form $\mathrm{I}_2 + uv$ with $u, v \in \mathbf{A}^{2\times 1}$, $vu = 0$ and v unimodular.

Exercise 3. Let a, b, u, $v \in \mathbf{A}$ satisfy $1 = au + bv$. Show, only using the properties of the Mennicke symbol appearing in Proposition 2.2, that $\{a, b\} = \{u, v\} = \{a - v, b + u\}$.

Exercise 4. A stably free $\mathbf{A}$-module E of rank r is said to be *of type t* if $E \oplus \mathbf{A}^t \simeq \mathbf{A}^{r+t}$. Here we are interested in the relations between on the one hand the isomorphism classes of the stably free modules of rank $n-1$, of type 1, and on the other hand the $\mathbb{GL}_n(\mathbf{A})$-set $\mathrm{Um}_n(\mathbf{A})$ consisting of the unimodular vectors of $\mathbf{A}^n$.

1. Let $x \in \mathrm{Um}_n(\mathbf{A})$. Prove that the module $\mathbf{A}^n/\mathbf{A}x$ is stably free of rank $n-1$, of type 1, and that for $x' \in \mathrm{Um}_n(\mathbf{A})$, we have $\mathbf{A}^n/\mathbf{A}x \simeq \mathbf{A}^n/\mathbf{A}x'$ if and only if $x \overset{\mathbb{GL}_n(\mathbf{A})}{\sim} x'$. Show that we thus obtain a (first) bijective correspondence: $x \longleftrightarrow \mathbf{A}^n/\mathbf{A}x$

$$\boxed{\frac{\mathrm{Um}_n(\mathbf{A})}{\mathbb{GL}_n(\mathbf{A})} \overset{(1)}{\simeq} \frac{\text{stably free modules of rank } n-1, \text{ of type } 1}{\text{isomorphism}}}$$

What are the unimodular vectors that correspond to a free module?

2. Let $x \in \mathrm{Um}_n(\mathbf{A})$. Show that $x^\perp \overset{\mathrm{def}}{=} \operatorname{Ker} {}^{\mathrm{t}}x$ is a stably free module of rank $n-1$, of type 1, and that for $x' \in \mathrm{Um}_n(\mathbf{A})$, we have $x^\perp \simeq x'^\perp$ if and only if $x \overset{\mathbb{GL}_n(\mathbf{A})}{\sim} x'$. Prove that we thus obtain a (second) bijective correspondence: $x \longleftrightarrow x^\perp$

$$\boxed{\frac{\mathrm{Um}_n(\mathbf{A})}{\mathbb{GL}_n(\mathbf{A})} \overset{(2)}{\simeq} \frac{\text{stably free modules of rank } n-1, \text{ of type } 1}{\text{isomorphism}}}$$

3. If E is stably free of rank r and of type t, the same goes for its dual $E^\star$. For $t = 1$, describe the involution of $\mathrm{Um}_n(\mathbf{A})/\mathbb{GL}_n(\mathbf{A})$ induced by the involution $E \leftrightarrow E^\star$.

4. Let x, x', $y \in \mathbf{A}^n$ such that ${}^{\mathrm{t}}xy = {}^{\mathrm{t}}x'y = 1$. Why do we have $x \overset{\mathbb{GL}_n(\mathbf{A})}{\sim} x'$? Explicate $g \in \mathbb{GL}_n(\mathbf{A})$ such that $gx = x'$, g of the form $\mathrm{I}_n + uv$ with $vu = 0$ and v unimodular. Deduce that for $n \geqslant 3$, $g \in \mathbb{E}_n(\mathbf{A})$, and so $x \overset{\mathbb{E}_n(\mathbf{A})}{\sim} x'$.

Exercise 5. *(Autodual stably free modules of type* 1*)*

1. Let a, $b \in \mathbf{A}$, $x = (x_1, \dots, x_n) \in \mathbf{A}^n$ with $n \geqslant 3$ and $ax_1 + bx_2$ be invertible modulo $\langle x_3, \dots, x_n \rangle$ (in particular, x is unimodular).
   Let $x' = (-b, a, x_3, \dots, x_n)$. Explicate $z \in \mathbf{A}^n$ such that $\langle x \,|\, z \rangle = \langle x' \,|\, z \rangle = 1$. Deduce, for $G = \mathbb{GL}_n(\mathbf{A})$ (or better yet for $G = \mathbb{E}_n(\mathbf{A})$), that
   $$x \overset{G}{\sim} x' \overset{G}{\sim} (a, b, x_3, \dots, x_n).$$
2. Let $x, y \in \mathbf{A}^4$ such that $\langle x \,|\, y \rangle = 1$. Show that $x \overset{\mathbb{E}_4(\mathbf{A})}{\sim} y$. In particular, the stably free module $x^\perp = \operatorname{Ker} {}^{\mathrm{t}}x$ is isomorphic to its dual.
3. Analogous question to the previous one by replacing 4 with any even number $n \geqslant 4$.

Some solutions, or sketches of solutions

Exercise 1. *2.* We establish the formulas

$$N = (\mathrm{I}_n + UV)^{-1} = \mathrm{I}_n - UMV,\ M = (\mathrm{I}_m + VU)^{-1} = \mathrm{I}_m - VNU$$

4. We know that $\mathrm{I}_n + UV$ is invertible. Let $N = (\mathrm{I}_n + UV)^{-1}$, $M = (\mathrm{I}_m + VU)^{-1}$. We have therefore $N + UVN = \mathrm{I}_n = N + NUV$ and $M + VUM = \mathrm{I}_m = M + MVU$. We realize the following elementary operations

$$\begin{bmatrix} \mathrm{I}_n + UV & 0 \\ 0 & M \end{bmatrix} \begin{bmatrix} \mathrm{I}_n & -NU \\ 0 & \mathrm{I}_m \end{bmatrix} = \begin{bmatrix} \mathrm{I}_n + UV & -U \\ 0 & M \end{bmatrix},$$

$$\begin{bmatrix} \mathrm{I}_n + UV & -U \\ 0 & M \end{bmatrix} \begin{bmatrix} \mathrm{I}_n & 0 \\ V & \mathrm{I}_m \end{bmatrix} = \begin{bmatrix} \mathrm{I}_n & -U \\ MV & M \end{bmatrix},$$

then

$$\begin{bmatrix} \mathrm{I}_n & -U \\ MV & M \end{bmatrix} \begin{bmatrix} \mathrm{I}_n & U \\ 0 & \mathrm{I}_m \end{bmatrix} = \begin{bmatrix} \mathrm{I}_n & 0 \\ MV & MVU + M \end{bmatrix} = \begin{bmatrix} \mathrm{I}_n & 0 \\ MV & \mathrm{I}_m \end{bmatrix},$$

and finally

$$\begin{bmatrix} \mathrm{I}_n & 0 \\ MV & \mathrm{I}_m \end{bmatrix} \begin{bmatrix} \mathrm{I}_n & 0 \\ -MV & \mathrm{I}_m \end{bmatrix} = \begin{bmatrix} \mathrm{I}_n & 0 \\ 0 & \mathrm{I}_m \end{bmatrix}.$$

We therefore have explicated matrices α, β, γ, $\delta \in \mathbb{E}_{n+m}(\mathbf{A})$ such that

$$\begin{bmatrix} \mathrm{I}_n + UV & 0 \\ 0 & (\mathrm{I}_m + VU)^{-1} \end{bmatrix} \alpha\,\beta\,\gamma\,\delta = \mathrm{I}_{n+m},$$

hence

$$\begin{bmatrix} \mathrm{I}_n + UV & 0 \\ 0 & (\mathrm{I}_m + VU)^{-1} \end{bmatrix} = \delta^{-1}\,\gamma^{-1}\,\beta^{-1}\,\alpha^{-1} =$$

$$\begin{bmatrix} \mathrm{I}_n & 0 \\ MV & \mathrm{I}_m \end{bmatrix} \begin{bmatrix} \mathrm{I}_n & -U \\ 0 & \mathrm{I}_m \end{bmatrix} \begin{bmatrix} \mathrm{I}_n & 0 \\ -V & \mathrm{I}_m \end{bmatrix} \begin{bmatrix} \mathrm{I}_n & NU \\ 0 & \mathrm{I}_m \end{bmatrix}.$$

In the special case where $VU = 0$, we have shown that

$$\begin{bmatrix} \mathrm{I}_n + UV & 0 \\ 0 & \mathrm{I}_m \end{bmatrix} \in \mathbb{E}_{n+m}(\mathbf{A}).$$

Exercise 2. By using $ad' = 1 + bc'$, $ad = 1 + bc$, we obtain for $A'^{-1}A$

$$\begin{bmatrix} d' & -b \\ -c' & a \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} ad' - bc & bd' - bd \\ ac - ac' & ad - bc' \end{bmatrix} = \begin{bmatrix} 1 + b(c' - c) & b(d' - d) \\ a(c - c') & 1 + b(c - c') \end{bmatrix}.$$

By replacing $b(c' - c)$ with $a(d' - d)$, we see that $A'^{-1}A = \mathrm{I}_2 + uv$ with

$$u = \begin{bmatrix} d' - d \\ c - c' \end{bmatrix}, \ v = \begin{bmatrix} a & b \end{bmatrix}, \ vu = 0, \text{ and } v \text{ unimodular.}$$

Exercise 3. We have $\{au, b\} = \{a, b\}\{u, b\}$.
But $au = 1 - bv$ so $\{au, b\} = \{1 - bv, b\} = \{1, b\} = 1$. Recap: $\{a, b\}\{u, b\} = 1$.
Similarly, $\{u, b\}\{u, v\} = 1$, so $\{a, b\} = \{u, v\}$.
Finally, $(a - v)u + (b + u)v = 1$, so $\{a - v, b + u\} = \{u, v\}$.

Exercise 4. *1.* Let $y \in \mathbf{A}^n$ such that ${}^{\mathrm{t}}yx = 1$.
We have $\mathbf{A}^n = \mathbf{A}x \oplus \operatorname{Ker} {}^{\mathrm{t}}y$ and so $\mathbf{A}^n/\mathbf{A}x \simeq \operatorname{Ker} {}^{\mathrm{t}}y$ is stably free.
If $x \overset{\mathbb{GL}_n(\mathbf{A})}{\sim} x'$, it is clear that $\mathbf{A}^n/\mathbf{A}x \simeq \mathbf{A}^n/\mathbf{A}x'$.
Conversely, let $\varphi : M = \mathbf{A}^n/\mathbf{A}x \to M' = \mathbf{A}^n/\mathbf{A}x'$ be an isomorphism. We have $\mathbf{A}^n \simeq M \oplus \mathbf{A}x \simeq M' \oplus \mathbf{A}x'$. We define $\psi : \mathbf{A}x \to \mathbf{A}x'$, $ax \mapsto ax'$. Then $\varphi \oplus \psi$ seen in $\mathbb{GL}_n(\mathbf{A})$ transforms x into x', so $x \overset{\mathbb{GL}_n(\mathbf{A})}{\sim} x'$.
A unimodular vector $x \in \mathbf{A}^n$ provides a free module $\mathbf{A}^n/\mathbf{A}x$ if and only if x is part of a basis of $\mathbf{A}^n$.

2. Let $M = x^\perp$, $M' = x'^\perp$ and assume $M \simeq M'$. By denoting by $\overset{\circ}{M} \subseteq (\mathbf{A}^n)^\star$ the orthogonal of $M \subseteq \mathbf{A}^n$, we have $\overset{\circ}{M} = \mathbf{A}\,{}^{\mathrm{t}}x$ and $\overset{\circ}{M'} = \mathbf{A}\,{}^{\mathrm{t}}x'$. If $\langle x \,|\, y\rangle = 1$, $\langle x' \,|\, y'\rangle = 1$, we have $\mathbf{A}^n = \mathbf{A}y \oplus M = \mathbf{A}y' \oplus M'$, hence an automorphism of $\mathbf{A}^n$ transforming M into M' (send y to y'), then by duality, an automorphism u of $(\mathbf{A}^n)^\star \simeq \mathbf{A}^n$ transforming $\mathbf{A}\,{}^{\mathrm{t}}x$ into $\mathbf{A}\,{}^{\mathrm{t}}x'$. We deduce $u({}^{\mathrm{t}}x) = \varepsilon\,{}^{\mathrm{t}}x'$ with $\varepsilon \in \mathbf{A}^\times$. Then, $\varepsilon^{-1}\,{}^{\mathrm{t}}u$ transforms x into x'.

3. If $G = E \oplus F$, then $G^\star \simeq E^\star \oplus F^\star$; with $G = \mathbf{A}^{r+t} \simeq G^\star$, $F = \mathbf{A}^r \simeq F^\star$, we obtain the result. The involution induced over $\mathrm{Um}_n(\mathbf{A})/\mathbb{GL}_n(\mathbf{A})$ is the following: to the class modulo $\mathbb{GL}_n(\mathbf{A})$ of $x \in \mathrm{Um}_n(\mathbf{A})$, we associate the class modulo $\mathbb{GL}_n(\mathbf{A})$ of an element $y \in \mathrm{Um}_n(\mathbf{A})$ that satisfies $\langle x \,|\, y\rangle = 1$. Naturally, there are several y that are suitable but their class modulo $\mathbb{GL}_n(\mathbf{A})$ is well-defined.

4. We have $\mathbf{A}^n = \mathbf{A}y \oplus x^\perp = \mathbf{A}y \oplus x'^\perp$ hence $x^\perp \simeq x'^\perp \simeq \mathbf{A}^n/\mathbf{A}y$ so $x \overset{\mathbb{GL}_n(\mathbf{A})}{\sim} x'$.
To determine $g \in \mathbb{GL}_n(\mathbf{A})$ realizing $gx = x'$, we use $\mathbf{A}^n = \mathbf{A}x \oplus y^\perp = \mathbf{A}x' \oplus y^\perp$.
Generally, let $G = E \oplus F = E' \oplus F$; to explicate some automorphism of G mapping E to E', we proceed as follows. Let π be the projection over E, π' be the projection over E' and $p = \mathrm{I}_G - \pi$, $p' = \mathrm{I}_G - \pi'$.
The projectors p and p' have the same image F. Let $h = p' - p = \pi - \pi'$.
We obtain $h^2 = 0$ and $(\mathrm{I}_G - h)p(\mathrm{I}_G + h) = p'$, or $(\mathrm{I}_G - h)\pi(\mathrm{I}_G + h) = \pi'$. Therefore $\mathrm{I}_G - h$ is an automorphism of G transforming $\operatorname{Im}\pi = E$ into $\operatorname{Im}\pi' = E'$.
Here $E = \mathbf{A}x$, $E' = \mathbf{A}x'$, $F = y^\perp$, so

$$\pi(z) = \langle z \,|\, y\rangle x, \quad \pi'(z) = \langle z \,|\, y\rangle x', \quad h(z) = \langle z \,|\, y\rangle(x - x').$$

The desired automorphism of $\mathbf{A}^n$ that transforms x into x' is therefore

$$\mathrm{I}_n - h : z \mapsto z + \langle z \,|\, y\rangle(x' - x) \quad \text{i.e.} \quad \mathrm{I}_n - h = \mathrm{I}_n + uv$$

with $u = x' - x \in \mathbf{A}^{n\times 1}$, $v = {}^{\mathrm{t}}y \in \mathbf{A}^{1\times n}$; we indeed have $vu = 0$ and v unimodular.

Exercise 5. *1.* The key to the problem is found in the double equality, for some u in $\mathbf{A}$, $z_1 = u(a + x_2)$, $z_2 = u(b - x_1)$, which implies

$$z_1x_1 + z_2x_2 = u(ax_1 + bx_2) = z_1b + z_2(-a).$$

Let u such that $u(ax_1 + bx_2) + z_3x_3 + \cdots + z_nx_n = 1$ and $z = (z_1, z_2, z_3, \ldots, z_n)$. We then have $\langle z \mid x \rangle = \langle z \mid x' \rangle = 1$. By Exercise 4, $x \overset{G}{\sim} x'$. As $(b, -a) \overset{\mathbb{E}_2(\mathbf{A})}{\sim} (a, b)$, we have $x \overset{G}{\sim} (a, b, x_3, \ldots, x_n)$.

2. As $x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 = 1$, we have

$$(x_1, x_2, x_3, x_4) \overset{G}{\sim} (y_1, y_2, x_3, x_4) \overset{G}{\sim} (y_1, y_2, y_3, y_4)$$

The rest of the question immediately stems from this.

3. Analogous method to the previous question.

Bibliographic comments

Section 2 and the proof of Theorem 4.9 follow very closely the presentation in [Gupta & Murthy]. For the most part we have only transformed a few abstract local-global arguments into concrete arguments via the use of the local-global machinery with prime ideals explained in Section XV-5.

Section 3 is directly inspired by [Lam06, chapter VI, section 2].

Annex. Constructive logic

Contents

Introduction

This annex is devoted to presenting a few basic concepts of constructive mathematics in Bishop's style, illustrated by the three founding works [Bishop, Bishop & Bridges, MRR].

By constructive logic, we mean the logic of constructive mathematics.

1. Basic objects, Sets, Functions

Non-negative integers and constructions are two primitive notions. They cannot be defined.

Other primitive notions are closely tied to common language and are difficult to place. For example the equality of the number 2 in two distinct occurrences.

The formalization of a piece of mathematics can be used to better understand what we are doing to it. However, to speak about a formalism it is necessary to understand a lot of things that are of the same type of complexity as the non-negative integers. Thus, the formalism is only a tool and it cannot replace intuition and basic experience (for example the non-negative integers, the constructions): as powerful as a computer may be, it will never understand "what it does," or, as René Thom used to say, "All that is rigorous is insignificant."

Sets

A *set* $(X, =_X, \neq_X)$ is defined by saying:

— how to construct an element of the set (we say that we have defined a *preset* X)

— what is the meaning of the *equality* of two elements of the set (we have to prove that it is indeed an equivalence relation)

— what is the meaning of the *distinction*[1] of two elements of the set (we then say that the elements are *discernible* or *distinct*). We need to show the following properties:

- $(x \neq_X y \ \wedge\ x =_X x' \ \wedge\ y =_X y') \ \Rightarrow\ x' \neq_X y'$,
- $x \neq_X x$ is impossible,
- $x \neq_X y \ \Rightarrow\ y \neq_X x$.

[1] This terminology *is not* a homage to Pierre Bourdieu. All in all, we prefer *distinction* to *non-equality*, which presents the disadvantage of a negative connotation, and to *inequality* which is rather used in the context of order relations. For the real numbers for example, it is the equality and not the distinction that is a negative assertion.

Ordinarily, we drop the index X for the symbols $=$ and $\neq$. If the distinction is not specified, it is implicitly defined as meaning the absurdity of the equality.

A distinction relation is called a *separation* relation if it satisfies the following *cotransitivity* property (for three arbitrary elements x, y, z of X):

– $x \neq_X y \;\Rightarrow\; (x \neq_X z \;\vee\; y \neq_X z)$.

A separation relation $\neq_X$ is said to be *narrow* if $x =_X y$ is equivalent to the absurdity of $x \neq_X y$. In a set with a narrow separation, distinction is often more important than equality.

A set $(X, =_X, \neq_X)$ is said to be *discrete* if we have

$$\forall x, y \in X \; (x =_X y \vee x \neq_X y).$$

In this case the distinction is a narrow separation and it is equivalent to the absurdity of the equality.

The non-negative integers

The set $\mathbb{N} = \{0, 1, 2, \ldots\}$ of non-negative integers is considered as a priori well-defined. However, note that constructively this is a *potential infinity* and not an *actual infinity*. By the idea of a potential infinite we mean that the infiniteness of $\mathbb{N}$ is apprehended as an essentially negative notion; we never stop exhausting the non-negative integers. On the contrary, the semantic of $\mathbb{N}$ in classical mathematics is that of a completed infinite, which exists "somewhere," at least in a purely ideal way.

A non-negative integer can be encoded in the usual way. The comparison of two integers given in a coded form can be made reliably. In short, the set of non-negative integers is a discrete set and the order relation is *decidable*

$$\forall n, m \in \mathbb{N} \quad (n < m \quad \vee \quad n = m \quad \vee \quad n > m)$$

Sets of pairs

When two sets are defined their *Cartesian product* is also naturally defined: the fabrication of the pairs of objects is an elementary construction. Equality and distinction over a Cartesian product are naturally defined.

Functions

The set $\mathbb{N}^{\mathbb{N}}$ of sequences of non-negative integers depends on the primitive notion of construction. An element of $\mathbb{N}^{\mathbb{N}}$ is a construction that takes as input an element of $\mathbb{N}$ and gives as output an element of $\mathbb{N}$. The equality of two elements in $\mathbb{N}^{\mathbb{N}}$ is the *extensional equality*

$$(u_n) =_{\mathbb{N}^{\mathbb{N}}} (v_n) \quad \text{signifies} \quad \forall n \in \mathbb{N} \;\; u_n = v_n.$$

Thus, the equality between two elements of $\mathbb{N}^{\mathbb{N}}$ a priori asks for an infinity of "elementary computations," actually the equality demands a proof.

The distinction of two elements of $\mathbb{N}^\mathbb{N}$ is the *extensional distinction* relation

$$(u_n) \neq_{\mathbb{N}^\mathbb{N}} (v_n) \quad \overset{\text{def}}{\iff} \quad \exists n \in \mathbb{N} \ \ u_n \neq v_n.$$

Thus, the distinction of two elements of $\mathbb{N}^\mathbb{N}$ can be observed by a simple computation.

1.1. Example. *The distinction of* $\mathbb{N}^\mathbb{N}$ *is a narrow separation relation.*

Cantor's diagonalization argument is constructive. It shows that $\mathbb{N}^\mathbb{N}$ is *much more complicated* than $\mathbb{N}$. From a constructive point of view, $\mathbb{N}$ and $\mathbb{N}^\mathbb{N}$ are only potential infinities: it holds no meaning to say that a potential infinity is *greater* than another.

Digression. When you say "I give you a sequence of non-negative integers," you must prove that the construction $n \mapsto u_n$ that you propose works for any input n. Moreover, when you say "Let us consider an arbitrary sequence of non-negative integers $(u_n)_{n\in\mathbb{N}}$," the only thing that you know for certain is that for all $n \in \mathbb{N}$, you have $u_n \in \mathbb{N}$, and that this u_n is nonambiguous: you can for example conceive the sequence as given by an oracle. Actually, you could a priori ask, symmetrically, what exactly is the construction $n \mapsto u_n$, and a proof that this construction works for every input n.

However, in the constructivism à la Bishop, we make no specific assumptions regarding "what the legitimate constructions from $\mathbb{N}$ to $\mathbb{N}$ are," nor on "what precisely is a proof that a construction works." Thus we are in a dissymmetrical situation.

This dissymmetry has the following consequence. Everything you prove has a computational content, but everything you prove is also valid from a classical point of view. Classical mathematics could regard constructive mathematics as only speaking of constructive objects, and Bishop's constructive mathematics is certainly primarily interested in constructive objects (see [17]). But in fact, the constructive proofs à la Bishop work for any type of mathematical object.[2] The theorems that we find in [Bishop & Bridges] and [MRR] are valid in classical mathematics, but they also support the Russian constructive interpretation (in which all the mathematical objects are words from a formal language that we could fix once and for all) or yet again Brouwer's intuitionist philosophy, which has a significantly idealistic component. ■

After this digression let us get back on topic: functions. Generally, a *function* $f : X \to Y$ is a construction that takes as input some $x \in X$ and a proof that $x \in X$, and gives as output some $y \in Y$ and a proof that $y \in Y$.

[2] ... if there exist nonconstructive mathematical objects.

In addition, this construction must be *extensional*

$$x =_X x' \Rightarrow f(x) =_Y f(x') \qquad \text{and} \qquad f(x) \neq_Y f(x') \Rightarrow x \neq_X x'.$$

When X and Y are well-defined sets, we consider (in constructive mathematics à la Bishop) that the set $\mathcal{F}(X, Y)$ of functions $f : X \to Y$ is also well-defined. For the equality and the distinction we take the usual extensional definitions.

A function $f : X \to Y$ is *injective* if it satisfies

$$f(x) =_Y f(x') \Rightarrow x =_X x' \quad \text{and} \quad x \neq_X x' \Rightarrow f(x) \neq_Y f(x').$$

Finite, bounded, enumerable and countable sets

We now give a certain number of pertinent constructive definitions related to the concepts of finite, infinite and countable sets in classical mathematics.

- A set is said to be *finite* if there is a bijection between this set and the set of integers $< n$ for a certain integer n (this is the definition given page 84).
- A set X is said to be *finitely enumerable* if there is a surjective map $[0, n[\to X$ for some integer n (this is the definition given page 84).
- A preset X is said to be *enumerable* if we have given a means to enumerate it that allows it to possibly be empty, which happens in practice as follows.[3] We give some $\alpha \in \{0, 1\}^{\mathbb{N}}$ and some operation φ that satisfy the following two assertions:
  – if $\alpha(n) = 1$ then φ constructs from the input n an element of X,
  – every element of X is constructed as such.
- A set is said to be *countable* if it is enumerable (as a preset) and discrete.
- If n is a nonzero integer, we say that a set *has at most n elements* if for every family $(a_i)_{i=0,\dots,n}$ in the set there exist integers h and k $(0 \leqslant h < k \leqslant n)$ such that $a_h = a_k$.
- A set X is *bounded in number*, or *bounded*, if there exists some nonzero integer n such that X has at most n elements (this is the definition given page 410).
- A set X is *weakly finite* if for every sequence $(u_n)_{n \in \mathbb{N}}$ in X there exist m and $p > m$ such that $u_m = u_p$.
- A set X is *infinite* if there exists an injective map $\mathbb{N} \to X$.

1.2. Example. An infinite and countable set can be put in bijection with $\mathbb{N}$.

[3] The definition given on page 84 is only for nonempty sets.

Subsets of a set

A subset of a set $(X, =_X, \neq_X)$ is defined by a property $P(x)$ *regarding the elements of* X, i.e. satisfying

$$\forall x, y \in X \ \big(\, (\, x = y \ \wedge \ P(x) \,) \ \implies \ P(y) \, \big).$$

An element of the subset $\{ \, x \in X \mid P(x) \, \}$ is given by a pair (x, p) where x is an element of X and p is a proof that $P(x)$.[4] Two properties concerning the elements of X define the same subset when they are equivalent.

We can also present this as follows, which, although amounting to the same thing, causes a slightly milder headache to the newcomer. A subset of X is given by a pair (Y, φ) where Y is a set and φ is an injective function of Y into X.[5] Two pairs (Y, φ) and (Y', φ') define the same subset of X if we have

$$\forall y \in Y \ \exists y' \in Y' \ \varphi(y) = \varphi'(y') \quad \text{and} \quad \forall y' \in Y' \ \exists y \in Y \ \varphi(y) = \varphi'(y').$$

In constructive mathematics the subsets of a set X are not considered to form a set, but a *class*. This class is clearly not a set (in the sense given earlier). The intuition is the following: the sets are sufficiently well-defined classes so that we can universally or existentially quantify over their elements. For this, it is necessary for the procedure of construction of elements to be clear.

Recall that a subset Y of X is said to be *detachable* when we have a test for "$x \in Y$?" when $x \in X$. The detachable subsets of X form a set that can be identified with $\{0, 1\}^X$.

Constructively, we do not know of any detachable subsets of $\mathbb{R}$, besides $\emptyset$ and $\mathbb{R}$: *there are no holes in the continuum without the logic of the excluded middle.*

Remark. An interesting constructive variant for "a subset Y_1 of X" is obtained by considering a pair (Y_1, Y_2) of subsets of X that satisfy the following two properties

$$\forall x_1 \in Y_1 \ \forall x_2 \in Y_2 \ \ x_1 \neq_X x_2 \quad \text{and} \quad \forall x \in X \ \neg(x \notin Y_1 \ \wedge \ x \notin Y_2).$$

The *complement* is then given by the pair (Y_2, Y_1), which re-establishes a certain symmetry. ∎

The class of subsets of a set

Let $\mathrm{P}(X)$ be the class of subsets of the set X. If we admitted $\mathrm{P}(\{0\})$ as a

[4] For example, a nonnegative real number is *slightly more than* a real number.

[5] For example we can define the real numbers $\geqslant 0$ as those that are given by the Cauchy sequences of non-negative rational numbers.

set, then $\mathrm{P}(X)$ would also be a set and there would be a natural bijection between $\mathrm{P}(X)$ and $\mathcal{F}\big(X,\mathrm{P}(\{0\})\big)=\mathrm{P}(\{0\})^X$.

This shows that all the difficulties with the set of subsets are focused on the class $\mathrm{P}(\{0\})$, i.e. the class of *truth values*. In classical mathematics, we admit that this class is a set with two elements. This is the *Law of Excluded Middle* **LEM**:

$$\mathrm{P}(\{0\})=\{\{0\},\emptyset\}$$

(the class of truth values reduces to the set $\{\mathsf{True},\mathsf{False}\}$) and we obviously no longer have any issues with $\mathrm{P}(X)$.

2. Asserting means proving

In constructive mathematics truth is also the result of a construction. If P is a mathematical assertion, we write " $\vdash P$ " for "we have a proof of P."

The elementary assertions can be tested by simple computations. For example, the comparison of two non-negative integers. When an assertion means an infinity of elementary assertions (e.g. the Goldbach conjecture[6]), constructive mathematics consider it not to be a priori "true or false." A fortiori, the assertions having an even greater logical complexity are not considered (from a constructive point of view) as having a priori the truth value True or False.

This must not be necessarily considered as a philosophical position concerning truth, but it is surely a mathematical position concerning mathematical assertions. Actually, it is necessary to assume this position; in order to be of computational significance, all theorems must be proven constructively.

Downright philosophical digression. This position is also to be distinguished from the position that consists in saying that there certainly are different possible mathematical universes, for instance one in which the continuum hypothesis[7] is true, another in which it is false. This position is naturally perfectly defendable (Cantor, and no doubt Gödel, would have rejected it in the name of a Platonic realism of Ideas), but it is of little interest to constructive mathematics à la Bishop which have as its object of study an abstraction of the concrete universe of finite computations, with the idea that this abstraction must correspond as closely as possible to the reality that it wants to describe. Thus, the continuum hypothesis is in this framework rather considered as empty of meaning, because it is vain to

[6] Every even number $\geqslant 4$ is the sum of two prime numbers.

[7] The continuum hypothesis is, in classical set theory, the assertion that there is no cardinal strictly between that of $\mathbb{N}$ and that of $\mathbb{R}$, in other words, that every infinite subset of $\mathbb{R}$ is equipotent to $\mathbb{N}$ or to $\mathbb{R}$.

want to compare potential infinites according to their size. If we desire to compare them according to their complexity, we quickly realize that there is no hope of defining a true total order relation on this mess. Consequently, the continuum hypothesis today seems to be nothing other than a game of experts in the formal theory of ZF. But each one of us is free to believe Plato, or even Cantor, or Zermelo-Frankel, or yet again Ð why not Ð to believe in the multiplicity of worlds. No one will ever be able to prove the latter wrong. In fact nothing says that the ZF game will not one day prove to be really useful, for instance in understanding certain subtle points of mathematics that have a concrete meaning. ■

3. Connectives and quantifiers

Here we give the "Brouwer-Heyting-Kolmogorov" explanation for the constructive meaning of the usual logical symbols. They are only informal explanations, not definitions.[8]

These are "detailed" explanations, as for the logical connectives and the quantifiers, regarding what we mean by the slogan "asserting means proving." When we write $\vdash P$ we imply that we have a constructive proof of P. We will make this explicit by giving a name, for example p, to this mathematical object that is the proof of P. Then the explanations regard these particular objects p, but all of this remains informal.

Conjunction: $\vdash P \wedge Q$ means: "$\vdash P$ and $\vdash Q$" (as for classical logic). In other terms: a proof of $P \wedge Q$ is a pair (p, q) where p is a proof of P and q a proof of Q.

Disjunction: $\vdash P \vee Q$ means: "$\vdash P$ or $\vdash Q$" (which does not work with classical logic). In other terms: a proof of $P \vee Q$ is a pair (n, r) with $n \in \{0, 1\}$. If $n = 0$, r must be a proof of P, and if $n = 1$, r must be a proof of Q.

Implication: $\vdash P \Rightarrow Q$ has the following meaning:
a proof of $P \Rightarrow Q$ is a construction $p \mapsto q$ that transforms every proof p of P into a proof q of Q.

Negation: $\neg P$ is an abbreviation of $P \Rightarrow 0 =_{\mathbb{N}} 1$.

Universal quantifier: (similar to implication). *A quantification is always a quantification on the objects of a previously defined set.* Let $P(x)$ be a property regarding the objects x of a set X.

[8] For Kolmogorov's point of view, more precisely on "the logic of problems", see [121, Kolmogorov] and [33, Coquand].

Then $\vdash \forall x \in X \;\; P(x)$ has the following meaning: we have a construction $(x, q) \mapsto p(x, q)$ that takes as input any pair (x, q), where x is an object and q is a proof that $x \in X$, and gives as output a proof $p(x, q)$ of the assertion $P(x)$.

For a quantification on $\mathbb{N}$, giving a non-negative integer x (in the standard form) suffices to prove that $x \in \mathbb{N}$: the proof q in the pair (x, q) above can be omitted.

3.1. Example. *Suppose that the properties P and Q depend on a variable $x \in \mathbb{N}$. Then a proof of $\forall x \in \mathbb{N} \; \big(P(x) \vee Q(x)\big)$ is a construction $\mathbb{N} \ni x \mapsto \big(n(x), r(x)\big)$, where $n(x) \in \{0, 1\}$: if $n(x) = 0$, $r(x)$ is a proof of $P(x)$, and if $n(x) = 1$, $r(x)$ is a proof of $Q(x)$.* ■

Existential quantifier: (similar to disjunction) *A quantification is always a quantification on the objects of a previously defined set.* Let $P(x)$ be a property regarding the objects x of a set X. Then $\vdash \exists x \in X \; P(x)$ has the following meaning: a proof of $\exists x \in X \;\; P(x)$ is a triple (x, p, q) where x is an object, p is a proof of $x \in X$, and q a proof of $P(x)$.

3.2. Example. *Let $P(x, y)$ be a property regarding the non-negative integers x and y. Then the assertion*

$$\vdash \forall x \in \mathbb{N} \;\; \exists y \in \mathbb{N} \;\; P(x, y)$$

means: here is a pair (u, p) where u is a construction $u : x \mapsto y = u(x)$ from $\mathbb{N}$ to $\mathbb{N}$ and p is a proof of $\vdash \forall x \in \mathbb{N} \; P\big(x, u(x)\big)$. ■

3.3. Example. (Propositional logics)
The class of truth values in constructive mathematics is a Heyting algebra. NB: By P({0}) being a class and not a set we simply mean that the connectives $\wedge$, $\vee$ and $\to$ and the constants True and False satisfy the axioms of the Heyting algebras.

In particular, let A, B, C be mathematical properties. We have the following equivalences.

$\vdash \;\; \big((A \Rightarrow C) \;\wedge\; (B \Rightarrow C)\big) \;\; \Longleftrightarrow \;\; \big((A \;\vee\; B) \;\Rightarrow\; C\big)$
$\vdash \;\; \big(A \Rightarrow (B \Rightarrow C)\big) \;\; \Longleftrightarrow \;\; \big((A \;\wedge\; B) \;\Rightarrow\; C\big)$
$\vdash \;\; \neg(A \;\vee B\;) \;\; \Longleftrightarrow \;\; (\neg A \wedge \neg B)$
$\vdash \;\; (A \Rightarrow B) \;\; \Longrightarrow \;\; (\neg B \;\Rightarrow\; \neg A)$
$\vdash \;\; \neg\neg\neg A \;\; \Longleftrightarrow \;\; \neg A$

In addition, if we have $\vdash \; A \;\vee \neg A$ and $\vdash \; B \;\vee \neg B$, then we have

$\vdash \;\; \neg\neg A \;\; \Longleftrightarrow \;\; A$
$\vdash \;\; \neg(A \;\wedge B\;) \;\; \Longleftrightarrow \;\; (\neg A \vee \neg B)$
$\vdash \;\; (A \Rightarrow B) \;\; \Longleftrightarrow \;\; (\neg A \vee B)$ ■

Remark. Since $\neg\neg\neg A \Leftrightarrow \neg A$, a property C is equivalent to a property $\neg B$ (for a certain property B not yet specified) if and only if $\neg\neg C \Rightarrow C$. Thus, in constructive mathematics we can define the concept of *negative property.* In classical mathematics, the concept is pointless since every property is negative. In constructive mathematics, care must be taken because True is also a negative property, since $\mathsf{False} \Rightarrow \mathsf{False}$, $\neg\mathsf{False}$ is equal to True. ■

4. Mechanical computations

Here we discuss a point that classical mathematicians often fail to appreciate. A function from $\mathbb{N}$ to $\mathbb{N}$ is given by a construction. The usual constructions correspond to algorithmic programs that can run on an "ideal" computer.[9] This leads to the notion of *mechanical computations.* A function $f \in \mathbb{N}^{\mathbb{N}}$ obtained by such a mechanical computation is called a *recursive function.* The subset $\mathsf{Rec} \subset \mathbb{N}^{\mathbb{N}}$ formed by the recursive functions can then be described more formally as we will now explain.

Recall that a *primitive recursive function* is a function $\mathbb{N}^k \to \mathbb{N}$ that can be defined by composition or by simple recurrence from primitive recursive functions already defined (we start with the constant functions and addition $+$). Let us denote by Prim_2 the set of primitive recursive functions $\mathbb{N}^2 \to \mathbb{N}$. We easily prove that Prim_2 is an enumerable set.

A function $\beta \in \mathsf{Prim}_2$ can be thought of as simulating the execution of a program as follows. For an input n we compute $\beta(n, m)$ for $m = 0, 1, \ldots$ until $\beta(n, m) \neq 0$ (intuitively: until the program reaches the instruction Halt). Then, the function $\alpha \in \mathsf{Rec}$ computed by the "program" $\beta \in \mathsf{Prim}_2$ is: $f : n \mapsto \beta(n, m_n) - 1$ where m_n is the first value of m such that $\beta(n, m) \neq 0$.

Thus, we obtain a surjective map from a subset *Rec* of Prim_2 onto Rec, and Rec can be identified with the preset *Rec* equipped with the suitable equality and distinction. This means that Rec is defined as a "quotient"([10]) of a subset of an enumerable set. The elements of the subset *Rec* of Prim_2 are defined by the following condition:

$$\beta \in \mathit{Rec} \overset{\text{def}}{\iff} (*) \ : \ \forall n \in \mathbb{N} \ \ \exists m \in \mathbb{N} \quad \beta(n, m) \neq 0.$$

From a classical point of view, for any $\beta \in \mathsf{Prim}_2$, the above assertion $(*)$ is true or false in the absolute, in reference to the logic of the excluded middle (or, if you prefer, to the actual infinity of $\mathbb{N}$): the notion of a mechanical computation can thus be defined without any reference to a primitive notion of construction.

[9] A computer having all the space and time necessary for the considered computation.

[10] Since Rec is the image of *Rec* under a surjective map.

However, from a constructive point of view, the assertion $(*)$ must be proven, and such a proof is itself a construction. Thus *the notion of a mechanical computation depends on the notion of construction, which cannot be defined.*

To finish this section, let us note that the Russian constructivism à la Markov admits as a fundamental principle the equality $\mathsf{Rec} = \mathbb{N}^{\mathbb{N}}$, a principle sometimes called the **false Church's thesis**. See [Beeson, Bridges & Richman] and [164, Richman]. The true **Church's thesis** is that no automated system of computation will ever be able to compute other functions than the recursive functions: we will be able to improve the performances of computers, but no automated system of computation will be able to surpass what they know how to compute "in principle" (i.e. if they dispose of the necessary time and space). The true Church's thesis is extremely likely, but obviously it is unlikely to have a proof.

5. Principles of omniscience

A *principle of omniscience* is a principle that, although true in classical mathematics, clearly poses a problem in constructive mathematics, because it a priori assumes knowledge of what happens with a potential infinity. The word omniscience here is therefore valid for "prescience of the potential infinite." The principles of omniscience in general have strong counterexamples in Russian constructive mathematics. They however cannot be disproven in constructive mathematics à la Bishop, because they are compatible with classical mathematics.

The Little Principle of Omniscience

Let $\alpha = (\alpha_n) \in \{0,1\}^{\mathbb{N}}$ be a *binary sequence*, i.e. a construction that gives for each non-negative integer (as input) an element of $\{0,1\}$ (as output). Consider the following assertions

$$\begin{aligned} P(\alpha) &: \alpha_n = 1 \text{ for some } n, \\ \neg P(\alpha) &: \alpha_n = 0 \text{ for all } n, \\ P(\alpha) \vee \neg P(\alpha) &: P(\alpha) \text{ or } \neg P(\alpha), \\ \forall \alpha \ \big(P(\alpha) \vee \neg P(\alpha)\big) &: \text{for every binary sequence } \alpha,\ P(\alpha) \text{ or } \neg P(\alpha). \end{aligned}$$

A constructive proof of $P(\alpha) \vee \neg P(\alpha)$ should provide an algorithm that either shows that $\alpha_n = 0$ for all n, or computes a non-negative integer n such that $\alpha_n = 1$.

Such an algorithm is much too efficient, because it would allow us to automatically solve a great number of important conjectures. In fact we know that if such an algorithm exists, it is certainly not "mechanically computable": a program that runs on a machine can surely not accomplish such a thing even when we impose the limitation on the input α that it be an explicit primitive recursive binary sequence. This impossibility is a grand theorem of computability theory, often indicated under the name "undecidability of the Halting Problem."

Undecidability of the Halting problem (We cannot know everything)
In three immediately equivalent forms:

- *We cannot automatically assure the halting of programs: there exists no program T that can test if an arbitrary program P will eventually reach its Halt instruction.*
- *There exists no program that can test if an arbitrary primitive recursive sequence is identically null.*
- *There exists no program U that takes as input two integers, gives as output a Boolean, and that enumerates all the programmable binary sequences (the sequence $n \mapsto U(m,n)$ is the m^{th} sequence enumerated by U).*

Not only does this theorem, in its last formulation, resemble Cantor's theorem which asserts that we cannot enumerate the set of binary sequences, but the (very simple) proof is essentially the same.

Although the previous theorem does not a priori forbid the existence of an effective but not mechanizable procedure to systematically solve this type of problem, it confirms the intuitive idea according to which new ingenuity will always have to be shown to progress in our knowledge of the mathematical world.

Thus, from a constructive point of view, we reject the *Limited Principle of Omniscience.*

LPO: If (α_n) is a binary sequence, then either there exists some n such that $\alpha_n = 1$, or $\alpha_n = 0$ for every n.

Here it is in a more concentrated form.

LPO: $$\forall \alpha \in \mathbb{N}^{\mathbb{N}},\ \ (\alpha \neq 0\ \vee\ \alpha = 0)$$

We will call an *elementary property* a property equivalent to

$$\exists n\ \alpha(n) \neq 0$$

for a certain $\alpha \in \mathbb{N}^{\mathbb{N}}$.

The principle **LPO** has several equivalent forms. Here are a few of them.

1. If A is an *elementary* property, we have $A \vee \neg A$.
2. Every sequence in $\mathbb{N}$ is either bounded, or unbounded.
3. Every decreasing sequence in $\mathbb{N}$ is constant from a certain rank.

4. From a bounded sequence in $\mathbb{N}$ we can extract a constant infinite subsequence.
5. Every enumerable subset of $\mathbb{N}$ is detachable.
6. Every enumerable subset of $\mathbb{N}$ is either finite, or infinite.
7. For every double sequence of integers $\beta : \mathbb{N}^2 \to \mathbb{N}$ we have
$$\forall n \, \exists m \;\; \beta(n,m) = 0 \quad \vee \quad \exists n \, \forall m \;\; \beta(n,m) \neq 0$$
8. Every detachable subgroup of $\mathbb{Z}$ is generated by a single element.
9. Every subgroup of $\mathbb{Z}^p$ generated by an infinite sequence is finitely generated.
10. $\forall x \in \mathbb{R}$, $(\ x \neq 0 \ \vee \ x = 0\ )$.
11. $\forall x \in \mathbb{R}$, $(\ x > 0 \ \vee \ x = 0 \ \vee \ x < 0\ )$.
12. Every monotone bounded sequence in $\mathbb{R}$ converges.
13. From a bounded sequence in $\mathbb{R}$ we can extract a convergent subsequence.
14. Every real number is either rational or irrational.
15. Every finitely generated vector subspace of $\mathbb{R}^n$ admits a basis.
16. Every separable Hilbert space admits
    – either a finite Hilbert basis
    – or a countable Hilbert basis.

The Lesser Limited Principle of Omniscience

Another, weaker, principle of omniscience **LLPO** (Lesser Limited Principle of Omniscience) is the following.

LLPO: If A and B are two elementary properties, we have
$$\neg(A \ \wedge \ B) \quad \Longrightarrow \quad (\neg A \ \vee \ \neg B)$$

This principle **LLPO** has several equivalent forms.

1. $\forall\, \alpha$, β non-decreasing sequences $\in \mathbb{N}^{\mathbb{N}}$, if $\forall n \, \alpha(n)\beta(n) = 0$, then $\alpha = 0$ or $\beta = 0$.
2. $\forall \alpha, \beta \in \mathbb{N}^{\mathbb{N}}$, if $\forall n, m \in \mathbb{N} \ \alpha(n) \neq \beta(m)$ then $\exists \gamma \in \mathbb{N}^{\mathbb{N}}$ such that
$$\forall n, m \in \mathbb{N} \quad \big(\gamma(\alpha(n)) = 0 \ \wedge \ \gamma(\beta(m)) = 1\big).$$
3. $\forall \alpha \in \mathbb{N}^{\mathbb{N}}$, $\exists k \in \{0, 1\}$, $(\ \exists n \ \alpha(n) = 0 \ \Rightarrow \ \exists m \ \alpha(2m + k) = 0)$.
4. $\forall x \in \mathbb{R} \quad (\ x \leqslant 0 \ \vee \ x \geqslant 0\ )$ (this allows us to make many proofs by dichotomy with the real numbers.)
5. $\forall x, y \in \mathbb{R} \quad (\ xy = 0 \ \Rightarrow \ (\ x = 0 \ \vee \ y = 0\ )\ )$.
6. The image of an interval $[a, b] \subset \mathbb{R}$ under a uniformly continuous real function is an interval $[c, d]$.

7. A uniformly continuous real function over a compact metric space attains its least upper bound and its greatest lower bound.
8. KL_1 (one of the versions of König's lemma) Every explicit, infinite, finitely branching tree has an infinite path.

It is known that if an algorithm exists for the third item it cannot be "mechanically computable" (i.e. recursive): we can construct mechanically computable α and β satisfying the hypothesis, but for which no mechanically computable γ satisfies the conclusion. Similarly, Kleene's singular tree is an infinite countable recursive finitely branching tree that has no infinite recursive path. This gives a "recursive counterexample" for KL_1.

We will now prove the equivalence $\mathsf{KL}_1 \Leftrightarrow \mathsf{LLPO}$. [11]

An explicit infinite finitely branching tree can be defined by a set $A \subset \mathsf{Lst}(\mathbb{N})$ of lists of integers satisfying the following properties (the first four corresponding to the notion of an explicit finitely branching tree).

- The empty list $[\,]$ represents the root of the tree, it belongs to A,
- an $a = [a_1, \dots, a_n] \in A$ represents both a node of the tree and the path that goes from the root to the node,
- if $[a_1, \dots, a_n] \in A$ and $n \geqslant 1$, then $[a_1, \dots, a_{n-1}] \in A$,
- if $a = [a_1, \dots, a_n] \in A$ the x's $\in \mathbb{N}$ such that $[a_1, \dots, a_n, x] \in A$ form a segment $\{\, x \in \mathbb{N} \mid x < \mu(a) \,\}$ where $\mu(a)$ is explicitly given in terms of a: the branches stemming from a are numbered $0, \dots, \mu(a) - 1$.
- For all $n \in \mathbb{N}$ there is at least one $[a_1, \dots, a_n] \in A$ (the tree is explicitly infinite).

Thus the subset A of $\mathsf{Lst}(\mathbb{N})$ is detachable (this is ultimately what the word "explicit" means here), and A is countable.

Proof of $\boldsymbol{\mathsf{KL}_1} \Leftrightarrow \boldsymbol{\mathsf{LLPO}}$.
We use the variant of LLPO given in item 1.
Assume KL_1. Let $\alpha, \beta \in \mathbb{N}^{\mathbb{N}}$ as in item 1. Consider the following tree. The root has two children. They form two distinct paths that grow indefinitely without ever branching out, until $\alpha(n) \neq 0$ or $\beta(n) \neq 0$ (if this ever occurs). If this occurs with $\alpha(n) \neq 0$, we stop the left branch and we continue the one on the right. If it occurs with $\beta(n) = 0$, we do the opposite. Explicitly giving an infinite branch in this tree amounts to certifying in advance that $\alpha = 0$ or $\beta = 0$.

[11] As for all the proofs in this annex, it is informal and we do not specify in which formal framework it could be written. The readers will notice in this proof a use of a construction by induction which actually stems from the Axiom of Dependent Choice, generally considered as non-problematic in constructive mathematics.

Conversely, assume **LLPO**. Consider an explicit infinite finitely branching tree. Suppose without loss of generality that the tree is binary: beyond a node there are at most two branches. We prove by induction that we can select up to depth n a path that reaches a node K_n underneath which the tree is infinite. This is true for $n = 0$ by hypothesis. If this is true for n, there is at least one branch underneath the selected node K_n. If there are two, consider the sequences α_n and $\beta_n \in \mathbb{N}^{\mathbb{N}}$ defined as follows

— $\alpha_n(m) = 0$ if there is at least one branch of length m below K_n going to the right-hand side, otherwise $\alpha_n(m) = 1$

— $\beta_n(m) = 0$ if there is at least a branch of length m below K_n going to the left-hand side, otherwise $\beta_n(m) = 1$.

By induction hypothesis the sequences $(\alpha_n)_{n\in\mathbb{N}}$ and $(\beta_n)_{n\in\mathbb{N}}$ are non-decreasing and their product is null. We apply item 1 of **LLPO**: one of the two sequences is null and this gives us the means to select the path on the right or the left. □

The Law of Excluded Middle

The Law of Excluded Middle (**LEM**) states that $P \vee \neg P$ is true for every proposition P. This extremely strong principle of omniscience implies **LPO**. It implicitly assumes that sets such as $\mathbb{N}$ or $\mathbb{N}^{\mathbb{N}}$ or even significantly more complicated, are *actual infinities*. It also implies that every set X is discrete if we define $x \neq_X y$ as meaning $\neg(x =_X y)$.

6. Problematic principles in constructive mathematics

By a *problematic principle* we mean a principle that, although satisfied in practice if we do constructive mathematics in Bishop's style, is constructive unprovable. In classical mathematics, these principles are known as true or known as false.

For example, in practice, if some $\alpha \in \mathbb{N}^{\mathbb{N}}$ is constructively well-defined, it can be computed by a program.

In other words, in practice, the **false Church's thesis**, which we can write in the form $\boxed{\mathsf{Rec} = \mathbb{N}^{\mathbb{N}}}$, is satisfied in constructive mathematics. But it cannot be proven in the minimalist framework of constructive mathematics à la Bishop, which is compatible with classical mathematics, because the false Church's thesis is a principle that is false in classical mathematics, in virtue of a cardinality argument. However, Russian constructive mathematics takes it as a fundamental axiom.

Here we will (briefly) only examine two problematic principles, both true in classical mathematics.

Markov's Principle

Markov's Principle, **MP**, is the following

$$\forall x \in \mathbb{R} \quad (\neg x = 0 \Rightarrow x \neq 0).$$

Asserting **MP** amounts to saying: for every binary sequence α, if it is impossible for all its terms to be null, then it must have a nonzero term.

Or even: if A is an elementary property then $\neg\neg A \Rightarrow A$.

The Russian constructive school admits **MP**. Actually, for some $\alpha \in \mathbb{N}^{\mathbb{N}}$, it seems impossible to give a constructive proof of $\neg(\alpha = 0)$ without finding some n such that $\alpha(n) \neq 0$. Thus **MP** is valid from a practical point of view in the constructivism à la Bishop. Note that **LPO** clearly implies **MP**.

Principles of uniform continuity

The principle of uniform continuity asserts that every pointwise continuous function over a compact metric space is uniformly continuous. It is equivalent to the same assertion in a special case, which is itself very close to one of the classical forms of König's lemma. It is of particular interest to study the mutual relations between the following problematic principles, especially as they frequently appear in classical analysis.

UC$^+$ Every pointwise continuous function $f : X \to Y$, with X a compact metric space and Y a metric space, is uniformly continuous.

UC Every pointwise continuous function $f : \{0,1\}^{\mathbb{N}} \to \mathbb{N}$ is uniformly continuous.

Min Every uniformly continuous real function > 0 over a compact metric space is bounded below by a real > 0.

Min$^-$ Every uniformly continuous real function > 0 over a compact interval $[a, b]$ is bounded below by a real > 0.

Min$^+$ Every continuous real function > 0 over a compact metric space is bounded below by a real > 0.

FAN An explicit binary tree A that has no infinite path (i.e. $\forall \alpha \in \{0,1\}^{\mathbb{N}}\ \exists m \in \mathbb{N}\ \alpha|^m \notin A$) is finite.

In the formulation of **FAN**, we see that this principle is seemingly related to **LLPO** (see the last equivalent form **KL**$_1$ cited on page 972). Actually, we can show that it is a consequence of **LPO**. But this is not a principle of omniscience. Besides, it does not imply **LLPO**. In constructive mathematics, **LLPO** is obviously false in practice, whereas **FAN** is satisfied in practice, because each time that we know how to constructively prove that a finitely branching tree has no infinite path, we also know how to prove that it is finite.

Exercises and problems

Exercise 1. Give proofs for examples 1.1, 1.2, 3.1, 3.2 and 3.3.

Exercise 2. Explain why the notions of a finite set, a finitely enumerable set, a bounded set, a weakly finite set, and an enumerable bounded set cannot be identified in constructive mathematics. Explain why these notions coincide if we admit **LEM**.

Exercise 3. Prove a few of the equivalences mentioned for **LPO**.

Exercise 4. Prove a few of the equivalences mentioned for **LLPO**.

Bibliographic comments

The controversy on the nature and the use of the infinite in mathematics was very strong at the beginning of the 20^{th} century: see for example Hilbert [106, 1926], Poincaré [152, 1909], H. Weyl [198, 1918], [Brouwer, 1951] and [Infinito, 1987]). The debate seems at first to have ended in favor of the point of view represented by classical logic. Actually, since the 60s and especially since the publication of Bishop's book, the two points of view are considerably less contradictory than when they first appeared.
A few interesting references on this theme: [Lorenzen, 1962], [166, Fred Richman, 1990], [Dowek2, 2007] and [140, Per Martin-Löf, 2008].

Constructive logic is often called "intuitionistic logic." It was developed as a formal system by A. Heyting.

The article [135, Lorenzen, 1951] which informally uses the constructive point of view in the study of the formal system Principia Mathematica by Whitehead and Russell and makes the connection with the purely algebraic theory of distributive lattices deserves a thorough study.

There are pleasant presentations of such formal systems in the books [Lorenzen, 1962] and [David, Nour & Raffali, 2001].

The small book [Dowek1, 1995] also gives an interesting informal presentation.

Concerning the discussion on the links between effectiveness and recursiveness, see [39, Coquand], [105, Heyting] and [176, Skolem].

The book [Beeson, 1985] carries out a systematic study of several problematic principles in constructive mathematics. For Kleene's singular tree, see [Beeson, page 68] and [Kleene & Vesley, 1965].

The development and the comparison of formal systems able to serve as frameworks for the constructive mathematics employed in [Bishop] or [MRR] has been a very active research subject for a long time. We make sure to note the preponderant influence of the constructive theory of the types

CTT of Per Martin-Löf, [138, 139] and [Martin-Löf, 1984], and of the theory **CZF** of Peter Aczel and Michael Rathjen ([1, Aczel] and [Aczel & Rathjen]). See also the recent developments in [HoTT, 2014] and Thierry Coquand's webpage: `http://www.cse.chalmers.se/~coquand/`.

Let us also cite the beautiful book [Feferman, 1998] which is inline with the propositions of Hermann Weyl.

For a discussion of the "Fan Theorem", see [34, Coquand].

The systematic study of the comparison (in constructive mathematics) of principles of omniscience (such as **LPO** or **LLPO**), as well as that of problematic principles (such as **MP** or **FAN**), has recently been the subject of a major boom. On this subject, we can refer to [12, 13, 14, Berger&al.] and [110, 111, 112, Ishihara].

Tables of theorems

Dynamic methods

Concrete local-global principles

Closed covering principles

Stability under scalar extension

Theorems

The basic local-global principle and systems of linear equations

The method of undetermined coefficients

Finitely presented modules

Finitely generated projective modules, 1

Strictly finite algebras and Galois algebras

The dynamic method

Flat modules

Local rings, or just about

Finitely generated projective modules, 2

Distributive lattices, lattice-groups

Prüfer and Dedekind rings

Krull dimension

The number of generators of a module

The local-global principle

Dynamic machineries and various local-global principles are indicated pages 977 and 978.

Extended projective modules

Bibliography

[Abdeljaoued & Lombardi] ABDELJAOUED A., LOMBARDI H. *Méthodes Matricielles. Introduction à la Complexité Algébrique.* Springer, (2003). 102

[Aczel & Rathjen] ACZEL P., RATHJEN M. *Notes on Constructive Set Theory,* `http://www1.maths.leeds.ac.uk/~rathjen/book.pdf`. 976

[Adams & Loustaunau] ADAMS W., LOUSTAUNAU P. *An Introduction to Gröbner Bases.* American Mathematical Society, (1994). 35

[Apéry & Jouanolou] APÉRY F., JOUANOLOU J.-P. *Élimination. Le cas d'une variable.* Hermann, (2006). 176

[Atiyah & Macdonald] ATIYAH M.F., MACDONALD I.G. *Introduction to Commutative Algebra.* Addison Wesley, (1969). xxvii

[Basu, Pollack & Roy] BASU S., POLLACK R., ROY M.-F. *Algorithms in real algebraic Geometry.* Springer, (2006). 176, 219

[Bass] BASS H. *Algebraic K-theory.* W. A. Benjamin, Inc., New York-Amsterdam, (1968). 832, 843, 942

[Beeson] BEESON M. *Foundations of Constructive Mathematics.* Springer-Verlag, (1985). 193, 969, 975

[Bhaskara Rao] BHASKARA RAO K. *The Theory of Generalized Inverses over a Commutative Ring.* Taylor & Francis. Londres, (2002). 48, 79

[Bigard, Keimel & Wolfenstein] BIGARD A., KEIMEL K., WOLFENSTEIN S. *Groupes et anneaux réticulés.* Springer LNM 608, (1977). 676

[Birkhoff] BIRKHOFF G. *Lattice theory.* Third edition. American Mathematical Society Colloquium Publications, Vol. XXV American Mathematical Society, Providence, R.I., (1967). 676

[Bishop] BISHOP E. *Foundations of Constructive Analysis.* McGraw Hill, (1967). 193, 411, 960, 975

[Bishop & Bridges] BISHOP E., BRIDGES D. *Constructive Analysis.* Springer-Verlag, (1985). 193, 411, 960, 962

[Bourbaki] BOURBAKI. *Commutative Algebra.* Chapters 1-7. English translation of Algèbre Commutative, Hermann, Paris. Springer-Verlag, Berlin 1989. Chapters 8-9. Reprint from the original. Springer-Verlag, Berlin 2006. Chapter 10. Reprint from the original. . Springer-Verlag, Berlin 2007. xxvii, 616

[Bridges & Richman] BRIDGES D., RICHMAN F. *Varieties of Constructive Mathematics.* London Math. Soc. LNS 97. Cambridge University Press, (1987). 193, 969

[Brouwer] BROUWER L. *Brouwer's Cambridge Lectures on Intuitionism, 1951.* (Van Dalen ed.) Cambridge University Press, (1981). 975

[Burris & Sankappanavar] Burris S., Sankappanavar H. *A Course in Universal Algebra*. Springer, (1981). 243

[Cartan & Eilenberg] Cartan H., Eilenberg S. *Homological algebra.* Princeton University Press, (1956). 743

[COCOA] Kreuzer M., Robbiano L. *Computational commutative algebra.* Springer Verlag, Berlin. Vol. 1 (2000), Vol. 2 (2005) xxvii

[Cohn] Cohn P. *Basic Algebra. Groups, rings and fields.* (2nd edition) Springer Verlag, (2002). 243

[Cox] Cox D. *Galois theory.* Wiley-Interscience, (2004). 443

[Cox, Little & O'Shea] Cox D., Little J, O'Shea D. *Ideals, Varieties, and Algorithms.* (2nd edition) Springer Verlag UTM, (1998). xxvii

[CPMPCS] *Concepts of proof in mathematics, philosophy, and computer science. (Based on the Humboldt-Kolleg, Bern, Switzerland, September 9–13, 2013).* Eds: Probst D., Schuster P. Berlin: De Gruyter, (2016). 994

[CRA] Eds: Fontana M., Kabbaj S.-E., Wiegand S. *Commutative ring theory and applications.* Lecture notes in pure and applied mathematics vol 231. M. Dekker, (2002). 993, 999

[Curry] Curry H. B. *Foundations of mathematical logic.* McGraw-Hill Book Co., Inc., New York, (1963). 676

[David, Nour & Raffali] David R., Nour K., Raffali C. *Introduction à la logique*. Dunod, (2001). 975

[Demeyer & Ingraham] Demeyer F., Ingraham E. *Separable algebras over commutative rings.* Springer Lecture Notes in Mathematics 181, (1971). 383

[Dowek1] Dowek G. *La logique.* Flammarion. Collection Dominos, (1995). 975

[Dowek2] Dowek G. *Les métamorphoses du calcul. Une étonnante histoire de mathématiques.* Le Pommier, (2007). 975

[Edwards89] Edwards H. *Divisor Theory.* Boston, MA: Birkhäuser, (1989). xvi

[Edwards05] Edwards H. *Essays in Constructive Mathematics.* Springer Verlag, (2005). xvi

[Eisenbud] Eisenbud D. *Commutative Algebra with a view toward Algebraic Geometry.* Springer Verlag, (1995). xxvii, 383, 805

[Elkadi & Mourrain] Elkadi M., Mourrain B. *Introduction à la résolution des systèmes polynomiaux.* Collection Mathématiques & Applications, 59, Springer Verlag, Berlin (2007). xxvii

[Feferman] Feferman S. *In the Light of Logic.* Oxford University Press, (1998). 976

[Frege-Gödel] van Heijenoort J. (ed.), *From Frege to Gödel: a source book in mathematical logic.* Harvard University Press, Cambridge, Massachussets (1967). (third printing, 2002). 997

[Freid & Jarden] FREID M. D., JARDEN M. *Field Arithmetic.* Springer-Verlag, (1986). 696

[von zur Gathen & Gerhard] VON ZUR GATHEN J. GERHARD J. *Modern computer algebra.* Cambridge University Press, Cambridge, (2003). xxvii

[Gilmer] GILMER R. *Multiplicative Ideal Theory.* Queens papers in pure and applied Math, vol. 90, (1992). xxvii, 485, 743, 805

[Glaz] GLAZ S., *Commutative Coherent Rings.* Lecture Notes in Math., vol. 1371, Springer Verlag, Berlin-Heidelberg-New York, second edition, (1990). xxvii

[Grätzer] GRÄTZER G. *General Lattice Theory.* Birkhäuser, second edition, (2003). 676

[Gupta & Murthy] GUPTA S., MURTHY M. *Suslin's work on linear groups over polynomial rings and Serre's conjecture.* ISI Lecture Notes 8. The Macmillan Company of India Limited, (1980). 951, 954, 958

[HoTT] *Homotopy Type Theory: Univalent Foundations of Mathematics.* `http://homotopytypetheory.org/` (2014). 976

[Infinito] TORALDO DI FRANCIA G. (ed.), *L'infinito nella scienza.* Istituto della Enciclopedia Italiana, Rome, (1987). 975

[Ireland & Rosen] IRELAND K., ROSEN M. *A classical introduction to modern number theory.* Graduate Texts in Mathematics, vol. 84, Springer-Verlag, Berlin-Heidelberg-New York, (1989). 124

[Ischebeck & Rao] ISCHEBECK F., RAO R. *Ideals and Reality. Projective modules and number of generators of ideals.* Springer Monograph in Mathematics, Berlin-Heidelberg-New York, (2005). 243, 912

[Jaffard] JAFFARD, P. *Théorie de la dimension dans les anneaux de polynômes* Gauthier-Villars, Paris, (1960). 805

[Jensen, Ledet & Yui] JENSEN C., LEDET A., YUI N. *Generic Polynomials, Constructive Aspects of the Inverse Galois Problem.* Cambridge University Press, MSRI Publications 45, (2002). 616

[Johnstone] JOHNSTONE P. *Stone spaces.* Cambridges studies in advanced mathematics 3. Cambridge University Press, (1982). 661, 676, 805

[Kaplansky] KAPLANSKY I. *Commutative rings.* Boston, Allyn and Bacon, (1970). xxvii

[Kleene & Vesley] KLEENE S.C., VESLEY R. *The Foundations of intuitionistic mathematics.* Amsterdam (North-Holland), (1965). 975

[Knight] KNIGHT J. *Commutative Algebra.* London Mathematical Society LNS 5. Cambridge University Press, (1971). 896

[Kunz] KUNZ E. *Introduction to Commutative Algebra and Algebraic Geometry.* Birkhäuser, (1991). xvii, xxvii, 243, 299, 533, 822, 842, 896, 908

[Lafon & Marot] LAFON J.-P., MAROT J. *Algèbre locale.* Hermann, Paris, (2002). xxvii, 511, 533

[Lakatos] LAKATOS I. *Proofs and refutations.* Cambridge: Cambridge University Press. (1976). xxvi

[Lam] LAM T.Y. *Serre's conjecture.* Lecture Notes in Mathematics, Vol. 635. Springer Berlin Heidelberg New York, (1978). 941

[Lam06] LAM T.Y. *Serre's Problem on Projective Modules.* Springer Berlin Heidelberg New York, (2006). xxvii, 243, 894, 912, 916, 918, 922, 936, 941, 958

[Lancaster & Tismenetsky] LANCASTER P., TISMENETSKY M. *The Theory of Matrices, 2/e.* Academic Press, (1985). 48

[Lawvere & Rosebrugh] LAWVERE W., ROSEBRUGH R. *Sets for Mathematics.* Cambridge University Press, (2003). 243

[Lorenzen] LORENZEN P. *Metamathematik.* Mannheim: Bibliographisches Institut, (1962). 975

[Mac Lane] MAC LANE, S. *Categories for the Working Mathematician,* Second edition, Springer, (1998). 243

[Martin-Löf] MARTIN-LÖF P. *Intuitionistic type theory.* Notes by Giovanni Sambin. Studies in Proof Theory. Lecture Notes, 1. Bibliopolis, Naples, (1984). 976

[Matsumura] MATSUMURA H. *Commutative ring theory.* Cambridge studies in advanced mathematics 8. Cambridge University Press, (1989). xxvii, 822

[MITCA] EDS: BREWER J., GLAZ G., HEINZER W., OLBERDING B. *Multiplicative Ideal Theory in Commutative Algebra: A tribute to the work of Robert Gilmer.* Springer, (2006) 992, 996

[MRR] MINES R., RICHMAN F., RUITENBURG W. *A Course in Constructive Algebra.* Universitext. Springer-Verlag, (1988). v, xvi, 31, 35, 79, 193, 202, 208, 242, 251, 264, 382, 387, 398, 420, 442, 476, 501, 533, 676, 680, 857, 960, 962, 975

[Mora] MORA T. *Solving Polynomial Equation Systems I: The Kronecker-Duval Philosophy.* Cambridge University Press, (2003) xxvii

[Northcott] NORTHCOTT D. *Finite free resolutions.* Cambridge tracts in mathematics No 71. Cambridge University Press, (1976). xxvii, 79, 220, 243, 298, 299, 880

[PFCM] CROSILLA L., SCHUSTER P., EDS. *From Sets and Types to Analysis and Topology: Towards Practicable Foundations for Constructive Mathematics.* Oxford University Press, (2005). 994, 998

[Pohst & Zassenhaus] POHST, ZASSENHAUS *Algorithmic algebraic number theory (Encyclopedia of Mathematics and its Applications).* Cambridge University Press, (1989). 443

[Rao & Mitra] RAO C., MITRA S. *Generalized Inverses of Matrices and its Applications.* John Wiley & Sons, (1971). 79

[Raynaud] RAYNAUD M. *Anneaux locaux henséliens.* Springer Lecture Notes in Mathematics 169, (1970). 511, 533

[SINGULAR] GREUEL G.-M., PFISTER G. *A Singular Introduction to Commutative Algebra.* Springer (2002). `http://www.singular.uni-kl.de/` xxvii

[Stacks-Project] STACKS-PROJECT. `http://stacks.math.columbia.edu` xxvii, 242

[TAPAS] COHEN A., CUYPERS H., STERK H. (eds) *Some Tapas of Computer Algebra.* Springer Verlag, (1999). xxvii

[Tignol] TIGNOL J.-P. *Galois' theory of algebraic equations.* World Scientific Publishing Co., Inc., River Edge, NJ, (2001). 443

[Yengui] YENGUI I. *Constructive commutative algebra. Projective modules over polynomial rings and dynamical Gröbner bases.* Springer LNM no. 2138 (2015). xvi, 442

[Zaanen] ZAANEN A. *Introduction to Operator Theory in Riesz Spaces.* Springer Verlag, (1997). 677

Articles

[1] ACZEL P. *Aspects of general topology in constructive set theory.* Ann. Pure Appl. Logic. **137**, (2006), 3–29. 976

[2] AUBRY P., VALIBOUZE A. *Using Galois Ideals for Computing Relative Resolvents.* J. Symbolic Computation. **30**, (2000), 635–651. 443

[3] AUSLANDER M., GOLDMAN O. *The Brauer group of a commutative ring.* Trans. Amer. Math. Soc. **97**, (1960), 367–409. 383

[4] AVIGAD J. *Methodology and metaphysics in the development of Dedekind's theory of ideals.* In: José Ferreirós and Jeremy Gray, editors, The Architecture of Modern Mathematics, Oxford University Press. (2006), 159–186. 680, 743

[5] BANASCHEWSKI B. *Radical ideals and coherent frames.* Comment. Math. Univ. Carolin. **37** (2), (1996), 349–370. 805

[6] BARHOUMI S. *Seminormality and polynomial rings.* Journal of Algebra. **322**, (2009), 1974–1978. 941

[7] BARHOUMI S., LOMBARDI H. *An Algorithm for the Traverso-Swan theorem on seminormal rings.* Journal of Algebra. **320**, (2008), 1531–1542. 907, 941

[8] BARHOUMI S., LOMBARDI H., YENGUI I. *Projective modules over polynomial rings: a constructive approach.* Math. Nachrichten. **282** (2009), 792–799. 942

[9] BASU R., RAO R., KHANNA R. *On Quillen's Local Global Principle.* Contemporary Mathematics, Commutative Algebra and Algebraic Geometry, Volume 390, (2005), 17–30. 941

[10] BASS H. *Torsion free and projective modules.* Trans. Amer. Math. Soc. **102**, (1962), 319–327. 858

[11] Bazzoni S., Glaz S. *Prüfer rings.* in [MITCA], 55–72. 486

[12] Berger J. *Constructive Equivalents of the Uniform Continuity Theorem.* Journal of Universal Computer Science. **11** (12), (2005), 1878–1883. 976

[13] Berger J., Bridges D. *A fan-theoretic equivalent of the antithesis of Specker's theorem.* Proc. Koninklijke Nederlandse Akad. Wetenschappen. Indag. Math. **18** (2), (2007), 195-202. 976

[14] Berger J., Ishihara H. *Brouwer's fan theorem and unique existence in constructive analysis.* Math. Logic Quarterly. **51**, (2005), 360–364. 976

[15] Bernstein D. *Factoring into coprimes in essentially linear time.* Journal of Algorithms. **54**, (2005), 1–30. 680

[16] Bernstein D. *Fast ideal arithmetic via lazy localization.* Cohen, Henri (ed.), Algorithmic number theory. Second international symposium, ANTS-II, Talence, France, May 18-23, 1996. Proceedings. Berlin: Springer. Lect. Notes Comput. Sci. 1122 (1996), 27–34. 680

[17] Bishop, E. *Mathematics as a numerical language.* in Intuitionism and Proof Theory. Eds. Myhill, Kino, and Vesley, North-Holland, Amsterdam, (1970). 962

[18] Boniface J., Schappacher N. *"Sur le concept de nombre en mathématique": cours inédit de Leopold Kronecker à Berlin (1891).* Rev. Histoire Math. **7**, (2001), 206–275. 82

[19] Bosma W., Cannon J., Playoust C. *The Magma algebra system. I. The user language.* J. Symbolic Comput. **24**, (1997), 235–265. 444

[20] Brandl R. *Integer polynomials that are reducible modulo all primes.* Amer. Math. Month. **93** (4), (1986), 286–288. 443

[21] Brenner H. *Lifting chains of prime ideals.* J. Pure Appl. Algebra. **179**, (2003), 1–5. 806

[22] Brewer J., Costa D. *Projective modules over some non-Noetherian polynomial rings.* J. Pure Appl. Algebra. **13** (2), (1978), 157–163. 942

[23] Brewer J., Costa D. *Seminormality and projective modules over polynomial rings.* J. Algebra. **58** (1), (1979), 208–216. 941

[24] Brewer J., Klinger L. *Pole assignability and the invariant factor theorem in Prüfer domains and Dedekind domains.* J. Algebra. **111**, (1987), 536–545. 743

[25] Buchmann J., Lenstra H. *Approximating rings of integers in number fields.* J. Théor. Nombres Bordeaux. **6** (2), (1994), 221–260. 680, 681

[26] Cahen, P.-J., *Construction B, I, D et anneaux localement ou résiduellement de Jaffard. (B, I, D construction and locally or residually Jaffard rings).*, Archiv der Mathematik, **54**, (1990), 125–141. 805

[27] Caniglia L., Cortinas G., Danón S., Heintz J., Krick T., Solernó P. *Algorithmic Aspects of Suslin's Proof of Serre's Conjecture.* Computational Complexity. **3**, (1993), 31–55. 942

[28] Cannon J., Bosma W. *Handbook of Magma functions.* Version 2.14, Oct. 2007, 4400 pages. 444

[29] Cederquist J., Coquand T. *Entailment relations and Distributive Lattices.* Logic Colloquium '98 (Prague), 127–139, Lect. Notes Log., 13. Assoc. Symbol. Logic, Urbana, (2000). 676

[30] Chase S., Harrison D., Rosenberg A. *Galois theory and Galois cohomology of commutative rings.* Mem. Amer. Math. Soc. **52**, (1965), 15–33. 383

[31] Chervov A., Talalaev D. *Hitchin systems on singular curve I.* Theor. Math. Phys. **140**, (2004), 1043–1072. 616

[32] Chervov A., Talalaev D. *Hitchin systems on singular curve II. Glueing subschemes.* Int. J. Geom. Meth. Mod. Phys **4**, (2007), 751–787. 616

[33] Coquand T. *Kolmogorov's contribution to intuitionistic logic.* p. 19–40 in: Kolmogorov's Heritage in Mathematics. Charpentier E., Lesne A., Nikolski N. (Eds.). Sringer, (2007). 966

[34] Coquand T. *About Brouwer's fan theorem.* Revue internationale de philosophie. **230**, (2004), 483–489. 976

[35] Coquand T. *Sur un théorème de Kronecker concernant les variétés algébriques.* C. R. Acad. Sci. Paris, Ser. I **338**, (2004), 291–294. 808

[36] Coquand T. *On seminormality.* Journal of Algebra. **305** (1), (2006), 585–602. 896, 900, 941

[37] Coquand T. *A refinement of Forster's theorem.* Techincal report (2007). 808, 843, 942

[38] Coquand T. *Space of valuations*, Annals of Pure and Applied Logic, **157**, (2009), 97–109. 806

[39] Coquand T. *Recursive functions and constructive mathematics.* p. 159–167 in: Bourdeau M., Dubucs J. (Eds.), Calculability and Constructivity. Historical and Philosophical Aspects. Logic, Epistemology and the Unity of Science, Vol. 34. Springer (2014). 975

[40] Coquand T., Ducos L., Lombardi H., Quitté C. *L'idéal des coefficients du produit de deux polynômes.* Revue des Mathématiques de l'Enseignement Supérieur. **113** (3), (2003), 25–39. 79

[41] Coquand T., Ducos L., Lombardi H., Quitté C. *Constructive Krull Dimension. I: Integral Extensions.* Journal of Algebra and Its Applications. **8**, (2009), 129–138. 805

[42] Coquand T., Lombardi H. *A logical approach to abstract algebra (survey).* Math. Struct. in Comput. Science. **16**, (2006), 885–900. xxviii

[43] Coquand T., Lombardi H. *Hidden constructions in abstract algebra (3) Krull dimension of distributive lattices and commutative rings*, in [CRA], 477–499. 805, 806

[44] Coquand T., Lombardi H. *Constructions cachées en algèbre abstraite (3) Dimension de Krull, Going Up, Going Down.* Technical report (2001) http://hlombardi.free.fr/publis/GoingUpDownFrench.pdf (english version http://hlombardi.free.fr/publis/GoingUpDown.pdf). 805, 806

[45] Coquand T., Lombardi H. *Some remarks on normal rings*, dans [CPMPCS] 141–149. 744

[46] Coquand T., Lombardi H., Neuwirth S. *Lattice-ordered groups generated by an ordered group and regular systems of ideals.* The Rocky Mountain Journal of Mathematics, **49** (2019), 1449–1489. https://arxiv.org/abs/1701.05115 442, 676

[47] Coquand T., Lombardi H., Neuwirth S. *Regular entailment relations*, pp. 103–114 in “Paul Lorenzen – mathematician and logician. Contributions presented at the workshop, Konstanz, Germany, March 8–9, 2018” (2021). https://arxiv.org/abs/1912.09480 442, 676

[48] Coquand T., Lombardi H., Quitté C. *Generating non-Noetherian modules constructively.* Manuscripta mathematica. **115**, (2004), 513–520. 808, 843

[49] Coquand T., Lombardi H., Quitté C. *Dimension de Heitmann des distributive lattices et des anneaux commutatifs.* Publications Mathématiques de Besançon. Théorie des nombres (2006). 51 pages. 805, 808, 813, 843

[50] Coquand T., Lombardi H., Roy M.-F. *An elementary characterization of Krull dimension*, in [PFCM], 239–244. 805

[51] Coquand T., Lombardi H., Schuster P. *A nilregular element property.* Archiv der Mathematik, **85**, (2005), 49–54. 760, 806, 842

[52] Coquand T., Persson H. *Valuations and Dedekind Prague theorem.* J. Pure Appl. Algebra. **155**, (2001), 121–129. 676

[53] Cortiñas G., Haesemayer C., Walker M.E. and Weibel C. *A negative answer to a question of Bass.* Proc. AMS. **139**, (2011), 1187–1200. 911

[54] Coste M., Lombardi H., Roy M.-F. *Dynamical method in algebra: Effective Nullstellensätze.* Annals of Pure and Applied Logic. **111**, (2001), 203–256. 896

[55] Couchot F. *Finitely presented modules over semihereditary rings.* Communications in Algebra, **35** (9), (2007) 2685–2692. 743

[56] Dedekind R. *Über einen arithmetischen Satz von Gauss.* Mitt. dtsch. math. Ges. Prag. (1892), 1–11. 176

[57] Dedekind R. *Über die Begründung der IdealTheorie.* Nachr. K. Ges. Wiss. Göttingen. (1894), 272–277. 680

[58] Della Dora J., Dicrescenzo C., Duval D. *About a new method for computing in algebraic number fields.* In Caviness B.F. (Ed.) EUROCAL ’85. Lecture Notes in Computer Science 204, 289–290. Springer (1985). 397, 426, 896

[59] Díaz-Toca G. *Galois theory, splitting fields and computer algebra.* J. Symbolic Computation. **41** (11), (2006), 1174–1186. 443

[60] Díaz-Toca G., Gonzalez-Vega L., Lombardi H. *Generalizing Cramer's Rule: Solving uniformly linear systems of equations.* SIAM Journal on Matrix Analysis and Applications. **27** (3), (2005), 621–637. 533

[61] Díaz-Toca G., Gonzalez-Vega L., Lombardi H., Quitté C. *Modules projectifs de type fini, applications linéaires croisées et inverses généralisés.* Journal of Algebra. **303** (2), (2006), 450–475. 79, 224, 533, 590

[62] Díaz-Toca G., Lombardi H. *A polynomial bound on the number of comaximal localizations needed in order to make free a projective module.* Linear Algebra and its Application. **435**, (2011), 354–360. 299

[63] Díaz-Toca G., Lombardi H., Quitté C. *L'algèbre de décomposition universelle.* Proceedings du colloque TC2006 (Granada), 169–184. 443

[64] Díaz-Toca G., Lombardi H. *Dynamic Galois Theory.* Journal of Symbolic Computation. **45**, (2010), 1316–1329. 443

[65] Drach J. *Essai sur la théorie générale de l'intégration et sur la classification des transcendantes.* Ann. Sci. Ec. Norm. Sup. **3** (15), (1898), 243–384. 176, 442

[66] Ducos L. *Effectivité en théorie de Galois. Sous-résultants.* Université de Poitiers, Thèse doctorale. Poitiers (1997). 443

[67] Ducos L. *Construction de corps de décomposition grâce aux facteurs de résolvantes. (French) [Construction of splitting fields in favour of resolvent factors].* Communications in Algebra. **28** (2), (2000), 903–924. 443

[68] Ducos L. *Vecteurs unimodulaires et systèmes générateurs.* Journal of Algebra. **297**, (2006), 566–583. 843

[69] Ducos L. *Sur la dimension de Krull des anneaux noethériens.* Journal of Algebra. **322**, (2009), 1104–1128. 842, 896

[70] Ducos L. *Polynômes à valeurs entières: un anneau de Prüfer de dimension 2.* (2011) To appear in Communications in Algebra. 709

[71] Ducos L., Lombardi H., Quitté C., Salou M. *Théorie algorithmique des anneaux arithmétiques, des anneaux de Prüfer et des anneaux de Dedekind.* Journal of Algebra. **281**, (2004), 604–650. 486, 743

[72] Ducos L., Valibouze A., Yengui I. *Computing syzygies over $V[X_1, \ldots, X_k]$, V a valuation domain.* Journal of Algebra **425**, (2015), 133–145. 442

[73] Edwards H. *The genesis of ideal theory.* Arch. Hist. Exact Sci. **23** (4), (1980/81), 321–378. 743

[74] Eisenbud D., Evans E., Jr. *Generating modules efficiently: theorems from algebraic K-theory.* J. Algebra. **27**, (1973), 278–305. 817, 843

[75] Eisenbud D., Evans E., Jr. *Every algebraic set in n-space is the intersection of n hypersurfaces.* Inventiones math. **19**, (1973), 107–112. 842

[76] Ellouz A., Lombardi H., Yengui I. *A constructive comparison of the rings $\mathbf{R}(X)$ and $\mathbf{R}\langle X\rangle$ and application to the Lequain-Simis Induction Theorem.* Journal of Algebra. **320** (2008), 521–533. 932, 942

[77] Español L. *Dimensión en álgebra constructiva.* Doctoral thesis. Universidad de Zaragoza, Zaragoza, 1978. 805, 843

[78] Español L. *Constructive Krull dimension of lattices.* Rev. Acad. Cienc. Zaragoza (2) **37**, (1982), 5–9. 805

[79] Español L. *Le spectre d'un anneau dans l'algèbre constructive et applications à la dimension.* Cahiers de topologie et géométrie différentielle catégorique. **24** (2), (1983), 133–144. 805

[80] Español L. *Dimension of Boolean Valued Lattices and Rings.* Journal of Pure and Applied Algebra. **42**, (1986), 223–236. 805

[81] Español L. *The spectrum lattice of Baer rings and polynomials.* Categorical algebra and its applications. (Louvain-La-Neuve, 1987), 118–124, Lecture Notes in Math., 1348, Springer, Berlin-New York, (1988). 79, 805

[82] Español L. *Finite chain calculus in distributive lattices and elementary Krull dimension.* Contribuciones cientificas en honor de Mirian Andres Gomez. Eds. L. Lamban, A. Romero y J. Rubio, Servicio de Publicaciones, Universidad de La Rioja, Logrono, Spain, (2010). 794, 805

[83] Estes R., Guralnick R. *Module equivalences: local to global when primitive polynomials represent units.* J. of Algebra. **77**, (1982), 138–157. 533

[84] Ferrand D. *Les modules projectifs de type fini sur un anneau de polynômes sur un corps sont libres.* Sém. Bourbaki, exposé **484**, (1975-1976), 202–221. 941

[85] Ferrero M., Paques A. *Galois theory of commutative rings revisited.* Contributions to Algebra and Geometry. **38**, (1997), 399–410. 383

[86] Fitchas N., Galligo A. *Nullstellensatz effectif et Conjecture de Serre (Théorème de Quillen-Suslin) pour le Calcul Formel.* Math. Nachr. **149**, (1990), 231–253. 942

[87] Fontana M., Loper A. *An historical overview of Kronecker function rings, Nagata rings and related star and semistar operations.* in [MITCA], 169–187. 176

[88] Forster O. *Über die Anzahl der Erzeugenden eines Ideals in einem Noetherschen Ring.* Math. Z. **84**, (1964), 80–87. 843

[89] Fuchs L. *Über die Ideale arithmetischer ringe.* Math. Helv. **23**, (1949), 334–341. 485

[90] Carl Friedrich Gauss *Demonstratio nova altera theorematis omnem functionem algebraicam rationalem integram unius variabilis in factores reales primi vel secundi gradus resolvi posse.* Comm. Recentiores (Gottingae). **3** (1816), 107–142. Also in Werke III, 31–56. English translation: `http://www.monad.me.uk/misc/gauss-web.php` on the web page of Paul Taylor. `http://www.monad.me.uk/` 82

[91] Geissler K., Klüners J. *Galois Group Computation for Rational Polynomials.* J. Symbolic Computation. **30**, (2000), 653–674. 443

[92] Gillman L., Henriksen M. *Some remarks about elementary divisor rings.* Trans. Amer. Soc. **82**, (1956) 362–365 227

[93] Gilmer R., Heitmann R. *On Pic R[X] for R seminormal.* J. Pure Appl. Algebra. **16** (1980), 251–257. 941

[94] Gilmer R., Hoffmann, J. *A characterization of Prüfer domains in terms of polynomials.* Pacific J. Math. **60** (1), (1975), 81–85. 743

[95] Glaz S. *Finite conductor properties of* $\mathbf{R}(X)$ *and* $\mathbf{R}\langle X\rangle$. in: Proceeding of conference in honor to J. Huckaba's retirement, Missouri, (1999). Marcel Dekker Lecture Notes. 941

[96] Glaz, S., Vasconcelos W. *Gaussian polynomials.* Marcel Dekker Lecture Notes 186 (1997), 325–337. 79

[97] Goldman O. *Determinants in projective modules.* Nagoya Math. J. **18**, (1961), 27–36. 298

[98] Hallouin E. *Parcours initiatique à travers la théorie des valuations.* Rapport technique. Université de Poitiers, (1996). `http://www.picard.ups-tlse.fr/~hallouin/eh-valuation.ps` 147

[99] Hallouin E. *Calcul de fermeture intégrale en dimension 1 et factorisation intégrale.* Thèse. Université de Poitiers, (1998). `http://www.picard.ups-tlse.fr/~hallouin/eh-these.ps` 743

[100] Heitmann R. *Generating ideals in Prüfer domains.* Pacific J. Math. **62**, (1976), 117–126. 843

[101] Heitmann R. *Generating non-Noetherian modules efficiently.* Michigan Math. **31** 2 (1984), 167–180. xxiv, 808, 812, 813, 842, 843

[102] Heitmann R., Levy L. *1 1/2 and 2 generator ideals in Prüfer domains.* Rocky Mountain J. Math. **5** (3), (1975), 361–673. 743

[103] Hermida J., Sánchez-Giralda T. *Linear Equations over Commutative Rings and Determinantal Ideals.* Journal of Algebra. **99**, (1986), 72–79. 462, 485

[104] Hess F. *Computing Riemann-Roch space in algebraic function fields.* Journal of Symbolic Computation. **33**, (2002), 425–445. 744

[105] Heyting A. *After thirty years.* In: 1962 Logic, Methodology and Philosophy of Science (Proc. 1960 Internat. Congr.) pp. 194–197 Stanford Univ. Press, Stanford, Calif. 975

[106] Hilbert D. *Über das Unendliche.* Math. Annalen **95** (1926), 161–190. English translation in [Frege-Gödel] 367–392. 975

[107] Hochster M. *Prime ideal structure in commutative rings.* Trans. Amer. Math. Soc. **142**, (1969), 43–60. 805

[108] Horrocks G. *Projective modules over an extension of a local ring.* Proc. Lond. Math. Soc. **14**, (1964), 714–718. 941

[109] Hulpke A. *Konstruktion transitiver Permutationsgruppen.* Dissertation, Rheinisch-Westfälische Technische Hochschule, Aachen, Germany. (1996). 443

[110] Ishihara H. *Constructive reverse mathematics: compactness properties.* in [PFCM], 245–267. 976

[111] Ishihara H. *Weak König lemma implies Brouwer's fan theorem: a direct proof.* Notre Dame J. Formal Logic **47**, (2006), 249–252. 976

[112] Ishihara H. *Reverse mathematics in Bishop's constructive mathematics.* Philosophia Scientiae, Cahier Spécial **6**, (2006), 43–59. 976

[113] Jacobsson C., Löfwall C. *Standard Bases for General Coefficient Rings and a New Constructive Proof of Hilbert's Basis Theorem.* J. Symb. Comput. **12**, (1991), 337–372. 79

[114] Johnstone, P. *The art of pointless thinking: a student's guide to the category of locales.* Category theory at work (Bremen, 1990), 85–107, Res. Exp. Math., 18, Heldermann, Berlin, 1991. 676

[115] Joyal A. *Spectral spaces and distibutive lattices.* Notices AMS **18**, (1971), 393. 805

[116] Joyal A. *Le théorème de Chevalley-Tarski.* Cahiers de topologie et géometrie différentielle catégorique. (1975). 805, 843

[117] van der Kallen W. *The K2 of rings with many units.* Ann. Sci. É.N.S. 4th série. **10**, (1977), 473–515. 533

[118] Kaplansky I. *Elementary divisors and modules.* Transactions of the AMS. **66**, (1949), 464–491. 227, 243

[119] Kaplansky I. *Modules over Dedekind Rings and Valuation Rings.* Trans. Amer. Math. Soc. **72**, (1952), 327–340. 743

[120] Klüners J., Malle G. *Explicit Galois realization of transitive groups of degree up to 15.* J. Symbolic Comput. **30** (6), (2000), 675–716. 443

[121] Kolmogorov A. *Zur Deutung der intuitionistischen Logik.* Math. Zeitschr., **35** (1932) 58–65. 966

[122] Kronecker L. *Zur Theorie der Formen höherer Stufen.* Ber. K. Akad. Wiss. Berlin (1883), 957–960. (Werke 2, 417–424). 92, 176

[123] Kronecker L. *Grundzüge einer arithmetischen Theorie der algebraischen Grössen.* J. reine angew. Math. **92**, (1882) 1–123. Reprinted in *Leopold Kronecker's Werke*, II, 237–387. 808

[124] Landau, S., Miller, G. *Solvability by radicals is in polynomial time.* J. Comput. Syst. Sci. **30**, (1985), 179–208. 443

[125] Lecerf, G. *Fast separable factorization and applications.* Applicable Algebra in Engineering, Communication and Computing, **19** (2) (2008), 135–160. 382

[126] Lequain, Y., Simis, A. *Projective modules over $R[X_1, ..., X_n]$, R a Prüfer domain.* J. Pure Appl. Algebra. **18** (2), (1980), 165–171. 570, 933

[127] Lombardi H. *Le contenu constructif d'un principe local-global avec une application à la structure d'un module projectif de type fini.* Publications Mathématiques de Besançon. Théorie des nombres. Fascicule (1997), 94–95 & 95–96. 896

[128] Lombardi H. *Platitude, localisation et anneaux de Prüfer: une approche constructive.* 64 pages. Publications Mathématiques de Besançon. Théorie des nombres. Années 1998-2001. 486, 743

[129] Lombardi H. *Dimension de Krull, Nullstellensätze et Évaluation dynamique.* Math. Zeitschrift, **242**, (2002), 23–46. 805, 806

[130] Lombardi H. *Un anneau de Prüfer.* Third International Meeting on Integer-Valued Polynomials. Actes des rencontres du CIRM, **2** (2010). `http://acirm.cedram.org/cgi-bin/browse` 709

[131] Lombardi H., Quitté C. *Constructions cachées en algèbre abstraite (2) Le principe local global.* in [CRA] 461–476. 942

[132] Lombardi H., Quitté C. *Seminormal rings (following Thierry Coquand).* Theoretical Computer Science. **392**, (2008), 113–127. 941

[133] Lombardi H., Quitté C., Yengui I. *Hidden constructions in abstract algebra (6) The theorem of Maroscia, Brewer and Costa.* Journal of Pure and Applied Algebra. **212** 7 (2008), 1575–1582. 942

[134] Lombardi H., Yengui I. *Suslin's algorithms for reduction of unimodular rows.* Journal of Symbolic Computation. **39**, (2005), 707–717. 942

[135] Lorenzen, P. *Algebraische und logistische Untersuchungen über freie Verbände.* Journal of Symbolic Logic **16** (1951), 81–106. `http://www.jstor.org/stable/2266681`. Translation by Stefan Neuwirth: *Algebraic and logistic investigations on free lattices*, `http://arxiv.org/abs/1710.08138`. 676, 975

[136] Lorenzen, P. *Die Erweiterung halbgeordneter Gruppen zu Verbandsgruppen.* Math. Z. **58** (1953), 15–24. `http://eudml.org/doc/169331`. 442, 676

[137] Maroscia P. *Modules projectifs sur certains anneaux de polynômes.* C.R.A.S. Paris **285** série A (1977), 183–185. 942

[138] Per Martin-Löf. *An intuitionistic theory of types: Predicative part.* In H. E. Rose and J. C. Shepherdson, editors, Logic Colloquium'73, pages 73–118. North Holland, (1975). 976

[139] Martin-Löf P. *An intuitionistic theory of types*, 127–172, in: Twenty-five years of constructive type theory (Venice, 1995), Oxford Logic Guides, 36, Oxford Univ. Press, New York, 1998. 976

[140] Per Martin-Löf *The Hilbert-Brouwer controversy resolved?* in: One hundred years of intuitionism (1907-2007), (Cerisy), (Mark Van Atten & al., editors) Publications des Archives Henri Poincaré, Birkhäuser Basel, (2008), pp. 243–256. 975

[141] Mertens F. *Über einen algebraischen Satz.* Ber. K. Akad. Wiss. Wien (1892). 176

[142] Mnif A., Yengui I. *An algorithm for unimodular completion over Noetherian rings.* J. Algebra. **316**, (2007), 483–498. 942

[143] Mulmuley K. *A fast parallel algorithm to compute the rank of a matrix over an arbitrary field.* Combinatorica, **7**/1, (1987), 101–104. 590

[144] Murthy M. *Generators of a general ideal.* in: A tribute to C. S. Seshadri, (Chennai, 2002). Trends in Math., Birkhäuser, Basel, (2003), 379–384. 843

[145] Murthy M., Pedrini C. *K_0 and K_1 of polynomial rings.* in Algebraic K-Theory II, Lecture Notes in Math. 342, (1973), 109–121. 913

[146] Nashier B., Nichols W. *Ideals containing monics.* Proc. Amer. Math. Soc. **99**, (1987), 634–636. 912

[147] Nicholson W. *Lifting idempotents and exchange rings.* Trans. Amer. Math. Soc. **229**, (1977), 269–278. 526

[148] Northcott D. *A generalization of a theorem on the content of polynomials.* Proc. Cambridge Philos. Soc. **55**, (1959), 282–288. 79, 176

[149] Orange S., Renault G., Valibouze A. *Calcul efficace de corps de décomposition.* Technial Report LIP6 2003/005. 443

[150] Perdry H. *Strongly Noetherian rings and constructive ideal theory.* J. Symb. Comput. **37**, (2004), 511–535. 79

[151] Perdry H. *Lazy bases: a minimalist constructive theory of Noetherian rings.* Math. Log. Quart. **54**, (2008), 70–82. 79

[152] Poincaré H. *La logique de l'infini*, Revue de Métaphysique et de Morale **17**, 461–482, (1909) Reprint in *Dernières pensées*, Flammarion (1913). 975

[153] Prüfer H. *Untersuchunger uber teilbarkeitseigenschaften in korpen.* Angew. Mat. **168**, (1932), 1–36. 485, 743

[154] Quentel Y. *Sur une caractérisation des anneaux de valuation de hauteur 1.* C. R. Acad. Sci., Paris, Ser. A **265**, (1967), 659–661. 743

[155] Querré J. *Sur le groupe de classes de diviseurs.* C. R. Acad. Sci., Paris. **284**, (1977), 397–399. 941

[156] Quillen D. *Projective modules over polynomial rings.* Invent. Math. **36**, (1976), 167–171. 941

[157] Rao R. *On projective $R_{f_1,\dots,f_t}$-modules.* Amer. J. Math. **107**, (1985), 387–406. 952

[158] Rao R. *An elementary transformation of a special unimodular vector to its top coefficient vector.* Proc. Amer. Math. Soc. **93**, (1985), 21–24. 925, 952

[159] Rao R. *A note on the Serre dimension of polynomial rings.* J. Pure Appl. Algebra **38**, (1985), 87–90. 952

[160] Rao R., Selby J. *Quillen-Suslin theory revisited.* J. Pure Appl. Algebra **211**, (2007), 541–546. 941

[161] Richman F. *Constructive aspects of Noetherian rings.* Proc. Amer. Mat. Soc. **44**, (1974), 436–441. 31, 79

[162] Richman F. *Seidenberg's condition P.* in: Constructive Mathematics. Springer LNM 873 (1981), 1–11. 382

[163] Richman F. *Finite dimensional algebras over discrete fields.* L. E. J. Brouwer centenary symposium, Troelstra and van Dalen eds., North-Holland Pub. Co. (1982), 397–411. 382

[164] Richman F. *Church Thesis without tears.* Journal of Symbolic Logic. **48** (3), (1983), 797–803. 969

[165] Richman F. *Non trivial uses of trivial rings.* Proc. Amer. Math. Soc. **103**, (1988), 1012–1014. 533

[166] Richman F. *Intuitionism as generalization.* Philosophia Mathematica. **5**, (1990), 124–128. 975

[167] Roitman M. *On projective modules over polynomial rings.* Journal of Algebra. **58**, (1979), 51–63. 941

[168] Roitman M. *On stably extended projective modules over polynomial rings.* Proc. Amer. Math. Soc. **97**, (1986), 585–589. 936

[169] Rota Gian Carlo. *The many lives of lattice theory.* Notices Amer. Math. Soc. **44** 11 (1997), 1440–1445. 680

[170] Sander T. *Existence and uniqueness of the real closure of an ordered field without Zorn's Lemma.* J. Pure and Applied Algebra **73**, (1991), 165–180. 442

[171] Seidenberg A. *What is Noetherian ?* Rend. Sem. Mat. e Fis. Milano **44**, (1974), 55–61. 31, 79

[172] Seidenberg A. *On the Lasker-Noether decomposition theorem.* Amer. J. Math **106**, (1984), 611–638. 79

[173] Serre J.-P. *Géométrie algébrique et géométrie analytique.* Ann. Inst. Fourier Grenoble **6**, (1955-1956), 1–42. xxi, 446

[174] Serre J.-P. *Modules projectifs et espaces fibrés à fibre vectorielle.* Séminaire P. Dubreil, Année 1957/1958. 842

[175] Simis A., Vasconcelos W. *Projective modules over $R[X]$, R a valuation ring, are free.* Notices. Amer. Math. Soc. **18** (5), (1971). 942

[176] Skolem T. *A critical remark on foundational research.* Norske Vid. Selsk. Forh., Trondheim **28**, (1955), 100–105. 975

[177] Soicher L., McKay J. *Computing Galois groups over the rationals.* J. Number Theory. **20**, (1985), 273–281. 443

[178] Stauduhar R. *The determination of Galois groups.* Math. Comp. **27**, (1973), 981–996. 443

[179] Steel A. *A New Scheme for Computing with Algebraically Closed Fields.* Lecture Notes In Computer Science **2369**. Proceedings of the 5th International Symposium on Algorithmic Number Theory, (2002), 491–505. 443

[180] Steel A. *Computing with algebraically closed fields.* Journal of Symbolic Computation. **45**, 342–372, (2010). 443

[181] Stone M. H. *Topological representations of distributive lattices and Brouwerian logics.* Cas. Mat. Fys. **67**, (1937), 1–25. 747, 805

[182] Storch U. *Bemerkung zu einem Satz von M. Kneser.* Arch. Math. **23**, (1972), 403–404. 842

[183] Suslin A. *Projective modules over polynomial rings are free. (Russian).* Dokl. Akad. Nauk SSSR. **229** (5), (1976), 1063–1066. 941

[184] Suslin A. *On the structure of the special linear group over polynomial rings. (Russian).* Izv. Akad. Nauk. SSSR Ser. Mat. **41**, (1977), 235–252. English translation: Math. USSR Izvestija. **11** (2), 221–238.

[185] Suslin A. *Stably Free Modules. (Russian).* Mat. Sb. (N.S.) **102**, (1977), 537–550. English translation: Math. USSR Sb. **31**, 479–491. 299

[186] Swan R. *Factorization of Polynomials over Finite Fields.* Pacific Journal of Mathematics. **12** (3), (1962), 1099–1106. 168

[187] Swan R. *The Number of Generators of a Module.* Math. Z. **102**, (1967), 318–322. 843

[188] Swan R. *On Seminormality.* Journal of Algebra. **67**, (1980), 210–229. 900, 941

[189] Swan R. *Algebraic vector bundles on the 2-sphere.* Rocky Mountain Journal of Mathematics, **23** (1993), 1443–1469. 8

[190] Tennenbaum J. B. *A constructive version of Hilbert's basis theorem.* Dissertation, University of California San Diego, (1973). 79

[191] Traverso C. *Seminormality and the Picard group.* Ann. Scuola Norm. Sup. Pisa. **24**, (1970), 585–595. 900, 941

[192] Valibouze A. *Sur le corps des racines d'un polynôme.* Acta Arithmetica. **131** (1), (2008), 1–27. 443

[193] Vaserstein L.N. (with A.A. Suslin) *Serre's problem on projective modules over polynomial rings and algebraic K-theory.* Funk. An. **8**, (1974), 65–66 = Funct. Anal. Appl. **8**, 148–150.

[194] Vaserstein L.N. *Serre's problem on projective modules over polynomial rings after Suslin and Quillen.* (1976), unpublished notes. 922

[195] Vaserstein L.N. (with A.A. Suslin) *Serre's problem on projective modules over polynomial rings and algebraic K-theory.* Izv. Akad. Nauk SSSR Ser. Mat. **40**, (1976), 993–1054 = Math. USSR Izv. **10**, 937–1001.

[196] Vessiot E. *Sur la théorie de Galois et ses diverses généralisations.* Ann. Sci. E.N.S. 3ème série **21**, (1904), 9–85. 442

[197] Van der Waerden. Review Zentralblatt für Math **24**, (1941), 276. 842

[198] Weyl H. *Das Kontinuum, Kritische Untersuchungen über die Grundlagen der Analysis.* Veit, Leipzig (1918). Italian: *Il Continuo. Indagine critiche sui fondamenti dell' Analisi.* translated by A. B. Veit Riccioli, Bibliopolis, Naples (1977). English: *The Continuum. A critical examination of the foundations of Analysis.* translated by S. Polard and T. Bole. Thomas Jefferson Press, University Press of America (1987). French: *Le continu et autres écrits.* Traduits et commentés par Jean Largeault. Librairie Vrin (1994). 975

[199] Yengui I. *An algorithm for the divisors of monic polynomials over a commutative ring.* Math. Nachr. **260**, (2003), 93–99. 895

[200] Yengui I. *Dynamical Gröbner bases.* Journal of Algebra **301**, (2006), 447–458. Corrigendum: [201] 896

[201] Yengui I. Corrigendum to *Dynamical Gröbner bases* [J. Algebra 301 (2) (2006) 447–458] and to *Dynamical Gröbner bases over Dedekind rings* [J. Algebra 324 (1) (2010) 12–24]. Journal of Algebra. **339**, (2011), 370–375. 1003

[202] Yengui I. *Making the use of maximal ideals constructive.* Theoretical Computer Science. **392**, (2008) 174–178. 896

[203] Yengui I. *The Hermite ring conjecture in dimension one.* Journal of Algebra. **320**, (2008), 437–441. 936

[204] Yengui I. *Stably free modules over $R[X]$ of rank $>$ $\dim R$ are free.* Mathematics of Computation. **80**, (2011), 1093–1098. 936

Index of notations

		page

Examples

$\mathrm{Der}_{\mathbb{R}}(\mathbf{B}, M)$	the $\mathbf{B}$-module of the derivations of $\mathbf{B}$ in M	6
$\mathrm{Der}(\mathbf{B})$	the $\mathbf{B}$-module of the derivations of $\mathbf{B}$	6
$\Omega_{\mathbf{B}/\mathbb{R}}$	the $\mathbf{B}$-module of the differentials (of Kähler) of $\mathbf{B}$, see also page 340	7

The basic local-global principle and systems of linear equations

$\pi_{\mathbf{A},\mathfrak{a}}$	the canonical homomorphism $\mathbf{A} \to \mathbf{A}/\mathfrak{a}$	18
$\mathbf{A}^{\times}$	the multiplicative group of invertible elements of $\mathbf{A}$	19
$\mathbf{A}_S$	(or $S^{-1}\mathbf{A}$) the localized ring of $\mathbf{A}$ at S	19
$j_{\mathbf{A},S}$	the canonical homomorphism $\mathbf{A} \to \mathbf{A}_S$	19
S^{sat}	the saturated monoid of the monoid S	20
$\mathbf{A}[1/s]$	(or $\mathbf{A}_s$) the localized ring of $\mathbf{A}$ at $s^{\mathbb{N}}$	20
$(\mathfrak{b} : \mathfrak{a})_{\mathbf{A}}$	the conductor of the ideal $\mathfrak{a}$ into the ideal $\mathfrak{b}$	20
$(P : N)_{\mathbf{A}}$	the conductor of the module N into the module P	20
$\mathrm{Ann}_{\mathbf{A}}(x)$	the annihilator of the element x	20
$\mathrm{Ann}_{\mathbf{A}}(M)$	the annihilator of the module M	20
$(N : \mathfrak{a})_M$	$\{\, x \in M \mid \mathfrak{a}x \subseteq N \,\}$	20
$(N : \mathfrak{a}^{\infty})_M$	$\{\, x \in M \mid \exists n \ \mathfrak{a}^n x \subseteq N \,\}$	20
$\mathrm{Reg}\,\mathbf{A}$	monoid of the regular elements of $\mathbf{A}$	21
$\mathrm{Frac}\,\mathbf{A}$	total ring of fractions of $\mathbf{A}$	21
$\mathbf{A}^{m \times p}$	(or $\mathbb{M}_{m,p}(\mathbf{A})$) matrices with m rows and p columns	22
$\mathbb{M}_n(\mathbf{A})$	$\mathbb{M}_{n,n}(\mathbf{A})$	22
$\mathbb{GL}_n(\mathbf{A})$	group of invertible matrices	22
$\mathbb{SL}_n(\mathbf{A})$	group of matrices with determinant 1	22
$\mathbb{AG}_n(\mathbf{A})$	projection matrices	22
$\mathrm{D}_{\mathbf{A}}(\mathfrak{a})$	(or $\sqrt{\mathfrak{a}}$) nilradical of the ideal $\mathfrak{a}$ of $\mathbf{A}$	24
$\mathbf{A}_{\mathrm{red}}$	$\mathbf{A}/\mathrm{D}_{\mathbf{A}}(0)$: reduced ring associated with $\mathbf{A}$	24
$\mathrm{c}_{\mathbf{A},\underline{X}}(f)$	(or $\mathrm{c}(f)$) ideal of $\mathbf{A}$, content of the polynomial $f \in \mathbf{A}[\underline{X}]$	24
$\mathrm{rk}_{\mathbf{A}}(M)$	rank of a free module, see also the generalizations to the finitely generated projective modules pages 257, 275 and 545	40
$\mathrm{Adj}\ B$	(or $\widetilde{B}$) cotransposed matrix of B	40

The method of undetermined coefficients

Krull dimension

The number of generators of a module

Index