# L'algèbre constructive

T. Coquand, H. Lombardi

Décembre 2012

## Table des matières

**Introduction** 1

**1 Quelques exemples** 2
1.1 Matrices idempotentes . . . 2
1.2 Matrices injectives . . . 3
1.3 Résolutions libres finies . . . 4
1.4 Le théorème de Quillen-Suslin . . . 4
1.5 Le Positivstellensatz de Krivine-Stengle . . . 5

**2 Nouvelles méthodes** 5

**3 Simplifier les démonstrations** 6
3.1 Un lemme de Gauss . . . 6
3.2 Seminormalité . . . 6

**4 Trouver des définitions constructivement acceptables** 7

**5 Améliorer les résultats...** 9
5.1 La théorie des anneaux de Dedekind . . . 9
5.2 La cloture algébrique . . . 10

**6 La question nœthérienne** 11

**Bibliographie** 12

## Introduction

Nous profitons de la parution récente du livre [ACMC] pour faire une présentation générale de l'algèbre constructive.

L'avant-propos du livre commence par une fière citation de Poincaré :

*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.

Le plus étonnant est bien que le contenu de l'ouvrage se conforme de très près à ces préceptes, qui pourraient sembler a priori incompatibles avec la pratique mathématique courante.

Un autre extrait de l'avant-propos résume bien la méthode générale adoptée par les auteurs.

*Dans la mesure où nous voulons un traitement algorithmique de l'algèbre commutative, nous ne pouvons pas utiliser toutes les facilités que donnent l'usage systématique du lemme de Zorn et du principe du tiers exclu en mathématiques classiques. Sans doute, le lecteur comprend bien qu'il est difficile d'implémenter le lemme de Zorn en Calcul Formel. Le refus du principe du tiers exclu doit par contre lui sembler plus dur à avaler. Ce n'est de notre part qu'une constatation pratique. Si dans une démonstration classique, vous trouvez un raisonnement qui conduit à un calcul du type : "si $x$ est inversible, faire ceci, sinon faire cela", il est bien clair que cela ne se traduit directement*

*sous forme d'un algorithme que dans le cas où l'on dispose d'un test d'inversibilité dans l'anneau en question. C'est pour insister sur cette difficulté, que nous devons contourner en permanence, que nous sommes amenés à parler souvent des deux points de vue, classique et constructif, sur un même sujet.*

Le livre [ACMC] fait suite au livre [MRR] de Mines, Richman et Ruitenburg et se situe dans la tradition de l'algèbre explicite à la Kronecker. Avant ce livre, de nombreux articles de Seidenberg (notamment [50]), de Richman et de bien d'autres avaient déjà montré la viabilité de ce point de vue. Le développement du Calcul Formel a également eu une influence décisive sur le changement d'appréciation des mathématiciens à l'égard des mathématiques "explicites".

L'algèbre constructive a pour but premier de donner une version complètement sûre des résultats de l'algèbre "usuelle". En particulier, tous les résultats obtenus en algèbre constructive ont la signification d'algorithmes certifiés qui réalisent les conclusions de chaque théorème lorsque les hypothèses du théorème sont données sous forme explicite.

Voyons ceci de plus près.

La logique des mathématiques constructives est basée sur une utilisation des mots "ou" et "il existe" avec leur sens intuitif explicite. Il s'ensuit que les démonstrations constructives fournissent toujours la conclusion sous forme explicite lorsque les hypothèses sont données sous forme explicite.

En fait une démonstration constructive ne demande pas que l'hypthèse soit fournie selon un algorithme qui serait d'une forme précisée a priori. Ainsi l'hypothèse peut aussi bien être fournie par une boite noire dont on ne connait pas le fonctionnement interne. Ceci n'enlève rien au caractère constructif de la démonstration, car celle-ci fournit la conclusion à partir des hypothèses au moyen de constructions claires, que les hypothèses soient fournies par une boite noire ou par un algorithme. Par exemple une fonction réelle constructivement définie prend en entrée n'importe quel réel donné par une suite de Cauchy de rationnels $(u_n)_{n\in\mathbb{N}}$ satisfaisant la contrainte $\forall n,\ |u_{n+1}-u_n|<2^{-n}$, que cette suite soit ou non calculable par une Machine de Turing.

De la même manière, en algèbre, si dans l'hypothèse d'un théorème il y a "Soit $M$ un module plat", on ne réclame pas de connaître un algorithme précis qui explicite la platitude du module, mais seulement de savoir que la platitude sera certifiée dans chaque cas concret où l'on souhaitera l'utiliser. En terme de programmation, cela signifie en général que de la démonstration constructive on peut extraire un programme dans lequel les hypothèses sont données par ce que l'on appelle des oracles.

Ceci rend l'algèbre constructive souvent plus proche de l'algèbre classique que du Calcul Formel.

La logique des mathématiques classiques est très différente. En mathématiques classiques, toute propriété qui a une signification claire est vraie "ou" fausse, même lorsque l'on n'a aucun moyen de décider explicitement si elle est vraie ou fausse.

D'un point de vue constructif, le "ou" des mathématiques classiques est en fait une version affaiblie du "ou" constructif. Et l'affirmation "$A\vee\neg A$" des mathématiques classiques (le principe du tiers exclu) est interprétée comme signifiant seulement "$\neg(\neg A\wedge\neg\neg A)$" (qui est vraie, mais sans intérêt).

Un même théorème de mathématiques classiques peut avoir plusieurs versions constructives distinctes, car les mathématiques constructives ont des énoncés plus précis, dans lesquels le mot "explicite" peut se manifester sous des formes diverses, souvent imprévisibles lorsque l'on se situe d'un point de vue classique.

Les mathématiques classiques peuvent alors être considérées comme une partie des mathématiques constructives. Cette partie où l'on rajoute dans les hypothèses que l'axiome du choix et le tiers exclu sont supposés réalisés de manière explicite.

En terme de programmation, cela signifierait en particulier que l'on introduit des oracles qui répondent aux questions du style "telle propriété est-elle vraie dans l'univers mathématique considéré ?", chaque fois que l'on désire connaître la réponse (i.e., chaque fois que l'on invoque le principe du tiers exclu). Le "programme de Hilbert" consisterait alors à démontrer par des moyens purement finitistes que si l'on a obtenu un théorème qui est vrai indépendammant des réponses fournies par ce type d'oracles, alors le théorème pourrait aussi être obtenu sans jamais utiliser ces oracles. Formulé ainsi, ce "programme de Hilbert" pourrait sembler extrêmement plausible. Il se heurte cependant au théorème d'incomplétude de Gödel, qui exclut la possibilité d'une démonstration purement finitiste dont il est question, au moins lorsque l'on se situe dans un champ mathématique suffisamment vaste.

Naturellement le mathématicien classique n'a aucune raison d'accepter que les mathématiques classiques soient une petite partie des mathématiques constructives. Il préfère penser que le tiers exclu et l'axiome du choix sont absolument vrais dans l'univers mathématique qu'il considère. Dans ces conditions il identifie autant que faire se peut les mots "explicite" et "récursif" (au sens de la théorie du calcul mécanisable et des machines de Turing). Et du coup, le mathématicien classique considère que les mathématiques constructives sont une partie des mathématiques classiques, cette partie qui ne s'occupe que de certains objets (ceux qui peuvent être mécaniquement construits), et ne s'intéresse qu'à certaines propriétés (celles qui ont un contenu "récursif").

Ce genre de débat ne sera jamais clos, et notre intention n'est nullement de le clore.

Plutôt que tenter de convaincre le lecteur et la lectrice de la *justesse* du point de vue constructif, nous essayons dans le texte qui suit de les convaincre de sa *pertinence*.

Nous parlerons essentiellement d'algèbre commutative. Dans tout cet article, on notera $\mathbf{A}$ un anneau commutatif unitaire, arbitraire sauf précision contraire.

# 1 Quelques exemples

## 1.1 Matrices idempotentes

La théorie des matrices idempotentes sur un anneau commutatif est essentiellement la même chose que la théorie des modules projectifs de type fini, car un module projectif de type fini peut être défini comme un module isomorphe à l'image d'une matrice idempotente.

Le Théorème 1 dans Bourbaki Algèbre Commutative[1] concernant les modules projectifs de type fini affirme que pour un $\mathbf{A}$-module projectif de type fini $P$ il existe des éléments $s_1$, …, $s_n$ de l'anneau tels que $\langle s_1, \ldots, s_n\rangle = \langle 1\rangle$ et sur chaque anneau $\mathbf{A}[1/s_i]$ le module $P$ devient libre de rang fini.

La démonstration utilise force idéaux premiers ou maximaux et ne fournit aucun moyen de trouver les $s_i$ en question. Vous n'en trouverez pas non plus trace dans les exercices. Si vous demandez à un expert des modules projectifs de type fini, en général il ne connait pas la réponse non plus, même s'il publie des articles extrêmement savants sur les modules projectifs de type fini. Pourtant Poincaré nous demande de ramener tout discours sur l'infini (ici le discours utilisant l'infinité des idéaux maximaux le l'anneau, idéaux qui sont eux-mêmes des objets de nature infinie) à un discours sur le fini (ici la matrice idempotente dont le module est isomorphe à l'image).

Cela signale que dans les mathématiques usuellement pratiquées, il y a quelque chose qui cloche. Qu'un résultat de nature si simple n'intéresse pas les experts est vraiment étrange. Certainement ils n'ont jamais lu Poincaré.

Si $F \in \mathbb{M}_n(\mathbf{A})$ est une matrice idempotente dont l'image est isomorphe à $P$, le théorème de Bourbaki signifie que la matrice $F$ devient semblable sur chaque anneau $\mathbf{A}_{s_i} = \mathbf{A}[1/s_i]$ à une matrice de projection canonique de rang $r_i$ pour un entier $r_i$. NB : la matrice de projection de rang $k$ est la matrice

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

Où sont donc cachés les éléments $s_i$ et les entiers $r_i$ dans la matrice $F$ ?

Voici une réponse qui utilise une astuce un peu magique[2]. Il s'agit de trouver une base du $\mathbf{A}_{s_i}$-module libre $\mathbf{A}_{s_i}^n$ dont certains éléments soient dans l'image de la matrice $F$, et d'autres soient dans son noyau, qui est aussi l'image de $G = \mathrm{I}_n - F$. Vous partez donc de la merveilleuse identité $\mathrm{I}_n = F + G$ et vous développez le déterminant du second membre en utilisant le fait que le déterminant est une fonction multilinéaire des colonnes de la matrice sur laquelle il opère. Vous obtenez ainsi une égalité

$$1 = \sum_{J\subseteq\{1,\ldots,n\}} \det(F_J),$$

1. Section II-5.2, page 138 de l'édition Springer des chapitres I à IV.
2. Des démarches constructives plus conceptuelles, et plus proches de la démonstration abstraite de Bourbaki, sont exposées dans [ACMC, Chapitres V, X et XV]

la somme est indexée par les $2^n$ parties $J$ de $\{1,\dots,n\}$ et la matrice $F_J$ est celle qui a pour colonne $j$ la colonne $j$ de $F$ si $j \in J$ et la colonne $j$ de $G = \mathrm{I}_n - F$ si $j \notin J$. Quand vous inversez $\det(F_J)$, notons $s_J$ cet élément, les colonnes de la matrice $F_J$ forment une base de $\mathbf{A}_{s_J}^n$ et donc la matrice $F$ devient semblable à $\mathrm{I}_{r_J,n}$ avec $r_J = \#J$. En effet, pour une colonne $C_j$ de $F_J$ avec $j \in J$ on a $FC_j = C_j$, et pour une colonne $C_j$ avec $j \notin J$ on a $FC_j = 0$.
Conjecture : dans la situation générique, on ne peut pas descendre en dessous de $2^n$ éléments $s_i$ pour les localisations (voir cependant [23]).

## 1.2 Matrices injectives

Une matrice $F \in \mathbb{M}_{m,n}(\mathbf{A})$ représente une application linéaire de $\mathbf{A}^m$ dans $\mathbf{A}^n$.

Un critère d'injectivité non évident est que la matrice $F$ est injective si, et seulement si, sont idéal déterminantiel d'ordre $n$, noté $\mathcal{D}_{\mathbf{A},n}(F)$ ou $\mathcal{D}_n(F)$ (c'est l'idéal engendré par les mineurs d'ordre $n$), est fidèle.

L'implication difficile est : $(*)$ "$F$ injective $\Rightarrow \mathcal{D}_n(F)$ fidèle."

Voici une démonstration typique de cette implication en mathématiques classiques lorsque l'anneau est réduit. On raisonne par l'absurde, on suppose $F$ injective et l'on considère un $x \neq 0$ tel que $x\mathcal{D}_m(F) = 0$. Puisque $x$ est non nul, il existe[3] un idéal premier minimal $\mathfrak{p}$ tel que $x \notin \mathfrak{p}$. L'anneau $\mathbf{A}_\mathfrak{p}$ localisé en $\mathfrak{p}$ est local, zéro-dimensionnel (car $\mathfrak{p}$ est minimal), et réduit, donc c'est un corps. Et la matrice reste injective, donc elle est de rang $m$. Donc un de ses mineurs d'ordre $m$, notons le $\mu$, est inversible dans $\mathbf{A}_\mathfrak{p}$, i.e., $\mu \in \mathbf{A} \setminus \mathfrak{p}$. Mais $x\mu = 0$, donc $x \in \mathfrak{p}$, contradiction.

Sans utiliser la machinerie locale-globale de décryptage des démonstrations à idéaux premiers minimaux ([ACMC, Section XV-7]), qui fonctionnerait ici, voici une démonstration constructive qui utilise des localisations de nature élémentaire, obtenues en inversant certains éléments de l'anneau fournis par la matrice elle-même, et n'a pas besoin de supposer l'anneau réduit. On a besoin de la notion d'éléments "coréguliers" dans un anneau.

Des éléments $s_1$, …, $s_n$ sont dit coréguliers si l'idéal $\langle s_1,\dots,s_n\rangle$ est fidèle, autrement dit si l'implication suivante est satisfaite, pour tout $x \in \mathbf{A}$ : "si les $xs_i$ sont tous nuls, alors $x$ est nul".

On vérifie facilement qu'un idéal de type fini est nul, ou fidèle, si, et seulement si, il est nul (ou fidèle) après localisation en des éléments coréguliers. De même un élément est nul (ou régulier) si, et seulement si, il est nul (ou régulier) après localisation en des éléments coréguliers.

On démontre alors l'implication $(*)$ par récurrence sur le nombre de colonnes $n$ comme suit.
Pour $n = 1$ il n'y a rien à faire. Voyons le passage de $n-1$ à $n$.
Puisque $F$ est injective, les coefficients de la première colonne sont des éléments coréguliers. Il nous suffit de démontrer que l'idéal $\mathcal{D}_m(F)$ est fdèle après avoir inversé séparément chacun de ces éléments. Lorsque l'on inverse l'un de ces éléments, notons le $a$, la matrice devient équivalente (sur l'anneau $\mathbf{A}_a$) à une matrice du type $\begin{array}{|c|c|}\hline 1 & 0 \\ \hline 0 & G \\ \hline \end{array}$.
En outre $G$ est injective donc par hypothèse de récurrence l'idéal $\mathcal{D}_{n-1}(G)$ est fidèle sur $\mathbf{A}_a$. Enfin $\mathcal{D}_{\mathbf{A}_a,n-1}(G) = \mathcal{D}_{\mathbf{A}_a,n}(F)$.

Si l'on met cette démonstration à plat (i.e. si l'on déroule la récurrence) on voit que les éléments qui interviennent dans les localisations sont des produits de mineurs de la matrice. C'est cela qui se cachait derrière les (complémentaires des) idéaux premiers minimaux de la démonstration classique.

## 1.3 Résolutions libres finies

La théorie des résolutions libres finies est une théorie qui étudie les suites exactes de matrices :

$$L_\bullet : \qquad 0 \to L_m \xrightarrow{A_m} L_{m-1} \xrightarrow{A_{m-1}} \cdots\cdots \xrightarrow{A_2} L_1 \xrightarrow{A_1} L_0, \quad L_k = \mathbf{A}^{p_k}.$$

Ici, $A_k$ est une matrice $\in \mathbb{M}_{p_{k-1},p_k}(\mathbf{A})$. On a $\mathrm{Im}(A_k) = \ker(A_{k-1})$ pour $k = m, \dots, 1$.
On est intéressé par les propriétés des matrices $A_k$ ainsi que par la structure du $\mathbf{A}$-module $M = \mathrm{Coker}(A_1) = L_0/\mathrm{Im}(A_1)$ (la suite exacte ci-dessus constitue une résolution libre de ce module).

Un très bon livre de référence sur le sujet est le livre de Northcott [46]. Il reste néanmoins dans cet ouvrage de nombreuses démonstrations très abstraites et non constructives.

3. Par le lemme de Zorn et le principe du tiers exclu.

Comme le sujet en lui-même est basé sur des objets tout à fait concrets, on pouvait s'attendre à ce qu'une version constructive convenable de la théorie puisse être écrite sans trop s'écarter du texte original de Northcott.

Les outils nécessaires (notamment des définitions constructivement acceptables pour les concepts essentiels de la théorie) ont été mis au point et utilisés pour démontrer tous les théorèmes essentiels du livre de Northcott dans l'article [20]. On peut consulter une synthése en http://hlombardi.free.fr/publis/ACMC-FFR. Le tout premier pas consistait en la caractérisation des matrices injectives, que nous avons envisagée dans la section 1.2.

## 1.4 Le théorème de Quillen-Suslin

Ce théorème, parfois appelé "conjecture de Serre" affirme qu'un module projectif de type fini sur un anneau de polynomes à coefficients dans un corps est libre (cf. [33, 48, 56]).

De manière équivalente et plus terre à terre, toute matrice idempotente d'ordre $n$ (sur un tel anneau) est semblable à une matrice de projection canonique $\mathrm{I}_{k,n}$ pour un certain $k$.

La démonstration de Quillen [48] étend le résultat au cas d'un anneau principal.

Plus tard, le résultat a été étendu aux anneaux de Bezout intègres de dimension $\leq 1$ ([8, 45]).

Enfin le résultat a été étendu à tous les anneaux de Bezout intègres (voir [35], qui utilise [53]).

Des algorithmes pour le théorème de Quillen-Suslin sont parus dans la littérature du Calcul Formel pour le cas des corps, voire pour le cas des anneaux principaux ([1, 27, 36, 47]). Ils sont en général basés sur la démonstration de Suslin (voir cependant [34]). Ces algorithmes utilisent des bases de Gröbner et fonctionnent grâce à la nœtherianité.

Il était important de savoir quels calculs explicites se cachent dans la démonstration de Quillen et dans son théorème de recollement (le "Quillen-patching" de la littérature). De même pour certains lemmes magiques de Suslin, ainsi que pour les arguments éthérés qui se trouvent dans les démonstrations pour les théorèmes "sans hypothèse nœthérienne", pour lesquels aucun algorithme n'avait été publié.

La compréhension de la démonstration de Quillen, débouchant sur un algorithme "sans utilisation de la nœthérianité" a été faite pour le cas des corps dans [42]. Ceci a été étendu au cas des anneaux de Bezout intègres dimension $\leq 1$ dans [43], puis au cas de tous les anneaux de Bezout intègres dans [26]. Un exposé synthétique de ces résultats de mathématiques constructives est donné dans [ACMC, Chapitre XVI].

Le décryptage d'un lemme crucial de Suslin a été fait par Yengui dans [59]. Une étude de la possibilité d'utiliser ce lemme dans certains cas particuliers pour obtenir des algorithmes efficaces a été faite dans [44].

## 1.5 Le Positivstellensatz de Krivine-Stengle

Considérons le Positivstellensatz de Krivine-Stengle [32, 54], qui constitue un raffinement du 17ème problème de Hilbert. Ce dernier demandait de montrer qu'un polynôme de $\mathbb{Q}[X_1, \ldots, X_n]$ partout $\geq 0$ dans $\mathbb{R}^n$ est une somme de carrés de fractions rationnelles. Une solution positive fut apportée par Artin. Les démonstrations abstraites originelles ressemblent à des tours de magie, car une identité algébrique d'un certain type est affirmée exister sans que rien apparemment dans la démonstration ne permette de la construire.

La situation est ici bien plus dramatique qu'avec une démonstration non constructive du Nullstellensatz, car dans ce dernier cas, si l'on réussit à trouver des bornes pour la solution en mathématiques classiques, la solution explicite est récupérable par l'algèbre linéaire.

Ainsi, non seulement la démonstration du Positivstellensatz en algèbre constructive fournit des bornes (ce que la démonstration classique ne fournit pas) mais elle fournit un algorithme, le premier sur le marché [37, 19].

S'agit-il d'un algorithme intéressant ? C'est au lecteur de juger. Mais s'il juge l'algorithme sans intérêt car "trop cher", cela veut dire qu'il sépare les mathématiques en deux domaines : les mathématiques purement abstraites d'une part, les purement concrètes d'autre part (celles qui tournent sur machine), et qu'il ne voit "pas d'intérêt" pour le domaine des mathématiques algorithmiques "tout court". Il nous semble bien au contraire qu'un algorithme "cher" est toujours beaucoup mieux que "pas d'algorithme du tout" ou qu'un algorithme "sans bornes explicites".

Signalons aussi l'article [22] qui expose un raffinement remarquable de la solution du 17ème problème de Hilbert. Le résultat a été obtenu séparément, et publié simultanément par des auteurs de différentes sensibilités, (algèbre classique [21], algèbre constructive [29]).

Enfin le Positivstellensatz effectif (pour les corps réels clos) a été adapté aux cas des corps valués algébriquement clos dans [19]. Ici le théorème dans sa forme générale n'était pas connu auparavant.

# 2 Nouvelles méthodes

Concernant les nouvelles méthodes introduites en algèbre constructive ces dernières années et mises en œuvre dans [ACMC] on peut consulter les deux surveys [15, 40].

L'idée générale sous-jacente est que le "programme de Hilbert pour l'algèbre abstraite" est tout à fait réalisable, selon les lignes qui suivent.

Les objets idéaux de l'algèbre abstraite, inaccessibles d'un point de vue constructif, doivent être remplacés par des spécifications incomplètes de ces mêmes objets.

Les démonstrations abstraites concernant les objets idéaux peuvent alors être relues comme des démonstrations concrètes concernant leurs spécifications incomplètes.

Pour le moment, la possibilité de réaliser le programme de Hilbert en algèbre selon ces lignes est un fait purement expérimental, mais qui reçoit régulièrement de nouvelles confirmations.

Cette idée générale se décline de différentes façons selon les contextes.

Par exemple plutôt que considérer le spectre de Zariski d'un anneau, on considère le treillis de ses ouverts quasi-compacts, qui est un objet "concret" car il s'identifie à l'ensemble des radicaux d'idéaux de type fini.

De manière générale, les espaces spectraux peuvent être vus comme les espaces duaux des treillis distributifs[4] (cf. l'article fondateur de Stone [55] et [13, 15, 12], [ACMC, Section XIII-1]). Il se trouve, et nous pensons que ce n'est pas un hasard, que les espaces spectraux "intéressants" (ceux qui permettent d'obtenir de jolis théorèmes concrets) sont les espaces duaux de treillis distributifs concrets assez simples à décrire constructivement. Cependant, en règle générale on n'a pas accès constructivement aux points de ces espaces spectraux : pour "voir les points" il faut le principe du tiers exclu et le lemme de Zorn.

On peut également comprendre en termes d'espaces spectraux l'utilisation constructive de la théorie des modèles comme dans [19] (voir aussi [15, 40]). Ici les treillis distributifs sont les treillis des faits démontrables dans un contexte fixé (dans les théories formelles géométriques du premier ordre) et les points des espaces spectraux duaux sont les modèles de ces théories formelles.

# 3 Simplifier les démonstrations

Un autre but de l'algèbre constructive est de simplifier les démonstrations. C'est la raison pour laquelle la plupart des résultats de l'algèbre de base donnés dans [MRR] sont obtenus de manière plus élégante et sous des hypothèses plus minimales que dans les autres ouvrages de base.

## 3.1 Un lemme de Gauss

Ce lemme de Gauss (d'abord prouvé pour $\mathbb{Z}$) énonce que si $\mathbf{A}$ est un anneau factoriel, alors $\mathbf{A}[X]$ également. La démonstration usuelle utilise la décomposition en facteurs premiers. On trouve dans [MRR] la version généralisée suivante : *si* $\mathbf{A}$ *est un anneau intègre à pgcd, alors l'anneau* $\mathbf{A}[X]$ *est également un anneau à pgcd.* La démonstration est extrêmement simple et élégante. Le livre [MRR] est rempli de démonstrations très simples et élégantes de ce style.

Dans [ACMC] ce lemme (XI-3.14) est vu comme une conséquence du lemme de Dedekind-Mertens, un résultat fondamental qui a disparu des traités usuels d'algèbre.

Concernant la propriété de décomposition en facteurs premiers, le passage de $\mathbf{A}$ à $\mathbf{A}[X]$ est par contre problématique. Le cas le plus simple est celui où $\mathbf{A}$ est un corps, cas particulièrement évident d'anneau factoriel : comme il n'y a pas d'éléments non nuls et non inversibles, il n'y a jamais rien à factoriser ! Par contre dans ce cas ultra simple, la décomposition en facteurs premiers d'un polynôme de $\mathbf{A}[X]$ n'est pas soluble par un algorithme général. Pour obtenir une telle décomposition, on a besoin d'un test d'irréductibilité pour les polynômes qui fournisse un facteur strict en cas de réponse négative.

4. L'espace spectral dual d'un treillis distributif $T$ est l'ensemble des morphismes $\varphi : T \to \{0,1\}$ (où $0 < 1$) avec pour base d'ouverts les $U_a = \{\, \varphi \mid \varphi(a) = 1 \,\}$. En langage moderne, Stone établit en mathématiques classiques que la catégorie des treillis distributifs est antiéquivalente à la catégorie des espaces spectraux.

## 3.2 Seminormalité

Le théorème de Traverso-Swan parle du groupe de Picard d'un anneau commutatif. Les éléments de ce groupe sont les types d'isomorphie des modules projectifs de rang 1. Un tel module est l'image d'une matrice idempotente $F$ "de rang 1" (i.e., une matrice idempotente qui satisfait $\det(\mathrm{I} + XF) = 1 + X$). La loi de groupe est donnée par le produit tensoriel. L'inverse du type d'isomorphie du module $M = \mathrm{Im}(F)$ est donné par le module dual $M^\star$, isomorphe à l'image de la matrice transposée $F^{\mathrm{T}}$.

**Théorème de Traverso-Swan** [58, 57]
*Soit un anneau réduit* $\mathbf{A}$, $m \geq 1$, *et* $\mathbf{A}[\underline{X}] = \mathbf{A}[X_1, \ldots, X_m]$. *Les propriétés suivantes sont équivalentes.*

1. *Le morphisme naturel de* $\mathrm{Pic}(\mathbf{A})$ *dans* $\mathrm{Pic}(\mathbf{A}[\underline{X}])$ *est un isomorphisme.*
2. *Pour toute matrice idempotente* $M = \big(m_{ij}(X)\big)_{1\leq i,j\leq n} \in \mathbb{M}_n(\mathbf{A}[\underline{X}])$ *telle* $M(0) = \mathrm{I}_{1,n}$ *il existe* $f_1, \ldots, f_n, g_1, \ldots, g_n \in \mathbf{A}[\underline{X}]$ *tels que* $m_{ij} = f_i g_j$ *pour tous* $i$, $j$.
3. $\mathbf{A}$ *est seminormal, i.e., chaque fois que* $a$ *et* $b \in \mathbf{A}$ *satisfont* $a^2 = b^3$, *il existe un* $c \in \mathbf{A}$ *tel que* $a = c^3$ *et* $b = c^2$.

Chaque terme de l'équivalence est de nature élémentaire, l'équivalence *1.* $\Leftrightarrow$ *2.* et l'implication *1.* $\Rightarrow$ *3.* sont relativement simples, et de nature constructive immédiate, mais l'implication *3.* $\Rightarrow$ *2.* n'avait pas de démonstration constructive jusqu'à très récemment (cf. [11]).

La démonstration de Traverso traite le cas nœthérien intègre (avec une restriction technique), et peut sans doute être rendue constructive pour un anneau "pleinement Lasker-Noether" au sens de [MRR] (en mathématiques classiques tout anneau noethérien est pleinement Lasker-Noether).

La démonstration de Swan qui ramène le cas général au cas nœthérien intègre est très abstraite, sans algorithme visible pour la concrétiser.

En analysant certaines démonstrations simples du résultat pour des cas particuliers dans la littérature on trouve que le cas où l'anneau est supposé intégralement clos avait presque déjà une démonstration constructive.

À partir d'une démonstration constructive de nature élémentaire élaborée pour le cas intégralement clos, le passage au cas d'un anneau seminormal intègre, ou aussi bien à celui d'un anneau seminormal arbitraire peut se faire grâce à la compréhension de *ce que signifie* (en termes de calcul) l'argument suivant recevable en mathématiques classiques : dans le cas seminormal, aller voir ce qui se passe après localisation en un premier minimal arbitraire.

Ce travail a été réalisé dans l'article [11] et repris en détail dans [ACMC, Section XVI-1]. Cela a même débouché sur des algorithmes relativement simples qui utilisent la théorie des sous-résultants [4, 5].

Voici donc un résultat classique qui n'avait pas d'algorithme et pour lequel la démonstration découverte par les méthodes de l'algèbre constructive, non seulement fournit un algorithme, mais encore est nettement plus simple et plus facile à comprendre que tout ce que l'on trouve dans la littérature non constructive.

De nombreux mathématiciens ont une préférence naturelle pour les démonstrations simples et explicites, et le travail décrit ci-dessus pour le théorème de Traverso-Swan a pu être réalisé pour bien d'autres théorèmes d'algèbre par des mathématiciens qui ne se réclament d'aucune philosophie particulière.

Le fait est que, vu la nature de l'hypothèse et de la conclusion dans le théorème de Traverso-Swan, un mathématicien constructif, parce qu'il ne croit pas que l'axiome du choix et le principe du tiers exclu puissent réaliser des miracles, est a priori "certain" que le défi peut être relevé, et qu'une démonstration constructive pourra être obtenue. La bonne surprise ici est que cette démonstration est assez simple, ce qui n'était absolument pas prévisible.

Le lecteur peut demander : "Que signifie précisément un algorithme qui réalise l'implication *3.* $\Rightarrow$ *2.* ?" C'est la chose suivante : en utilisant les constructions autorisées par le fait que $\mathbf{A}$ est semi-normal, pour n'importe quelle matrice idempotente $M = M(X)$ avec $M(0) = \mathrm{I}_{1,n}$, on sait construire les polynômes $f_i$ et $g_i \in \mathbf{A}[\underline{X}]$.

On obtient même plus généralement la construction suivante. Lorsque $\mathbf{A}$ est réduit, non nécessairement seminormal, on construit un anneau $\mathbf{A}^\bullet$ zéro-dimensionnel réduit contenant $\mathbf{A}$, et l'on calcule

- des éléments $c_1, \ldots, c_r$ de $\mathbf{A}^\bullet$ tels que
  - $c_1^2$ et $c_1^3 \in \mathbf{A}$,

– $c_2^2$ et $c_2^3 \in \mathbf{A}[c_1]$,
– $c_3^2$ et $c_3^3 \in \mathbf{A}[c_1, c_2]$,
– ...,
– $c_r^2$ et $c_r^3 \in \mathbf{A}[c_1, \ldots, c_{r-1}]$,
– et des polynômes $f_i$ et $g_i \in \mathbf{A}[c_1, \ldots, c_r][\underline{X}]$

tels que l'on ait $f_i g_j = m_{ij}$ pour tous $i, j$. Si $\mathbf{A}$ est seminormal, les $c_i$ sont dans $\mathbf{A}$ et l'anneau $\mathbf{A}^\bullet$ n'intervient plus dans la construction.

# 4 Trouver des définitions constructivement acceptables

Un objectif important de l'algèbre constructive est aussi de donner des définitions constructivement acceptables pour certains concepts de l'algèbre classique qui nécessitent apparemment le tiers exclu et le lemme de Zorn.

Une fois de telles définitions mises au point, il est possible d'envisager des algorithmes pour les théorèmes qui utilisent ces définitions.

Un cas typique est la définition de la dimension de Krull, qui intervient comme hypothèse dans des théorèmes importants comme le théorème de Kronecker[5], le stable range de Bass, le splitting off de Serre [52] et le théorème Forster [28].

Une autre dimension présente dans certaines variantes de ces théorèmes est la dimension du spectre maximal.

Voici tout d'abord ce qui concerne la dimension de Krull. L'article [38] propose une définition constructivement acceptable[6], grâce à laquelle est établie une généralisation du Nullstellensatz (un nouveau théorème de mathématiques classiques).

Cette définition est rendue plus intuitive dans l'article [18] (voir aussi [13, 14, 16, 17, 39] et [ACMC, Chapitre XIII]) et se présente comme suit.

Nous notons $\mathrm{D}_{\mathbf{A}}(I) = \sqrt[\mathbf{A}]{I}$ le radical de l'idéal $I$ dans l'anneau $\mathbf{A}$, et $I_x$ l'idéal engendré par $x$ et par les $y$ tels que $xy$ est nilpotent, i.e. $xy \in \mathrm{D}_{\mathbf{A}}(0)$.

Les idéaux $\mathrm{D}_{\mathbf{A}}(I)$ pour les $I$ de type fini forment ce que l'on appelle le treillis de Zariski de l'anneau $\mathbf{A}$. C'est un treillis distributif dont l'espace dual est le fameux spectre de Zariski $\mathrm{Spec}(\mathbf{A})$ (qui hante les mathématiques classiques).

**Théorème pour la dimension de Krull**
*Un anneau commutatif est de dimension de Krull $-1$ si, et seulement si, il est trivial.*
*Soit $\ell$ un entier $\geq 0$ et $\mathbf{A}$ un anneau commutatif. Les propriétés suivantes sont équivalentes.*

1. *La dimension de Krull de $\mathbf{A}$ est $\leq \ell$*
2. *Pour tous $x_0, \ldots, x_\ell \in \mathbf{A}$ il existe $b_0, \ldots, b_\ell \in \mathbf{A}$ tels que*

$$\left.\begin{array}{rcl} \mathrm{D}_{\mathbf{A}}(b_0 x_0) & = & \mathrm{D}_{\mathbf{A}}(0) \\ \mathrm{D}_{\mathbf{A}}(b_1 x_1) & \leq & \mathrm{D}_{\mathbf{A}}(b_0, x_0) \\ \vdots & \vdots & \vdots \\ \mathrm{D}_{\mathbf{A}}(b_\ell x_\ell) & \leq & \mathrm{D}_{\mathbf{A}}(b_{\ell-1}, x_{\ell-1}) \\ \mathrm{D}_{\mathbf{A}}(1) & = & \mathrm{D}_{\mathbf{A}}(b_\ell, x_\ell) \end{array}\right\} \tag{1}$$

3. *Pour tous $x_0, \ldots, x_\ell \in \mathbf{A}$ il existe $a_0, \ldots, a_\ell \in \mathbf{A}$ et $m_0, \ldots, m_\ell \in \mathbb{N}$ tels que*

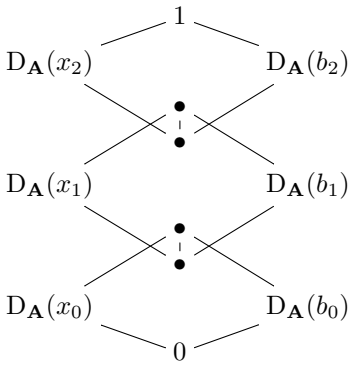
$$x_0^{m_0}(x_1^{m_1} \cdots (x_\ell^{m_\ell}(1 + a_\ell x_\ell) + \cdots + a_1 x_1) + a_0 x_0) = 0$$

4. *Pour tout $x \in \mathbf{A}$ l'anneau quotient $\mathbf{A}/I_x$ est de dimension de Krull $\leq \ell - 1$.*

Par exemple, pour la dimension $\leq 2$, le point *2.* correspond au dessin suivant dans le treillis de

5. Si la dimension de Krull de $\mathbf{A}$ est $< n$ tout idéal de type fini a même radical d'un idéal à $n$ générateurs.
6. Une définition est "constructivement acceptable" si elle est de nature élémentaire, si elle est satisfaite constructivement par les principaux exemples utiles connus, et si elle est équivalente en mathématiques classiques à la définition usuelle.

Zariski de $\mathbf{A}$. Notez que $\mathrm{D}_{\mathbf{A}}(xy) = \mathrm{D}_{\mathbf{A}}(x) \wedge \mathrm{D}_{\mathbf{A}}(y)$ et $\mathrm{D}_{\mathbf{A}}(x,y) = \mathrm{D}_{\mathbf{A}}(x) \vee \mathrm{D}_{\mathbf{A}}(y)$.




L'équivalence *1.* $\Leftrightarrow$ *4.* est assez simple à démontrer en mathématiques classiques.
Les points *2.*, *3.* et *4.* ont une signification constructive claire, sans recours aux idéaux premiers. Enfin l'équivalence des points *2.*, *3.*, *4.* est constructive.

Un tel théorème, qui est aussi intéressant pour les mathématiques classiques, aurait bien sûr pu être obtenu sans préocupations constructives. Mais de telles préocupations ont facilité cette découverte.

En ce qui concerne la dimension du spectre maximal, Heitmann [31] a remarqué que celle-ci intervenait dans la littérature uniquement dans le cas nœthérien. Il a proposé de la remplacer, dans le cas général, par la dimension de l'espace spectral suivant : $\mathrm{Jspec}(\mathbf{A})$ est le plus petit sous-espace spectral de $\mathrm{Spec}(\mathbf{A})$ contenant le spectre maximal, c'est-à-dire encore $\mathrm{Jspec}(\mathbf{A})$ est l'adhérence du spectre maximal, pour la topologie constructible, dans $\mathrm{Spec}(\mathbf{A})$, munie de la topologie induite par $\mathrm{Spec}(\mathbf{A})$. Notons $\mathrm{Jdim}(\mathbf{A})$ la dimension de l'espace spectral défini par Heitmann.

De même que la dimension de Krull est la dimension du treillis distributif formé par les radicaux d'idéaux de type fini, on peut démontrer que la Jdim est la dimension du treillis distributif formé par les radicaux de Jacobson d'idéaux de type fini[7]. Ceci permet de donner une définition constructivement acceptable de la Jdim (cf. [17] et [ACMC, section XIV-2]).

Mieux encore, dans [16] (voir aussi [ACMC, section XIV-2]), une nouvelle dimension, notée $\mathrm{Hdim}(\mathbf{A})$, appelée dimension de Heitmann, est introduite. Elle est "meilleure" que la Jdim : elle est a priori inférieure, et elle se manipule beaucoup mieux dans les démonstrations. Elle est définie par récurrence, en copiant la définition de la dimension de Krull via le point *4.* ci-dessus.

**Définition.** *On définit* $\mathrm{Hdim}(\mathbf{A})$ *par récurrence comme suit.*
- $\mathrm{Hdim}(\mathbf{A}) = -1$ *si et seulement si* $\mathbf{A}$ *est trivial.*
- *Pour* $\ell \geq 0$, $\mathrm{Hdim}(\mathbf{A}) \leq \ell$ *si et seulement si pour tout* $x \in \mathbf{A}$, $\mathrm{Hdim}(\mathbf{A}/J_x) \leq \ell - 1$ *où* $J_x$ *est l'idéal engendré par* $x$ *et par les* $y$ *tels que* $xy \in \mathrm{J}_{\mathbf{A}}(0)$ *(i.e.* $\forall z \in \mathbf{A}$, $1 + xyz$ *est inversible).*

Dans les articles [10, 14, 16, 17, 24] (voir aussi [39] et [ACMC, Chapitre XIV]) ont été démontrés pour la dimension de Krull, avec des variantes pour la dimension de Heitmann, le théorème de Kronecker, le stable range de Bass, le splitting off de Serre, le théorème de Forster-Swan [57] et le théorème de simplification de Bass.

Aucun de ces théorèmes n'avait auparavant une démonstration constructive. Ne serait-ce que parce que l'on ne disposait pas d'une définition constructivement acceptable de la dimension de Krull.

La dimension de Heitmann a été élaborée grâce au point de vue constructif.

Enfin certaines versions laissées ouvertes pour la Jdim par Heitmann dans son article remarquable de 1984 (remarquable parce qu'il se libère de tout hypothèse nœthérienne) sont désormais prouvées pour la Hdim, donc a fortiori pour la Jdim.

En particulier le théorème de Forster-Swan et le splitting off de Serre pour la Jdim (sans hypothèse nœthérienne) ont été démontrés pour la première fois dans [16].

7. En mathématiques classiques, le radical de Jacobson $\mathrm{J}_{\mathbf{A}}(I)$ d'un idéal $I$ est défini comme l'intersection des idéaux maximaux qui contiennent $I$.
Une définition constructivement acceptable est $\mathrm{J}_{\mathbf{A}}(I) := \{x \in \mathbf{A} \mid \forall y \in \mathbf{A},\ 1+xy \in (\mathbf{A}/I)^{\times}\}$. Le radical de Jacobson de $\mathbf{A}$ est l'idéal $\mathrm{J}_{\mathbf{A}}(0)$.

# 5 Améliorer les résultats...

... en ne les faisant dépendre que de leurs hypothèses vraiment nécessaires. C'était par exemple le cas pour le théorème de Forster-Swan et le splitting off de Serre avec la Jdim, sans hypothèse nœthérienne.

## 5.1 La théorie des anneaux de Dedekind

La théorie usuelle des anneaux de Dedekind se concentre sur la décomposition des idéaux en facteurs premiers.

Une forme constructive de cette théorie est développée dans [MRR, Chapitre XIII] et le théorème fondamental de stabilité par extensions entières séparables est obtenu *sous certaines hypothèses constructivement restrictives mais toujours satisfaites en mathématiques classiques*, du style : "on sait décomposer certains polynômes[8] en facteurs premiers".

Cette théorie est intéressante pour deux raisons. D'une part elle nous dit ce qui se cache exactement dans le théorème usuel des mathématiques classiques (des hypothèses de décomposition en facteurs premiers dans les anneaux de polynômes sur certains corps). D'autre part la théorie est directement applicable à la plupart des exemples usuels, par exemple les anneaux d'entiers des corps de nombres.

Cette théorie est cependant "incomplète" au moins de deux points de vue. Tout d'abord l'essence véritable des anneaux de Dedekind devrait être préservée par extensions entières séparables sans aucune hypothèse restrictive du type indiqué. D'autre part, même quand les hypothèses de [MRR] sont satisfaites, il est notoire que la mise en pratique, non seulement de la factorisation complète des idéaux, mais également d'objectifs plus simples et plus raisonnables, se heurte à un obstacle considérable, à savoir la difficulté de construire un système générateur fini pour la structure de $\mathbf{A}$-module d'une extension entière séparable intégralement close $\mathbf{B}$ de $\mathbf{A}$. Pour ce faire, il faut déjà savoir factoriser le discriminant dans $\mathbf{A}$.

Lenstra a souligné ce fait pour la théorie des nombres dans [9] (voir aussi [7]) et a indiqué que l'on pouvait développer des algorithmes qui n'attendent pas d'avoir calculé une $\mathbb{Z}$-base d'un anneau d'entiers avant de commencer à faire certains calculs dans cet anneau (actuellement tous les logiciels de Calcul Formel, même Magma et Pari, jettent l'éponge lorsque le discriminant d'un corps de nombres est un entier qu'ils n'arrivent pas à factoriser). Au contraire, ce sont certains calculs faisables dans l'anneau sans connaître la base d'entiers (par exemple inverser un idéal de type fini) qui peuvent parfois permettre d'obtenir cette base.

Dedekind estimait lui-même que le théorème fondamental concernant les anneaux d'entiers de corps de nombres était le fait que pour tout idéal de type fini $I$ et $a \in I$ on peut en trouver un autre idéal de type fini $J$ tel que $IJ = \langle a \rangle$ (cf. [3]). En termes modernes : la chose la plus importante pour un anneau de Dedekind, c'est d'être un anneau *arithmétique* (un anneau arithmétique intègre est appelé un *domaine de Prüfer*).

Or bien que le théorème selon lequel une extension entière et intégralement close d'un domaine de Prüfer est un domaine de Prüfer soit démontré depuis longtemps, et bien que sa démonstration soit déjà constructive dans les exercices de Bourbaki, on ne le trouve pas dans les livres de base usuels d'algèbre. Les étudiants sont donc amenés à étudier la théorie des anneaux de Dedekind sans jamais apprendre à "inverser un idéal de type fini", ce qui était pourtant la chose essentielle aux yeux de Dedekind. On peut sérieusement se demander combien d'enseignants universitaires sauraient eux-mêmes expliquer ce type d'algorithme, sur lequel se sont concentrés les efforts de Kronecker et Dedekind lorsqu'ils ont élaboré la théorie des nombres.

En outre il n'était pas clair a priori qu'une démonstration constructive soit disponible dans le cas d'un anneau arithmétique non intègre.

Une théorie satisfaisante au regard des objections précédentes a été développée en algèbre constructive dans la thèse de Maimouna Salou à Besançon, un article plus complet est paru dans le Journal of Algebra [25] et cette théorie est exposée dans [ACMC, Chapitre XII].

On obtient notamment sous forme algorithmique les résultats suivants.

- Un anneau intégralement clos cohérent de dimension $\leq 1$ est arithmétique (une version généralisée est également obtenue pour un anneau normal cohérent).
- Le théorème un et demi pour les idéaux inversibles d'un anneau de dimension $\leq 1$.

8. Dans $\mathbf{K}[X]$ ou $\mathbf{K}$ est un corps résiduel arbitraire de l'anneau de départ

- Un théorème de factorisation partielle pour les familles finies d'idéaux de type fini d'un anneau de Dedekind[9]. NB : l'importance des théorèmes de factorisation partielle est soulignée par [6].
- Plusieurs théorèmes de stabilité pour les extensions entières. Le cas des anneaux arithmétiques réduits (éventuellement de dimension $\leq 1$), celui des anneaux arithmétiques réduits cohérents (éventuellement de dimension $\leq 1$), celui des anneaux de Dedekind pour les extensions séparables.
- Tout anneau arithmétique réduit cohérent nœthérien est de dimension $\leq 1$.

À noter : dans le cas arithmétique, "réduit et cohérent" équivaut au fait que tout élément a pour annulateur un idéal engendré par un idempotent. Par ailleurs, "arithmétique, réduit et cohérent" signifie la même chose que "semi-héréditaire", i.e., tout idéal de type fini est un module projectif.

### 5.2 La cloture algébrique

Un traitement constructif de la cloture algébrique d'un corps a été mis au point pour le Calcul Formel par Jean Della Dora, Claire Dicrescenzo et Dominique Duval (le système D5).

Il s'agit là d'une avancée tout à fait remarquable, qui a inauguré la mise en place des nouvelles méthodes en algèbre constructive.

Alors qu'il est connu que l'on ne peut pas construire en toute généralité la cloture algébrique d'un corps, le système D5 réalise "le programme de Hilbert pour la cloture algébrique". Il montre comment on peut remplacer la cloture algébrique usuelle (constructivement inaccessible) par un objet dynamique parfaitement bien défini d'un point de vue constructif, cet objet dynamique permet de comprendre "les calculs qui se cachent dans la cloture algébrique usuelle".

Cette méthode dynamique permet souvent de gérer l'absence de tiers exclu en mathématiques constructives et peut être considérée comme une exploitation rationnelle de l'idée d'évaluation paresseuse en informatique.

La version dynamique et constructive de la théorie de Galois d'un polynôme séparable, valable sur un corps même sans algorithme de factorisation des polynômes, est exposée dans le chapitre VII de [ACMC].

I. Yengui l'applique en Calcul Formel pour certains calculs reliés aux bases de Gröbner (cf. [30, 60]).

## 6 La question nœthérienne

La nœthérianité est omniprésente en algèbre commutative classique. On peut considérer que cette notion n'est pas complètement élucidée du point de vue constructif : plusieurs définitions constructivement acceptables sont possibles pour ce concept, toutes équivelentes en mathématiques classiques mais pas en mathématiques constructives. La définition proposée par Richman [49] et Seidenberg [51] (toute suite croissante d'idéaux de type fini admet deux termes consécutifs égaux) permet en tout cas de rendre compte de nombreux résultats de mathématiques classiques sur le sujet.

#### Théorème de la base de Nœther

Richman et Seidenberg ont donné deux versions constructives du théorème de la base de Nœther : *si* $\mathbf{A}$ *est un anneau nœthérien alors* $\mathbf{A}[X]$ *également.* La version Richman est la suivante. *Si* $\mathbf{A}$ *est nœthérien cohérent et fortement discret, alors il en va de même pour* $\mathbf{A}[X]$ (la version Seidenberg supprime "fortement discret" dans l'hypothèse et dans la conclusion). Notons aussi que la version Richman (ou la version Seidenberg) du théorème implique la version Nœther en mathématiques classiques de manière instantanée.

Ce théorème a été redécouvert par des chercheurs du Calcul Formel et il se trouve par exemple dans le livre [2] de Adams et Loustaunau avec un habillage "bases de Gröbner". Mais naturellement les auteurs ne se rendent pas compte qu'ils redémontrent le théorème de Richman, pour la bonne raison qu'ils n'ont sans doute jamais lu le livre [MRR], ni accordé la moindre attention aux articles de Richman et Seidenberg de 1974. Naturellement, c'est un simple exercice de donner un

9. Une définition constructivement acceptable pour un anneau de Dedekind est "anneau arithmétique réduit cohérent nœthérien fortement discret". Cela inclut les anneaux de Dedekind en mathématiques classiques, mais n'implique pas que l'on sache décomposer tout idéal de type fini fidèle en facteurs premiers.

habillage “base de Gröbner” (donc directement acceptable par la communauté du calcul formel) de la démonstration de Richman[10].

### Décomposition primaire de Lasker-Nœther

Il en va exactement de même pour la décomposition primaire de Lasker-Nœther, qui est explicite depuis Seidenberg (sous certaines hypothèses précises, toujours vérifiées en mathématiques classiques) et qui est exposée de manière limpide dans [MRR], dans la section VIII-8 sur les “fully Lasker Nœther ring”.

### L’algorithme de Buchberger

La terminaison de l’algorithme de Buchberger est usuellement prouvée de façon non constructive, et il n’y a donc pas de bornes qui peuvent être déduites de la démonstration. Le folklore dit que des bornes sur les degrés sont “en double exponentielle” (par rapport aux degrés du départ). Cela semble clair dans le cas des idéaux homogènes, et pour le cas général, il est possible de modifier l’algorithme pour se ramener au cas homogène.

Une démonstration constructive de l’algorithme (cf. [41]) est une adaptation de la méthode de Richman à la situation Buchberger. Puisqu’elle est constructive, cette démonstration fournit ipso facto une borne. Très mauvaise borne, car la démonstration constructive la plus immédiate, comme la démonstration classique, est basée sur le lemme de Dickson, qui est de complexité intrinsèquement “Ackerman”.

Cela présente-t-il un intérêt ? Au moins, cela sert à savoir ce qui se cache exactement dans la démonstration classique usuelle de l’algorithme : des bornes “Ackerman”. Ce que l’on ne savait pas avant d’avoir rendu la démonstration constructive.

## Références


[MRR] Mines R., Richman F., Ruitenburg W. *A Course in Constructive Algebra.* Universitext. Springer-Verlag, (1988). 1, 6, 7, 9, 11

[ACMC] Lombardi H., Quitté C. *Algèbre Commutative, Méthodes Constructives.* Calvage & Mounet, (2011). 1, 3, 4, 5, 6, 7, 8, 9, 10, 11

[1] Almeida M., D’Alfonso L., Solernó P. *On the degrees of bases of free modules over a polynomial ring.* Math. Zeitschrift **231** (1999), 679–706. 4

[2] Adams W., Loustaunau P. *An Introduction to Gröbner Bases,* American Mathematical Society, (1994). 11

[3] Avigad J. *Methodology and metaphysics in the development of Dedekind’s theory of ideals.* Preprint 2005 10

[4] Barhoumi S. *Seminormality and polynomial rings.* Journal of Algebra **322** (2009), 1974–1978. 7

[5] Barhoumi S., Lombardi H. *An algorithm for the Traverso-Swan theorem on seminormal rings.* Journal of Algebra **320** (2008), 1531–1542. 7

[6] Bernstein, D. *Factoring into coprimes in essentially linear time.* Journal of Algorithms **54** (2005), 1-30 10

[7] 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. No 1122, 27–34 (1996). 10

[8] Brewer J., Costa D. *Projective modules over some non-Nœtherian polynomial rings.* J. Pure Appl. Algebra **13** (1978), no. 2, 157–163. 4

[9] Buchmann J., Lenstra H. *Approximating rings of integers in number fields.* J. Théor. Nombres Bordeaux **6** (2) (1994), 221–260. 10


10. Ici les mathématicens constructifs sont un peu dans la situation des russes d’il y a 40 ans, qui avaient souvent “déjà démontré le résultat”, mais comme c’était publié en russe et que cela n’a pas été traduit assez vite, personne en Occident ne le savait. La différence avec les mathématiciens russes, c’est que les mathématiciens constructifs publient en anglais et en français, mais pour autant, on les crédite rarement de leurs résultats lorsqu’ils sont redécouverts en Calcul Formel.

[10] Coquand T. *Sur un théorème de Kronecker concernant les variétés algébriques* C. R. Acad. Sci. Paris, Ser. I **338** (2004), 291–294. 9

[11] Coquand T. *On seminormality.* Journal of Algebra, **305** (1), (2006), 585–602. 6, 7

[12] Coquand T. *Space of valuations*, Annals of Pure and Applied Logic, **157** (2009), 97–109. 6

[13] Coquand T., Lombardi H. *Hidden constructions in abstract algebra (3) Krull dimension of distributive lattices and commutative rings.* dans : Commutative ring theory and applications. Eds : Fontana M., Kabbaj S.-E., Wiegand S. Lecture notes in pure and applied mathematics vol 231. M. Dekker. (2002) 477–499. 6, 8

[14] Coquand T., Lombardi H. *A short proof for the Krull dimension of a polynomial ring.* American Math. Monthly. **112** (9) (2005), 826–829. 8, 9

[15] Coquand T., Lombardi H. *A logical approach to abstract algebra.* (survey) Math. Struct. in Comput. Science **16** (2006), 885–900. 5, 6

[16] Coquand T., Lombardi H., Quitté C. *Generating non nœtherian modules constructively.* Manuscripta mathematica **115**, (2004), 513–520. 8, 9

[17] Coquand T., Lombardi H., Quitté C. *Dimension de Heitmann des treillis distributifs et des anneaux commutatifs.* Publications Mathématiques de Besançon. Algèbre et Théorie des Nombres. (2006), 57–100. 8, 9

[18] Coquand T., Lombardi H., Roy M.-F. *An elementary characterisation of Krull dimension.* Paru dans From Sets and Types to Analysis and Topology : Towards Practicable Foundations for Constructive Mathematics (L. Crosilla, P. Schuster, eds.). Oxford University Press. (2005) 239–244. 8

[19] Coste M., Lombardi H., Roy M.-F. *Dynamical method in algebra : Effective Nullstellensätze.* Annals of Pure and Applied Logic **111**, (2001) 203–256. 5, 6

[20] Coquand T., Quitté C. *Constructive finite free resolutions.* Manuscripta Math., **137**, (2012), 331–345. 4

[21] Delzell C. *Continuous, piecewise-polynomial functions which solve Hilbert's 17th problem.* J. reine angew. Math. **440** (1993), 157–73. 5

[22] Delzell C., González-Vega L, Lombardi H. *A continuous and rational solution to Hilbert's 17th problem and several Positivstellensatz cases*, in : Computational Algebraic Geometry. Eds. Eyssette F., Galligo A.. Birkhäuser (1993) Progress in Math. No 109. (colloque MEGA 92) (1993), 61–76. 5

[23] 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. 3

[24] Ducos L. *Vecteurs unimodulaires et systèmes générateurs.* Journal of Algebra **297**, (2006), 566–583. 9

[25] Ducos L., Lombardi H., Quitté C. et Salou M. *Théorie algorithmique des anneaux arithmétiques, de Prüfer et de Dedekind.* Journal of Algebra. **281**, (2004), 604–650. 10

[26] 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. 5

[27] Fitchas N., Galligo A. *Nullstellensatz effectif et Conjecture de Serre (Théorème de Quillen-Suslin) pour le Calcul Formel.* Math. Nachr. **149**, (1990), 231–253. 4

[28] Forster O. *Über die Anzahl der Erzeugenden eines Ideals in einem Nœtherschen Ring.* Math. Z. **84** (1964), 80–87. 7

[29] González-Vega L., Lombardi H. : *A Real Nullstellensatz and Positivstellensatz for the Semi-polynomials over an Ordered Field.* Journal of Pure and Applied Algebra. **90** (1993), 167–188. 5

[30] Hadj Kacem A., Yengui I., *Dynamical Gröbner bases over Dedekind rings.* J. Algebra **324** (2010), 12-24. 11

[31] Heitmann, R. *Generating non-Nœtherian modules efficiently.* Michigan Math. **31** 2, (1984), 167–180. 8

[32] Krivine J.-L. : *Anneaux préordonnés.* Journal d'Analyse Mathématique **12** (1964), 307–326. 5

[33] Lam T. Y. *Serre's conjecture.* Lecture Notes in Mathematics, Vol. 635. Springer-Verlag, Berlin-New York, 1978. 4

[34] Laubenbacher, R., Woodburn, C. *An algorithm for the Quillen-Suslin theorem for monoid rings. Algorithms for algebra (Eindhoven, 1996).* J. Pure Appl. Algebra **117/118** (1997), 395–429. 4

[35] 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. 4

[36] Logar A., Sturmfels B. *Algorithms for the Quillen-Suslin theorem.* J. Algebra **145** no. 1, (1992), 231–239. 4

[37] Lombardi H. *Effective real nullstellensatz and variants*, in : Effective Methods in Algebraic Geometry. Eds. Mora T., Traverso C. Birkhaüser (1991). Progress in Math. No 94 (MEGA 90), 263–288 5

[38] Lombardi H. *Dimension de Krull, Nullstellensätze et Évaluation dynamique.* Math. Zeitschrift, **242**, (2002), 23–46. 8

[39] Lombardi H. *Dimension de Krull explicite. Application aux théorèmes de Kronecker, Bass, Serre et Forster.* Notes de cours. 2005 8, 9

[40] Lombardi H. *Algèbre dynamique, espaces topologiques sans points et programme de Hilbert.* (survey) Annals of Pure and Applied Logic **137** (2006), 256–290. 5, 6

[41] Lombardi H., Perdry H. *The Buchberger Algorithm as a Tool for Ideal Theory of Polynomials Rings in Constructive Mathematics*, in Gröbner Bases and Applications (Proc. of the Conference 33 Years of Gröbner Bases), Cambridge University Press, London Mathematical Society Lecture Notes Series, No 251, 1998, 393–407. 11

[42] Lombardi H., Quitté C. *Constructions cachées en algèbre abstraite (2) Le principe local-global*, dans : Commutative ring theory and applications. Eds : Fontana M., Kabbaj S.-E., Wiegand S. Lecture notes in pure and applied mathematics vol 131. M. Dekker. (2002) 461–476. 5

[43] 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. 5

[44] Lombardi H., Yengui I. *Suslin's algorithms for reduction of unimodular rows.* J. Symb. Comp. 39 (2005), 707–717. 5

[45] Maroscia P. *Modules projectifs sur certains anneaux de polynomes.* C.R.A.S. Paris **285** série A (1977), 183–185. 4

[46] Northcott D. *Finite free resolutions.* Cambridge tracts in mathematics No 71. Cambridge University Press, (1976). 4

[47] Park, H., Woodburn, C. *An algorithmic proof of Suslin's stability theorem for polynomial rings.* J. Algebra **178** no. 1 (1995), 277–298. 4

[48] Quillen D. *Projective modules over polynomial rings.* Invent. Math. **36** (1976), 167–171. 4

[49] Richman F. *Constructive aspects of Nœtherian rings.* Proc. Amer. Mat. Soc. **44** (1974), 436–441. 11

[50] Seidenberg A. *Constructions in Algebra*, Trans. Amer. Math Soc. **197** (1974), 273–313. 1

[51] Seidenberg A. *What is Nœtherian ?* Rend. Sem. Mat. e Fis. di Milano **44** (1974), 55–61. 11

[52] Serre J.-P. *Modules projectifs et espaces fibrés à fibre vectorielle.* Séminaire P. Dubreil, Année 1957/1958. 7

[53] Simis A., Vasconcelos W. *Projective modules over $R[X]$, R a valuation ring, are free.* Notices. Amer. Math. Soc. **18** (5) 1971. 4

[54] Stengle G., *A Nullstellensatz and a Positivstellensatz in semialgebraic Geometry*, Math. Annalen, **207** (1974), 87–97. 5

[55] Stone M. *Topological representations of distributive lattices and Brouwerian logics.* Cas. Mat. Fys. **67**, (1937), 1–25. 6

[56] Suslin A. *Projective modules over polynomial rings are free. (Russian).* Dokl. Akad. Nauk SSSR **229** no. 5 (1976), 1063–1066. 4

[57] Swan R. *The Number of Generators of a Module.* Math. Z. **102** (1967), 318–322. 6, 9

[58] Traverso C. *Seminormality and the Picard group*. Ann. Scuola Norm. Sup. Pisa, **24** (1970), 585–595. 6

[59] Yengui I., *Making the use of maximal ideals constructive*. Theoretical Computer Science **392** (2008), 174–178. 5

[60] Yengui I., *Dynamical Gröbner bases*. Journal of Algebra **301** (2006), 447–458.
*Corrigendum to Dynamical Gröbner bases [J. Algebra 301 (2) (2006) 447–458] and to Dynamical Gröbner bases over Dedekind rings [J. Algebra 324 (2010) 12–24]*. J. Algebra **339** (2011) 370–375. 11