No d'ordre : 905 Anneé 2002

titre de la thèse :

THÉORIE ALGORITHMIQUE DES ANNEAUX ARITHMÉTIQUES, DES ANNEAUX DE PRÜFER ET DES ANNEAUX DE DEDEKIND

Par

SALOU IDI MALAM Maïmouna

Soutenue le lundi 15 avril 2002

Président du jury :
R. GOBLOT, Professeur à l'Université des Sciences et Technologies-Lille I.

Directeur de Thèse :
H. LOMDARDI, H.D.R, Maître de conférences à l'Université de Franche-Comté

Rapporteurs :
V. BARUCCI, Professeure à l'Université La Sapienza-Roma I (Italie)

J. BREWER, Professeur à Florida Atlantic University, Boca Raton (USA)

D. DUVAL, Professeure à l'Université Joseph Fourier-Grenoble I/I.M.A.G.

Examinateurs :
V. FLECKINGER, Professeur à l'Université de Franche-Comté

G. GRAS, Professeur à l'Université de Franche-Comté

C. QUITTÉ, Maître de conférences à l'Université de Poitiers

R. RIOBOO, Maître de conférences à l'Université Pierre et Marie Curie - Paris VI

Remerciements

Je voudrais exprimer toute ma reconnaissance à mon directeur de thèse Henri Lombardi pour avoir accepté de m'encadrer. Toujours disponible, il a su me faire confiance et me donner goût à la recherche.

Ma reconnaissance va aussi à Marie-Francoise Roy qui m' a incitée à venir en France pour poursuivre mes études.

Mes remerciements à mes rapporteurs V. Barrucci, J. Brewer, et D. Duval pour s'être interessés à cette thèse.

Je remercie Remi Goblot pour m'avoir fait l'honneur de présider le jury.

Mes remerciements à Georges Gras et Vincent Fleckinger pour avoir accepté de faire partie du jury.

Toute ma reconnaisance aussi a Claude Quitté pour ses remarques, ses discussions, et le trés grand interêt qu'il a porté sur ce travail.

Je remercie Renaud Rioboo pour m'avoir aidée à faire mes premiers pas en Axiom, et pour avoir accepté de faire partie du jury.

Je tiens particulièrement à remercier Lionel Ducos avec qui j'ai réalisé la plupart de mes implémentations en Axiom, et qui m'a beaucoup appris en programmation.

Je remercie aussi la coopération française pour son soutien financier.

Mes remerciements à L'Ambassade du Niger à Paris, et à La délégation régionale de l'Egide de Strasbourg pour leur aide et leur disponibilité.

Je remercie tous les menbres du Laboratoire de Mathématiques.
Merci particulièrement à Catherine Pagani, Catherine Vuillemenot, Odile Henry et Jacques Vernerey, pour leur grande disponibilité.
Je n'oublie pas Lise-Marie Perruche et Mariette Jobard du service de la scolarité 3ème cycle.

Je remercie chaleureusement tous les thésards du laboratoire pour leur aide, et l'atmosphère conviviale qui règne au sein du groupe.

Et enfin je n'aurais jamais entrepris ce travail sans le soutien de toute ma famille au Niger, plus particulièrement de mon mari qui a supporté de longs mois d'absence affin que je puisse finir cette thèse. Qu'ils trouvent ici l'expression de ma profonde gratitude.

Table des matières

Introduction **1**

1 Préliminaires **5**
1.1 Résolution de systèmes linéaires . . . 5
1.2 Nilpotents, non diviseurs de zéros, idempotents . . . 7
1.3 Modules projectifs de type fini . . . 12
1.4 Anneaux de petite dimension . . . 13

2 Idéaux localement principaux et idéaux inversibles **17**
2.1 Matrices de localisation principale . . . 17
Produit de deux idéaux localement principaux . . . 19
Puissances d'un idéal localement principal . . . 22
Intersection de deux idéaux de type fini . . . 22
2.2 Idéaux projectifs de type fini . . . 22
2.3 Idéaux inversibles . . . 24
2.4 Les idéaux fractionnaires . . . 25

3 Anneaux arithmétiques **27**
3.1 Construction de la matrice de localisation principale . . . 27
3.2 Anneaux arithmétiques fortement discrets . . . 29
3.3 Le treillis des idéaux de type fini d'un anneau arithmétique . . . 30

4 Anneaux de Prüfer cohérents **33**
4.1 Anneaux de Prüfer . . . 33
4.2 Anneaux de Prüfer cohérents . . . 33
4.3 Systèmes linéaires et modules de présentation finie . . . 34
Le cas local . . . 34
Noyau d'une matrice . . . 35
Sous-module de type fini d'un module libre . . . 36
Structure des modules de présentation finie . . . 36
4.4 Factorisations d'idéaux . . . 37
Produits d'idéaux maximaux inversibles . . . 37
Factorisations complètes . . . 38
Factorisations partielles . . . 38

5 Extensions entières d'un anneau de Prüfer **41**
5.1 Idéaux intégralement clos et anneaux normaux . . . 41
5.2 Le cas intègre . . . 42
5.3 Le cas général . . . 44
5.4 Les cas cohérent et fortement discret . . . 47

6 Anneaux de Prüfer cohérents de dimension ≤ 1 **49**
6.1 Factorisation et dimension 1 . . . 49
6.2 Tout idéal de type fini est engendré par 2 éléments . . . 50
Le théorème un et demi . . . 51
6.3 Pour $n \geq 3$, $\mathbf{SL}_n(\mathbf{A}) = \mathbf{E}_n(\mathbf{A})$ . . . 51

6.4 Une propriété caractéristique simple 52

7 Anneaux de Dedekind **55**
7.1 Les anneaux de Dedekind sont à factorisation partielle 55
Groupes réticulés noethériens 55
7.2 Le théorème un et demi 57
7.3 Structure des idéaux et des modules de présentation finie 58

Conclusion **63**

Annexe 1 : Codes Axiom **65**

Annexe 2 : Exemples et résultats expérimentaux **83**
7.4 Clôture intégrale 83
7.5 Exemples de calculs de la matrice de localisation principale, et de la matrice de projection 83
7.6 Exemples de calculs sur les idéaux 85

Références **87**

Introduction

Les définitions usuelles d'anneau de Dedekind se prêtent mal à un traitement algorithmique.

Premièrement, la notion de noetheriannité est délicate (du point de vue algorithmique). Deuxièmement les questions de factorisation réclament en général des hypothèses extrêmement fortes. Par exemple, même si $\mathbf{K}$ est un corps tout à fait explicite, il n'y a pas de méthode générale (valable sur tous les corps) pour factoriser les polynômes de $\mathbf{K}[X]$.

Ainsi un aspect essentiel de la théorie des anneaux de Dedekind, à savoir que la clôture intégrale d'un anneau de Dedekind dans une extension finie de son corps de fractions reste un anneau de Dedekind, ne fonctionne plus en toute généralité (d'un point de vue algorithmique) si on exige la factorisation complète des idéaux (voir par exemple le traitement de cette question dans le livre d'algèbre constructive de Mines, Richman et Ruitenburg [16]).

Par ailleurs, même si une factorisation complète est en théorie faisable (dans les anneaux d'entiers des corps de nombres par exemple), on se heurte très rapidement à des problèmes d'une complexité rédhibitoire comme celui de factoriser le discriminant (tâche en pratique impossible si celui-ci a plusieurs centaines de chiffres). Aussi Lenstra et Buchmann ([3]) ont-ils proposé de travailler dans les anneaux d'entiers sans disposer d'une $\mathbb{Z}$-base. Un fait algorithmique important est qu'il est toujours facile d'obtenir une *factorisation partielle* pour une famille d'entiers naturels, c'est-à-dire une décomposition de chacun de ces entiers en produits de facteurs pris dans une famille d'entiers deux à deux étrangers (cf. [1] voir aussi [2]).

Le but de ce travail est de montrer la validité générale d'un tel point de vue et de donner des outils performants dans ce cadre.

Un début d'implémentation informatique nous a permis de comprendre le rôle crucial et simplificateur des *anneaux arithmétiques* (conformément à une intuition de Gian Carlo Rota [21]), qui sont les anneaux dans lesquels le treillis des idéaux est distributif, et de ce que nous appelons les *matrices de localisation principale*, qui sont les matrices qui explicitent la machinerie calculatoire des idéaux de type fini localement principaux. Ces matrices de localisation principale sont omniprésentes dans notre système de calculs et conduisent à ce que nous pensons être des simplifications remarquables, même pour la théorie algébrique des nombres élémentaire.

La volonté de repousser le plus tard possible la mise en place des hypothèses noethériennes nous a également guidé dans la voie d'une solution algorithmique de certains des problèmes les plus importants dans un cadre plus simple et moins rigide que celui des anneaux de Dedekind. C'est le cadre des anneaux qui ont les deux propriétés suivantes :

- les idéaux de type fini sont projectifs (ceci caractérise ce que nous appelons un *anneau de Prüfer cohérent*).
- la dimension de Krull est ≤ 1 (concept que nous manipulons dans une version totalement algorithmique).

Dans le cas local ce sont les anneaux de valuation dont le groupe de valuation est de rang 1 (c'est-à-dire isomorphe à un sous-groupe de $\mathbb{R}$).

De même, nous avons été amenés à étudier les anneaux de Prüfer cohérents "à factorisation partielle" (qui dans le cas local sont des anneaux de valuation dont le groupe de valuation est isomorphe à un sous-groupe de $\mathbb{Q}$). Nous pensons que ces anneaux constituent le cadre de travail naturel suggéré par [3].

Enfin pour ce qui concerne les anneaux de Dedekind, nous nous sommes libérés de l'hypothèse usuelle d'intégrité (car elle se conserve difficilement d'un point de vue algorithmique par extension algébrique) et nous avons abandonné la factorisation totale des idéaux de type fini (pour la même raison) au profit du seul caractère noethérien. Cette condition (convenablement formulée) implique la factorisation partielle des idéaux de type fini. Dans le cas local, nos anneaux de Dedekind sont les anneaux de valuation dont le groupe de valuation *se comporte dans les calculs comme* un groupe isomorphe à $\mathbb{Z}$. Plus précisément, ce groupe est un groupe totalement ordonné qui vérifie une condition de noethériannité formulée constructivement comme suit : toute suite décroissante d'éléments >0 admet deux termes consécutifs égaux. Ceci implique en maths classiques que le groupe est isomorphe à $\mathbb{Z}$ mais il n'existe aucune procédure algorithmique capable d'expliciter le générateur positif du groupe.

Nous avons accompagné notre travail théorique d'une implémentation de certains algorithmes en Axiom, et nous donnons dans le texte quelques remarques relatives à cette implémentation.

Voici maintenant une présentation plus détaillée de notre travail.

Dans la section 1 nous faisons quelques rappels de résultats classiques d'algèbre commutative élémentaire qui nous seront utiles sous leur forme constructive (en général mal connue).

Dans la section 2 nous introduisons les idéaux localement principaux dans leur version constructive et nous décrivons la machinerie calculatoire des matrices de localisation principale qui aboutit à une description algorithmique précise de nombreuses opérations arithmétiques usuelles sur les idéaux de type fini lorsqu'ils sont localement principaux. Nous donnons aussi quelques renseignements plus précis pour le cas particulier des idéaux projectifs et pour celui des idéaux inversibles.

Dans la section 3 nous traitons les anneaux arithmétiques, c'est-à-dire les anneaux où tous les idéaux de type fini sont localement principaux, de manière entièrement algorithmique. Un anneau arithmétique $\mathbf{A}$ est défini comme un anneau tel que pour tous x_1, x_2 dans $\mathbf{A}$, il existe $u, v, w \in \mathbf{A}$ vérifiant $u\,x_2 = v\,x_1$ et $w\,x_2 = (1-u)\,x_1$. Dans le cas où la divisibilité est explicite, nous obtenons un traitement assez satisfaisant des systèmes linéaires.

Dans la section 4 nous introduisons les anneaux de Prüfer cohérents. Ils peuvent être définis comme les anneaux arithmétiques quasi intègres (i.e., l'annulateur de tout élément est un idéal principal engendré par un idempotent). En particulier un anneau arithmétique intègre est un anneau de Prüfer cohérent. Un anneau arithmétique intègre est appelé un domaine de Prüfer (voire un anneau de Prüfer[1]) dans

[1] Notre définition sans hypothèse d'intégrité pour les anneaux de Prüfer provient de [10], dans lequel les auteurs mettent en évidence une propriété déterminantielle remaquable de ces anneaux, cf. aussi [13] pour un traitement constructif.

la littérature classique. Nous obtenons des algorithmes précis pour la résolution des systèmes linéaires et pour les résultats importants suivants.

Proposition 4.9 *Sur un anneau de Prüfer cohérent le noyau d'une application linéaire* $\varphi : \mathbf{A}^n \to \mathbf{A}^m$ *entre modules libres de dimensions finies est facteur direct. Autrement dit* $\operatorname{Ker}\varphi = \operatorname{Im}\pi$ *où* $\pi : \mathbf{A}^n \to \mathbf{A}^n$ *est une projection.*

Theorem 4.1 *Sur un anneau de Prüfer cohérent tout sous-module de type fini* M *d'un module libre est projectif, isomorphe à une somme directe d'idéaux de type fini. En particulier tout module projectif de type fini est isomorphe à une somme directe d'idéaux de type fini. Si* M *est de rang constant* r*, il est isomorphe à une somme directe de* r *idéaux inversibles.*

Proposition 4.10 *Si* $\mathbf{A}$ *est un anneau de Prüfer cohérent, alors tout module de présentation finie est somme directe de son sous-module de torsion et d'un sous-module projectif.*

Enfin dans la sous-section 4.4 nous introduisons les problèmes de factorisation d'idéaux. Nous définissons un domaine de Dedekind à factorisation complète comme un anneau intègre à divisibilité explicite dans lequel tout idéal de type fini se décompose en produit d'idéaux maximaux inversibles. Nous discutons brièvement cette notion pour en dégager une autre, un peu moins forte mais que nous pensons très utile, celle d'anneau de Prüfer à factorisation partielle, c'est-à-dire un anneau de Prüfer cohérent où chaque élément d'une famille finie d'idéaux inversibles admet une base de factorisation partielle : une famille d'idéaux inversibles deux à deux étrangers qui factorise chacun des idéaux de la famille de départ.

Dans la section 5 nous montrons comment la machinerie calculatoire des matrices de localisation principale se transfère d'un anneau de Prüfer à une extension entière normale (théorèmes 5.1 et 5.2). Nous explicitons aussi un cas particulièrement important où un anneau de Prüfer cohérent reste tel par extension entière normale :

Theorem 5.3 *Soit* $\mathbf{A}$ *un anneau de Prüfer cohérent. Soit* $f(X) \in \mathbf{A}[X]$ *un polynôme unitaire dont le discriminant est non diviseur de zéro. Soit* $\mathbf{A}' = \mathbf{A}[X]/\langle f(X)\rangle$ *et* $\mathbf{B}$ *la clôture intégrale de* $\mathbf{A}'$ *dans son anneau total des fractions. Alors* $\mathbf{B}$ *est un anneau de Prüfer cohérent.*
En outre si $\mathbf{A}$ *est fortement discret (resp. noethérien), alors il en va de même pour* $\mathbf{B}$*.*

Ainsi, lorsque nous passons d'un anneau de Prüfer $\mathbf{A}$ à une extension entière normale $\mathbf{B}$ nous maîtrisons les systèmes linéaires et l'arithmétique de base des idéaux de type fini de $\mathbf{B}$. Si $\mathbf{B}$ est obtenu en rajoutant un nombre fini d'éléments séparables explicites, il se peut qu'il soit extrêmement difficile d'obtenir une présentation finie de $\mathbf{B}$ comme $\mathbf{A}$-module (c'est par exemple le cas pour des extensions d'anneaux d'entiers avec de grands discriminants). Cela ne nous empêchera pas de mener à bien les calculs. Si nous travaillons au départ avec un sous-anneau $\mathbf{B}_1$ de $\mathbf{B}$, la structure de $\mathbf{A}$-module étant connue pour $\mathbf{B}_1$, nos calculs (par exemple celui de l'inverse d'un idéal de type fini de $\mathbf{B}_1$, inversible dans $\mathbf{B}$ mais pas dans $\mathbf{B}_1$) peuvent nous amener de manière automatique à améliorer notre connaissance de $\mathbf{B}$ et à considérer un nouveau sous-anneau $\mathbf{B}_2$ qui en constituera une meilleure "approximation" avec de nouveau une structure de $\mathbf{A}$-module connue.

Dans la section 6 nous étudions les anneaux de Prüfer cohérents de dimension ≤ 1. Nous obtenons une version algorithmique des théorèmes suivants.

Theorem 6.2 *Soit dans un anneau de Prüfer cohérent de dimension ≤ 1 des idéaux de type fini deux à deux étrangers $P_1, \ldots, P_n$ et un idéal inversible I. Alors on peut écrire $I = I_0 \cdot I_1 \cdots I_n$ avec les idéaux de type fini I_j deux à deux étrangers et $P_j^{m_j} \subseteq I_j$ pour des entiers m_j convenable. Cette écriture est unique et on a $I_j = I + P_j^{m_j} = I + P_j^{1+m_j}$.*

Theorem 6.3 (théorème "deux générateurs") *Dans un anneau quasi intègre de dimension ≤ 1 tout idéal de type fini projectif est engendré par deux éléments. En conséquence sur un anneau de Prüfer cohérent de dimension ≤ 1 tout idéal de type fini est engendré par deux éléments.*

Theorem 6.5 *Soit $n \geq 3$ et $(x_1, \ldots, x_n)$ un vecteur unimodulaire sur un anneau de Prüfer cohérent $\mathbf{A}$ de dimension ≤ 1. Ce vecteur est la première colonne d'une matrice de $\mathbf{E}_n(\mathbf{A})$. En particulier $\mathbf{SL}_n(\mathbf{A}) = \mathbf{E}_n(\mathbf{A})$ pour $n \geq 3$. Et pour $n \geq 2$ tout vecteur unimodulaire est la première colonne d'une matrice de $\mathbf{SL}_n(\mathbf{A})$.*

Theorem 6.6 *Un anneau normal quasi intègre cohérent de dimension ≤ 1 est un anneau de Prüfer.*

Dans la section 7 nous étudions les anneaux de Dedekind, que nous définissons sans condition d'intégrité ni de factorisation complète, comme des anneaux de Prüfer cohérents noethériens (à divisibilité explicite).

Nous maîtrisons les extensions finies séparables grâce au théorème 5.3. Nous obtenons une version algorithmique des théorèmes suivants.

Theorem 7.1 *Soit $\mathbf{A}$ un anneau de Dedekind. Alors toute famille finie d'idéaux inversibles de $\mathbf{A}$ admet une factorisation partielle. Autrement dit un anneau de Dedekind est un anneau de Prüfer à factorisation partielle.*

Theorem 7.2 (théorème un et demi) *Soient $\mathbf{A}$ un anneau de Dedekind et I un idéal de type fini de $\mathbf{A}$ contenant un non diviseur de zéro a. Il existe un élément b de $\mathbf{A}$ tel que $I = \langle a, b\rangle$.*

Proposition 7.5 *Soit $\mathbf{A}$ un anneau de Dedekind tel que $\mathrm{Rad}(\mathbf{A})$ contienne un non diviseur de zéro. Alors $\mathbf{A}$ est un anneau de Bezout.*

Lemme 7.7 *Soit $\mathbf{A}$ un anneau de Dedekind. Soient I et J deux idéaux de type fini (entiers) avec I inversible. Il existe $u \in \mathrm{F}(\mathbf{A})$ tel que l'idéal $u\,I$ est entier et étranger à J.*

Theorem 7.3 *Sur un anneau de Dedekind, tout module projectif M de rang $k \geq 2$ est isomorphe à $\mathbf{A}^{k-1} \oplus I$, où I est un idéal inversible. En particulier il est engendré par $k+1$ éléments. Le résultat est valable pour tout anneau de Prüfer cohérent vérifiant le lemme 7.7.*

Theorem 7.4 *Soient $\mathbf{A}$ un anneau de Dedekind et $x_1, \ldots, x_n \in \mathbf{A}$. Il existe une matrice inversible M qui transforme $(x_1, \ldots, x_n)$ en $(y_1, y_2, 0, \ldots, 0)$. Le résultat est valable pour tout anneau de Prüfer cohérent vérifiant le lemme 7.7.*

Dans les annexes, nous donnons les codes Axiom de nos programmes et quelques résultats expérimentaux lors de leur exécution.

1 Préliminaires

Cette section introductive contient quelques rappels de résultats classiques qui nous seront utiles sous leur forme constructive (en général mal connue) lorsque nous entrerons dans le vif du sujet.

1.1 Résolution de systèmes linéaires

L'exemple de $\mathbb{Z}$

La résolution des systèmes linéaires dans $\mathbb{Z}$ est donnée par la réduction de Smith de n'importe quelle matrice par manipulations élémentaires de lignes et de colonnes. Une matrice en forme réduite de Smith vérifie : les seuls éléments non nuls $(d_i)_{i=1,..,k}$ ($k \leq \inf(n,m)$) sont sur la diagonale (d_i en position (i,i)), et on a $d_i | d_{i+1}$. Si $d_1 = \cdots = d_r = 1$, $d_{r+1}, \ldots, d_{r+s} \neq 0, 1$, et $d_{r+s+1} = \cdots = d_k = 0$, cela signifie qu'après un changement linéaire (élémentaire en un sens précis) de variables, le système initial est ramené à la forme :

$$\begin{array}{rcl} x_1 &=& c_1 \\ \vdots & \vdots & \vdots \\ x_r &=& c_r \end{array} \qquad \begin{array}{rcl} d_{r+1}\, x_{r+1} &=& c_{r+1} \\ \vdots & \vdots & \vdots \\ d_{r+s}\, x_{r+s} &=& c_{r+s} \end{array} \qquad \begin{array}{rcl} 0 &=& c_{r+s+1} \\ \vdots & \vdots & \vdots \\ 0 &=& c_n \end{array}$$

où les c_i sont obtenus par transformations élémentaires successives de la colonne "second membre" initiale.

Ceci donne une discussion complète du système linéaire, y compris lorsque le second membre dépend de paramètres.

De manière équivalente on a une description claire et précise du noyau (libre en facteur direct), de l'image (libre) et du conoyau (somme directe d'un libre et de modules cycliques) de toute matrice.

Cette situation si claire et agréable est à peu près celle que nous trouverons avec les anneaux de Prüfer cohérents, avec une machinerie calculatoire à peine plus compliquée que celle des réductions de Smith sur $\mathbb{Z}$ (la principale complication viendra de ce que les idéaux de type fini ne sont plus nécessairement principaux). En outre nous serons capables d'expliquer simplement comment la machinerie calculatoire se transfère à une extension entière de l'anneau de départ.

Anneaux cohérents

Nous rappelons maintenant une situation générale dans laquelle les systèmes linéaires sont résolubles de manière explicite en un sens raisonnable (quoique moins précis que pour les anneaux de Prüfer cohérents) : c'est celle des anneaux cohérents fortement discrets.

Définition 1.1 *Un anneau est dit* cohérent *si tout idéal de type fini est de présentation finie. Autrement dit pour toute équation $LX = 0$ ($L \in \mathbf{A}^{1\times n}$, $X \in \mathbf{A}^{n\times 1}$), il existe $m \in \mathbb{N}$, $G \in \mathbf{A}^{n\times m}$ tels que*

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

Un $\mathbf{A}$-module M est dit cohérent si tout sous-module de type fini est de présentation finie.

Dans la suite nous employons l'expression *anneau cohérent* au sens constructif, autrement dit la matrice G peut être calculée explicitement à partir de L, et chaque fois qu'on a un $X \in \mathbf{A}^{n\times 1}$ tel que $LX = 0$ on peut calculer un $Y \in \mathbf{A}^{m\times 1}$ tel que $X = GY$.

Un anneau est cohérent si et seulement si d'une part l'intersection de deux idéaux de type fini est un idéal de type fini, et d'autre part l'annulateur de tout élément est un idéal de type fini. ([16], théorème 2.4, page 82)

Proposition 1.2 *Sur un anneau cohérent le noyau d'une application linéaire entre modules libres de dimensions finies est un module de type fini. De manière équivalente, les solutions d'un système linéaire sans second membre forment un sous-module de type fini de* $\mathbf{A}^{n\times 1}$*, dont on peut calculer explicitement un système fini de générateurs.*

Preuve Pour tout système d' équations $LX = 0$ avec $L \in \mathbf{A}^{p\times n}$ et $X \in \mathbf{A}^{n\times 1}$, la résolution peut se faire par étapes successives. En effet la première équation du système soit $L_1X = 0$ nous donne (grâce à la cohérence) une matrice $G_1 \in \mathbf{A}^{n\times m_1}$, telle que $L_1X = 0 \iff \exists\, Y \in \mathbf{A}^{m_1\times 1}\ X = G_1Y$.
En remplacant X dans l' équation suivante on a $L_2G_1Y = 0$ et on obtient une nouvelle matrice $G_2 \in \mathbf{A}^{m_1\times m_2}$ telle que

$$\begin{array}{rcl} L_1X = L_2X = 0 & \iff & \exists\, Y \in \mathbf{A}^{m_1\times 1}\ X = G_1Y \text{ et } L_2G_1Y = 0 \\ & \iff & \exists\, Z \in \mathbf{A}^{m_2\times 1}\ X = G_1G_2Z \end{array}$$

Finalement, les solutions sont de la forme $X = G_1G_2 \dots G_pZ$ avec
$G_i \in \mathbf{A}^{m_{i-1}\times m_i}$ et $Z \in \mathbf{A}^{m_p\times 1}$ (avec $m_0 = n$). □

Le quotient d'un anneau cohérent par un idéal de type fini est un anneau cohérent.

Anneaux fortement discrets

Un ensemble G est appelé *discret* s'il y a un test d'égalité dans G. Si G est un groupe (noté additivement), cela signifie qu'on a constructivement

$$\forall x \in G, \quad x = 0 \ \text{ ou } \ x \neq 0.$$

Une partie S d'un ensemble G est dite *détachable* s'il y a un test pour l'appartenance à S dans G. Cela signifie qu'on a constructivement

$$\forall x \in G, \quad x \in S \ \text{ ou } \ \neg(x \in S).$$

Définition 1.3 *Un* $\mathbf{A}$*-module* M *est dit* fortement discret *si tous ses sous-modules de type fini sont détachables. Un anneau* $\mathbf{A}$ *est dit* fortement discret *s'il l'est en tant que* $\mathbf{A}$*-module.*

Il revient au même de dire que le module M est fortement discret ou que tous ses quotients par des sous-modules de type fini sont discrets.

Nous lisons la définition de manière constructive : lorsque $x \in M$ est testé positivement pour l'appartenance au sous-module $\langle x_1, \dots, x_n\rangle$ on doit avoir explicitement des a_i tels que $\sum_i a_ix_i = x$.

Proposition 1.4 *Sur un anneau cohérent fortement discret les solutions d'un système linéaire peuvent être calculées sous la forme* $X_0 + GY$ *où* X_0 *est une solution particulière et* G *est la matrice obtenue a partir du système homogène en appliquant la proposition 1.2.*

Preuve Le résultat est clair lorsqu'il y a une seule équation. On procède ensuite comme dans la preuve de la proposition 1.2 pour trouver X_0 et la matrice G du système homogène. □

Localisations en des monoïdes comaximaux

Définition 1.5

(1) *On appelle* monoïde d'un anneau $\mathbf{A}$ *une partie de* $\mathbf{A}$ *contenant* 1 *et stable pour la multiplication.*

(2) *Des monoïdes* $S_1, \ldots, S_n$ *sont dits* comaximaux, *si et seulement si :*

$$\forall\, s_1 \in S_1, \ldots, \forall\, s_n \in S_n, \quad \exists a_1, \ldots, a_n \in \mathbf{A}, \quad \sum\nolimits_{i=1}^{n} a_i s_i = 1.$$

(3) *Des éléments* $s_1, \ldots, s_n$ *sont dits* comaximaux *si et seulement si* $\langle s_1, \ldots, s_n \rangle = \mathbf{A}$, *ce qui revient à dire que les monoïdes qu'ils engendrent sont comaximaux.*

Notez que nous n'excluons pas le cas des monoïdes contenant 0 : il arrive qu'on ne sache pas si un monoïde S contient ou ne contient pas 0, mais comme il fait partie d'une famille de monoïdes comaximaux, on tient à localiser aussi en S de manière à pouvoir appliquer un principe local-global.

La notion de monoïdes comaximaux est intéressante en vertu des nombreux principes "local-global" dans lesquels ils interviennent. Citons le principe essentiel suivant, dont la preuve est d'ailleurs immédiate.

Théorème 1.1 (principe local-global pour la résolution des systèmes linéaires) *Soient* $S_1, \ldots, S_n$ *des monoïdes comaximaux de* $\mathbf{A}$, *soit* B *une matrice* $\in \mathbf{A}^{m\times p}$ *et* C *un vecteur colonne* $\in \mathbf{A}^{m\times 1}$. *Alors on a l'équivalence :*

Le système linéaire $BX = C$ *admet une solution dans* $\mathbf{A}^{p\times 1}$

$$\Longleftrightarrow$$

$\forall i \in \{1, \ldots, n\}$ *le système linéaire* $BX = C$ *admet une solution dans* $\mathbf{A}_{S_i}^{p\times 1}$

En particulier un élément d'un anneau est nul, nilpotent, inversible ou non diviseur de zéro si et seulement si il a la même propriété après localisation en des monoïdes comaximaux.

Un anneau est cohérent si et seulement si il a la même propriété après localisation en des monoïdes comaximaux.

1.2 Nilpotents, non diviseurs de zéros, idempotents

Le radical et le nilradical

Pour tout anneau $\mathbf{A}$ nous notons $\mathrm{Rad}(\mathbf{A})$ le *radical (de Jacobson)* de $\mathbf{A}$, c'est-à-dire l'idéal $\{x \in \mathbf{A} \mid 1 + x\mathbf{A} \subseteq \mathbf{A}^\times\}$. Le *nilradical*, c'est-à-dire l'ensemble des

nilpotents, sera noté $\mathrm{N}(\mathbf{A})$. On a $\mathrm{N}(\mathbf{A}) \subseteq \mathrm{Rad}(\mathbf{A})$. Un anneau est dit *réduit* si $\mathrm{N}(\mathbf{A}) = 0$.

Du point de vue constructif, un anneau $\mathbf{A}$ est *local* si et seulement si pour tout $a \in \mathbf{A}$, a ou $1+a$ est inversible. Un quotient d'un anneau local est local (y compris le quotient trivial). Le radical d'un anneau local est égal à l'ensemble des x qui vérifient l'implication suivante :

$$(\, x \text{ inversible}\,) \implies 1 =_{\mathbf{A}} 0$$

(ceci est vrai également avec l'anneau trivial).

Le truc du déterminant (determinant trick en anglais)

C'est la remarque suivante.

Lemme 1.6 *Si M est un $\mathbf{A}$-module* de type fini *et I un idéal tels que $IM = M$ alors il existe x dans I tel que $(1-x)\,M = 0$.*

Preuve Si $M = \mathbf{A}v_1 + \cdots + \mathbf{A}v_n$ on a une matrice A à coefficients dans I telle que $A\,{}^t(v_1, \ldots, v_n) = {}^t(v_1, \ldots, v_n)$ c'est-à-dire $(\mathrm{I}_n - A)\,{}^t(v_1, \ldots, v_n) = 0$. On a $\det(\mathrm{I}_n - A) = 1 - x$ avec $x \in I$ et $(1-x)\,{}^t(v_1, \ldots, v_n) = 0$. □

En particulier si $I \subseteq \mathrm{Rad}(\mathbf{A})$ cela donne $M = 0$ (lemme de Nakayama).

Corollaire 1.7 *Si I est un idéal de type fini idempotent il existe un idempotent r tel que $I = \langle r \rangle$.*

Systèmes fondamentaux d'idempotents orthogonaux

Lorsqu'on connaît un idempotent r dans un anneau $\mathbf{A}$ on dispose des deux "composantes" $r\mathbf{A} \simeq \mathbf{A}_r \simeq \mathbf{A}/\langle s\mathbf{A}\rangle$ et $s\mathbf{A} \simeq \mathbf{A}_s \simeq \mathbf{A}/\langle r\mathbf{A}\rangle$ où $s = 1 - r$. L'anneau est isomorphe au produit de ses deux composantes, qui jouissent en général des mêmes propriétés que l'anneau $\mathbf{A}$.

Un *système fondamental d'idempotents orthogonaux* (sfio) dans $\mathbf{A}$ est une famille d'éléments $(r_1, \ldots, r_m)$ tels que $r_i r_j = 0$ si $i \neq j$ et $\sum_i r_i = 1$. Les r_i sont alors des idempotents.

L'anneau est ainsi "cassé" en composantes A_{r_i}. La plupart des problèmes (en particulier la résolution des systèmes linéaires) qui se posent dans $\mathbf{A}$ peuvent être traités séparément dans chaque composante, et les composantes sont totalement indépendantes les unes des autres.

Les idempotents d'un anneau forment une algèbre de Boole : le produit est le même que dans l'anneau, le pgcd de r et r' est $r + r' - rr'$ et leur somme (dans l'algèbre de Boole) est $r + r' - 2rr'$. Un idempotent r est dit *minimal* si $rr' = r$ ou 0 pour tout autre idempotent r'.

Anneaux intègres, sans diviseur de zéro et localement sans diviseur de zéro, modules sans torsion

Nous disons qu'un élément x d'un anneau $\mathbf{A}$ est *non diviseur de zéro* si la multiplication par x est injective. Cela implique que 0 est non diviseur de zéro dans l'anneau trivial et qu'un non diviseur de zéro reste non diviseur de zéro dans tout localisé, même si le localisé est trivial. Ce détail a son importance d'un point de vue

algorithmique lorsqu'on doit localiser en un monoïde S sans savoir si la localisation conduit à un anneau trivial ou non (c'est-à-dire sans savoir si $0 \in S$ ou non).

L'*anneau total des fractions* d'un anneau $\mathbf{A}$ est l'anneau $\mathrm{F}(\mathbf{A})$ des fractions x/y avec y non diviseur de zéro dans $\mathbf{A}$.

Constructivement un *anneau intègre* est défini comme un anneau discret dans lequel tout élément non nul est non diviseur de zéro. Ainsi dans un anneau intègre l'annulateur d'un élément est explicite, et il est égal à 0 ou 1.

Une condition un peu plus faible (du point de vue constructif) est de demander que l'anneau soit *sans diviseur de zéro* c'est-à-dire qu'il vérifie l'axiome suivant :

$$\forall a, b \in \mathbf{A} \quad (ab = 0 \implies (a = 0 \text{ ou } b = 0)) \tag{1}$$

Les anneaux *localement sans diviseur de zéro* sont définis par la propriété suivante :

$$\forall a, b \in \mathbf{A} \quad (ab = 0 \implies \exists s, t \in \mathbf{A} : s + t = 1,\ sa = 0,\ tb = 0). \tag{2}$$

Un anneau est localement sans diviseur de zéro si et seulement si il a la même propriété après localisation en des monoïdes comaximaux.

Nous généralisons comme suit la notion usuelle de *module sans torsion* (définie dans le cas intègre).

Définition 1.8 *Soit* $\mathbf{A}$ *un anneau et* M *un* $\mathbf{A}$*-module.*

- *Un élément* x *de* M *est appelé un* élément de torsion *s'il existe un non diviseur de zéro* $a \in \mathbf{A}$ *tel que* $ax = 0$*. Les éléments de torsion forment un sous-module appelé le* sous-module de torsion *de* M*.*
- *Si* $\mathbf{A}$ *est localement sans diviseur de zéro on dit que* M *est* sans torsion *si on a :*

$$\forall x \in M,\ \forall a \in \mathbf{A} \quad (ax = 0 \implies \exists s, t \in \mathbf{A} : s + t = 1,\ sa = 0,\ tx = 0) \tag{3}$$

Anneaux quasi-intègres

Une généralisation naturelle de la notion d'anneau intègre est la suivante.

Définition 1.9 *Un anneau est dit* quasi intègre *si tout idéal principal est projectif, c'est-à-dire encore :*

$$\forall x \ \exists r, \ \ r^2 = r \ \text{ et } \ \mathrm{Ann}(x) = \langle r \rangle \tag{4}$$

La terminologie anglaise est *pp*-ring (principal ideals are projective). Une autre terminologie française est "anneau faiblement de Baer".

Remarque d'implémentation : Pour déclarer un anneau quasi intègre on déclare que c'est un anneau commutatif avec un constructeur $x \mapsto r$ qui réalise explicitement la condition (4).

On a facilement :

Fait 1.10

- *Un anneau quasi intègre est discret si et seulement si l'ensemble de ses idempotents est discret.*

- *Un produit fini d'anneaux quasi intègres est quasi intègre.*
- *Un anneau quasi intègre qui a un nombre fini d'idempotents (ou, ce qui revient au même, qui possède un sfio formé d'idempotents minimaux) est un produit d'anneaux intègres.*
- *Un module sur un anneau quasi intègre est sans torsion si et seulement si son sous-module de torsion est réduit à* 0.

En pratique, un anneau quasi intègre, même non discret, se comporte presque comme un anneau intègre. Par exemple si on veut exécuter un algorithme prévu pour un anneau intègre avec un anneau quasi intègre, on remplace chaque branchement du style

$$\text{si } a = 0 \text{ alors action 1 sinon action 2}$$

par un "scindage" : on considère l'idempotent r_a annulateur de a et l'anneau "en cours" $\mathbf{A}_i$ est alors remplacé par ses deux composantes $\mathbf{A}_{i1} = r_a\,\mathbf{A}_i$ et $\mathbf{A}_{i2} = (1-r_a)\,\mathbf{A}_i$. Dans la composante $\mathbf{A}_{i1}$ on exécute l'action 1, et dans la composante $\mathbf{A}_{i2}$ on exécute l'action 2.

Il peut sembler a priori que tous ces scindages successifs produisent un nombre de branches à croissance exponentielle. En fait la situation est souvent algorithmiquement plus simple, comme dans l'exemple qui suit.

Lemme 1.11 *Dans un anneau quasi intègre l'annulateur de tout idéal de type fini est un idéal engendré par un idempotent. Plus précisement si* $I = \langle x_1, \dots, x_n\rangle$ *alors* $\mathrm{Ann}(I) = \langle r_1 \cdots r_n\rangle$ *où* $\langle r_i\rangle = \mathrm{Ann}\,\langle x_i\rangle$ *et* r_i *idempotent. En outre* $\mathrm{Ann}(I) = \mathrm{Ann}(x)$ *pour un* $x = x_1 + t_2x_2 + \cdots + t_nx_n \in I$ *où les* t_i *sont idempotents.*

Preuve Soit en effet s_i tel que $s_i + r_i = 1$, on a : $(s_1+r_1)(s_2+r_2)\cdots(s_n+r_n) = 1$, d'où $s_1 + r_1(s_2 + r_2(\cdots(s_n + r_n)\cdots) = 1$ et on obtient un sfio :

$$s_1 + r_1s_2 + r_1r_2s_3 + \cdots + r_1r_2\cdots r_{n-1}s_n + r_1r_2\cdots r_n = 1.$$

($t_1 = s_1$, $t_2 = r_1s_2$, $t_3 = r_1r_2s_3, \dots$, $t_{n+1} = r_1r_2\cdots r_n$). Posons $x = x_1 + r_1x_2 + r_1r_2x_3 + \cdots + r_1r_2\cdots r_{n-1}x_n = t_1x_1 + t_2x_2 + \cdots + t_nx_n$, alors $\mathrm{Ann}\,\langle x_1, \dots, x_n\rangle = \mathrm{Ann}(x) = \langle r_1\cdots r_n\rangle$. En effet dans chaque composante $t_i\mathbf{A}$, $(i = 1, \dots, n)$, $x = t_ix = t_ix_i$ est non diviseur de zéro (puisque $x_i = s_ix_i$ est non diviseur de zéro dans $s_i\mathbf{A}$) et dans la composante $t_{n+1}\mathbf{A}$, $x = 0$. □

Dans un anneau localement sans diviseur de zéro l'annulateur d'un élément est toujours un idéal idempotent. Puisqu'un idéal de type fini idempotent est engendré par un idempotent on obtient.

Fait 1.12 *Un anneau localement sans diviseur de zéro cohérent est quasi intègre.*

Dire qu'un anneau est égal à son anneau total de fractions revient à dire que tout élément non diviseur de zéro est inversible.

Nous donnons maintenant un résultat qui est à la base du système **D5**. En calcul formel ce système permet de calculer dans la côture algébrique d'un corps sans utiliser d'algorithme de factorisation des polynômes (cf. [6]).

Dans le cas du système **D5** et en mathématiques classiques, l'hypothèse et la conclusion seraient que l'anneau est isomorphe à un produit fini de corps.

Proposition 1.13 *Soit* $\mathbf{K}$ *un anneau quasi intègre dans lequel tout élément non diviseur de zéro est inversible (par exemple un produit fini de corps discrets). Soit* $f(X) \in \mathbf{K}[X]$ *un polynôme unitaire dont le discriminant est inversible. Soit* $\mathbf{K}' = \mathbf{K}[X]/\langle f(X)\rangle$. *Alors* $\mathbf{K}'$ *est un anneau quasi intègre dans lequel tout élément non diviseur de zéro est inversible.*

Preuve Nous donnons d'abord une preuve qui fonctionne sous l'hypothèse suivante : $\mathbf{K}$ est un corps discret. On a $\mathbf{K}' = \mathbf{K}[X]/\langle f(X)\rangle$ avec $c(X)f(X) + d(X)f'(X) = \mathrm{disc}(f)$ inversible dans $\mathbf{K}$. On note x la classe de X dans $\mathbf{K}'$. Soit $g(x) \in \mathbf{K}'$ ($g(X) \in \mathbf{K}[X]$, $\deg(g) < \deg(f)$). On considère le pgcd $h(X)$ de $f(X)$ et $g(X)$ qui se calcule par l'algorithme d'Euclide. On obtient

$$a(X)f(X) + b(X)g(X) = h(X)$$

avec h unitaire. Si $h = 1$, $g(x)$ est inversible dans $\mathbf{K}'$ et son annulateur est 0. Si $\deg(h) > 0$ on obtient

$$f(X) = h(X)f_1(X) \qquad \text{et} \qquad g(X) = h(X)g_1(X)$$

avec

$$a(X)f_1(X) + b(X)g_1(X) = 1 \tag{5}$$

Le résultant de h et f_1 divise le discriminant de f donc est inversible. On considère l'identité

$$u(X)h(X) + v(X)f_1(X) = \mathrm{Res}(h, f_1) \tag{6}$$

Si on pose $e_1 = e_1(x) = u(x)h(x)/\mathrm{Res}(h, f_1) = u_1(x)h(x)$ et $e_2 = e_2(x) = v(x)f_1(x)/\mathrm{Res}(h, f_1) = v_1(x)f_1(x)$ on a

$$e_1e_2 = 0,\ e_1 + e_2 = 1,\ e_1 = u_1h,\ e_2 = v_1f_1,\ e_1f_1 = e_2h = 0$$

donc e_1 et e_2 sont deux idempotents orthogonaux avec $\langle e_1\rangle = \mathrm{Ann}(f_1) = \langle h\rangle$, $\langle e_2\rangle = \mathrm{Ann}(h) = \langle f_1\rangle$, et on a des isomorphismes explicites

$$e_2\mathbf{K}' \simeq \mathbf{K}'/\langle e_1\rangle \simeq \mathbf{K}[X]/\langle f(X), e_1(X)\rangle = \mathbf{K}[X]/\langle h(X)\rangle$$

et

$$e_1\mathbf{K}' \simeq \mathbf{K}'/\langle e_2\rangle \simeq \mathbf{K}[X]/\langle f(X), e_2(X)\rangle \simeq \mathbf{K}[X]/\langle f_1(X)\rangle\ .$$

En multipliant (5) et (6) on obtient $m(x)f_1(x) + n(x)g(x) = 1$ donc $e_1gn = e_1$, i.e., e_1g est inversible dans $e_1\mathbf{K}'$. Et e_2g, multiple de e_2h, est nul. Ceci montre que l'annulateur de g dans $\mathbf{K}'$ est l'idempotent e_2. En particulier on a obtenu que les éléments non diviseur de zéro de $\mathbf{K}'$ sont tous inversibles.

Pour traiter le cas général, on peut utiliser la méthode indiquée juste après le fait 1.10. Nous ne donnons pas les détails dans la mesure où nous présentons un algorithme plus satisfaisant plus loin (proposition 1.20). □

1.3 Modules projectifs de type fini

Une *matrice de projection* est par définition une matrice carrée P vérifiant $P^2 = P$. Elle représente la projection sur son image parallèlement à son noyau.

Un $\mathbf{A}$-module *projectif de type fini* M est par définition un facteur direct dans un module libre $\simeq \mathbf{A}^n$ c'est-à-dire encore un module isomorphe à l'image d'une matrice de projection P.

Si on définit $R_M(X)$ par $R_M(1+X) = \det(\mathrm{I}_n + XP)$ on a $R_M(1) = 1$ et $R_M(X)R_M(Y) = R_M(XY)$ de sorte que si $R_M(X) = \sum_i r_i X^i$ le système $(r_0, r_1, \ldots, r_n)$ est un sfio avec $r_0 = \mathrm{Ann}(M)$. Le polynôme $R_M(X)$ n'est autre que le déterminant de la multiplication par X dans le module M. Un module projectif de type fini est dit *de rang constant* k si $R_M(X) = X^k$. En général $M = \oplus_k r_k M$ et $r_k M$ est de rang constant k sur $\mathbf{A}_{r_k}$ (notez que sur l'anneau trivial, le module trivial a tous les rangs simultanément).

Un module projectif de type fini M est dit de rang $\leq k$ si $R_M(X)$ est de de gré $\leq k$. Cela revient à dire que tous les mineurs d'ordre $> k$ de la matrice P sont nuls, ou encore que pour tout localisé $\mathbf{A}_S$, si M_S est libre, il est libre de rang $\leq k$.

Un module garde son caractère projectif de type fini (ou projectif de rang k) par changement d'anneau de base.

On a aussi le principe local-global suivant : *un module est projectif de type fini (resp. projectif de rang k) si et seulement si il a la même propriété après localisation en des monoïdes comaximaux.*

En fait on peut trouver à partir de la matrice P des éléments comaximaux tels que tous les localisés de $\mathrm{Im}\, P$ soient non seulement projectifs de type fini mais libres.

Voici une description précise des modules projectifs de rang ≤ 1.

Proposition 1.14 *Soit $M = \mathbf{A}x_1 + \cdots + \mathbf{A}x_n$ un module de type fini. Il est projectif de rang ≤ 1 si et seulement si il existe une matrice $P = (p_{ij}) \in \mathbf{A}^{n\times n}$ qui vérifie les propriétés suivantes :*

(1) *$P^2 = P$ et tout mineur d'ordre 2 de P est nul.*

(2) *Pour tous $i, j, \ell \in \{1, \ldots, n\}$ on a $p_{\ell i}x_j = p_{\ell j}x_i$.*

(3) *L'annulateur de M est engendré par $1 - \mathrm{Tr}(P)$ (qui est idempotent d'après le (1)).*

Dans ce cas, l'application linéaire $\varphi : \mathbf{A}^n \to M$, $(\alpha_1, \ldots, \alpha_n) \mapsto \sum_i \alpha_i x_i$ et la projection $\psi : \mathbf{A}^n \to \mathbf{A}^n$ de matrice P vérifient : $\mathrm{Im}\,(\mathrm{I}_n - \psi) = \mathrm{Ker}\,\psi = \mathrm{Ker}\,\varphi$ et la factorisation qu'on en déduit établit un isomorphisme entre $\mathrm{Coker}\,(\mathrm{I}_n - \psi) \simeq \mathrm{Im}\,\psi$ et M. Enfin sur le localisé $\mathbf{A}_{p_{ii}}$ le module devient libre, de base x_i.

Preuve Nous démontrons seulement la partie directe. Supposons que M soit projectif de rang ≤ 1. L'application φ est scindée via une section $s : M \to \mathbf{A}^n$ puisque le module M est projectif. On pose $s(x_j) = P_j$ si bien que $\varphi \circ s = \mathrm{Id}_M$, $s \circ \varphi = \psi$ est un projecteur qui transforme e_j (le j-ème vecteur de la base canonique) en P_j, et s est un isomorphisme de M sur $\mathrm{Im}\, s = \mathrm{Im}\,\psi$. La matrice P de ψ est $(P_1|P_2|\cdots|P_n)$. On a clairement $P^2 = P$ et $\mathrm{Coker}\,(\mathrm{I}_n - \psi) \simeq \mathrm{Im}\,\psi \simeq M$. Le fait que le rang de $M \simeq \mathrm{Im}\, P$ est ≤ 1 implique que les mineurs d'ordre 2 de P sont nuls. On en déduit les égalités (2) car il suffit de les transformer par s. On voit facilement que sur le localisé $\mathbf{A}_{p_{ii}}$ le module devient libre de base x_i tandis

que sur le localisé $\mathbf{A}_{1-\mathrm{Tr}(P)}$ le module devient nul. Le calcul montre d'ailleurs que $R_M(X) = 1 - \mathrm{Tr}(P) + \mathrm{Tr}(P)X$. □

Définition 1.15 *Soient $x_1, \ldots, x_n$ des éléments d'un $\mathbf{A}$-module. On apppelle* matrice de projection *pour $(x_1, \ldots, x_n)$ une matrice $P = (p_{ij})$ d'éléments de $\mathbf{A}$ qui vérifie les conditions* (1), (2), (3) *énoncées à la proposition 1.14.*

Dans la proposition 1.14 le point (1) signifie que P est une matrice de projection de rang ≤ 1. Donnons également des précisions sur les matrices des projections de rang exactement 1.

Proposition 1.16 *Soit une matrice carrée $P = (p_{ij}) \in \mathbf{A}^{n\times n}$. Notons P_i sa i-ème colonne.*

(1) *P est la matrice d'une projection de rang 1 si et seulement si sont vérifiées les deux propriétés*
   - $\forall i, j \;\; p_{ii}\, P_j = p_{jj}\, P_i$
   - $\sum_i p_{ii} = 1$

(2) *P est la matrice d'une projection sur un module libre de rang 1 si et seulement si il existe $x_1, \ldots, x_n$, $\alpha_1, \ldots, \alpha_n$ dans $\mathbf{A}$ tels que :*
   - $\forall i, j \;\; p_{ij} = \alpha_j\, x_i$
   - $\sum_i \alpha_i\, x_i = 1$

   Dans ce cas le vecteur colonne ${}^t(x_1, \ldots, x_n)$ est une base de l'image de P.

Un vecteur $(x_1, \ldots, x_n)$ comme dans (2) ci-dessus est appelé un *vecteur unimodulaire* : un vecteur est donc unimodulaire exactement lorsqu'il engendre un sous-module libre facteur direct.

1.4 Anneaux de petite dimension

Une définition constructive

La définition qui suit est constructive et équivalente à la définition classique usuelle (cf. [5, 14]).

Définition 1.17 *Un anneau $\mathbf{A}$ est dit* zéro-dimensionnel *(au sens de la dimension de Krull) si on a*

$$\forall x \in \mathbf{A} \;\; \exists n \in \mathbb{N} \;\; \exists a \in \mathbf{A} \quad x^n(1 - ax) = 0$$

Un anneau $\mathbf{A}$ est dit de dimension ≤ 1 *(au sens de la dimension de Krull) si on a*

$$\forall x, y \in \mathbf{A} \;\; \exists n \in \mathbb{N} \;\; \exists a, b \in \mathbf{A} \quad y^n(x^n(1 - ax) - by) = 0$$

Notez que tout quotient ou localisé d'un anneau zéro-dimensionnel (resp. de dimension ≤ 1) est automatiquement un anneau zéro-dimensionnel (resp. de dimension ≤ 1). Les résultats classiques suivants ont une preuve constructive facile (avec la définition 1.17) :

Lemme 1.18

- *Si $\mathbf{A}/\mathrm{N}(\mathbf{A})$ est zéro-dimensionnel (resp. de dimension ≤ 1) alors $\mathbf{A}$ également.*

– *Si* $\mathbf{A}$ *est zéro-dimensionnel (resp. de dimension* ≤ 1*) après localisation en des monoïdes comaximaux, alors il est zéro-dimensionnel (resp. de dimension* ≤ 1*).*

Anneaux zéro dimensionnels

Lorsque $x^n(1-ax) = 0$ dans un anneau $\mathbf{A}$, on a $x^{2n}a^n = x^n$ et l'élément $s = x^n a^n$ est un idempotent. Dans la composante $\mathbf{A}_s$, x est inversible et dans la composante $\mathbf{A}_{1-s}$, x est nilpotent. En fait $\mathbf{A}[1/x] = \mathbf{A}_s$. On en déduit immédiatement.

Lemme 1.19

– *Sur un anneau zéro-dimensionnel tout élément non diviseur de zéro est inversible (ceci revient à dire que l'anneau est égal à son anneau total des fractions).*

– *Sur un anneau zéro-dimensionnel tout élément du radical est nilpotent.*

– *Un anneau est local zéro-dimensionnel si et seulement si tout élément est inversible ou nilpotent.*

– *Un anneau zéro-dimensionnel réduit est un anneau quasi intègre. Bien mieux : tout idéal de type fini est engendré par un idempotent.*

– *Si* $\mathbf{A}$ *est quasi intègre l'anneau total des fractions de* $\mathbf{A}$ *est zéro-dimensionnel et quasi intègre.*

– *Un anneau est zéro-dimensionnel réduit si et seulement si il est quasi intègre et tout élément non diviseur de zéro est inversible.*

Preuve Pour le quatrième point il suffit de remarquer que tout idéal principal est engendré par un idempotent. □

Un anneau zéro-dimensionnel réduit est encore appelé un Von-Neuman regular ring dans la littérature anglaise. Cela ressemble beaucoup à un produit fini de corps. En pratique cela se comporte de la même manière.

La preuve suivante fournit une alternative (et une généralisation) sans doute plus simple pour la proposition 1.13.

Proposition 1.20 *Soit* $\mathbf{A} \subseteq \mathbf{B}$ *des anneaux avec* $\mathbf{A}$ *zéro-dimensionnel et* $\mathbf{B}$ *entier sur* $\mathbf{A}$*, alors* $\mathbf{B}$ *est zéro-dimensionnel.*

Preuve On suppose sans perte de généralité que $\mathbf{A}$ est réduit. Soit $x \in \mathbf{B}$ et $x^{n+1} + a_n x^n + \cdots + a_1 x + a_0 = 0$ une relation de dépendance intégrale de x sur $\mathbf{A}$. Notons r_i l'idempotent annulateur de a_i et $s_i = 1 - r_i$. Comme dans la preuve du lemme 1.11 on a le sfio $t_0 = s_0$, $t_1 = r_0 s_1$, $t_2 = r_0 r_1 s_2, \ldots$, $t_n = r_0 r_1 \cdots r_{n-1} s_n$, $t_{n+1} = r_0 r_1 \cdots r_n$. En outre chaque a_i est non diviseur de zéro donc inversible dans l'anneau $s_i\mathbf{A}$ et donc aussi dans la composante $t_i\mathbf{A}$. Cela donne :

$$t_i(x^{n+1} + a_n x^n + \cdots + a_i x^i) = 0\,.$$

Si $b_i a_i = s_i$ cela se réécrit après multiplication par b_i

$$\left(t_i b_i x^{n+1-i} + \cdots + t_i a_{i+1} b_i\right) x + t_i\big)\, x^i = 0$$

ce qui se réécrit, après multiplication par x^{n+1-i}

$$x^{n+1}(t_i + c_i\, x) = 0$$

L'addition de ces égalités pour $i = 0, \ldots, n+1$ fournit le résulltat cherché. □

Modules projectifs sur les anneaux zéro dimensionnels

Proposition 1.21 *Tout module projectif de type fini de rang constant sur un anneau zéro-dimensionnel est libre. Tout idéal projectif est engendré par un idempotent. Le seul idéal projectif de rang* 1 *est* $\langle 1\rangle$.

Preuve On considère une matrice de projection P avec $\det(\mathrm{I}+XP)=(1+X)^k$. Il faut montrer qu'elle se diagonalise en une matrice de projection standard.
1) Idée générale d'une preuve : on suppose d'abord l'anneau réduit. Si $\mathbf{A}$ était un corps discret, on aurait une procédure explicite pour cela. On exécute l'algorithme en remplaçant les branchements (gouvernés par des tests à 0) par des scindages (vu le lemme 1.19). A la fin on a cassé l'anneau en des composantes et dans chaque composante la diagonalisation a été obtenue avec le même rang. Tout ceci se recolle car les composantes de l'anneau sont totalement indépendantes les unes des autres. Si l'anneau n'est pas réduit, on obtient une diagonalisation modulo des nilpotents, ce qui se rectifie facilement en une diagonalisation usuelle. Si $v_1,\dots,v_n$ est la base "diagonale modulo des nilpotents", si $P(v_i)=v_i+\epsilon_i$ (avec des nilpotents pour coordonnées de ϵ_i), on remplace v_i par $u_i=v_i+\epsilon_i$, et si $P(v_j)=\epsilon_j$, on remplace v_j par $u_j=v_j-\epsilon_j$, et $u_1,\dots,u_n$ forme bien une base car le déterminant de la matrice des u_j sur les v_i est inversible (il est égal à $1+\epsilon$ avec ϵ nilpotent).
2) Preuve algorithmique plus précise et "plus rapide" dans le cas d'une matrice de rang 1. Appelons p_i la i-ème colonne de $P=(p_{ij})$. Notons s_i l'idempotent tel que $\mathbf{A}[1/p_{ii}]=\mathbf{A}_{s_i}$, avec $r_i=1-s_i$, et $r=\prod r_i$. Dans $\mathbf{A}_r$, tous les p_{ii} sont nilpotents, et leur somme égale à 1. Donc $\mathbf{A}_r$ est trivial et $r=0$. En raisonnant comme au lemme 1.11 on a le sfio $t_1=s_1$, $t_2=r_1s_2$, $t_3=r_1r_2s_3,\dots$, $t_{n+1}=r_1r_2\cdots r_n$, avec $x=t_1p_{11}+t_2p_{22}+\cdots+t_np_{nn}$ non diviseur de zéro (donc inversible). On en déduit que le vecteur $V=t_1p_1+\cdots+t_np_n=(v_1,\dots,v_n)$ est unimodulaire : $t_1v_1+\cdots+t_nv_n=x$, et V est une base de $\operatorname{Im}P$. On peut d'ailleurs si on veut diagonaliser la matrice P comme suit. Notons S_i la matrice obtenue à partir de I_n en échangeant les colonnes 1 et i. Soit $S=t_1\mathrm{I}_n+t_2S_2+\ldots+t_nS_n$. On a $S^2=I_n$ donc $\det(S)^2=1$ et $Q=S^{-1}PS$ a comme coefficient en position $(1,1)$ l'élément x non diviseur de zéro donc inversible. Si q_1 est le premier vecteur colonne de Q et si $(e_1,\dots,e_n)$ est la base canonique, on a une nouvelle base $(q_1,e_2,\dots,e_n)$. Comme $Q^2=Q$ et tous les mineurs d'ordre 2 sont nuls, par rapport à cette nouvelle base la matrice Q prend la forme

$$\begin{bmatrix}1&\alpha_2&\dots&\alpha_n\\0&0&\dots&0\\\vdots&\vdots&&\vdots\\0&0&\dots&0\end{bmatrix}$$

Et par rapport à la base $(q_1,e_2-\alpha_2q_1,\dots,e_n-\alpha_nq_1)$ on obtient la matrice canonique de projection de rang 1.
Enfin pour la toute dernière affirmation, on considère l'annulateur $\langle r\rangle$ de l'idéal I. Dans la composante $r\mathbf{A}$ on a $I=0$ et dans la composante $(1-r)\mathbf{A}$, l'idéal I est principal engendré par un x non diviseur de zéro donc inversible, en conclusion $I=\langle 1-r\rangle$. □

Remarque : En fait si M est un module projectif de type fini avec $R_M(X) = \sum_{k=0}^{n} r_k X^k$ on a $M \simeq \oplus_{k=0}^{n} r_k \mathbf{A}^k$ puisque $r_k M$ est libre de rang k sur $r_k\mathbf{A}$.

Vecteurs et matrices unimodulaires sur les anneaux zéro dimensionnels

Rappelons qu'un vecteur dans A^n est dit *unimodulaire* si ses coordonnées sont des éléments comaximaux. Une matrice carrée est dite *unimodulaire* si son déterminant est égal à 1. Les matrices carrées unimodulaires d'ordre n forment le groupe noté $\mathbf{SL}_n(\mathbf{A})$. Une matrice carrée est dite *élémentaire* si elle est obtenue à partir de la matrice identité en modifiant un coefficient non diagonal. Les matrices élémentaires engendrent un sous-groupe de $\mathbf{SL}_n(\mathbf{A})$, noté $\mathbf{E}_n(\mathbf{A})$ et appelé *groupe élémentaire*.

Si on a un homomorphisme surjectif $\mathbf{B} \to \mathbf{A}$ toute matrice de $\mathbf{E}_n(\mathbf{A})$ se relève en une matrice de $\mathbf{E}_n(\mathbf{B})$, ce qui ne marche pas en général pour les matrices unimodulaires.

Proposition 1.22 *Soit $n \geq 2$ et $(x_1, \ldots, x_n)$ un vecteur unimodulaire sur un anneau zéro-dimensionnel. Ce vecteur est la première colonne d'une matrice de $\mathbf{E}_n(\mathbf{A})$. En conséquence pour tout n $\mathbf{SL}_n(\mathbf{A}) = \mathbf{E}_n(\mathbf{A})$.*

Preuve Puisque le vecteur est unimodulaire, son annulateur est nul. Comme dans les preuves précédentes, on introduit un élément non diviseur de zéro $x = x_1 + t_2x_2 + t_3x_3 + \cdots + t_nx_n$. Par manipulations élémentaires le vecteur $(x_1, \ldots, x_n)$ est transformé en le vecteur $(x, x_2, \ldots, x_n)$, puis, comme x est inversible, en le vecteur $(x, 0, \ldots, 0)$, puis en le vecteur $(x, 1, \ldots, 0)$, et enfin en le vecteur $(1, 0, \ldots, 0)$. □

Dimension de Krull ≤ 1

Vérifions deux résultats classiques énoncés dans le lemme suivant lorsqu'on utilise la définition constructive 1.17.

Lemme 1.23 *Soit un anneau $\mathbf{A}$ de dimension ≤ 1 et u un non diviseur de zéro.*

(1) *L'anneau $\mathbf{A}/\langle u\rangle$ est zéro-dimensionnel.*

(2) *Si $z \in \mathrm{Rad}(\mathbf{A})$ il existe un entier n tel que $z^n \in \langle u\rangle$.*

Preuve

• Pour tout x on a une égalité $u^n(x^n(1-ax)-bu) = 0$ donc $x^n(1-ax)-bu = 0$ donc $x^n(1-ax) \equiv 0 \ mod\ u$.

• Dans l'égalité ci-dessus, si $x \in \mathrm{Rad}(\mathbf{A})$, $1-ax$ est inversible. □

La proposition suivante est un résultat classique qui résulte du "going up", mais nous sommes intéressés par une preuve constructive lorsqu'on utilise la définition 1.17.

Proposition 1.24 *Une extension entière d'un anneau de dimension ≤ 1 est un anneau de dimension ≤ 1.*

Il semble difficile de simplifier la preuve constructive (via le going up sous sa forme constructive générale) qu'on trouve dans [5] et cette dernière est trop longue pour être expliquée ici. Mais peut être on peut avoir une preuve simplifiée sous une hypothèse plus forte qui sera vérifiée dans nos applications, par exemple en supposant l'anneau de départ (voire les deux) quasi intègre ?

2 Idéaux localement principaux et idéaux inversibles

Définition 2.1 *Un idéal de type fini I d'un anneau $\mathbf{A}$ est dit* localement principal *s'il existe des monoïdes comaximaux $S_1, \ldots, S_n$ de $\mathbf{A}$ tels que chaque I_{S_j} est principal dans $\mathbf{A}_{S_j}$.*

Dans la suite, lorsque nous parlons d'un idéal localement principal nous sous-entendons toujours qu'il est de type fini.

2.1 Matrices de localisation principale

Définition 2.2 *Soient $x_1, \ldots, x_n$ des éléments de $\mathbf{A}$. On apppelle* matrice de localisation principale (dans $\mathbf{A}$) *pour $(x_1, \ldots, x_n)$ une matrice $A = (a_{ij})$ d'éléments de $\mathbf{A}$ qui vérifie :*

$$\left\{ \begin{array}{lll} \alpha) & \sum a_{ii} = 1 & \\ \beta) & a_{\ell j} x_i = a_{\ell i} x_j & \forall\, i, j, \ell \in \{1, \ldots, n\} \end{array} \right. \tag{7}$$

Remarquez que l'idéal $I = \langle x_1, \ldots, x_n \rangle$ devient principal, égal à $\langle x_i \rangle$, après localisation en a_{ii}. La condition "I est localement principal" équivaut en Mathématiques classiques à la localisation en n'importe quel idéal premier P, car l'un des a_{ii} au moins n'appartient pas à P, et dans $\mathbf{A}_P$ qui est un des localisés de $\mathbf{A}_{a_{ii}}$, on a $I = \langle x_i \rangle$.
Remarquez aussi que les conditions $\beta)$ signifient que les lignes de la matrice A sont "proportionnelles" à $(x_1, \ldots, x_n)$.

Remarque : Dans le cas intègre et si la divisibilité est explicite, on a la situation suivante. Si les x_i sont tous non nuls, pour connaître la matrice A il suffit de se donner les éléments diagonaux a_{ii}, lesquels doivent vérifier : $\sum_i a_{ii} = 1$, et $a_{ii} x_j$ multiplede x_i pour tous i, j, ce qui donne les a_{ij}. En effet, pour vérifier que l'égalité $a_{\ell j} x_i = a_{\ell i} x_j$ a bien lieu, il suffit de la multiplicer par x_ℓ. Si maintenant certains des x_i sont nuls mais pas tous, on peut supposer sans perte de généralité que les lignes et colonnes correspondantes sont nulles, et la matrice ne concerne en fait que les x_i non nuls.

Lemme 2.3 *Soit $I = \langle x_1, \ldots, x_n \rangle$ un idéal de type fini. Si I est principal, alors $(x_1, \ldots, x_n)$ admet une matrice de localisation principale.*

Preuve : Supposons $I = \langle x_1, \ldots, x_n \rangle = \langle g \rangle$. 0n a $g = \sum_{i=1}^n u_i x_i$ et $x_i = g y_i$. Posons $b_{ij} = u_i y_j$, alors pour tous $i, j, \ell \in \{1, \ldots, n\}$ on a $b_{\ell j}\, x_i = u_\ell\, g\, y_i\, y_j = b_{\ell i}\, x_j$. En outre

$$x_i \left(\sum_{k=1}^n b_{kk} \right) = \sum_{k=1}^n u_k\, y_k\, g\, y_i = y_i \left(\sum_{k=1}^n u_k\, x_k \right) = y_i\, g = x_i$$

Donc

$$\left(1 - \sum_{k=1}^n b_{kk} \right) x_i = 0, \text{ et } 1 - \sum_{k=1}^n b_{kk} \in \mathrm{Ann}(x_i) \text{ pour tout } i.$$

Soit $c = 1 - \sum_{k=1}^n b_{kk}$. Prenons $a_{ij} = b_{ij}$ pour $(i, j) \neq (n, n)$ et $a_{nn} = b_{nn} + c$, alors (a_{ij}) est bien une matrice de localisation principale pour $(x_1, \ldots, x_n)$. □

Proposition 2.4 *Soit $I = \langle x_1, \dots, x_n \rangle$ un idéal de type fini. L'idéal I est localement principal si et seulement si $(x_1, \dots, x_n)$ admet une matrice de localisation principale.*

Preuve : La condition est clairement suffisante. Montrons qu'elle est nécessaire. Le système linéaire qui définit la matrice de localisation principale a une solution localement, donc aussi globalement (principe local-global de base). Ceci termine la preuve.
Rappelons comment cela fonctionne. L'idéal I est localement principal, donc il existe des monoïdes comaximaux $S_1, \dots, S_m$ dans $\mathbf{A}$ tels que $(x_1, \dots, x_n)$ admet une matrice de localisation principale (a^i_{kl}) dans $\mathbf{A}_{S_i}$ pour tout $i \in \{1, \dots, m\}$, c'est-à-dire :

$$\text{dans } \mathbf{A}_{S_i} \quad \left\{ \begin{array}{rcll} \sum_{k=1}^n a^i_{kk} & = & 1 & \\ a^i_{\ell k} x_j & = & a^i_{\ell j} x_k & \forall\, j,k,\ell \in \{1,\dots,n\} \end{array} \right.$$

Donc il existe $s_i \in S_i$ tel que

$$\text{dans } \mathbf{A} \quad \left\{ \begin{array}{rcll} s_i \sum_{k=1}^n a^i_{kk} & = & s_i & \\ s_i\, a^i_{\ell k} x_j & = & s_i\, a^i_{\ell j} x_k & \forall\, j,k,\ell \in \{1,\dots,n\} \end{array} \right.$$

On considère $u_1, \dots, u_m \in \mathbf{A}$ tels que $\sum_{i=1}^m s_i u_i = 1$, et on pose $a_{jk} = \sum_{i=1}^m s_i\, a^i_{jk}$. La matrice (a_{jk}) est alors une matrice de localisation principale dans $\mathbf{A}$ pour $(x_1, \dots, x_n)$. □

Un corollaire immédiat et important est qu'un idéal localement principal reste localement principal dans tout quotient, tout localisé, toute extension de l'anneau de base (et même dans toute extension d'un sous anneau qui contient à la fois les générateurs et leur matrice de localisation principale). Enonçons ceci sous forme d'un fait.

Fait 2.5 *Soit $I = \langle x_1, \dots, x_n \rangle$ un idéal localement principal et (a_{ij}) une matrice de localisation principale pour $(x_1, \dots, x_n)$. Soit $\mathbf{A}_1$ le sous anneau de $\mathbf{A}$ engendré par les x_i et les a_{ij}, et $\varphi : \mathbf{A}_1 \to \mathbf{B}$ un homomorphisme d'anneaux. Alors $\langle \varphi(x_1), \dots, \varphi(x_n) \rangle$ est localement principal dans $\mathbf{B}$.*

Proposition 2.6 *Soit $I = \langle x_1, \dots, x_n \rangle$ un idéal localement principal de $\mathbf{A}$ et $A = (a_{ij})$ une matrice de localisation principale pour $(x_1, \dots, x_n)$. Alors nous avons les résultats suivants :*

1. $(x_1, \dots, x_n)\, A = (x_1, \dots, x_n)$
2. *x_i annule tout mineur d'ordre 2 de A, et $x_i(A^2 - A) = 0$ pour tout i, donc $\langle x_1, \dots, x_n \rangle (A^2 - A) = 0$*
3. *Si $\mathbf{A}_i = \mathbf{A}[1/a_{ii}]$ est le localisé obtenu en rendant a_{ii} inversible, on a $I\mathbf{A}_i = \langle x_i \rangle_{\mathbf{A}_i}$.*
4. $\langle x_1, \dots, x_n \rangle\, \langle a_{1j}, \dots, a_{nj} \rangle = \langle x_j \rangle$.
5. *Plus généralement, si $a = \sum \alpha_i x_i$ et ${}^t(y_1, \dots, y_n) = A\, {}^t(\alpha_1, \dots, \alpha_n)$ alors $\langle x_1, \dots, x_n \rangle \langle y_1, \dots, y_n \rangle = \langle a \rangle$. En outre si $\mathrm{Ann}(I) = 0$ la matrice ${}^tA$ est une matrice de localisation principale pour $(y_1, \dots, y_n)$.*
6. *En particulier si $\sum \alpha_i x_i = 0$ et ${}^t(y_1, \dots, y_n) = A\, {}^t(\alpha_1, \dots, \alpha_n)$, alors $\langle x_1, \dots, x_n \rangle \langle y_1, \dots, y_n \rangle = 0$.*

(7) *Soit* $\underline{x} : (\alpha_i) \mapsto \sum_i \alpha_i x_i$ *la forme linéaire associée à* $(x_1, \ldots, x_n)$, $N = \mathrm{Ann}\,\langle x_1, \ldots, x_n\rangle$ *et* $N^{(n)}$ *le produit cartésien* $\{(\nu_1, \ldots, \nu_n) \mid \&_i\,(\nu_i \in N)\} \subseteq A^n$, *alors* $\mathrm{Ker}\,\underline{x} = \mathrm{Im}(\mathrm{I}_n - A) + N^{(n)}$.

(8) *Pour tout* $i = 1, \ldots, n-1$ *l'intersection* $\langle x_1, \ldots, x_i\rangle \cap \langle x_{i+1}, \ldots, x_n\rangle$ *est l'idéal de type fini engendré par les* n *coordonnées de* $(x_1, \ldots, x_i, 0, \ldots 0)\,(\mathrm{I}_n - A)$.

Preuve : Le (3) est clair, le (4) et le (6) sont des cas particuliers du (5).
(1) le j-ème élément de $(x_1, \ldots, x_n)\,A$ s'écrit :

$$\sum\nolimits_{i=1}^{n} a_{ij}x_i \;=\; \sum\nolimits_{i=1}^{n} a_{ii}x_j \;=\; x_j$$

(2) Montrons que x_i annule tout mineur d'ordre 2 de A :

$$x_i(a_{j\ell}\,a_{kh} - a_{jh}\,a_{k\ell}) \;=\; a_{ji}\,x_\ell\,a_{kh} - a_{ji}\,x_h\,a_{k\ell} \;=\; a_{ji}\,a_{k\ell}\,x_h - a_{ji}\,x_h\,a_{k\ell} \;=\; 0.$$

Posons $A^2 = (b_{ij})$, avec $b_{ij} = \sum_{k=1}^{n} a_{ik}a_{kj}$. Alors $x_h(b_{ij} - a_{ij}) = (\sum_{k=1}^{n} a_{ik}a_{kj}x_h) - a_{ij}x_h$. Or $x_h a_{ik}a_{kj} = x_h a_{ij}a_{kk}$, donc

$$x_h(b_{ij} - a_{ij}) \;=\; x_h a_{ij}\left(\sum\nolimits_{k=1}^{n} a_{kk}\right) - a_{ij}x_h \;=\; 0.$$

(5) Notons que $a_{ii}\,a \;=\; \sum_j \alpha_j\,x_j\,a_{ii} \;=\; \sum_j \alpha_j\,x_i\,a_{ij} \;=\; \left(\sum_j \alpha_j\,a_{ij}\right) x_i \;=\; y_i\,x_i$ donc $a = \sum y_i x_i$, et $a \in \langle x_1, \ldots, x_n\rangle\,\langle y_1, \ldots, y_n\rangle$. D'autre part,

$$x_i\,y_j = x_i \sum\nolimits_k \alpha_k\,a_{jk} = \sum\nolimits_k \alpha_k\,a_{ji}\,x_k = \left(\sum\nolimits_k \alpha_k\,x_k\right) a_{ji} = a_{ji}\,a$$

donc $x_i y_j \in \langle a\rangle$.
Montrons enfin que ${}^tA$ est une matrice de localisation principale pour $(y_1, \ldots, y_n)$ si $\mathrm{Ann}(I) = 0$. En effet d'une part la trace est égale à 1 et d'autre part, puisque x_h annule tout mineur d'ordre 2 de A on obtient

$$x_h\,a_{ji}\,y_k \;=\; \sum\nolimits_k x_h\,a_{ji}\,a_{k\ell}\,\alpha_\ell \;=\; \sum\nolimits_k x_h\,a_{ki}\,a_{j\ell}\,\alpha_\ell \;=\; x_h\,a_{ki}\sum\nolimits_k a_{j\ell}\,\alpha_\ell \;=\; x_h\,a_{ki}\,y_j.$$

(7) L'inclusion $\mathrm{Ker}\,\underline{x} \subseteq \mathrm{Im}(\mathrm{I}_n - A) + N^{(n)}$ résulte du (6) et l'inclusion réciproque de (1).
(8) Résulte du (7) en remarquant que se donner un élément a de $J = \langle x_1, \ldots, x_i\rangle \cap \langle x_{i+1}, \ldots, x_n\rangle$ revient à se donner un élément $(\alpha_1, \ldots, \alpha_n)$ de $\mathrm{Ker}\,\underline{x}$: $a = \alpha_1 x_1 + \cdots + \alpha_i x_i = -\alpha_{i+1}x_{i+1} - \cdots - \alpha_n x_n$. Ainsi J est engendré par les coordonnées du vecteur $(z_1, \ldots, z_n) = (x_1, \ldots, x_i, 0, \ldots, 0)\,(\mathrm{I}_n - A)$. □

Produit de deux idéaux localement principaux

Proposition 2.7 *Soient* I *et* J *deux idéaux localement principaux engendrés respectivement par* n *et* m *éléments. Alors* IJ *est localement principal engendré par* $n + m - 1$ *éléments. Plus précisément, si* g *et* h *sont les polynômes dont les coefficients sont des générateurs de* I *et* J, *alors* IJ *est engendré par les coefficients du polynôme* $f = gh$.

Preuve Si $I = \langle x_1, \dots, x_n \rangle$, $J = \langle y_1, \dots, y_m \rangle$, si (a_{ij}) est une matrice de localisation principale pour $(x_1, \dots, x_n)$ et $(b_{k\ell})$ est une matrice de localisation principale pour $(y_1, \dots, y_m)$ alors la matrice des $c_{(ij)(k\ell)} = a_{ij}b_{k\ell}$ est une matrice de localisation principale pour les $x_j y_\ell$. En effet :

$$c_{(ij)(k\ell)}x_m y_n = a_{ij}b_{k\ell} = a_{im}b_{kn}x_j y_\ell = c_{(im)(kn)}x_j y_\ell$$

$$\text{et} \quad \sum_{i,j} c_{(ii)(jj)} = \sum_{i,j} a_{ii}b_{jj} = \left(\sum_{i=1}^{n} a_{ii}\right)\left(\sum_{j=1}^{m} b_{jj}\right) = 1$$

Donc IJ est localement principal.
Soit $(z_1, \dots, z_p)$ le vecteur des coefficients de f. On veut montrer que $IJ = \langle z_1, \dots, z_p \rangle$. Si les S_i (resp. les S'_k) sont des monoïdes comaximaux tels que $I_{S_i} = \langle x_i \rangle_{S_i}$ (resp. $J_{S'_k} = \langle y_k \rangle_{S'_k}$), alors les $S_i S'_k$ sont des monoïdes comaximaux et on a $(IJ)_{S_i S'_k} = \langle x_i y_k \rangle_{S_i S'_k}$. Dans un tel localisé on a $g = x_i g_i$, $h = y_k h_k$, avec les polynômes g_i et h_k qui ont un coefficient égal à 1. Un lemme classique[2] dit alors que l'idéal des coefficients de $g_i h_k$ est égal à $\langle 1 \rangle$. Donc l'idéal des coefficients de gh est égal à $\langle x_i y_k \rangle$, c'est-à-dire à $(IJ)_{S_i S'_k}$. L'égalité $IJ = \langle z_1, \dots, z_p \rangle$ a donc été prouvée dans tous les localisés et elle est vraie globalement. □

A titre d'exemple, explicitons la matrice de localisation principale sur le nouveau système générateur dans le cas où $n = m = 2$.
Supposons $I = \langle x_1, x_2 \rangle$ et $J = \langle y_1, y_2 \rangle$. Soit respectivement

$$A = \begin{bmatrix} s & v \\ w & t \end{bmatrix} \quad B = \begin{bmatrix} s' & v' \\ w' & t' \end{bmatrix}$$

des matrices de localisation principale pour (x_1, x_2) et (y_1, y_2) .
On a $s + t = 1, s' + t' = 1$ et $ss' + st' + s't + tt' = 1$
$IJ = \langle x_1, x_2 \rangle \langle y_1, y_2 \rangle = \langle x_1 y_1, x_1 y_2 + x_2 y_1, x_2 y_2 \rangle = \langle z_1, z_2, z_3 \rangle$.
Dans l'anneau localisé $\mathbf{A}_{ss'}$ on a $IJ = \langle x_1 y_1 \rangle$. On a les relations correspondantes dans $\mathbf{A}$:

$$\begin{cases} ss'(x_1 y_2 + x_2 y_1) = (sv' + vs')x_1 y_1 \\ ss' x_2 y_2 = vv' x_1 y_1 \end{cases}$$

Donc une matrice de localisation principale pour $(x_1 y_1, x_1 y_2 + x_2 y_1, x_2 y_2)$ dans $\mathbf{A}_{ss'}$ est

$$M_{ss'} = \begin{bmatrix} 1 & \dfrac{sv' + vs'}{ss'} & \dfrac{vv'}{ss'} \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

Dans $\mathbf{A}_{tt'}$, $IJ = \langle x_2 y_2 \rangle$, et on a les relations correspondantes dans $\mathbf{A}$:

$$\begin{cases} tt' x_1 y_1 = ww' x_2 y_2 \\ tt'(x_1 y_2 + x_2 y_1) = (wt' + w't)x_2 y_2 \end{cases}$$

[2] Si les coefficients de g et ceux de h sont comaximaux il en est de même pour les coefficients de gh : on peut trouver une preuve constructive dans [17].

Une matrice de localisation principale pour $(x_1y_1, x_1y_2 + x_2y_1, x_2y_2)$ dans $\mathbf{A}_{tt'}$ est

$$M_{tt'} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ \dfrac{ww'}{tt'} & \dfrac{wt' + w't}{tt'} & 1 \end{bmatrix}$$

Dans $\mathbf{A}_{st'}$, $IJ = \langle x_1y_2 \rangle$, on peut exprimer les 3 générateurs z_i comme multiples de x_1y_2, et x_1y_2 comme combinaison linéaire des z_i. Cela donne dans $\mathbf{A}$:

$$\begin{cases} st'x_1y_1 &= sw'x_1y_2 \\ st'(x_1y_2 + x_2y_1) &= (st' + vw')x_1y_2 \\ st'x_2y_2 &= vt'x_1y_2 \\ st'(x_1y_2 + x_2y_1) &= st'x_1y_2 + vt'x_1y_1, \quad \text{donc} \\ st'x_1y_2 &= -vt'x_1y_1 + st'(x_1y_2 + x_2y_1) \end{cases}$$

D'apres la proposition 2.3, la matrice

$$M_{st'} = \begin{bmatrix} -\dfrac{vw'}{st'} & -\dfrac{v(st' + vw')}{s^2t'} & -\dfrac{v^2}{s^2} \\ \dfrac{w'}{t'} & \dfrac{st' + vw'}{st'} & \dfrac{v}{s} \\ 0 & 0 & 0 \end{bmatrix}$$

est une matrice de localisation principale pour $(x_1y_1, x_1y_2 + x_2y_1, x_2y_2)$ dans $\mathbf{A}_{st'}$. Enfin dans l'anneau $\mathbf{A}_{s't}$, $I\,J = \langle x_2y_1 \rangle$. On a de la même façon dans $\mathbf{A}$:

$$\begin{cases} s'tx_1y_1 &= s'wx_2y_1 \\ s't(x_1y_2 + x_2y_1) &= (v'w + s't)x_1y_2 \\ s'tx_2y_2 &= v'tx_1y_2 \\ s't(x_1y_2 + x_2y_1) &= v'tx_1y_1 + s'tx_2y_1, \qquad \text{donc} \\ s'tx_2y_1 &= -v'tx_1y_1 + st'(x_1y_2 + x_2y_1) \end{cases}$$

D'après la proposition 2.3, comme matrice de localisation principale pour $(x_1y_1, x_1y_2 + x_2y_1, x_2y_2)$ dans $\mathbf{A}_{st'}$ on a

$$M_{s't} = \begin{bmatrix} -\dfrac{v'w}{s't} & -\dfrac{v'(s't + v'w)}{s'^2t} & -\dfrac{v'^2}{s'^2} \\ \dfrac{w}{t} & \dfrac{s't + v'w}{s't} & \dfrac{v'}{s'} \\ 0 & 0 & 0 \end{bmatrix}$$

Puisque $ss' + st' + s't + tt' = 1$, on obtient $ss' + s(s + t)t' + s'(s' + t')t + tt' = 1$ et $ss' + s^2t' + s'^2t + tt'(1 + s + s') = 1$. Donc on a la matrice suivante à coefficients dans $\mathbf{A}$: $M = s\,s'\,M_{ss'} + s^2\,t'\,M_{st'} + s'^2\,t\,M_{s't} + t\,t'(1 + s + s')\,M_{tt'}$. Précisément :

$$M = \begin{bmatrix} ss' - svw' - s'v'w & s(v' + vt') + s'(v + v't) - v^2w' - v'^2w & vv' + v^2t' + v'^2t \\ s^2w' + s'^2w & s(st' + vw') + s'(s't + v'w) & vst' + v's't \\ ww'(s + s' + 1) & (wt' + w't)(s + s' + 1) & tt'(s + s' + 1) \end{bmatrix}.$$

Et par construction la matrice M est une matrice de localisation principale dans $\mathbf{A}$ pour le système générateur (z_1, z_2, z_3) de IJ.

Puissances d'un idéal localement principal

Lemme 2.8 *Soit* $I = \langle x_1, \dots, x_k \rangle$ *un idéal localement principal, alors* $I^n = \langle x_1^n, \dots, x_k^n \rangle$.

Preuve On raisonne comme pour la proposition 2.7. L'égalité est vraie localement donc aussi globalement. □

En fait si une matrice de localisation principale pour $(x_1, \dots, x_k)$ est (a_{ij}) alors une matrice de localisation principale pour $(x_1^n, \dots, x_k^n)$ peut être obtenue comme suit. On pose $D = k(n-1)+1$. On peut trouver des c_i tels que

$$1 = (a_{11} + \cdots + a_{kk})^D = c_1(a_{11})^n + \cdots + c_k(a_{kk})^n$$

On pose $b_{\ell i} = c_\ell (a_{\ell i})^n$. Il vient $b_{11} + \cdots + b_{kk} = 1$ et $b_{\ell i}(x_j)^n = c_\ell (a_{\ell i} x_j)^n = c_l (a_{\ell j} x_i)^n = b_{\ell j}(x_i)^n$ donc (b_{ij}) est une matrice de localisation principale pour $(x_1^n, \dots, x_k^n)$.

En outre on peut donner une expression de $x_1^{n_1} \times \cdots \times x_k^{n_k}$ en fonction des $(x_i)^n$ lorsque $n = n_1 + \cdots + n_k$:

$$\begin{array}{rcl@{\qquad}rcl} x_1^{n_1} \cdots x_k^{n_k} & = & \sum_{i=1}^n b_{ii}\, x_1^{n_1} \cdots x_k^{n_k} & = & \sum_{i=1}^n c_i\, (a_{ii}x_1)^{n_1} \cdots (a_{ii}x_k)^{n_k} \\ & = & \sum_{i=1}^n c_i\, (a_{i1}x_i)^{n_1} \cdots (a_{ik}x_i)^{n_k} & = & \sum_{i=1}^n [c_i a_{i1}^{n_1} \cdots a_{ik}^{n_k}]\, x_i^n \end{array}$$

Intersection de deux idéaux de type fini dont la somme est un idéal localement principal

Lemme 2.9 *Soient* I *et* J *deux idéaux de type fini avec* $I+J$ *localement principal. L'intersection* $I \cap J$ *est un idéal de type fini qui vérifie*

$$(I \cap J)(I + J) = IJ.$$

Si en outre I *et* J *sont localement principaux alors* $I \cap J$ *est localement principal.*

Preuve Soit $I = \langle x_1, \dots, x_n \rangle$ et $J = \langle y_1, \dots, y_m \rangle$. L'idéal $I \cap J$ est de type fini d'après la proposition 2.6 (8). Considérons une localisation où $I + J$ est (par exemple) engendré par x_1. Alors $I_S = \langle x_1 \rangle$, $J_S \subseteq \langle x_1 \rangle = I_S$, $(I \cap J)_S = J_S$ et $(I+J)_S = I_S$. Ainsi l'égalité $(I \cap J)(I+J) = IJ$ est une égalité entre idéaux de type fini qui est vérifiée localement (en des monoïdes comaximaux) donc globalement. Enfin avec le même raisonnement si en outre I et J sont localement principaux, on voit que $I \cap J$ est principal. □

Remarque : Si A est une matrice de localisation principale pour (x_1, x_2) on a $\langle x_1 \rangle \cap \langle x_2 \rangle = \langle y_1, y_2 \rangle$ avec ${}^t(y_1, y_2) = A\, {}^t(x_2, 0) = A\, {}^t(0, x_1)$, et on vérifie que ${}^tA$ est une matrice de localisation principale pour (y_1, y_2).

2.2 Idéaux projectifs de type fini

Proposition 2.10 *Soit* $\underline{x} = (x_1, \dots, x_n) \in \mathbf{A}^{1\times n}$ *une forme linéaire* $\mathbf{A}^n \to \mathbf{A}$. *On suppose que* $I = \langle x_1, \dots, x_n \rangle$ *est localement principal et que* $\operatorname{Ann} I = \langle r \rangle$ *avec* r *idempotent. Soit* A *une matrice de localisation principale pour* $(x_1, \dots, x_n)$, $s = 1 - r$ *et* $P = \mathrm{I}_n - sA$.
Alors P *est une matrice de projection qui vérifie* $\operatorname{Im} P = \operatorname{Ker} \underline{x}$, *et* $\operatorname{Ker} P \simeq \operatorname{Coker} P \simeq \operatorname{Im} \underline{x} = I$. *En particulier* I *est projectif de rang* ≤ 1.

Preuve On vérifie immédiatement que sA est une matrice de projection pour $(x_1, \ldots, x_n)$ (cf. définition 1.15) et on applique la proposition 1.14. □

Le corollaire suivant est une conséquence immédiate des propositions 1.14 et 2.10.

Corollaire 2.11

- *Un idéal de type fini I est un module projectif si et seulement si il est localement principal et son annulateur est engendré par un idempotent.*
- *Plus précisément les rapports entre une matrice de localisation principale A et une matrice de projection A' pour un vecteur $(x_1, \ldots, x_n)$ sont les suivants. Si A est connue et si $\mathrm{Ann}\,\langle x_1, \ldots, x_n\rangle = \langle r\rangle$ (r idempotent), alors on peut prendre $A' = (1-r)\,A$. Si A' est connue, alors $\mathrm{Ann}\,\langle x_1, \ldots, x_n\rangle = \langle r\rangle$ avec $r = 1 - \mathrm{Tr}(A')$ et une matrice de localisation principale A est obtenue en rajoutant r à l'un quelconque des coefficients diagonaux de A'.*
- *Un idéal de type fini I est un module projectif de rang 1 si et seulement si il est localement principal et son annulateur est réduit à 0.*

Lemme 2.12 *Si I et J sont des idéaux projectifs d'un anneau $\mathbf{A}$, IJ également, et il est isomorphe à $I \otimes_{\mathbf{A}} J$.*

Preuve Voyons d'abord le cas où I et J sont de rang 1. On sait que IJ est localement principal (proposition 2.7) et il est clair que son annulateur est réduit à 0, donc c'est un projectif de rang 1. L'homomorphisme $I \otimes_{\mathbf{A}} J \to IJ : x \otimes y \mapsto xy$ est alors un homomorphisme surjectif entre modules projectif de type fini de même rang. C'est donc un isomorphisme. Le cas général se ramène au cas précédent. □

On a la propriété de simplification suivante.

Lemme 2.13 *Si I est projectif de rang 1, si J et J' sont deux idéaux tels que $IJ \subseteq IJ'$ (resp. $IJ = IJ'$) alors $J \subseteq J'$ (resp. $J = J'$).*

Preuve C'est un determinant trick. Soit en effet $I = \langle x_1, \ldots, x_n\rangle$, $X = {}^t(x_1, \ldots, x_n)$, A une matrice de localisation principale pour $(x_1, \ldots, x_n)$, $P = \mathrm{I}_n - A$ et $a \in J$. Puisque $aI \subseteq IJ'$, il existe une matrice M à coefficients dans J' telle que $aX = MX$. L'image de $a\mathrm{I}_n - {}^tM$ annule la forme linéaire associée à $(x_1, \ldots, x_n)$ donc $P\,(a\mathrm{I}_n - {}^tM) = a\mathrm{I}_n - {}^tM$, $a\,A = a\,(\mathrm{I}_n - P) = (\mathrm{I}_n - P)\,{}^tM$ est une matrice à coefficients dans J'. Enfin $a = \mathrm{Tr}(aA)$. □

Nous avons aussi un analogue du fait 2.5.

Fait 2.14 *Soit $I = \langle x_1, \ldots, x_n\rangle$ un idéal projectif de type fini et (a_{ij}) une matrice de projection pour $(x_1, \ldots, x_n)$. Soit $\mathbf{A}_1$ un sous anneau de $\mathbf{A}$ contenant les x_i et les a_{ij}, S un monoïde de $\mathbf{A}_1$ et $\mathbf{B} = S^{-1}\mathbf{A}_1$ le localisé de $\mathbf{A}_1$ en S. Alors $\langle x_1, \ldots, x_n\rangle$ est projectif dans $\mathbf{B}$.*

Remarque : On aurait pu prendre plus généralement pour $\mathbf{B}$ une extension plate de $\mathbf{A}_1$. Mais une extension arbitraire de $\mathbf{A}_1$ ne marcherait pas. Par exemple sur l'anneau $\mathbf{B} = \mathbf{A}/I$ l'idéal I reste localement principal mais devient nul : en tant que $\mathbf{A}$-module, I pourrait subir le changement d'anneau $\mathbf{A} \to \mathbf{B}$ et deviendrait un $\mathbf{B}$-module projectif de rang 1, donc pas du tout isomorphe à $I\,\mathbf{B}$.

2.3 Idéaux inversibles

Définition 2.15 *Un idéal I d'un anneau $\mathbf{A}$ est dit* inversible *si il existe un idéal J de $\mathbf{A}$ et un non diviseur de zéro $a \in \mathbf{A}$ tels que $IJ = \langle a \rangle$.*

NB : Si a est fixé, J est unique car $IJ = IJ_1 = \langle a \rangle$ implique $IJJ_1 = aJ = aJ_1$. Par ailleurs, si $a_1, \ldots, a_k \in I$, $b_1, \ldots, b_k \in J$ et $a_1b_1 + \cdots + a_kb_k = a$ alors $I' = \langle a_1, \ldots, a_k \rangle \subseteq I$, $J' = \langle b_1, \ldots, b_k \rangle \subseteq J$, et $\langle a \rangle \subseteq I'J' \subseteq IJ = \langle a \rangle$. Donc $IJ = IJ' = I'J$ ce qui implique $I = I'$ et $J = J'$. En particulier tout idéal inversible est de type fini.

Proposition 2.16 *Un idéal I est inversible si et seulement si il est de type fini, localement principal, et contient un non diviseur de zéro. Un idéal inversible est un module projectif de type fini de rang 1.*

Preuve :
• Si I est de type fini, localement principal, et contient un non diviseur de zéro a, alors il est inversible d'après le point (5) de la proposition 2.6. C'est un module projectif de type fini de rang 1 d'après le corollaire 2.11.
• Supposons I inversible. On a vu juste avant que I est de type fini. Reprenons les mêmes notations et montrons que $I = \langle a_1, \ldots, a_k \rangle$ est localement principal : on a $a_jb_\ell = c_{\ell j}a$ et on vérifie immédiatement que la matrice (c_{ij}) est une matrice de localisation principale pour $(a_1, \ldots, a_k)$, car les égalités qu'on doit vérifier sont vraies après multiplication par a. □

Remarques : Les idéaux inversibles sont donc des idéaux projectifs de rang 1, et il n'y a pas de différence entre une matrice de localisation principale et une matrice de projection pour un système générateur d'un idéal inversible.
Il serait intéressant de caractériser les anneaux pour lesquels tout idéal projectif de rang 1 est inversible (ce qui revient à dire qu'il contient un non diviseur de zéro).

Nous avons un analogue des faits 2.5 et 2.14.

Fait 2.17 *Soit $I = \langle x_1, \ldots, x_n \rangle$ un idéal inversible de $\mathbf{A}$ avec $x \in I$ non diviseur de zéro, et (a_{ij}) une matrice de localisation principale pour $(x_1, \ldots, x_n)$. Soit $\mathbf{A}_1$ un sous anneau de $\mathbf{A}$ contenant les x_i, x et les a_{ij}, et $\varphi : \mathbf{A}_1 \to \mathbf{B}$ un homomorphisme d'anneaux. Supposons que $\varphi(x)$ soit non diviseur de zéro dans $\mathbf{B}$ (par exemple si $\mathbf{B}$ est un localisé de $\mathbf{A}$ ou si $\mathbf{A} \subset \mathbf{B}$ intègre). Alors l'idéal $\langle \varphi(x_1), \ldots, \varphi(x_n) \rangle$ est inversible dans $\mathbf{B}$.*

Un exemple important d'idéaux maximaux inversibles

Nous donnons maintenant un exemple standard d'idéaux inversibles dans des extensions algébriques.

Proposition 2.18 *Soit $\mathbf{A}$ un anneau intègre, P un idéal maximal inversible, $\mathbf{K}$ le corps de fractions de $\mathbf{A}$ et $f(X) \in \mathbf{A}[X]$ un polynôme irréductible de $\mathbf{K}[X]$. On suppose que sur le corps résiduel $\mathbf{F}_P = \mathbf{A}/P$ le polynôme f se factorise en un produit de polynômes irréductibles (unitaires) deux à deux distincts : $f(X) = \prod_i g_i(X)$ sur $\mathbf{F}_P[X]$. Soit $\mathbf{B} = \mathbf{A}[x] = \mathbf{A}[X]/\langle f(X) \rangle$ (c'est un sous anneau de $\mathbf{L} = \mathbf{K}[x] = \mathbf{K}[X]/\langle f(X) \rangle$). Alors dans $\mathbf{B}$ l'idéal $P\mathbf{B}$ est égal au produit des idéaux $\langle g_i(x), P \rangle = Q_i$. Ces idéaux sont maximaux et inversibles.*

Preuve On constate facilement que les Q_i sont deux à deux comaximaux. Donc $\prod_i Q_i = \bigcap_i Q_i$. Par ailleurs, en tant que treillis, le treillis des idéaux contenant $P\mathbf{B}$ est isomorphe au trillis des idéaux de $\mathbf{B}/P\mathbf{B} \simeq \mathbf{A}[X]/\langle P, f(X)\rangle \simeq \mathbf{F}_P[X]/\langle f(X)\rangle$, donc les Q_i sont des idéaux maximaux de $\mathbf{B}$ et $\bigcap_i Q_i = P\mathbf{B}$. On conclut en remarquant que $P\mathbf{B}$ est inversible dans $\mathbf{B}$ (cf. le fait 2.17). □

"Quotient" d'un idéal de type fini par un idéal localement principal qui le contient

Proposition 2.19 *Soient I et J deux idéaux de type fini tels que $I \subseteq J$ et J localement principal. Alors il existe un idéal de type fini K, tel que $I = JK$. Si J est inversible, K est unique, on notera alors : $K = I \div J$. Si en outre I et localement principal, et I et J sont engendrés respectivement par n et m éléments, alors $I \div J$ est engendré par $n+m-1$ éléments.*

Preuve :
(1) Si $I = \langle x_1, \ldots, x_n\rangle$ pour chaque i on trouve K_i tel que $JK_i = \langle x_i\rangle$ en appliquant 2.6 (5). Ensuite K est la somme des K_i.
(2) Quotient de I par J lorsque J est inversible : il existe un non diviseur de zéro $a \in J$, et $J_1 \subseteq \mathbf{A}$ tels que $JJ_1 = \langle a\rangle$. Or $I = JK$, et $IJ_1 = JKJ_1 = aK$, donc IJ_1 est engendré par $n+m-1$ éléments (proposition 2.7). Supposons $IJ_1 = \langle z_1, \ldots, z_k\rangle$ $(k = n+m-1)$. On a $IJ_1 \subseteq JJ_1 = \langle a\rangle$. Pour tout $i \in \{1, ..., k\}$, il existe un élément b_i tel que $z_i = b_i a$. Soit alors $K = \langle b_1, \ldots, b_k\rangle$. On a $IJ_1 = aK$, donc $aJK = aI$ et $I = JK$ puisque a est non diviseur de zéro . □

Remarque : Notez que la dernière procédure indiquée commence par calculer aK. Pour obtenir les $n+m-1$ générateurs de K il faut ou bien avoir explicitement la division par a dans $\mathbf{A}$ (quand elle est possible), ou bien avoir au départ l'inclusion $I \subseteq J$ de manière explicite et utiliser ensuite une version complètement explicite de la proposition 2.7.

2.4 Les idéaux fractionnaires

Définition 2.20 *Un* idéal fractionnaire *d'un anneau $\mathbf{A}$ est un sous $\mathbf{A}$-module l'anneau total des fractions $\mathrm{F}(\mathbf{A})$ qui s'écrit sous la forme I/y où I est un idéal de $\mathbf{A}$ et y est non diviseur de zéro dans $\mathbf{A}$.*

La somme et le produit de deux idéaux fractionnaires (définis de manière naturelle) sont des idéaux fractionnaires. Nous noterons $\mathcal{F}_\mathbf{A}$ le monoïde multiplicatif des idéaux fractionnaires de $\mathbf{A}$.

Si $x_1, \ldots, x_n \in \mathrm{F}(\mathbf{A})$ nous notons encore $\langle x_1, \ldots, x_n\rangle$ l'idéal fractionnaire qu'ils engendrent.

Les lemmes qui suivent sont faciles.

Lemme 2.21 *Les idéaux fractionnaires de $\mathbf{A}$ inversibles dans $\mathcal{F}_\mathbf{A}$ sont ceux de la forme I/y avec I inversible au sens de la définition 2.15. Ils forment un groupe.*

Nous noterons $I \div J$ le quotient de deux idéaux dans $\mathcal{F}_\mathbf{A}$ lorsque J est inversible.

Lemme 2.22 *Lorsque J est inversible, on a*

$$I \div J = \{x \in \mathrm{F}(\mathbf{A})\,;\, x\,J \subseteq I\} = I \cdot (\langle 1\rangle \div J)\,.$$

Lemme 2.23 *Supposons $\mathbf{A}$ cohérent et soient I, J, K des idéaux fractionnaires de type fini.*

- *$I \cap J$ est un idéal fractionnaire de type fini. Si $I + J$ est inversible, $I \cap J$ est l'unique idéal fractionnaire L vérifiant $L\,(I + J) = I\,J$.*
- *Si $\mathbf{A}$ est intègre et $J \neq 0$, le module $L = \{x \in \mathrm{F}(\mathbf{A})\,;\, x\,J \subseteq I\}$ est un idéal fractionnaire de type fini. Nous le noterons encore $I \div J$. On a l'égalité $I \div (J \div K) = I \div J\,K$ (on suppose aussi $K \neq 0$).*
- *Si $\mathbf{A}$ est quasi intègre, $\langle r\rangle = \mathrm{Ann}(J)$ et $s = 1 - r$, nous noterons $I \div J$ pour $L = \{x \in s\,\mathrm{F}(\mathbf{A})\,;\, x\,J \subseteq I\}$: c'est un idéal fractionnaire de type fini.*

Il faut faire attention à cette notation. Si $I \in \mathcal{F}_{\mathbf{A}}$ n'est pas inversible, on peut avoir $I \div I \neq \langle 1\rangle$ même dans le cas intègre (voir plus loin le lemme 5.2).

Dire que I est inversible revient à dire que $I \cdot (\langle 1\rangle \div I) = \langle 1\rangle$.

Il est parfois plus pratique de raisonner avec des idéaux fractionnaires qu'avec des idéaux "usuels". Lorsqu'on est dans un tel contexte, les idéaux usuels, c'est-à-dire ceux contenus dans $\mathbf{A}$, sont appelés des *idéaux entiers*.

3 Anneaux arithmétiques

Définition 3.1 *Un anneau* $\mathbf{A}$ *est appelé* anneau arithmétique *si pour tous* x_1, x_2 *dans* $\mathbf{A}$, *il existe* $u, v, w \in \mathbf{A}$ *tels que :*

$$\left\{\begin{array}{rcl} u\,x_2 & = & v\,x_1 \\ w\,x_2 & = & (1-u)\,x_1 \end{array}\right. \tag{8}$$

D'après la proposition 2.4 cela revient à demander que tout idéal $I = \langle x_1, x_2\rangle$ *soit localement principal (les éléments* u, v, w, $1-u$ *sont les coefficients d'une matrice de localisation principale pour* (x_1, x_2)*).*

La définition implique que $\langle x_1,\ x_2\rangle \langle u, w\rangle = \langle x_1\rangle$. Inversement si on a un idéal J tel que $\langle x_1,\ x_2\rangle\, J = \langle x_1\rangle$ on en déduit facilement des éléments u, v, w convenables.

Lorsque $\mathbf{A}$ est intègre la définition se relit en disant que toute fraction $x \in \mathrm{F}(\mathbf{A})$ peut s'écrire de deux façons : $x = u/v = w/s$ $(u, v, w, s \in \mathbf{A})$ avec u et s étrangers.

Il y a de nombreuses autres propriétés qui peuvent caractériser les anneaux arithmétiques, en particulier le fait que les idéaux forment un treillis distributif. Voir [7, 12, 13]. Les résultats affirmés mais non démontrés dans le texte présent ont une preuve constructive qui peut être trouvée dans [13].

On a immédiatement

Fait 3.2 *Tout quotient et tout localisé d'un anneau arithmétique est un anneau arithmétique. Un anneau est arithmétique si et seulement si il a la même propriété après localisation en des monoïdes comaximaux.*

Dans le cas local on obtient.

Fait 3.3 *Un anneau* $\mathbf{A}$ *est local et arithmétique si et seulement si pour tous* $x, y \in \mathbf{A}$, x *divise* y *ou* y *divise* x. *Autrement dit tout idéal de type fini est principal et les idéaux de type fini sont totalement ordonnés pour l'inclusion.*

Ces anneaux sont les "valuation rings" de Kaplansky [11]. Nous prendrons cependant nos "anneaux de valuation" sans diviseur de zéro conformément à la terminologie de Bourbaki (cf. définition 4.1 page 33). Notez que du point de vue algorithmique, la disjonction constructive "x divise y ou y divise x" n'implique pas qu'il y ait un test de divisibilité dans $\mathbf{A}$.

Remarque d'implémentation : Pour déclarer un anneau arithmétique on déclare que c'est un anneau avec un constructeur $(x_1, x_2) \mapsto (u, v, w)$ répondant aux équations (8).

3.1 Construction de la matrice de localisation principale

La proposition suivante étend la propriété donnée dans la définition 3.1 au cas d'un idéal de type fini quelconque. Elle est la base de tous les calculs explicites dans les anneaux arithmétiques. La procédure indiquée dans la preuve est plus élémentaire que celle sous jacente à la preuve par récurrence qui vient immédiatement à l'esprit et qui utiliserait ensuite la proposition 2.4 pour construire la matrice de localisation principale.

Proposition 3.4 *Soit* $\mathbf{A}$ *un anneau arithmétique. Alors tout idéal de type fini est localement principal. Plus précisement pour tout* $(x_1, ..., x_n) \in \mathbf{A}^{1\times n}$*, il existe une matrice de localisation principale* $A = (a_{ij})$*. Elle peut être construite de manière itérative comme indiquée dans la preuve ci-dessous.*

Preuve Par définition la proposition est vraie pour $n = 2$. Supposons qu'elle est vraie a l'ordre $n-1$. Donc il existe une matrice $B = (b_{ij})_{1\leq i,j\leq n-1}$ telle que :

$$b_{\ell j}\, x_i = b_{\ell i}\, x_j \ \ (i, j, \ell = 1, ..., n-1) \qquad \text{et} \qquad \sum b_{ii} = 1$$

On pose $s_i = b_{ii}$. En considérant $\langle x_i, x_n\rangle$ pour $i = 1, ..., n-1$ on sait qu'il existe (u_i, v_i, w_i, t_i) pour chaque i tels que :

$$\left\{\begin{array}{rcl} u_i\, x_n &=& v_i\, x_i \\ w_i\, x_n &=& t_i\, x_i \\ u_i + t_i &=& 1 \end{array}\right.$$

• Nous avons

$$1 = \sum_{i=1}^{n-1} s_i = \sum_{i=1}^{n-1} s_i\,(u_i + t_i) = \sum_{i=1}^{n-1} s_i\, u_i + \sum_{i=1}^{n-1} s_i\, t_i$$

Posons $\boxed{a_{ii} = s_i\, u_i = S_i}$ et

$$\boxed{a_{nn} = S_n = \textstyle\sum_{i=1}^{n-1} s_i\, t_i},$$

de sorte que $\sum_{i=1}^{n} S_i = 1$
• D'autre part, pour $i \neq j \in \{1, \dots, n-1\}$

$$S_i\, x_j = a_{ii}\, x_j = s_i\, u_i\, x_j = u_i\,(s_i\, x_j) = u_i\, b_{ij}\, x_i.$$

On prend donc $\boxed{a_{ij} = u_i\, b_{ij}}$.
• On a aussi pour $i = 1, ..., n-1$

$$S_n\, x_i = a_{nn}\, x_i = \sum_{j=1}^{n-1} s_j\, t_j\, x_i = \sum_{j=1}^{n-1} t_j\, b_{jj}\, x_i = \sum_{j=1}^{n-1} t_j\, b_{ji}\, x_j = \sum_{j=1}^{n-1} w_j\, b_{ji}\, x_n.$$

On pose donc $\boxed{a_{ni} = \textstyle\sum_{j=1}^{n-1} b_{ji}\, w_j}$.
• Enfin on a pour $i = 1, ..., n-1$:

$$S_i x_n = a_{ii} x_n = s_i\, u_i\, x_n = s_i\, v_i\, x_i$$

et on pose $\boxed{a_{in} = s_i\, v_i}$.
En résumé, la matrice (a_{ij}) ainsi définie vérifie la relation $a_{ij}\, x_i = a_{ii}\, x_j$.
Montrons que de façon générale on a : $a_{kj}\, x_i = a_{ki}\, x_j$. Supposons la propriété vraie a l'ordre $n-1$, montrons qu'elle est vraie pour n. On peut supposer $i,\ j,\ k$ distincts et on a trois cas à examiner :
• Si $i,\ j,\ k \in \{1, \dots, n-1\}$, alors

$$a_{kj}\, x_i \ = \ (u_k\, b_{kj})\, x_i \ = \ u_k\,(b_{ki}\, x_j) \ = \ (u_k\, b_{ki})\, x_j \ = \ a_{ki}\, x_j.$$

• Pour $i = n$ et $j,\ k \in \{1, \dots, n-1\}$, on a

$$a_{kj}\, x_n \;=\; (u_k\, b_{kj})\, x_n \;=\; (v_k\, x_k)\, b_{kj} \;=\; v_k\, (b_{kk}\, x_j) \;=\; a_{kn}\, x_j.$$

• Enfin si $k = n$ et $i,\ j \in \{1, \dots, n-1\}$, on a

$$a_{nj}\, x_i \;=\; \Big(\sum\nolimits_{\ell=1}^{n-1} b_{\ell j}\, w_\ell\Big)\, x_i \;=\; \Big(\sum\nolimits_{\ell=1}^{n-1} b_{\ell i}\, x_j\Big)\, w_\ell \;=\; \Big(\sum\nolimits_{\ell=1}^{n-1} b_{\ell i}\, w_\ell\Big)\; x_j \;=\; a_{ni}\, x_j.$$

□

Remarque d'implémentation : Dans un anneau arithmétique la procédure de construction des matrices de localisation principale est l'outil de base qui permet de résoudre tous les autres problèmes.

Le cas des anneaux de Bezout

Rappelons qu'un *anneau de Bezout* est un anneau dans lequel les idéaux de type fini sont principaux.

Proposition 3.5 *Tout anneau de Bezout est un anneau arithmétique. Plus précisément soit $I = \langle x_1, ..., x_n\rangle$ un idéal de type fini, alors une matrice de localisation principale pour $(x_1, ..., x_n)$ se calcule comme suit :*
On considère les vecteurs $Y = (y_1, ..., y_n)$ avec $y_i\, d = x_i$ $(d = pgcd(x_i))$ et $U = (u_1, ..., u_n)$ avec u_i égal au i-ème coefficient de Bezout dans l'égalité $(u_1x_1 + \cdots + u_nx_n = d)$. La matrice recherchée est alors la matrice $A = {}^tU\, Y$ dans laquelle on remplace a_{nn} par $1 - \sum_{i=1}^{n} u_iy_i$.

Ceci est une conséquence du lemme 2.3.

3.2 Anneaux arithmétiques fortement discrets

Dans un anneau, on dit que *la relation de divisibilité est explicite* lorsqu'on a un test qui décide si un élément x (arbitraire) divise un autre élément y, et si en cas de réponse positive, on sait calculer un élément c tel que $xc = y$.

Proposition 3.6 *Un anneau arithmétique est fortement discret si et seulement si la relation de divisibilité est explicite. Autrement dit, lorsque la relation de divisibilité est explicite, on sait resoudre une équation linéaire $BX = c$ avec $B = (b_1, \dots, b_n)$: soit $A = (a_{ij})$ une matrice de localisation principale pour $(b_1, \dots, b_n)$, l'équation $BX = c$ admet une solution si et seulement si pour tout i on peut trouver c_i tel que $a_{ii}c = b_ic_i$, et alors une solution est $X = {}^t(c_1, \dots, c_n)$. En particulier on a $1 \in \langle b_1, \dots, b_n\rangle$ si et seulement si pour tout i b_i divise a_{ii}.*

Preuve
• Pour tout anneau $\mathbf{A}$ fortement discret et $x,\ y \in \mathbf{A}$, on a $(y \in \langle x\rangle)$ ou $\neg(y \in \langle x\rangle)$ i.e. $(x|y)$ ou $\neg(x|y)$. En outre dans les cas où $y \in \langle x\rangle$, un élément a tel que $y = ax$ est explicite.
• Supposons maintenant que la divisibilé est explicite.
Si $B\, X = c$, alors on a $a_{ii}\, B\, X \;=\; a_{ii}\, c$, donc

$$a_{ii}\, c \;=\; \sum_{j=1}^{n} a_{ii}\, b_j\, x_j \;=\; \left(\sum_{j=1}^{n} a_{ij}\, x_j\right)\; b_i$$

Si l'équation admet une solution, alors b_i divise $a_{ii}\,c$, et il existe c_i tel que $a_{ii}\,c = b_i\,c_i$. La divisibilité étant explicite, un tel c_i est connu. En prenant $x_i = c_i$ on a bien $B\,X = \sum x_i\,b_i = \sum c_i\,b_i = \sum a_{ii}\,c = c$. □

Remarque d'implémentation : Un anneau arithmétique fortement discret est décrit comme un anneau arithmétique avec un constructeur de *division explicite* (ou quotient exact) $(a, b) \mapsto (x, c)$ où x est un booléen qui prend la valeur vrai si et seulement si b divise a, auquel cas on a $a = bc$. On en déduit alors une procédure qui teste si une équation linéaire admet ou non une solution, et donne une solution en cas de réponse positive.

3.3 Le treillis des idéaux de type fini d'un anneau arithmétique

D'après le lemme 2.9 l'intersection de deux idéaux de type fini dans un anneau arithmétique est encore un idéal de type fini. Les idéaux de type fini forment donc un treillis. Certaines des propriétés de ce treillis ont déjà été précisées dans la section 2.1.

Les propriétés de distributivité

Proposition 3.7 *Soit* $\mathbf{A}$ *un anneau arithmétique et* I, J, K *trois idéaux de type fini.*

(1) $I + (J \cap K) = (I + J) \cap (I + K)$.
(2) $I \cap (J + K) = (I \cap J) + (I \cap K)$.
(3) $(J + K) : I = (J : I) + (K : I)$.
(4) $I\,(J \cap K) = (I\,J) \cap (I\,K)$.
(5) $I : (J \cap K) = (I : J) + (I : K)$.
(6) *la suite exacte courte ci-après est scindée :*

$$0 \longrightarrow A/(I \cap J) \xrightarrow{\delta} A/I \times A/J \xrightarrow{\sigma} A/(I + J) \longrightarrow 0$$

où $\delta(\hat{x}) = (\tilde{x}, \bar{x})$ *et* $\sigma(\tilde{x}, \bar{y}) = \pi(x - y)$.

Preuve Ces relations sont claires lorsque tous les idéaux concernés sont principaux. Donc elles sont vraies après localisation en des monoïdes comaximaux. Et on en déduit facilement qu'elles sont vraies globalement. □

Idéaux premiers inversibles

Dans le cadre d'un anneau fortement discret non trivial $\mathbf{A}$, un idéal de type fini maximal est, du point de vue constructif, un idéal de type fini P qui vérifie :

$$1 \notin P \quad \text{et} \quad \forall x \in \mathbf{A}\ (x \in P \text{ ou } \langle x \rangle + P = \langle 1 \rangle) \tag{9}$$

On en déduit que pour tout idéal de type fini I on a

$$I \subseteq P \ \text{ ou } \ I + P = \langle 1 \rangle \tag{10}$$

Proposition 3.8 *Dans un anneau arithmétique fortement discret, un idéal inversible premier est toujours maximal.*

Preuve Soit P un idéal inversible premier et $y \notin P$. On a immédiatement $P \cap \langle y \rangle = yP$. Puisque $(P \cap \langle y \rangle)(P + \langle y \rangle) = P \langle y \rangle$ on a $yP(P + \langle y \rangle) = yP$. Puisque P est inversible on en déduit $y(P + \langle y \rangle) = \langle y \rangle$. Donc $y = y(p + ay)$ avec $p \in P$ donc $y(1 - ay) \in P$ donc $1 - ay \in P$. □

Remarque : Dans un anneau de valuation un idéal est inversible si et seulement si il est principal engendré par un non diviseur de zéro. Mais l'idéal maximal n'est pas toujours principal, et il existe des idéaux premiers non maximaux si le groupe de valuation n'est pas archimédien.

4 Anneaux de Prüfer cohérents

4.1 Anneaux de Prüfer

Définition 4.1 *Un anneau est appelé* anneau de Prüfer *s'il est arithmétique et réduit. Si l'anneau est local, on dit que c'est un* anneau de valuation.

Tout quotient réduit et tout localisé d'un anneau de Prüfer est un anneau de Prüfer. Un anneau est de Prüfer si et seulement si il a la même propriété après localisation en des monoïdes comaximaux.

Remarque : Un anneau est de Prüfer si et seulement si tout idéal est plat. Dans le cas intègre cette définition équivaut à la définition usuelle. Dans le cas non intègre cette définition pour *anneau de Prüfer* a été proposée dans [10]. Une autre terminologie est "anneau de dimension faible globale nulle".

Anneaux localement sans diviseur de zéro

Un anneau dont tous les idéaux principaux sont plats est appelé *localement sans diviseur de zéro*. C'est le cas des anneaux de Prüfer.

Un anneau localement sans diviseur de zéro est réduit, il est caractérisé par la propriété suivante :

$$\forall a, b \in \mathbf{A} \quad (ab = 0 \ \Rightarrow \ \exists s, t \in \mathbf{A} : s + t = 1,\ sa = 0,\ tb = 0). \tag{11}$$

(en localisant en s, a devient nul, et en localisant en t, b devient nul). Un anneau localement sans diviseur de zéro se comporte à bien des égards comme un anneau intègre.

Remarque d'implémentation : Pour déclarer un anneau de Prüfer on déclare que c'est un anneau arithmétique réduit. Il n'y a donc pas de nouveau constructeur. Cependant on introduit une procédure qui réalise explicitement l'implication (11).

4.2 Anneaux de Prüfer cohérents

Dans un anneau arithmétique, l'intersection de deux idéaux de type fini est de type fini. Pour qu'il soit cohérent, il suffit donc que l'annulateur de tout élément soit de type fini. On en déduit en utilisant le fait 1.12, le lemme 1.11 et le corollaire 2.11.

Fait 4.2 *Un anneau de Prüfer est cohérent si et seulement si il est quasi intègre. Un anneau est un anneau de Prüfer cohérent si et seulement si tous ses idéaux de type fini sont projectifs. Dans un anneau de Prüfer cohérent, tout idéal de type fini dont l'annulateur est nul est inversible.*

Dans la littérature, de tels anneaux sont souvent appelés des anneaux *semi-héréditaires*.

Un quotient réduit d'un anneau de Prüfer cohérent par un idéal de type fini est un anneau de Prüfer cohérent. Tout localisé d'un anneau de Prüfer cohérent est un anneau de Prüfer cohérent.

Un anneau arithmétique intègre est un anneau de Prüfer cohérent. On peut le caractériser comme un anneau intègre dans lequel tous les idéaux de type fini non

nuls sont inversibles. Si en outre la divisibilité est explicite nous l'appelons un *domaine de Prüfer*

Remarque d'implémentation : Pour déclarer un anneau de Prüfer cohérent on déclare que c'est anneau arithmétique quasi intègre.

Quotient exact de deux idéaux de type fini dans un anneau de Prüfer cohérent

Lemme 4.3 *Soit* $\mathbf{A}$ *un anneau de Prüfer cohérent,* K, K' *deux idéaux de type fini de* $\mathbf{A}$, *et* x *un élément de* $\mathbf{A}$ *tel que* $xK = xK'$, $\mathrm{Ann}(x) = \langle r\rangle$ *(*r *idempotemt), et* $rK = rK' = 0$. *Alors* $K = K'$.

Le lemme suivant généralise la proposition 2.19.

Lemme 4.4 *Soit* I *et* J *deux idéaux de type fini dans un anneau de Prüfer cohérent avec* $I \subseteq J$ *et* $\mathrm{Ann}(J) = \langle r\rangle$. *Il existe alors un unique idéal* K *tel que* $I = JK$ *et* $rK = 0$. K *est appelé le* quotient exact *de* I *par* J. *On le note* $I \div J$. *Si* I *et* J *sont engendrés par* n *et* m *éléments on peut construire* $n + m - 1$ *générateurs pour* K.

Preuve : Puisque $\mathrm{Ann}(J) = \langle r\rangle$, il existe un élément $x \in J$ non diviseur de zéro tel que $\mathrm{Ann}(J) = \mathrm{Ann}(x) = \langle r\rangle$ (cf. lemme 1.11). Donc il existe un idéal de type fini J_1 tel que $JJ_1 = \langle x\rangle$.
Puisque $I \subseteq J$, il existe K' tel que $I = JK'$, car $\mathbf{A}$ est arithmétique. Posons $K = sK'$ $(s = 1-r)$, on a $rK = rsK' = 0$ et $I = JK' = JsK' = JK$. Et K est unique d'après le lemme 4.3 ($JK = I = JL \Rightarrow xK = xL = J_1JK = J_1JL = J_1I$). Pour les générateurs on calcule d'abord J_1 puis $J_1I = sK$ en appliquant la proposition 2.7. □

Remarques
1) Notez que la dernière procédure indiquée commence par calculer sK. La même remarque que celle qui suit la proposition 2.19 doit donc être faite ici : la procédure sera efficace surtout si l'anneau est fortement discret.
2) Les idéaux K' qui vérifient $JK' = I$ sont en fait tous les idéaux compris entre $K = I \div J$ et $K + r\mathbf{A}$, ce dernier est l'idéal transporteur usuellement noté $I : J$.

Lemme 4.5 *Soit* I *et* J *deux idéaux de type fini dans un anneau de Prüfer cohérent. Alors* $I \cap J$ *est égal au quotient exact de* IJ *par* $I + J$ *et on peut déterminer un système générateurs a* $n + m$ *éléments.*

Preuve Il est clair que si $\langle r\rangle = \mathrm{Ann}(I + J)$ alors $r\,(I \cap J) = 0$, donc l'affirmation résulte immédiatement des lemmes 4.4 et 2.9. □

4.3 Systèmes linéaires et modules de présentation finie

Pour la terminologie relative à la torsion voir la définition 1.8 et le fait 1.10.

Le cas local

Nous utiliserons les deux lemmes suivants qui traitent le cas local.

Lemme 4.6 *Un anneau de valuation est sans diviseur de zéro. Un anneau de valuation non trivial est cohérent si et seulement si il est discret (c'est-à-dire s'il est intègre). On dit alors que c'est un* domaine de valuation.

Lemme 4.7 *Soit* $\mathbf{A}$ *un domaine de valuation et* $\varphi : \mathbf{A}^n \to \mathbf{A}^m$ *un homomorphisme entre modules libres de rang fini. Alors,* $\operatorname{Ker}\varphi$ *et* $\operatorname{Im}\varphi$ *sont libres et* $\operatorname{Ker}\varphi$ *est facteur direct. De plus tout module de présentation finie est somme directe de son sous-module de torsion et d'un sous-module libre.*

Preuve Par manipulations élémentaires de lignes et de colonnes, on peut mettre la matrice de φ sous forme de Smith : les seuls éléments non nuls $(d_i)_{i=1,..,k}$ $(k \leq \inf(n,m))$ sont sur la diagonale (d_i en position (i,i)), et on a $d_i | d_{i+1}$. Après les changements de bases correspondant aux manipulations de lignes et de colonnes effectuées, on a donc :

$$\operatorname{Ker}\varphi = \{X \in \mathbf{A}^n,\ x_1 = \ldots = x_k = 0\} \simeq \mathbf{A}^{n-k}.$$
$$\operatorname{Im}\varphi = \{(d_1x_1, \ldots, d_kx_k, 0, \ldots, 0),\ x_i \in \mathbf{A}\} \simeq \mathbf{A}^k.$$

Donc $\operatorname{Ker}\varphi$ et $\operatorname{Im}\varphi$ sont libres de rang fini. Pour tout module de présentation finie M on a donc : $M \simeq \prod_{i=1}^{k} \mathbf{A}/\langle d_i\rangle \times \mathbf{A}^{m-k}$. Et en désignant le sous-module de torsion de M par $T(M)$, on a

$$T(M) \simeq \prod_{i=1}^{k} \mathbf{A}/\langle d_i\rangle$$

donc $M \simeq T(M) \oplus \mathbf{A}^{m-k}$. □

Noyau d'une forme linéaire et d'une matrice

Proposition 4.8 *Soit* $\mathbf{A}$ *un anneau de Prüfer cohérent. Pour tout vecteur* $L \in \mathbf{A}^{1\times n}$*, il existe une matrice de projection* $Q \in \mathbf{A}^{n\times n}$ *telle que* $\operatorname{Im} Q = \operatorname{Ker} L$.

Ceci est une conséquence de la proposition 2.10 et du lemme 1.11.

Notez que la cohérence de $\mathbf{A}$ est ainsi explicitée sous une forme particulièrement intéressante : le noyau d'une forme linéaire est non seulement de type fini mais facteur direct.

Remarque d'implémentation : Un anneau arithmétique quasi intègre à divisibilité explicite est la forme sous laquelle est introduit un anneau de Prüfer cohérent fortement discret. Pour un tel anneau on sait donc résoudre les systèmes linéaires au sens de la proposition 1.4.

Proposition 4.9 *Sur un anneau de Prüfer cohérent le noyau d'une application linéaire* $\varphi : \mathbf{A}^n \to \mathbf{A}^m$ *entre modules libres de dimensions finies est facteur direct. Autrement dit* $\operatorname{Ker}\varphi = \operatorname{Im}\pi$ *où* $\pi : \mathbf{A}^n \to \mathbf{A}^n$ *est une projection.*

Preuve : Nous faisons une preuve par récurrence sur le nombre m d'équations dans le système linéaire. Le cas d'une équation est traité par la proposition 4.8. Supposons qu'on ait un système linéaire avec $m \geq 1$ équations. Notons B la matrice A privée de sa dernière ligne et L cette ligne. Par hypothèse de récurrence on sait calculer une matrice de projection $Q \in \mathbf{A}^{n\times n}$ telle que $\operatorname{Im} Q = \operatorname{Ker} B$. La technique exposée à la proposition 1.2 demande de "porter la solution générale de $BX = 0$ dans la dernière équation". Cela revient à dire $\operatorname{Ker} A = \operatorname{Ker} B \cap \operatorname{Ker} L = \operatorname{Im} Q \cap \operatorname{Ker} L = Q(Q^{-1}(\operatorname{Ker} L)) = Q(\operatorname{Ker} LQ)$. Par la proposition 4.8 on calcule une matrice de

projection $P \in \mathbf{A}^{n\times n}$ telle que $\operatorname{Im} P = \operatorname{Ker} LQ$. De sorte que $\operatorname{Ker} A = Q(\operatorname{Im} P) = \operatorname{Im}(QP)$. Nous allons voir qu'en fait QP est une matrice de projection, ce qui terminera la construction. L'égalité $\operatorname{Im} P = \operatorname{Ker} LQ$ implique $\operatorname{Ker} Q \subseteq \operatorname{Im} P$, donc si $x \in \operatorname{Ker} Q$, $Q(P(x)) = Q(x) = 0$, c'est-à-dire $\operatorname{Ker} Q \subseteq \operatorname{Ker} QP$. Pour montrer que $(QP)^2 = QP$ nous montrons $QPQ = QP$. Les deux membres sont égaux (nuls) sur $\operatorname{Ker} Q$. Et le premier membre est égal à QP pour $x \in \operatorname{Im} Q$ puisqu'alors $Q(x) = x$. Donc les deux membres sont égaux sur $\operatorname{Ker} Q + \operatorname{Im} Q$, c'est-à-dire partout. □

La preuve ci-dessus est plus simple et plus efficace (algorithmiquement) que celle dans [13].

Remarque d'implémentation : Notez que dans le cas intègre on peut d'abord extraire de la matrice A des lignes linéairement indépendantes en nombre maximum (par la méthode du pivot de Gauss dans le corps des fractions par exemple) et appliquer l'algorithme de la preuve précédente seulement à la matrice extraite.

Image d'une matrice (sous-module de type fini d'un module libre)

Théorème 4.1 *Sur un anneau de Prüfer cohérent tout sous-module de type fini M d'un module libre est projectif, isomorphe à une somme directe d'idéaux de type fini. En particulier tout module projectif de type fini est isomorphe à une somme directe d'idéaux de type fini. Si M est de rang constant r, il est isomorphe à une somme directe de r idéaux inversibles.*

Preuve Considérons $M \subseteq \mathbf{A}^n$ et $\pi_n : \mathbf{A}^n \to \mathbf{A}$ la dernière forme coordonnée. L'idéal $\pi_n(M) = I_n$ est de type fini donc projectif, donc la restriction surjective $\pi'_n : M \mapsto I_n$ de π_n est scindée, et $M \simeq \operatorname{Im} \pi'_n \oplus \operatorname{Ker} \pi'_n = (M \cap \mathbf{A}^{n-1}) \oplus I_n$. On termine par induction sur n : $M \cap \mathbf{A}^{n-1}$ est de type fini puisque $\mathbf{A}$ est cohérent. On a donc écrit $M \simeq I_1 \oplus \cdots \oplus I_n$. Lorsque l'anneau est intègre, certains de ces idéaux sont nuls et les autres sont inversibles. Dans le cas général, si M est de rang r considérons un sfio $(s_1, \ldots, s_m)$ tel que dans chaque composante $s_i\mathbf{A}$ chacun des idéaux soit nul ou inversible. Alors pour chaque $i \in \{1, \ldots, m\}$ r des idéaux I_j sont idéaux inversibles dans la composante $s_i\mathbf{A}$ et les autres sont nuls. □

Structure des modules de présentation finie

Proposition 4.10 *Si $\mathbf{A}$ est un anneau de Prüfer cohérent, tout module de présentation finie est somme directe de son sous-module de torsion et d'un sous-module projectif.*

Preuve :
• Dans le cas local, $\mathbf{A}$ est un domaine de valuation et le résultat est vrai d'après le lemme 4.7.
• Dans le cas global, on localise en des éléments comaximaux (s_i). Soient T le sous-module de torsion du module de présentation finie M, et T_i celui de M_{s_i}. Alors $T_i = T_{s_i}$. Le module T_i est de type fini et facteur direct toujours d'après le lemme 4.7, donc T est de de type fini et facteur direct par un principe local-global. Alors M/T est sans torsion, donc plat (puisque $\mathbf{A}$ est de Prüfer), et de présentation finie (parce que T est de type fini). Ainsi $P = M/T$ est projectif de type fini et $M = T \oplus P$. □

Pour plus de détails voir [13].

4.4 Factorisations d'idéaux

Nous commençons par le cas le plus classique.

Factorisation en produit d'idéaux maximaux inversibles

Nous rappelons la proposition 3.8 : dans un anneau arithmétique à divisibilité explicite, tout idéal inversible premier est maximal.

Nous nous intéressons ici aux idéaux qui se décomposent en produits d'idéaux maximaux et inversibles.

Lemme 4.11 *Soit* $\mathbf{A}$ *un anneau fortement discret non trivial,* $P_1, \dots, P_n$ *des idéaux maximaux et inversibles. Si* $\prod_i P_i^{n_i} = \prod_i P_i^{m_i}$ *on a* $m_i = n_i$ *pour tout* i.

Preuve On raisonne avec des idéaux fractionnaires. Supposons $m_1 \geq n_1$. Après avoir divisé par $P_1^{n_1}$ on obtient $I = P_1^{m_1-n_1} \prod_{i>1} P_i^{n_i} = \prod_{i>1} P_i^{m_i} = J$, ce qui est absurde si $m_1 > n_1$ puisqu'on a à la fois $J \subseteq P_1$ et $P_1 + J = \langle 1 \rangle$, donc $1 \in P_1$. □

Proposition 4.12 *Soit* $\mathbf{A}$ *un anneau fortement discret,* $I, P_1, \dots, P_n$ *des idéaux de type fini avec les* P_i *maximaux et inversibles, et des entiers positifs* m_i. *Supposons* $\prod_i P_i^{m_i} \subseteq I$. *Alors il existe des entiers* $n_i \leq m_i$ *tels que* $I = \prod_i P_i^{n_i}$.

Preuve On raisonne avec des idéaux fractionnaires. On fait une preuve par récurrence sur $\sum_i m_i$. Si $I = \langle 1 \rangle$ (en particulier si $\sum_i m_i = 0$) le résultat est clair. Sinon I contient un des P_i (car sinon $I + \prod_i P_i^{m_i} = \langle 1 \rangle$), par exemple il contient P_1 et dans $\mathcal{F}_{\mathbf{A}}$ on a

$$P_1^{m_1-1} \prod_{i>1} P_i^{m_i} = \left(\prod_i P_i^{m_i} \right) \div P_1 \subseteq I \div P_1 = J \tag{12}$$

Et il suffit de recommencer avec J qui est un idéal entier puisque $I \subseteq P_1$. □

On en déduit par exemple.

Proposition 4.13 *Soit* $\mathbb{Z}[x] \simeq \mathbb{Z}[X]/\langle f(X) \rangle$ *avec* f *un polynôme unitaire irréductible. Si pour tout nombre premier* p *qui divise le dicriminant de* f *et tout facteur irréductible* g *de* f *dans* $\mathbb{F}_p[X]$ *l'idéal* $\langle p, g \rangle$ *est inversible dans* $\mathbb{Z}[x]$, *alors tout idéal de type fini non nul est inversible et se décompose en produit d'idéaux maximaux inversibles (en particulier* $\mathbb{Z}[x]$ *est un anneau arithmétique).*

Preuve Tout idéal de type fini non nul contient un entier non nul. En appliquant 4.12 il suffit donc de montrer que tout nombre premier est égal à un produit d'idéaux maximaux inversibles. Les idéaux maximaux de $\mathbb{Z}[x]$ sont les idéaux $\langle p, g \rangle$ où g est facteur irréductible de f dans $\mathbb{F}_p[X]$ (cf. la preuve de la proposition 2.18). Le cas où f n'a pas de facteur carré modulo p, c'est-à-dire lorsque p ne divise pas le discriminant de f, a déjà été traité dans la proposition 2.18. Dans le cas restant supposons que $f = \prod_i g_i^{n_i}$ modulo p. Alors on voit que $\prod_i \langle g_i, p \rangle^{n_i} \subseteq \langle p \rangle$. Puisqu'on suppose les $\langle g_i, p \rangle$ inversibles, on peut appliquer 4.12 et on obtient que $p\mathbb{Z}[x] = \prod_i \langle g_i, p \rangle^{m_i}$ ($m_i \leq n_i$). En fait, vue la structure du treillis des idéaux contenant p (cf. 2.18) on a nécessairement $m_i = n_i$. □

Factorisations complètes

Définition 4.14 *On appelle* domaine de Dedekind à factorisation complète *un anneau intègre fortement discret dans lequel tout idéal de type fini se décompose en produit d'idéaux maximaux inversibles.*

Cette définition implique clairement que les idéaux de type fini sont projectifs, donc que l'anneau est un anneau de Prüfer cohérent. Elle implique aussi la noethériannité puisque toute suite croissante d'idéaux de type fini doit pauser (rappelons qu'on dit qu'une suite pause si elle admet au moins deux termes consécutifs égaux).

La réciproque est vraie classiquement, mais du point de vue algorithmique il manque un ingrédient, décrit dans la proposition suivante.

Proposition 4.15 *Soit* $\mathbf{A}$ *un domaine de Prüfer. On suppose que l'on a un test qui décide si un idéal de type fini non nul* I *est maximal ou non, et en cas de réponse négative, donne un* x *tel que* $x \notin I$, $1 \notin I + \langle x \rangle$. *On suppose que tout suite croissante d'idéaux de type fini pause. Alors tout idéal de type fini se décompose en produit d'idéaux maximaux.*

Preuve Soit $I \neq \langle 1 \rangle$ un idéal de type fini. En utilisant de manière répétée le test de maximalité on trouve un maximal de type fini P_1 contenant $I = I_1$. On pose $I_2 = I_1 \div P_1$ et on recommence. La suite des idéaux de type fini I_n est strictement croissante tant que la décomposition n'est pas trouvée. □

Factorisations partielles

Le test de maximalité présent dans la proposition 4.15 est dans bien des cas une hypothèse trop forte et la proposition classique selon laquelle tout idéal se décompose en produit de maximaux inversibles dans un domaine de Prüfer cohérent et noethérien n'est alors plus valable du point de vue algorithmique.

C'est une raison importante pour laquelle il est intéressant d'étudier d'autres factorisations.

Définition 4.16 *Soit* $F = \{I_1, \ldots, I_n\}$ *une famille d'idéaux inversibles dans un anneau* $\mathbf{A}$. *On dit que* F *admet une* factorisation partielle *s'il existe une famille* $P = \{P_1, \ldots, P_k\}$ *d'idéaux inversibles deux à deux étrangers, telle que tout idéal* I_j *de* F *peut s'écrire sous la forme :* $I_j = P_1^{m_{1j}} \cdots P_k^{m_{kj}}$ *(certains des* m_{ij} *peuvent être nuls). On dit alors que* $\{P_1, \ldots, P_k\}$ *est une* base de factorisation partielle *pour la famille* F.

Notez que pour une famille F donnée s'il existe une base de factorisation partielle elle n'est généralement pas unique, par exemple chacun des P_i peut en général être encore décomposé en facteurs.

Définition 4.17 *Un anneau est appelé* anneau de Prüfer à factorisation partielle *si c'est un anneau de Prüfer cohérent, fortement discret et si toute famille finie d'idéaux inversibles admet une factorisation partielle.*

Dans le cas local, on a une caractérisation intéressante des anneaux de Prüfer à factorisation partielle :

Lemme 4.18 *Si* $\mathbf{A}$ *est un domaine de valuation à factorisation partielle et si* a, b *sont deux éléments non nuls de* $\mathrm{Rad}(\mathbf{A})$*, il existe* $p \in \mathrm{Rad}(\mathbf{A})$*, deux entiers* > 0 m *et* n *et deux éléments inversibles* u *et* v *tels que* $a = up^m$ *et* $b = vp^n$*. En conséquence un domaine de valuation est à factorisation partielle si et seulement si son groupe de valuation est isomorphe à un sous groupe de* $\mathbb{Q}$*.*

Preuve Comme les idéaux de type fini sont principaux et totalement ordonnés pour l'inclusion, une factorisation partielle ne peut contenir qu'un seul élément, du type $\langle p \rangle$. L'isomorphisme du groupe de valuation sur un sous-groupe de $(\mathbb{Q}, +)$ est alors donné en fixant un élément a non nul et non inversible (on suppose donc qu'il en existe au moins un) dont on donne l'image dans $\mathbb{Q}$: 1, de manière purement conventionnelle. □

Un anneau de Prüfer à factorisation partielle n'est donc pas nécessairement noethérien.

Dans un anneau de Prüfer à factorisation partielle non intègre, on a une décomposition pour n'importe quelle famille d'idéaux de type fini (non nécessairement inversibles) comme précisé dans la proposition suivante.

Proposition 4.19 *Soit* $\mathbf{A}$ *un anneau de Prüfer à factorisation partielle et* $F = (I_k)$ *une famille finie d'idéaux de type fini. Il existe un sfio* (r_j)*, tel que pour chaque* r_j *on peut trouver une famille* $(P_{j,1}, \ldots, P_{j,s_j})$ *d'idéaux deux à deux étrangers dans* A_{r_j} *telle que pour tout* k*,* $(I_k)_{r_j} = r_j I_k$ *vaut soit* $\langle 0 \rangle$*, soit* $\langle 1 \rangle$*, soit se factorise sous la forme :*

$$\prod_{t=1}^{s_j} P_{j,t}^{n_t}$$

(les n_t *sont* ≥ 0 *mais pas tous nuls)*

Preuve : $\mathbf{A}$ est un anneau de Prüfer cohérent donc pour tout i, $\mathrm{Ann}(I_i) = \langle e_i \rangle$ avec e_i idempotent. On a $I_i = 0$ dans $\mathbf{A}_{e_i}$, et inversible dans $\mathbf{A}_{f_i}$, où $f_i = 1 - e_i$. Ecrivons

$$\prod (e_i + f_i) = \sum r_j = 1$$

où les r_j sont les produits non nuls des e_i et f_ℓ obtenus après développement. Ainsi les r_j forment un sfio. Dans chaque localisé $\mathbf{A}_{r_j} (\simeq r_j \mathbf{A})$, chacun des idéaux I_i a pour annulateur $e_i r_j$ qui vaut soit 1, soit 0. Par conséquent I_k est soit nul, soit inversible dans $\mathbf{A}_{r_j}$. Dans chaque localisé, on considère les idéaux inversibles $I_{k,j} = I_k \mathbf{A}_{r_j} \neq \langle 1 \rangle$. Une factorisation partielle dans $\mathbf{A}$ des idéaux correspondants $\langle 1 - r_j \rangle + I_{k,j}$ (qui sont inversibles) donne alors la factorisation partielle souhaitée dans $\mathbf{A}_{r_j}$. □

5 Extensions entières d'un anneau de Prüfer

Le fait qu'une extension entière d'un anneau de Prüfer est encore un anneau de Prüfer est fondamental. Nous en donnerons une preuve élémentaire et algorithmique, nettement plus simple que celle qu'on peut trouver dans [13].

Pour nous guider, nous devons d'abord traiter de cette façon le cas intègre, qui est plus facile. Ensuite nous reprendrons les mêmes arguments dans le cas général, en remplaçant l'intégrité par le fait qu'on travaille avec des anneaux localement sans diviseur de zéro.

5.1 Idéaux intégralement clos et anneaux normaux

Définition 5.1 *Soit I un idéal d'un anneau $\mathbf{A}$ contenu dans un anneau $\mathbf{B}$.*

(1) *Un élément $x \in \mathbf{B}$ est dit* entier sur I *si il vérifie une relation de dépendance intégrale $x^{n+1} = a_1x^n + a_2x^{n-1} + \cdots + a_nx + a_{n+1}$ avec $\forall h\ a_h \in I^h$.*

(2) *L'idéal I est dit* intégralement clos (dans $\mathbf{A}$) *si tout $x \in \mathbf{A}$ entier sur I est dans I.*

(3) *L'anneau $\mathbf{A}$ est dit* normal *lorsque tout idéal principal est intégralement clos.*

(4) *L'anneau $\mathbf{A}$ est dit* intégralement clos dans $\mathbf{B}$ *si tout $x \in \mathbf{B}$ entier sur $\mathbf{A}$ est dans $\mathbf{A}$.*

(5) *L'anneau $\mathbf{B}$ est dit* entier sur $\mathbf{A}$ *si tout $x \in \mathbf{B}$ est entier sur $\mathbf{A}$.*

Un anneau normal est intégralement clos dans son anneau total des fractions. Lorsque l'anneau est intègre, la notion d'anneau normal coïncide avec la notion usuelle d'anneau intégralement clos dans son corps des fractions. Une définition équivalente plus abstraite en maths classiques d'un anneau normal est la suivante : un anneau dont le localisé en n'importe quel idéal premier est intègre et intégralement clos.

Constructivement on a le principe local-global suivant : *un anneau est normal si et seulement si il a la même propriété après localisation en des monoïdes comaximaux.*

Notez qu'un élément $x \in \mathbf{A}$ est entier sur l'idéal $I \subseteq \mathbf{A}$ si et seulement si $I\,(I + \langle x\rangle)^n = (I + \langle x\rangle)^{n+1}$. Donc un idéal I est intégralement clos (dans $\mathbf{A}$) si et seulement si il vérifie la propriété de simplification suivante :

$$\forall x \in \mathbf{A} \quad I\,(I + \langle x\rangle)^n = (I + \langle x\rangle)^{n+1} \implies I = I + \langle x\rangle$$

On vérifie facilement qu'un anneau normal est réduit et localement sans diviseur de zéro.

Un determinant trick fournit un cas important d'élément entier sur un idéal :

Lemme 5.2 *Soit $I \subseteq \mathbf{A}$ un idéal de type fini dont l'annulateur est réduit à 0, J un idéal de type fini et $x \in \mathrm{F}(\mathbf{A})$ vérifiant $x\,I \subseteq J\,I$. Alors x est entier sur J.*

NB : 1) On aurait pu prendre pour I n'importe quel module de type fini dont l'annulateur est réduit à 0.
2) Dans le cas cohérent intègre les éléments $x \in \mathrm{F}(\mathbf{A})$ tels que $x\,I \subseteq J\,I$ sont exactement les éléments de l'idéal fractionnaire $IJ \div I$.

Preuve Si $I = \langle a_1, \dots, a_n \rangle$ on a une matrice $A \in J^{n\times n}$ telle que $x\,{}^t(a_1, \dots, a_n) = A\,{}^t(a_1, \dots, a_n)$. Par suite $\det(x\mathrm{I}_n - A)$ annule ${}^t(a_1, \dots, a_n)$ donc est nul. □

Lemme 5.3 *Dans un anneau de Prüfer tout idéal de type fini (donc tout idéal) est intégralement clos. En particulier un anneau de Prüfer est normal.*

Preuve Soit $x \in \mathbf{A}$ entier sur un idéal de type fini I. On a pour un $n \geq 0$, $I(I + \langle x \rangle)^n = (I + \langle x \rangle)^{n+1}$. Puisque l'anneau est arithmétique, on a un idéal de type fini J tel que $(I + \langle x \rangle)J = \langle x \rangle$. Donc en multipliant par J^n on obtient $x^n I = x^n(I + \langle x \rangle)$ ce qui signifie qu'il existe un $y \in I$ tel que $x^{n+1} = x^n y$ c'est-à-dire $x^n(y - x) = 0$. Puisque l'anneau est localement sans diviseur de zéro, il existe s tel que $sx = 0$ et $(1 - s)(y - x) = 0$, et donc $x = (1 - s)y \in I$. □

5.2 Le cas intègre

Lemme 5.4 (cf. [9] lemme 22) *Soient* $\mathbf{A}$ *un anneau contenu dans un anneau* $\mathbf{B}$ *et* $x \in \mathbf{B}$ *un élément vérifiant une relation de dépendance algébrique du type :*

$$\gamma_0 x^m + \gamma_1 x^{m-1} + \cdots + \gamma_h x^{m-h} + \cdots + \gamma_m \;=\; 0 \quad (\star) \quad (\text{les } \gamma_i \in \mathbf{A})$$

Alors pour tout $k \in \{0, \dots, m\}$, *les éléments* $x_k = \gamma_0 x^k + \gamma_1 x^{k-1} + \cdots + \gamma_k$ *et* $y_k = \gamma_m (x^{-1})^k + \gamma_{m-1}(x^{-1})^{k-1} + \cdots + \gamma_k$ *sont entiers sur* $\mathbf{A}$.

Corollaire 5.5 *Soient* $\mathbf{A}$ *un anneau de Prüfer intègre,* $\mathbf{K}$ *son corps des fractions,* $\mathbf{L}$ *une extension algébrique de* $\mathbf{K}$, $\mathbf{B}$ *la clôture intégrale de* $\mathbf{A}$ *dans* $\mathbf{L}$ *et* a, b *deux éléments non nuls de* $\mathbf{B}$ *vérifiant une relation de dépendance algébrique du type :*

$$\gamma_0 a^m + \gamma_1 a^{m-1} b + \cdots + \gamma_k a^{m-k} b^k + \cdots + \gamma_m b^m \;=\; 0 \quad (\star) \quad (\gamma_0, \dots, \gamma_m \in \mathbf{A},\ \gamma_0, \gamma_m \neq 0)$$

Alors pour tout $k \in \{0, \dots, m\}$, *on peut trouver dans* $\mathbf{B}$ *des éléments* s_k, v_k, w_k, t_k *tels que :*

$$\left\{ \begin{array}{rcl} s_k\, a & = & v_k\, b \\ w_k\, a & = & t_k\, b \\ s_k + t_k & = & \gamma_k \end{array} \right.$$

Preuve Pour tout entier k

$$\left(\frac{1}{a^{m-k} b^k}\right) \sum_{j=0}^{m} \gamma_j a^{m-j} b^j \;=\; \sum_{j=0}^{m} \gamma_j \frac{a^{m-j}}{a^{m-k}} \frac{b^j}{b^k} \;=\; \sum_{j=0}^{m} \gamma_j a^{k-j} b^{j-k} \;=\; 0$$

Décomposons cette somme comme suit :

$$\gamma_k \;+\; \sum_{j<k} \gamma_j a^{k-j} b^{j-k} \;+\; \sum_{j>k} \gamma_j a^{k-j} b^{j-k} \;=\; \gamma_k + (-s_k) + (-t_k) \;=\; 0$$

Bien qu'a priori il s'agisse d'une somme dans $\mathbf{L}$ nous allons voir que les trois termes sont dans $\mathbf{B}$. Posons en effet $x = \dfrac{a}{b} \in \mathbf{L}$. On a

$$\begin{array}{rcl} s_k \;=\; -\sum_{j<k} \gamma_j x^{k-j} & = & -\left(\gamma_0 x^k + \gamma_1 x_{k-1} + \cdots + \gamma_{k-1} x\right) \\ & = & -\left(\gamma_0 x^k + \gamma_1 x_{k-1} + \cdots + \gamma_{k-1} x + \gamma_k\right) + \gamma_k\,. \end{array}$$

Or $\gamma_k \in \mathbf{A}$, et $x_k = \gamma_0 x^k + \gamma_1 x_{k-1} + \cdots + \gamma_{k-1} x + \gamma_k \in \mathbf{B}$ d'après le lemme 5.4, donc $s_k \in \mathbf{B}$. De même $t_k \in \mathbf{B}$. Notons que

$$s_k = -\left(\gamma_0 x^k + \gamma_1 x_{k-1} + \cdots + \gamma_{k-1} x\right) = -x\left(\gamma_0 x^{k-1} + \gamma_1 x_{k-2} + \cdots + \gamma_{k-1}\right)$$

En posant $v_k = \gamma_0 x^{k-1} + \gamma_1 x_{k-2} + \cdots + \gamma_{k-1}$, on obtient $s_k = x\, v_k$, c'est-à-dire $s_k\, b = a\, v_k$. De même $t_k = -(x^{-1})\,(\gamma_m (x^{-1})^{p-1} + + \cdots + \gamma_{k+1}(x^{-1})) = (x^{-1})\, w_k$, c'est-à-dire $a\, t_k = b\, w_k$. Et on a déjà vu que $\gamma_k = s_k + t_k$. □

Théorème 5.1 *Soient* $\mathbf{A}$ *un anneau de Prüfer intègre,* $\mathbf{F}$ *son corps des fractions,* $\mathbf{L}$ *une extension algébrique de* $\mathbf{F}$ *(c'est-à-dire un corps discret entier sur* $\mathbf{K}$*),* $\mathbf{B}$ *la clôture intégrale de* $\mathbf{A}$ *dans* $\mathbf{L}$*.*

(1) *Soient* a*,* b *deux éléments de* $\mathbf{B}$*. Alors on sait construire une matrice de localisation principale pour* (a, b) *dans* $\mathbf{B}$*.*

(2) *En particulier* $\mathbf{B}$ *est un anneau de Prüfer.*

(3) *Supposons qu'on connaisse une base de* $\mathbf{L}$ *comme espace vectoriel sur* $\mathbf{K}$*. Alors si* $\mathbf{A}$ *est fortement discret (resp. noethérien), il en va de même pour* $\mathbf{B}$*.*

Preuve On suppose sans perte de généralité que $ab \neq 0$. Posons $x = \dfrac{a}{b} \in \mathbf{L}$, il existe un polynôme $P = \sum_{j=0}^{n} \mu_j X^j \in \mathbf{A}[X]$, avec $P(x) = 0$, $\mu_0, \mu_n \neq 0$:

$$\sum\nolimits_{j=0}^{n} \mu_j\, x^j = 0 \qquad (1)$$

Puisque $\mathbf{A}$ est un anneau de Prüfer, on a une matrice de localisation principale (c_{ij}) dans $\mathbf{A}$ pour $(\mu_0, \ldots, \mu_n)$:

$$\begin{cases} \sum_k c_{kk} &= 1 \\ c_{ki}\, \mu_j &= c_{kj}\, \mu_i \end{cases}$$

En multipliant l'équation (1) par c_{k0}, on a $\mu_0 \left(\sum_{j=1}^{n} c_{kj} x^j\right) = 0$, donc $\sum_{j=1}^{n} c_{kj} x^j = 0$. D'après le corollaire 5.5, il existe dans $\mathbf{B}$ des éléments s_k, v_k, w_k, t_k, tels que

$$\begin{cases} s_k\, a &= v_k\, b \\ w_k\, a &= t_k\, b \\ s_k + t_k &= c_{kk} \end{cases}$$

En posant

$$\begin{array}{rclcrcl} s &=& \sum_{k=1}^{n} s_k\,, & & v &=& \sum_{k=1}^{n} v_k\,, \\ w &=& \sum_{k=1}^{n} w_k\,, & & t &=& \sum_{k=1}^{n} t_k \end{array}$$

on obtient :

$$\begin{cases} s\, b &= v\, a \\ w\, b &= t\, a \\ s + t &= \sum_k c_{kk} = 1 \end{cases}$$

et

$$\begin{bmatrix} s & v \\ w & t \end{bmatrix}$$

est une matrice de localisation principale pour (a, b).

Montrons maintenant dans le point (3) le cas fortement discret (pour la noetherianité, nous renvoyons à [13]). Dire qu'un anneau intègre est fortement discret revient à dire qu'il est une partie détachable de son corps de fractions. Soient $a, b \in \mathbf{B}$ avec $b \neq 0$. Soit $x = a/b$, tester si b divise a revient à tester si $x \in \mathbf{B}$. Puisqu'on connaît une base de $\mathbf{L}$ sur $\mathbf{K}$ on sait calculer le polynôme minimal unitaire $P(X)$ de x sur $\mathbf{K}$. Et $x \in \mathbf{B}$ si et seulement si $P \in \mathbf{A}[X]$. □

5.3 Le cas général

Le traitement donné pour le cas intègre s'adapte au cas localement sans diviseur de zéro en prenant quelques précautions. L'idée est d'introduire des localisations dans lesquelles "tout se passe comme" dans le cas intègre, chaque fois d'une simplification par un non diviseur de zéro était requise dans le cas intègre.

Lemme 5.6 *Soient* $\mathbf{A}$ *un anneau de Prüfer, contenu dans un anneau* $\mathbf{B}$ *normal et entier sur* $\mathbf{A}$, a, b *deux éléments de* $\mathbf{B}$ *vérifiant une relation de dépendance algébrique du type :*

$$\gamma_0 a^m + \gamma_1 a^{m-1} b + \cdots + \gamma_k a^{m-k} b^k + \cdots + \gamma_m b^m \;=\; 0 \quad (\star) \quad (\text{les } \gamma_i \in \mathbf{A})$$

Alors pour tout $k \in \{0, \ldots, m\}$, *on peut trouver dans* $\mathbf{B}$ *des éléments* s_k, v_k, w_k, t_k *tels que :*

$$\left\{ \begin{array}{rcl} s_k\, a & = & v_k\, b \\ w_k\, a & = & t_k\, b \\ s_k + t_k & = & \gamma_k \end{array} \right.$$

Preuve : On procède par récurrence sur m puis sur k.
Si $m = 1$ on a :

$$\left\{ \begin{array}{rcl} \gamma_0\, a & = & -\gamma_1\, b \\ 0\, a & = & 0\, b \\ \gamma_0 + 0 & = & \gamma_0 \end{array} \right.$$

et

$$\left\{ \begin{array}{rcl} 0\, a & = & 0\, b \\ -\gamma_0\, a & = & \gamma_1\, b \\ 0 + \gamma_1 & = & \gamma_1 \end{array} \right.$$

Supposons maintenant $m > 1$. En multipliant l'équation $(\star)$ par γ_0^{m-1} on obtient :

$$(\gamma_0 a)^m + \gamma_1 (\gamma_0 a)^{m-1} b + \cdots + \gamma_k \gamma_0^{k-1} (\gamma_0 a)^{m-k} b^k + \cdots + \gamma_m \gamma_0^{m-1} b^m \;=\; 0$$

Donc $\gamma_0\, a$ est entier sur l'idéal $b\,\mathbf{B}$ et puisque $\mathbf{B}$ est normal, on a $\gamma_0\, a \in b\,\mathbf{B}$.
Pour $k = 0$ on obtient donc le système :

$$\left\{ \begin{array}{rcll} \gamma_0\, a & = & c_0\, b & \\ 0\, a & = & 0\, b & \\ \gamma_0 + 0 & = & \gamma_0 & \text{avec } c_0 \in \mathbf{B} \end{array} \right. \tag{13}$$

Pour $k \geq 1$, on remplace $\gamma_0\, a$ par $c_0\, b$ dans l'égalité $(\star)$, et elle devient :

$$b\left((c_0 + \gamma_1) a^{m-1} + \gamma_2 a^{m-2} b^2 + \cdots + \gamma_k a^{m-k} b^k + \cdots + \gamma_m b^{m-1}\right) \;=\; 0$$

L'anneau $\mathbf{B}$ est normal, donc localement sans diviseur de zéro et il existe z et z' tels que $z + z' = 1$, $z\,b = 0$ et

$$z'\left((c_0+\gamma_1)a^{m-1} + \gamma_2 a^{m-2}b + \cdots + \gamma_\ell a^{m-\ell}b^{\ell-1} + \cdots + \gamma_m b^{m-1}\right) \;=\; 0$$

Intuitivement, on raisonne dans les deux localisations $\mathbf{A}_z$ et $\mathbf{A}_{z'}$. Dans $\mathbf{A}_{z'}$, on a

$$(c_0+\gamma_1)a^{m-1} + \gamma_2 a^{m-2}b + \cdots + \gamma_\ell a^{m-\ell}b^{\ell-1} + \cdots + \gamma_m b^{m-1} \;=\; 0\,.$$

Précisément, dans $\mathbf{A}$ on a

$$\gamma'_1 a^{m-1} + \gamma'_2 a^{m-2}b + \cdots + \gamma'_\ell a^{m-\ell}b^{\ell-1} + \cdots + \gamma'_m b^{m-1} \;=\; 0 \qquad (14)$$

avec $\gamma'_1 = z'(c_0+\gamma_1)$, $\gamma'_2 = z'\gamma_2$, … , $\gamma'_m = z'\gamma_m$.
• si $k = 1$, en appliquant le résultat (13) obtenu pour $k = 0$ avec une équation de degré m ainsi que le résultat analogue avec l'équation (14) de degré $m-1$ on obtient

$$(z'_1) \qquad \left\{\begin{array}{rcl} (c_0+\gamma_1)\,z'\,a &=& c_1\,b \\ -\gamma_0\,z'\,a &=& -c_0\,z'\,b \\ (c_0+\gamma_1)z' + (-c_0\,z') &=& \gamma_1\,z' \quad \text{avec } c_1 \in \mathbf{B} \end{array}\right.$$

• si $k > 1$, en appliquant l'hypothèse de récurrence avec $m-1$ on trouve des éléments s'_k, v'_k, w'_k, t'_k tels que :

$$(z'_k) \qquad \left\{\begin{array}{rcl} s'_k\,a &=& v'_k\,b \\ w'_k\,a &=& t'_k\,b \\ s'_k + t'_k &=& z'\,\gamma_k \end{array}\right.$$

Dans $\mathbf{A}_z$, $b = 0$, et la solution est triviale, et plus précisément dans $\mathbf{A}$ on a :

$$(z_k) \qquad \left\{\begin{array}{rcl} 0\,a &=& 0\,b \\ 0\,a &=& \gamma_k\,z\,b \\ 0 + \gamma_k\,z &=& \gamma_k\,z \end{array}\right.$$

Et il reste à faire la somme des égalités (z_k) et (z'_k) ($k = 1$ ou $k > 1$). □

Théorème 5.2 *Soit* $\mathbf{A}$ *un anneau de Prüfer, contenu dans* $\mathbf{B}$ *normal entier sur* $\mathbf{A}$*, alors* $\mathbf{B}$ *est un anneau de Prüfer.*

Preuve Soient a, b deux éléments de $\mathbf{B}$. Montrons qu'on sait construire une matrice de localisation principale pour (a,b) dans $\mathbf{B}$. On a par hypothèse deux polynômes unitaires $P, Q \in \mathbf{A}[X]$ tels que : $P(a) = a^n + \alpha_1 a^{n-1} + \cdots + \alpha_n = 0$, $Q(b) = b^m + \beta_1 b^{m-1} + \cdots + \beta_m = 0$. On raisonne par récurrence sur $m+n$. Si $m+n = 2$ on est dans $\mathbf{A}$ et la solution est triviale. Supposons $m+n \geq 3$ avec par exemple $m \geq 2$ (sinon, on échange les rôles de a et b). Considérons la matrice "de

type Sylvester" $M(X,Y)$ (avec m lignes de P et n lignes de Q) suivante :

$$\begin{bmatrix}
X^n & \alpha_1 X^{n-1} & \dots & \dots & \alpha_n & 0 & \dots & \dots & 0 \\
0 & X^n & \alpha_1 X^{n-1} & \dots & \dots & \alpha_n & & & \vdots \\
\vdots & & & & & & & & \vdots \\
\vdots & & & & & & & & \vdots \\
\vdots & & & \ddots & & & & \ddots & 0 \\
0 & \dots & \dots & 0 & X^n & \alpha_1 X^{n-1} & \dots & \dots & \alpha_n \\
Y^m & \beta_1 Y^{m-1} & \dots & & \dots & \beta_m & 0 & \dots & 0 \\
0 & Y^m & \beta_1 Y^{m-1} & \dots & & \dots & \beta_m & & \vdots \\
\vdots & & & & & & & \ddots & \vdots \\
0 & \dots & 0 & Y^m & \beta_1 Y^{m-1} & \dots & & \dots & \beta_m
\end{bmatrix}$$

Le déterminant de M,

$$R(X,Y) = \mu_0 X^{nm} + \mu_1 X^{nm-1} Y + \cdots\cdots + \mu_{nm-1} X Y^{nm-1} + \mu_{nm} Y^{nm}$$

est un polynôme homogène de degré $p = nm$ tel que $R(a,b) = 0$. On a aussi $\mu_0 = \beta_m^n$ et $\mu_p = \alpha_n^m$. On a donc :

$$\mu_0 a^p + \mu_1 a^{p-1} b + \cdots + \mu_k a^{p-k} b^k + \cdots + \mu_p b^p \;=\; 0 \tag{15}$$

On considère une matrice de localisation principale (c_{ij}) pour $(\mu_0, \dots, \mu_p)$:

$$c_{ki}\mu_j = c_{kj}\mu_i \quad \forall i,j,k\,, \qquad \sum c_{ii} = 1$$

Si on multiplie la relation (15) par c_{k0} on obtient :

$$\mu_0 \left(c_{k0} a^p + c_{k1} a^{p-1} b + \cdots + c_{kk} a^{p-k} b^k + \cdots + c_{kp} b^p \right) \;=\; 0$$

L'anneau $\mathbf{B}$ est normal, donc localement sans diviseur de zéro et il existe z et z' tels que $z + z' = 1$, $z\,\mu_0 = 0$ donc $z\,\beta_m = 0$, et

$$z' \left(c_{k0} a^p + c_{k1} a^{p-1} b + \cdots + c_{kk} a^{p-k} b^k + \cdots + c_{kp} b^p \right) \;=\; 0$$

Intuitivement, on raisonne dans les deux localisations $\mathbf{A}_z$ et $\mathbf{A}_{z'}$. Dans $\mathbf{A}_{z'}$, on a :

$$c_{k0} a^p + c_{k1} a^{p-1} b + \cdots + c_{kk} a^{p-k} b^k + \cdots + c_{kp} b^p \;=\; 0\,.$$

Précisément, dans $\mathbf{A}$ on a

$$c_{k0} z' a^p + c_{k1} z' a^{p-1} b + \cdots + c_{kk} z' a^{p-k} b^k + \cdots + c_{kp} z' b^p \;=\; 0\,.$$

D'après le lemme 5.6, il existe dans $\mathbf{B}$ des éléments s_k, v_k, w_k, t_k tels que :

$$\begin{cases} s_k\, a &=& v_k\, b \\ w_k\, a &=& t_k\, b \\ s_k + t_k &=& z'\, c_{kk} \end{cases} \tag{16}$$

Dans $\mathbf{A}_z$, $\beta_m = 0$ et on a $Q(b) = b^m + \beta_1 b^{m-1} + \cdots + \beta_{m-1} b = 0$. Précisément, dans $\mathbf{A}$ on a $z^m Q(b) = bz\, Q_1(bz) = bz\, ((bz)^{m-1} + (z\beta_1)(bz)^{m-2} + \cdots + (z^{m-1}\beta_{m-1})) = 0$. On introduit z_1 et z_1' tels que $z_1 + z_1' = 1$, $z_1\, zb = 0$ et $z_1'\, Q_1(bz) = 0$. Donc

$$\left\{\begin{array}{rcl} 0\, a & = & 0\, b \\ 0\, a & = & z z_1 c_{kk}\, b \\ 0 + z z_1 c_{kk} & = & z z_1 c_{kk} \end{array}\right. \tag{17}$$

Puisque $m \geq 2$ on a aussi ${z_1'}^{m-1} Q_1(bz) = Q_2(bzz_1') = 0$ avec Q_2 unitaire de degré $m-1$. En appliquant l'hypothèse de récurrence on a s, t, v, w, dans $\mathbf{B}$ tels que

$$\left\{\begin{array}{rcl} s\, a & = & v\, bzz_1' \\ w\, a & = & t\, bzz_1' \\ s + t & = & 1 \end{array}\right.$$

et donc

$$\left\{\begin{array}{rcl} szz_1' c_{kk}\, a & = & v(zz_1')^2 c_{kk}\, b \\ w c_{kk}\, a & = & t z z_1' c_{kk}\, b \\ szz_1' c_{kk} + t z z_1' c_{kk} & = & z z_1' c_{kk} \end{array}\right. \tag{18}$$

L'addition des trois systèmes (16), (17) et (18) nous donne s_k', v_k', w_k', t_k' tels que :

$$(S_k) \qquad \left\{\begin{array}{rcl} s_k'\, a & = & v_k'\, b \\ w_k'\, a & = & t_k'\, b \\ s_k' + t_k' & = & c_{kk} \end{array}\right.$$

Et il reste à faire la somme des systèmes (S_k) pour $k = 0, \ldots, p$. □

5.4 Les cas cohérent et fortement discret

Lemme 5.7 *Soit* $\mathbf{A}$ *un anneau intégralement clos dans son anneau total des fractions. Si* $\mathbf{A}$ *est quasi intègre, alors* $\mathbf{A}$ *est normal.*

Preuve Tout d'abord remarquons que $\mathbf{A}$ est localement sans diviseur de zéro donc réduit. Soient $x, y \in \mathbf{A}$ et $y^n = a_1 y^{n-1} x + \cdots + a_{n-1} y x^{n-1} + a_n x^n$ une relation de dépendance intégrale de y sur l'idéal $\langle x \rangle$. Soit r l'idempotent annulateur de x, $s = 1 - r$ et $a_i' = s a_i$. On a $r y^n = 0$, donc puisque $\mathbf{A}$ est réduit $ry = 0$ et $sy = y$. L'annulateur de $x' = r + x$ est 0. Et on a $y^n = a_1' y^{n-1} x' + \cdots + a_{n-1}' y {x'}^{n-1} + a_n' {x'}^n$. Donc $y = cx'$ avec $c \in \mathbf{A}$ et $y = sy = scx' = scx$. Donc $\mathbf{A}$ est normal. □

Proposition 5.8 *Soit* $\mathbf{A}$ *un anneau normal quasi intègre. Soit* $f(X) \in \mathbf{A}[X]$ *un polynôme unitaire dont le discriminant est non diviseur de zéro. Soit* $\mathbf{A}' = \mathbf{A}[X]/\langle f(X) \rangle$ *et* $\mathbf{B}$ *la clôture intégrale de* $\mathbf{A}'$ *dans son anneau total des fractions. Alors* $\mathbf{B}$ *est un anneau quasi intègre.*

Preuve Voici une preuve nettement plus simple que celle du théorème 15 dans [13]. Notons $\mathbf{K}$ l'anneau total des fractions de $\mathbf{A}$ et $\mathbf{L}$ celui de $\mathbf{A}'$ (c'est aussi celui de $\mathbf{B}$). On a $\mathbf{L} \simeq \mathbf{K}[X]/\langle f(X) \rangle$. Par la proposition 1.20 l'anneau $\mathbf{L}$ est zéro-dimensionnel et comme il est réduit, il est quasi intègre. Soit $x \in \mathbf{B}$ et r son annulateur idempotent dans $\mathbf{L}$. Puisque $r^2 = r$, r est entier sur $\mathbf{A}$ donc $r \in \mathbf{B}$, et l'idéal annulateur de x dans $\mathbf{B}$ est $r\mathbf{B}$. □

Théorème 5.3 *Soit* $\mathbf{A}$ *un anneau de Prüfer cohérent. Soit* $f(X) \in \mathbf{A}[X]$ *un polynôme unitaire dont le discriminant est non diviseur de zéro. Soit* $\mathbf{A}' = \mathbf{A}[X]/\langle f(X)\rangle$ *et* $\mathbf{B}$ *la clôture intégrale de* $\mathbf{A}'$ *dans son anneau total des fractions. Alors* $\mathbf{B}$ *est un anneau de Prüfer cohérent.*
En outre si $\mathbf{A}$ *est fortement discret (resp. noethérien), alors il en va de même pour* $\mathbf{B}$.

Preuve La première affirmation est conséquence de la proposition 5.8, du lemme 5.7 et du théorème 5.2 page 45. □

6 Anneaux de Prüfer cohérents de dimension ≤ 1

Un bon cadre d'étude est constitué par les anneaux de Prüfer cohérents de dimension ≤ 1 dans lesquels on a le "théorème deux générateurs" et le résultat important : un anneau quasi intègre cohérent normal de dimension ≤ 1 est un anneau de Prüfer. Pour diminuer le nombre de générateurs d'un idéal de type fini nous nous sommes inspirés de [22].

Dans le cas local on a immédiatement.

Lemme 6.1 *Si* $\mathbf{A}$ *est un domaine de valuation de dimension* ≤ 1*et si* a, b *sont deux éléments non nuls de* $\mathrm{Rad}(\mathbf{A})$ *il existe deux entiers* > 0 m *et* n *et deux éléments* x *et* y *tels que* $a = xb^m$ *et* $b = ya^n$*. En conséquence un domaine de valuation est de dimension* ≤ 1*si et seulement si son groupe de valuation est archimédien.*

6.1 Factorisation et dimension 1

Montrons que $\mathbb{Z}$ est de dimension ≤ 1 directement au sens de la définition 1.17.

Soit $x, y \in \mathbb{Z}$. On les suppose non nuls sans perte de généralité. Dire qu'il existe $n \in \mathbb{N}$, et $a, b \in \mathbb{Z}$, tels que $y^n(x^n(1-ax) - by) = 0$ revient à dire que $x^n(1-ax) \in \langle y \rangle$. Or la décomposition en facteurs premiers dans $\mathbb{Z}$ nous donne :

$$\begin{array}{rcccl} x & = & e_1^{\alpha_1} \cdots e_i^{\alpha_i} . f_1^{\beta_1} \cdots f_j^{\beta_j} & = & e.f \\ y & = & e_1^{\gamma_1} \cdots e_i^{\gamma_i} . g_1^{\delta_1} \cdots g_\ell^{\delta_\ell} & = & e'.g \end{array}$$

$\langle x, g \rangle = \langle 1 \rangle$, donc il existe u, v dans $\mathbb{Z}$, tels que $ux + vg = 1$, et $1 - ux = vg$. Alors pour un n assez grand (par exemple avec $n = \sup \gamma_i$), $x^n = e'.h$ et $x^n(1-ux) = e'.h.vg = (h.v)y$. D 'où $x^n(1-ux) \in \langle y \rangle$.

Plus généralement on a

Lemme 6.2 *Un anneau de Prüfer à factorisation partielle est de dimension* ≤ 1.

Preuve Soit $x,\ y \in \mathbf{A}$. On a $\mathrm{Ann}(x) = r$, avec $r + s = 1$ et $\mathrm{Ann}(y) = e$, avec $e + f = 1$. Alors $(r+s)(e+f) = e + rf + sf = 1$. Dans A_e et A_{rf}, pour tout $n > 0$, $a = b = 0$, la relation de la définition 1.17 est triviale.
Il suffit donc de la vérifier en localisant en sf. Dans A_{sf}, x et y sont non diviseurs de zéro. La factorisation partielle de $(\langle x \rangle, \langle y \rangle)$ nous donne :
$\langle x \rangle = P_1^{\alpha_1} \cdots P_i^{\alpha_i} Q_1^{\beta_1} \cdots Q_j^{\beta_j} = I.J$, et $\langle y \rangle = P_1^{\gamma_1} \cdots P_i^{\gamma_i} R_1^{\delta_1} \cdots R_k^{\delta_k} = K.H$ avec tous les exposants non nuls. Donc il existe n tel que I^n soit un multiple de K et $\langle x \rangle^n = K.M$. Comme $\langle x \rangle + H = 1$, il existe $a \in \langle x \rangle$ et $h \in H$ tels que $ax + h = 1$. On a $x^n(1-ax) \in \langle x \rangle^n . H \subset K.M.H \subset \langle y \rangle$.
Donc il existe $b \in \mathbf{A}_{sf}$, tel que $x^n(1-ax) = by$, et $y^n(x^n(1-ax) - by) = 0$.
Finalement dans $\mathbf{A}$ on a donc $sf(y^n(x^n(1-ax) - by)) = 0$, c'est-à-dire :
$(1-e-rf)(y^n(x^n(1-ax)-by)) = y^n(x^n(1-ax)-(sf)by)) = y^n(x^n(1-ax)-b'y)) = 0$
□

Soit dans un anneau de dimension ≤ 1 un élément y non diviseur de zéro et un autre élément x. On a une égalité $x^n(1-ax) = by$. Posons $J = \langle x \rangle$, $I = \langle y \rangle$, $I_1 = \langle y, 1-ax \rangle$, $I_2 = \langle y, x^n \rangle$. On a $\langle x^n \rangle + \langle 1-ax \rangle = \langle 1 \rangle$ et $I = \langle y \rangle = \langle y, 1-ax \rangle \langle y, x^n \rangle = I_1 I_2$ avec $I_1 + J = \langle 1 \rangle$ et $I_2 = \langle y, x^n \rangle = I + J^n = I + J^{n+1}$. Ainsi l'idéal I est décomposé en deux facteurs étrangers. Le premier facteur est

étranger à J et le deuxième contient une puissance de J. Sur un anneau de Prüfer cohérent, ceci se généralise aux idéaux de type fini.

Théorème 6.1 *Soit dans un anneau de Prüfer cohérent de dimension ≤ 1 deux idéaux de type fini I et J avec I inversible. Alors on peut écrire $I = I_1 I_2$ avec $I_1 + J = \langle 1 \rangle$ et $J^n \subseteq I_2$ pour un entier n convenable. Cette écriture est unique et on a $I_2 = I + J^n = I + J^{n+1}$.*

Preuve Supposons $I = I_1 I_2$ avec $I_1 + J = \langle 1 \rangle$ et $J^n \subseteq I_2$. Alors $1 - j \in I_1$ pour un certain $j \in J$ et $j^n \in I_2$ donc $I_1 + I_2 = \langle 1 \rangle$, donc $I = I_1 I_2 = I_1 \cap I_2$. Cela donne $I + J^n = (I_1 \cap I_2) + J^n = (I_1 + J^n) \cap (I_2 + J^n) = \langle 1 \rangle \cap I_2 = I_2$. Et $I_1 = I \div (I + J^n)$ (cf. proposition 3.7 (1)). Cela montre l'uncité si n est fixé.
Plus généralement pour tout entier $m > 0$ définissons $J_m = I \div (I + J^m)$. La suite J_m est croissante. On a $(J + J_m)(I + J^m) = IJ + J^{m+1} + J_m(I + J^m) = I + J^{m+1}$, donc ($I + J^m$ est inversible)

$$J + J_m = \langle 1 \rangle \iff I + J^m = I + J^{m+1}$$

et cela établit définitivement l'unicité de (I_1, I_2) avec $I_1 = J_m$ dès que $I + J^m = I + J^{m+1}$ (ce qui équivaut à $J + J_m = \langle 1 \rangle$ ou encore à $J_m = J_{m+1}$). L'existence est donc assurée dans le cas noethérien, mais la dimension ≤ 1 suffit. En effet on considère une famille de monoïdes comaximaux tels que les localisés de I et J soient tous deux principaux. La solution du problème est trouvée dans chaque cas d'après ce qu'on a dit juste avant. On considère alors un exposant n qui majore tous ceux qui ont été obtenus dans les différentes localisations. On calcule un système fini de générateurs pour $J_n = I \div (I + J^n)$. L'égalité $J + J_n = \langle 1 \rangle$ est vraie localement donc globalement, et le problème est résolu globalement. □

Un corollaire immédiat est le suivant.

Théorème 6.2 *Soit dans un anneau de Prüfer cohérent de dimension ≤ 1 des idéaux de type fini deux à deux étrangers $P_1, \ldots, P_n$ et un idéal inversible I. Alors on peut écrire $I = I_0 \cdot I_1 \cdots I_n$ avec les idéaux de type fini I_j deux à deux étrangers et $P_j^{m_j} \subseteq I_j$ pour des entiers m_j convenable. Cette écriture est unique et on a $I_j = I + P_j^{m_j} = I + P_j^{1+m_j}$.*

6.2 Tout idéal de type fini est engendré par 2 éléments

Nous rappelons la preuve du lemme suivant qui est une clé qui ouvre la boite des petits systèmes générateurs pour les idéaux.

Lemme 6.3 *(lemme 1.15 dans [22]) Soit I un idéal de type fini d'un anneau $\mathbf{A}$. Supposons que le $\mathbf{A}/I$-module I/I^2 est engendré par (les classes modulo I^2 de) $x_1, \ldots, x_n$. Soit $J = \langle x_1, \ldots, x_n \rangle$ alors I est engendré par $x_1, \ldots, x_n, e$ où e est dans A/J un idempotent qui engendre I/J.*

Preuve par hypothèse $I^2 + J = I$. Soit $I_1 = I/J$ (idéal de A/J). On a $I_1^2 = (I^2 + J)/J = I/J = I_1$. Puisque I_1 est un idéal de type fini idempotent il est engendré par un idempotent, qui est la classe modulo J d'un élément $e \in \mathbf{A}$ et il est clair que $I = J + \langle e \rangle$. □

Théorème 6.3 (théorème "deux générateurs") *Dans un anneau quasi intègre de dimension ≤ 1 tout idéal de type fini projectif est engendré par deux éléments. En conséquence sur un anneau de Prüfer cohérent de dimension ≤ 1 tout idéal de type fini est engendré par deux éléments.*

Preuve Considérons tout d'abord le cas d'un idéal de type fini I de rang 1 (donc contenant un non diviseur de zéro x). L'anneau $\mathbf{A}/\langle x\rangle$ est zéro-dimensionnel par le lemme 1.23, et a fortiori l'anneau $\mathbf{B} = \mathbf{A}/I$ est zéro-dimensionnel. Le $\mathbf{B}$-module I/I^2 est obtenu à partir du $\mathbf{A}$-module I par "extension des scalaires" de $\mathbf{A}$ à $\mathbf{B}$ et il est donc projectif de rang 1 sur $\mathbf{B}$. Comme $\mathbf{B}$ est zéro-dimensionnel le $\mathbf{B}$-module I/I^2 est principal (d'après 1.21). On conclut par le lemme 6.3.
Dans le cas général on raisonne dans l'anneau A_r où $1-r$ est l'idempotent annulateur de I. □

Le théorème un et demi

Nous ne savons pas si tout anneau de Prüfer cohérent de dimension ≤ 1 vérifie le *théorème un et demi*, qui s'énonce comme suit : *si I est un idéal inversible et $x \in I$ est non diviseur de zéro, alors il existe $y \in I$ tel que $I = \langle x, y\rangle$*. Cela semble improbable, mais plus plausible pour les anneau de Prüfer à factorisation partielle. Nous démontrerons ce théorème dans le cas noethérien (théorème 7.2 page 57).

Dans un anneau de Prüfer cohérent le théorème un et demi implique facilement : si I est un idéal de type fini et $x \in I$ a le même annulateur que I, alors il existe $y \in I$ tel que $I = \langle x, y\rangle$.

Voici une autre conséquence importante.

Théorème 6.4 *Soit $\mathbf{A}$ un anneau de Prüfer cohérent de dimension ≤ 1 vérifiant le théorème un et demi. Soit a un non diviseur de zéro et $S = 1 + a\mathbf{A}$. Alors le localisé $\mathbf{A}_S$ est un anneau de Bezout cohérent. En particulier si $a \in \mathrm{Rad}(\mathbf{A})$, $\mathbf{A}$ est un anneau de Bezout.*

Preuve Comme la cohérence se conserve par localisation il suffit de démontrer le cas particulier. Il suffit de montrer que tout idéal inversible I est principal. Soit $x_1 \in I$ non diviseur de zéro. On a une égalité $x_1^n(a^n(1-\alpha a) - \beta x_1) = 0$ donc $a^n(1-\alpha a) = \beta x_1$ donc $a^n \in \langle x_1\rangle \subseteq I$ (on aurait pu aussi invoquer le théorème 6.1). On a donc des éléments b, c tels que $I = \langle a^n, b\rangle = \langle a^{n+1}, c\rangle$. On a une égalité $a^n = \alpha a^{n+1} + \beta c$, donc $a^n(1-\alpha a) = \beta c$, et puisque $a \in \mathrm{Rad}(\mathbf{A})$ $a^n \in \langle c\rangle$ et $I = \langle a^{n+1}, c\rangle = \langle c\rangle$. □

6.3 Pour $n \geq 3$, $\mathbf{SL}_n(\mathbf{A}) = \mathbf{E}_n(\mathbf{A})$

Théorème 6.5 *Soit $n \geq 3$ et $(x_1, \ldots, x_n)$ un vecteur unimodulaire sur un anneau de Prüfer cohérent $\mathbf{A}$ de dimension ≤ 1. Ce vecteur est la première colonne d'une matrice de $\mathbf{E}_n(\mathbf{A})$. En particulier $\mathbf{SL}_n(\mathbf{A}) = \mathbf{E}_n(\mathbf{A})$ pour $n \geq 3$. Et pour $n \geq 2$ tout vecteur unimodulaire est la première colonne d'une matrice de $\mathbf{SL}_n(\mathbf{A})$.*

Preuve L'annulateur de $\langle x_1, \ldots, x_n\rangle$ est nul, donc par le lemme 1.11 on peut par manipulations élémentaires transformer le vecteur colonne $v = {}^t(x_1, \ldots, x_n)$ en un vecteur ${}^t(y_1, x_2, \ldots, x_n)$ où y_1 est non diviseur de zéro. Considérons l'anneau $\mathbf{B} = \mathbf{A}/\langle y_1\rangle$. Cet anneau est zéro-dimensionnel et le vecteur v devient ${}^t(0, x_2, \ldots, x_n)$

tout en restant unimodulaire. Puisque $n \geq 3$ on peut transformer dans $\mathbf{B}$ par manipulations élémentaires les coordonnées $x_2, \ldots, x_n$ en $1, 0, \ldots, 0$. Regardons dans $\mathbf{A}$ ce qu'on obtient alors : ${}^t(y_1, 1 + ay_1, z_3, \ldots, z_n)$, d'où ensuite, toujours par manipulations élémentaires ${}^t(y_1, 1, z_3, \ldots, z_n)$ puis ${}^t(1, 0, \ldots, 0)$. □

6.4 Une propriété caractéristique simple

Le lemme et le théorème suivants ont été démontrés en maths classiques dans [19]. Nous sommes intéressés par des preuves constructives.

Lemme 6.4 *Soit un anneau* $\mathbf{A}$ *local normal intègre cohérent de dimension* ≤ 1. *On suppose que* $\mathbf{A}$ *est discret et que le radical* $\mathrm{Rad}(\mathbf{A}) = M$ *de* $\mathbf{A}$ *est détachable. Alors* $\mathbf{A}$ *est un anneau de valuation.*

Preuve (I. Yengui) Soit $\mathbf{K}$ le corps des fractions de $\mathbf{A}$. Nous allons montrer que tout idéal de type fini est inversible.
Il suffit de traiter le cas $I = \langle a_1, \ldots, a_r \rangle$, $a_i \in \mathrm{Rad}(\mathbf{A}) = M$, $a_i \neq 0$. Nous raisonnons dans le monoïde $\mathcal{F}_{\mathbf{A}}$ des idéaux fractionnaires. Nous ne considérons que des idéaux fractionnaires de type fini non nuls et puisque $\mathbf{A}$ est cohérent nous rappelons que le quotient $I_1 \div I_2$ défini comme $\{x \in \mathbf{K}\,;\, x\, I_2 \subseteq I_1\}$ est un idéal fractionnaire de type fini (lemme 2.23). Ainsi $\mathbf{A} \div I$ est un idéal fractionnaire de type fini, et $W = I\,(\mathbf{A} \div I)$ est un idéal de type fini de $\mathbf{A}$. On veut montrer que $W = \mathbf{A}$. On commence par montrer que $\mathbf{A} \div W = \mathbf{A}$, comme suit.
Comme $\mathbf{A}$ est normal, on a

$$(\mathbf{A} \div I) \div (\mathbf{A} \div I) = \mathbf{A}$$

En effet si $y\,(\mathbf{A} \div I) \subseteq (\mathbf{A} \div I)$ alors puisque $(\mathbf{A} \div I)$ est de type fini, par un déterminant trick y est entier sur $\mathbf{A}$ donc appartient à $\mathbf{A}$ (cf. lemme 5.2). Or $(\mathbf{A} \div I) \div (\mathbf{A} \div I) = \mathbf{A} \div (I\,(\mathbf{A} \div I)) = \mathbf{A} \div W$ donc $\mathbf{A} \div W = \mathbf{A}$.
En conséquence, par une récurrence immédiate $\mathbf{A} \div W^k = \mathbf{A}$ pour tout $k > 0$.
Écrivons maintenant $W = I\,(\mathbf{A} \div I) = \langle x_1, \ldots, x_n \rangle$, $x_i \in \mathbf{A}$, $x_i \neq 0$. On veut montrer que l'un des x_i est inversible. Si $x_1, ..., x_{n-1} \in M$, puisque $\mathbf{A}$ est de dimension ≤ 1 et x_n est non nul, il existe des entiers naturels $k_1, ..., k_{n-1}$ tels que $x_i^{k_i} \in \langle x_n \rangle$, $1 \leq i \leq n-1$ (cf. lemme 1.23). Posons $k = k_1 + \cdots + k_{n-1} + 1$. Alors

$$W^k \subseteq \langle x_n \rangle \quad \text{et donc} \quad \mathbf{A} \div \langle x_n \rangle \subseteq \mathbf{A} \div W^k = \mathbf{A}.$$

Finalement $x_n^{-1} \in \mathbf{A}$ et $W = \mathbf{A}$. □

Le lemme précédent est la version locale du théorème suivant.

Théorème 6.6 *Un anneau normal cohérent de dimension* ≤ 1 *est un anneau de Prüfer.*

Preuve En maths classiques, le théorème résulte du lemme puisque les anneaux de Prüfer sont caractérisés comme les anneaux dont tous les localisés (en des idéaux premiers) sont des anneaux de valuation. Mais cette preuve ne donne naturellement pas la matrice de localisation principale pour un idéal de $\mathbf{A}$. Pour ce faire, on va reprendre la preuve précédente tout d'abord dans le cas d'un anneau intègre avec un idéal de type fini non nul I en appliquant la technique dite "du bon usage de

l'anneau trivial" (cf. [20]). La preuve est inchangée jusqu'au milieu. Puis on reprend comme ceci.

Écrivons maintenant $W = I\,(\mathbf{A} \div I) = x_1\mathbf{A} + \cdots + x_n\mathbf{A}$, $x_i \in \mathbf{A}$, $x_i \neq 0$. On veut montrer que $W = \mathbf{A}$ ou, ce qui revient au même, que l'anneau localisé $\mathbf{B} = \mathbf{A}_{1+W}$ est trivial. Or $x_1, ..., x_{n-1} \in \operatorname{Rad}\mathbf{B}$, $\mathbf{B}$ est de dimension ≤ 1 et x_n reste non diviseur de zéro dans $\mathbf{B}$, donc il existe des entiers naturels $k_1, ..., k_{n-1}$ tels que $x_i^{k_i} \in x_n\mathbf{B}$, $1 \leq i \leq n-1$ (cf. lemme 1.23). Posons $k = k_1 + \cdots + k_{n-1} + 1$. Alors

$$W^k \subseteq x_n\mathbf{B} \quad \text{et donc} \quad \mathbf{B} \div (x_n\mathbf{B}) \subseteq \mathbf{B} \div W^k = \mathbf{B}.$$

Donc $x_n^{-1} \in \mathbf{B}$ et $\mathbf{B} = 0$ puisque $x_n \in \operatorname{Rad}\mathbf{B}$.

Débarrassons nous maintenant de l'hypothèse d'intégrité. Nous ne supposerons même pas que l'anneau est discret ni que l'idéal de type fini est non nul. Tout d'abord, puisqu'un anneau normal est localement sans diviseur de zéro, un anneau normal cohérent est quasi intègre (lemme 1.12). Soit I un idéal de type fini, r l'idempotent annulateur de I et $s = 1-r$. On se place dans l'anneau A_s. Autrement dit, nous supposons sans perte de généralité que $\operatorname{Ann} I = 0$ (donc I contient un non diviseur de zéro). La preuve se déroule ensuite comme dans le cas intègre. On voit facilement que W contient un non diviseur de zéro qui joue le role de x_n dans la preuve précédente. □

7 Anneaux de Dedekind

Définition 7.1 *On appelle* anneau de Dedekind *un anneau de Prüfer cohérent noethérien et fortement discret. Dans le cas où il est intègre, on dira que c'est un domaine de Dedekind.*

7.1 Les anneaux de Dedekind sont à factorisation partielle

Dans cette sous-section "les suites croissantes d'idéaux de type fini pausent" est une définition constructive suffisante de la noetheriannité (c'est celle de Richman-Seidenberg, cf. [16]).

Théorème 7.1 *: Soit* $\mathbf{A}$ *un anneau de Dedekind. Alors toute famille finie d'idéaux inversibles de* $\mathbf{A}$ *admet une factorisation partielle. Autrement dit un anneau de Dedekind est un anneau de Prüfer à factorisation partielle.*

Rappelons que les idéaux inversibles d'un anneau de Prüfer forment la partie positive d'un groupe réticulé.

Le théorème 7.1 page 55 se déduit directement de la proposition 7.3 qui concerne les groupes réticulés noethériens.

Groupes réticulés noethériens

On appelle *groupe réticulé* un groupe ordonné dans lequel toute partie finie non vide admet une borne supérieure et une borne inférieure.

La théorie constructive des groupes réticulés est donnée dans [4].

Un groupe réticulé est dit *noethérien* si toute suite décroissante d'éléments ≥ 0 pause.

Nous notons : $G^+ = \{\ x \in G\ /\ \ x \geq 0\ \}$, et $G^{+\star} = \{\ x \in G\ /\ \ x > 0\ \}$

Rappelons que $a, b \in G^+$ sont dits *étrangers* si $a \wedge b = 0$.

Définition 7.2 *Soit* $F = (x_1, \ldots, x_n)$ *une famille d'éléments* > 0 *d'un groupe réticulé* G*. On dit que* F *admet une* factorisation partielle *s'il existe une famille* $P = (p_1, \ldots, p_k)$ *d'éléments* > 0 *deux à deux étrangers, telle que tout élément* x_i *de* F *peut s'écrire sous la forme :* $x_i = \sum_{j=1}^{k} m_{ij} p_j$ *(les* m_{ij} *sont dans* $\mathbb{N}$*). On dit alors que* $(p_1, \ldots, p_k)$ *est une* base de factorisation partielle *pour la famille* F*.*

Nous avons le résultat important suivant.

Proposition 7.3 *: Soit* $(G, 0, +, -, \vee, \wedge, <, =)$ *un groupe réticulé noethérien discret. Toute famille* $(x_1, \ldots, x_k)$ *d'éléments de* $G^{+\star}$ *admet une factorisation partielle : elle est donnée par une famille* $\{p_1, \ldots, p_\ell\} \in G^{+\star}$ *telle que :* $p_i \wedge p_j = 0$ *si* $i \neq j$*, et des entiers* $m_{ij} \geq 0$ *tels que,* $x_i = \sum_{j=1}^{\ell} m_{ij} p_j$*.*

Nous utiliserons le lemme suivant.

Lemme 7.4 *Pour toute famille d'éléments deux à deux étrangers* $\{p_1, \ldots, p_m\}$ *de* $G^{+\star}$ *et* $a \in G^+$*, on peut trouver des éléments deux à deux étrangers* $a_0, a_1, \ldots, a_m$ *dans* G^+ *tels que :*

(1) $a = \sum_{i=0}^{m} a_i$.

(2) *Pour tout* $i \in \{1, \ldots, m\}$ *il existe un entier* $n_i \geq 0$ *tel que* $a_i \leq n_i p_i$.

(3) *Pour tout* $i \in \{1, \dots, m\}$ $(a_0 \wedge p_i) = 0$.

Preuve : Pour un i fixé, on a :
Soit $x_0 = a$, $g_0 = x_0 \wedge p_i$, et $c_0 = g_0$.
De façon générale, on pose :
$x_k = x_{k-1} - g_{k-1}$, $g_k = c_k \wedge p_i$, et $c_k = c_{k-1} + g_k = g_0 + \cdots + g_k$.
La suite (x_n), est une suite d'élements positifs qui est décroissante, donc il existe n_i tel que $x_{n_i} = x_{n_i+1}$. On prend alors $a_i = c_{n_i} = g_0 + \cdots + g_{n_i}$. Noter que $a_i \leq n_i p_i$.
On construit ainsi $a_1, \dots, a_n$ tels que $a = a_1 + \cdots + a_n + a_0$, avec $a_i \leq n_i p_i$ pour $i \in \{1, ..., m\}$. Enfin on a pour tout i, $a_0 \wedge p_i = 0$, car sinon, il existerait un j, tel que $a_0 \wedge p_j \neq 0$. Or $a = a_j + b_j$, avec $a_j \wedge b_j = 0$. Si $a_0 \wedge p_j \neq 0$, alors $a_0 \leq a_j$, $a_0 \leq b_j$, et $a_j \wedge b_j \neq 0$. (absurde) □

Preuve (de la proposition 7.3) : On procède par récurrence sur k.
• Supposons $k = 2$, considérons les éléments x_1, x_2. Pour les besoins de la notation, appellons les a, b. Posons $L_1 = [a, b]$, $m_1 = 1$ $E_{1,a} = [1, 0]$, $E_{1,b} = [0, 1]$.
L'algorithme procède par étape, au début de l'étape k on a un entier naturel m_k et trois listes d'égale longueur : L_k, une liste d'éléments > 0 de G, $E_{k,a}$ et $E_{k,b}$ deux listes d'entiers naturels. A la fin de l'étape l'entier m_k et les trois listes sont remplacés par un nouvel entier et de nouvelles listes, qui servent pour la boucle suivante (à moins que l'algorithme termine). L'idée générale est la suivante : si x, y sont deux termes consécutifs de L_k non étrangers, on remplace dans L_k le segment x, y par le segment $x - (x \wedge y)$, $x \wedge y$, $y - (x \wedge y)$ (en omettant le premier et/ou le dernier terme s'il est nul). Nous appellerons cette procédure dans la suite : $R : (x, y) \mapsto$ le nouveau segment (de longueur 1, 2 ou 3). Notez que $x + y > (x - (x \wedge y)) + x \wedge y + (y - (x \wedge y))$.
Nous devons définir un invariant de boucle. Précisément les conditions vérifiées par l'entier m_k et les trois listes sont les suivantes :

- a est égal à la combinaison linéaire des éléments de L_k affectés des coefficients qu'on trouve dans $E_{k,a}$,
- b est égal à la combinaison linéaire des éléments de L_k affectés des coefficients qu'on trouve dans $E_{k,b}$,
- si $L_k = [x_{k,1}, \dots, x_{k,r_k}]$ les éléments $x_{k,j}$ et $x_{k,\ell}$ sont étrangers dès que
  - $j < m_k$ et $\ell \neq j$ ou
  - $j \geq m_k$ et $\ell \geq j + 2$

En bref, les $x_{k,j}$ sont deux à deux étrangers sauf peut-être certaines paires $(x_{k,j}, x_{k,j+1})$ avec $j \geq m_k$. Ces conditions constituent *l'invariant de boucle*. Il est clair qu'elles sont (trivialement) vérifiées au départ. L'algorithme termine à l'étape k si les éléments de L_k sont deux à deux étrangers. En outre, si l'algorithme ne termine pas à l'étape k on a $\sum_{x \in L_k} x > \sum_{z \in L_{k+1}} z$, donc la condition de noethériannité assure la terminaison de l'algorithme.
Il nous reste à expliquer le déroulement d'une étape et à vérifier l'invariant de boucle. Pour ne pas manipuler trop d'indices, faisons un léger abus de notation et écrivons $L_k = [p_1, \dots, p_n]$, $m_k = i$, $E_{k,a} = [\alpha_1, \dots, \alpha_n]$ et $E_{k,b} = [\beta_1, \dots, \beta_n]$.
Le segment x, y de L_k qui est traité par la procédure $R(x, y)$ est le suivant : si $p_i \wedge p_{i+1} \neq 0$ on prend $(x, y) = (p_i, p_{i+1})$ sinon on considère le plus petit indice j

(nécessairement $> i$) tel que $p_j \wedge p_{j+1} \neq 0$ et on prend $(x, y) = (p_j, p_{j+1})$. Si un tel indice n'existe pas, les éléments de L_k sont deux à deux étrangers et l'algorithme est terminé. Sinon on applique la procédure $R(x, y)$ et on met à jour l'entier (on peut prendre $m_{k+1} = j$) et les trois listes. Par exemple en posant $q_j = p_j \wedge p_{j+1}$, $p'_j = p_j - q_j$ et $p'_{j+1} = p_{j+1} - q_j$, si $p'_j \neq 0 \neq p'_{j+1}$, on aura :

$$\begin{array}{rcl} L_{k+1} & = & [p_1, \ldots, p_{j-1}, p'_j, q_j, p'_{j+1}, p_{j+2}, \ldots, p_n] \\ E_{k,a} & = & [\alpha_1, \ldots, \alpha_{j-1}, \alpha_j, \alpha_j + \alpha_{j+1}, \alpha_{j+1}, \alpha_{j+2}, \ldots \alpha_n] \\ E_{k,b} & = & [\beta_1, \ldots, \beta_{j-1}, \beta_j, \beta_j + \beta_{j+1}, \beta_{j+1}, \beta_{j+2}, \ldots \beta_n] \end{array}$$

On vérifie sans peine dans chacun des 4 cas possibles que l'invariant de boucle est conservé.

• Si $k > 2$, par hypothèse de récurrence on a pour les éléments $x_1, \ldots, x_{k-1}$ une base de factorisation partielle $[p_1, \ldots, p_n]$. En appliquant le lemme 7.4 à x_k et $[p_1, \ldots, p_n]$ on a : $x_k = \sum_{i=0}^{m} a_i$.
Le cas $(k = 2)$ nous donne pour chaque (a_i, p_i), $i \in [1, ..., n]$, une base de factorisation partielle S_i. Finalement la base de factorisation partielle de $[x_1, \ldots, x_k]$ est la concaténation des S_i et de $[a_0]$. □

7.2 Le théorème un et demi

Dans cette sous-section et la suivante, "les suites croissantes d'idéaux de type fini pausent" n'est plus une définition constructive suffisante de la noetheriannité pour assurer la terminaison de nos algorithmes. Il nous faut en fait une définition qui implique (dans le cas d'un anneau de Prüfer cohérent) que l'on ne peut pas raffiner indéfiniment des factorisations d'un idéal. Or un processus infini de raffinement de factorisations ne conduit à une suite croissante infinie d'idéaux de type fini qu'en vertu d'une forme non constructive du lemme de König.

Apparemment, la définition (plus forte) proposée par Jacobsson et Lofwall (cf. [8]) ou celle (encore plus forte) proposée par H. Perdry (cf. [18]) convient constructivement pour tous les théorèmes où intervient la noetheriannité dans ce mémoire.

Notez que du point de vue classique, les trois définitions constructives (distinctes constructivement) auxquelles nous faisons allusion sont équivalentes.

Théorème 7.2 (théorème un et demi) *Soient* **A** *un anneau de Dedekind et* I *un idéal de type fini de* **A** *contenant un non diviseur de zéro* a. *Il existe un élément* b *de* **A** *tel que* $I = \langle a, b \rangle$.

Preuve : Nous commençons par rappeler la preuve classique qui fonctionne dans le cas d'un anneau de Dedekind à factorisation complète. Décomposons l'idéal inversible $\langle a \rangle \div I$ en produit d'idéaux maximaux inversibles : $\langle a \rangle = I \cdot I_1$ avec $I_1 = P_1^{n_1} \cdots P_s^{n_s}$. Posons : $J = I \cdot P_1 \cdots P_s$ et $J_i = J \div P_i$. Soit $b_i \in J_i \setminus J$. On a $b_1 \notin I \cdot P_1$ car

$$(I \cdot P_1) \cap J_1 = (I \cdot P_1) \cap (I \cdot (P_2 \cdots P_s)) = I \cdot (P_1 \cap (P_2 \cdots P_s)) = I \cdot P_1 \cdot P_2 \cdots P_s = J$$

(la deuxième égalité résulte de la proposition 3.7). Par contre $b_2, \ldots, b_s \in I \cdot P_1$ donc $b = b_1 + \cdots + b_s \notin I \cdot P_1$. De même $b \notin I \cdot P_i$ $(i = 1, \ldots, s)$. Soit $K = \langle b \rangle \div I$, donc $\langle b \rangle = I \cdot K$. On a (pout tout i) $P_i \subsetneq K + P_i$ car sinon $P_i = K + P_i$ et $b \in I \cdot P_i$.

Or P_i est maximal donc $K + P_i = \langle 1 \rangle$. Donc $K + I_1 = K + P_1^{n_1} \cdots P_s^{n_s} = \langle 1 \rangle$ et $\langle a, b \rangle = \langle b \rangle + \langle a \rangle = (I \cdot K) + (I \cdot I_1) = I \cdot (K + I_1) = I \cdot \langle 1 \rangle = I$.
Reprenons la preuve précédente sans l'hypothèse de factorisation complète, et transformons là en une preuve qui n'utilise que des factorisations partielles. On va travailler avec des factorisations partielles de I_1. On remplace les idéaux maximaux $P_1, \ldots, P_s$ au dessus de I_1 par une famille d'idéaux de type fini deux à deux étrangers au dessus de I_1 : ceux qui interviennent dans une factorisation partielle. Au départ, on commence avec la factorisation partielle (I_1) : on fait comme si I_1 était maximal. Au cours de l'algorithme on est amené à calculer des factorisations de plus en plus fines de I_1. Dans ce contexte où les P_j ne sont peut-être pas maximaux, la preuve bute sur la phrase suivante : *Or P_i est maximal donc $K + P_i = \langle 1 \rangle$*. En effet nous savons seulement que $P_i \subsetneq K + P_i$. On doit donc tester pour chaque i si $K + P_i$ contient 1. Si toutes les réponses sont positives, la preuve se termine correctement. Si au moins une des réponses est négative, on calcule un raffinement de la factorisation partielle en cours en calculant une base de factorisation partielle pour $P_1, \ldots, P_s$ et pour les $K + P_i \neq \langle 1 \rangle$. Ceci casse les P_i correspondants (car $K + P_i$ est un diviseur strict de P_i). Et on recommence le calcul. Comme on ne peut pas raffiner indéfiniment les factorisations de I_1 cet algorithme termine à coup sûr. □

Puisqu'un anneau de Dedekind vérifie le théorème un et demi, on a le résultat suivant (cf. théorème 6.4) souvent formulé de manière équivalente (en maths classiques) en disant qu'un anneau de Dedekind qui n'a qu'un nombre fini d'idéaux premiers est un anneau de Bezout.

Proposition 7.5 *Soit* $\mathbf{A}$ *un anneau de Dedekind tel que* $\mathrm{Rad}(\mathbf{A})$ *contienne un non diviseur de zéro. Alors* $\mathbf{A}$ *est un anneau de Bezout.*

7.3 Structure des idéaux et des modules de présentation finie

On a en mathématiques classiques le lemme suivant fort utile, dont nous indiquons une preuve (non constructive).

Lemme 7.6 *Soit* $\mathbf{A}$ *un anneau noethérien intègre de dimension* ≤ 1. *Soient* I *et* J *deux idéaux avec* I *inversible. Il existe* $u \in \mathrm{F}(\mathbf{A})$ *tel que l'idéal* $u\,I$ *est entier et étranger à* J.

Preuve Soient $P_1, \ldots, P_n$ les idéaux maximaux au dessus de J. Puisque $\mathbf{A}$ est de dimension ≤ 1 nous savons qu'il existe des entiers α_i tels que

$$P_1^{\alpha_1} \cdots P_n^{\alpha_n} \subseteq J \subseteq P_1 \cap \cdots \cap P_n = P_1 \cdots P_n$$

On raisonne dans le monoïde des idéaux fractionnaires et on note I^{-1} l'inverse de I. Puisque $P_i \neq \langle 1 \rangle = I\,I^{-1}$, il existe $a_i \in I$ et $a'_i \in I^{-1}$ tels que $a_i\,a'_i \in \mathbf{A} \setminus P_i$. Par le théorème chinois il existe $\epsilon_i \in \mathbf{A}$ tel que $\epsilon_i \equiv 1$ modulo P_i et $\epsilon_i \equiv 0$ modulo P_j pour $i \neq j$. Posons $a = \sum_i \epsilon_i a_i$ et $a' = \sum_i \epsilon_i a'_i$; on a $a \in I$ et $a' \in I^{-1}$ donc $aa' \in \mathbf{A}$. En outre chaque $a_i a'_j$ est dans $\mathbf{A} = I I^{-1}$ donc

$$aa' = \sum\nolimits_{i,j} \epsilon_i \epsilon_j a_i a'_j \equiv a_k a'_k \not\equiv 0 \mod P_k$$

En conséquence $\langle aa'\rangle + P_k = \langle 1\rangle$ pour tout k et donc $\langle aa'\rangle + J = \langle 1\rangle$. Ainsi $\langle aa'\rangle \subseteq a'I \subseteq II^{-1} = \langle 1\rangle$ et $\langle 1\rangle = \langle aa'\rangle + J \subseteq a'I + J \subseteq \langle 1\rangle$. Ce qui donne la solution avec $u = a'$. □

La preuve précédente est constructive si $\mathbf{A}$ est un anneau intègre de dimension ≤ 1 *complètement Lasker Noether* au sens de l'algèbre constructive (cf. [16]). Mais l'hypothèse est trop forte pour nous.

Nous pouvons donner dans le cas qui nous intéresse ici une version constructive du lemme précédent en faisant subir à la preuve classique le même traitement que celui que nous avons fait subir à la preuve classique du théorème un et demi.

Lemme 7.7 *Soit* $\mathbf{A}$ *un anneau de Dedekind. Soient* I *et* J *deux idéaux (entiers) avec* I*, et* J *inversibles. Il existe* $u \in \mathrm{F}(\mathbf{A})$ *tel que l'idéal* $u\,I$ *est entier et étranger à* J*.*

Preuve On suppose sans perte de généralité que $\mathrm{Ann}(J) = 0$. Notre définition des anneaux de Dedekind inclut le caractère fortement discret. On reprend la preuve classique ci-dessus, en remplaçant les idéaux maximaux au dessus de J par une famille d'idéaux de type fini deux à deux étrangers au dessus de J : ceux qui interviennent dans une factorisation partielle. Au départ, on commence la factorisation partielle (J) : on fait comme si J était maximal. Au cours de l'algorithme on est amené à calculer des factorisations de plus en plus fines de J. Dans ce contexte où les P_j ne sont peut-être pas maximaux, la preuve bute sur la phrase suivante : *En conséquence* $\langle aa'\rangle + P_k = \langle 1\rangle$ *pour tout* k. En effet nous savons seulement que $aa' \in \mathbf{A} \setminus P_k$. On doit donc tester pour chaque k si $\langle aa'\rangle + P_k$ contient 1. Si toutes les réponses sont positives, la preuve se termine correctement. Si au moins une des réponses est négative, on calcule un raffinement de la base de factorisation partielle en cours, en rajoutant $\langle aa'\rangle$ dans la liste des idéaux à factoriser, ce qui cassera au moins l'un des P_k au dessus de J. Et on recommence le calcul. Comme on ne peut pas raffiner indéfiniment les factorisations de J cet algorithme termine à coup sûr. □

Théorème 7.3 *Sur un anneau de Dedekind, tout module projectif* M *de rang* $k \geq 2$ *est isomorphe à* $\mathbf{A}^{k-1} \oplus I$*, où* I *est un idéal inversible. En particulier il est engendré par* $k+1$ *éléments. Le résultat reste valable pour tout anneau de Prüfer cohérent vérifiant le lemme 7.7 page 59.*

Preuve D'après le théorème 4.1 page 36 M est une somme directe d'idéaux inversibles. Il suffit donc de traiter le cas $M \simeq I \oplus J$, avec des idéaux inversibles I et J. Par le lemme 7.7 on peut trouver un idéal I_1 tel que $I_1 \simeq I$ (comme $\mathbf{A}$-modules) et $I_1 + J = \langle 1\rangle$ (comme idéaux). On a alors la suite exacte courte

$$0 \longrightarrow I_1 \cap J \xrightarrow{\delta} I_1 \oplus J \xrightarrow{\sigma} I_1 + J = \mathbf{A} \longrightarrow 0$$

où $\delta(x) = (x, -x)$ et $\sigma(x, y) = x + y$. Elle est scindée et donc $M \simeq I \oplus J \simeq I_1 \oplus J \simeq \mathbf{A} \oplus I_1\,J$. □

Notez que si un module projectif de type fini n'est pas de rang constant, on a un théorème analogue en utilisant le sfio associé à M et la décomposition de M en somme directe de sous modules $r_k M$, chacun de rang constant sur $\mathbf{A}_{r_k}$.

Le théorème suivant semble faire partie du folklore en maths classiques. En voici une preuve constructive.

Théorème 7.4 *Soient* $\mathbf{A}$ *un anneau de Dedekind et* $x_1, \ldots, x_n \in \mathbf{A}$. *Il existe une matrice inversible* M *qui transforme* $(x_1, \ldots, x_n)$ *en* $(y_1, y_2, 0, \ldots, 0)$. *Le résultat est valable pour tout anneau de Prüfer cohérent vérifiant le lemme 7.7.*

Notez que ceci donne une nouvelle preuve (via le lemme 7.7) que tout idéal de type fini est engendré par deux générateurs (nous avions déjà les théorèmes 7.2 et 6.3).

Preuve Il suffit de traiter le cas où $n = 3$ et $\operatorname{Ann}\langle x_1, x_2, x_3\rangle = 0$. Soit A une matrice de localisation principale pour (x_1, x_2, x_3). Le module $K = \operatorname{Im}(\mathrm{I}_3 - A)$ est le noyau de la forme linéaire associée au vecteur ligne $X = (x_1, x_2, x_3)$ et c'est un module projectif de rang 2 en facteur direct dans $\mathbf{A}^3$. En appliquant le théorème 7.3 on en déduit que K contient un sous-module libre de rang 1 en facteur direct dans $\mathbf{A}^3$, c'est-à-dire un module $\mathbf{A}\,v$ où v est un vecteur unimodulaire de $\mathbf{A}^3$. Par le théorème 6.5, ce vecteur est la première ligne d'une matrice inversible M, et la première coordonnée de XM est nulle. □

Remarque d'implémentation : Nous donnons maintenant, dans le cas intègre, fortement discret et en caractéristique nulle, une méthode de construction de la matrice M moins sûre que celle qui résulte de la preuve précédente, mais qui semble en général plus rapide, et qui est plus facile à implémenter.

Il suffit de traiter le cas d'un vecteur (a, b, c). On commence par calculer une matrice de localisation principale A pour (a, b, c). On remarque qu'on a un test d'unimodularité pour les vecteurs de $\mathbf{A}^3$ (cf. proposition 3.6 page 29). La matrice de projection $P = \mathrm{I}_3 - A$ a dans son image un vecteur unimodulaire (u_1, u_2, u_3) que l'on peut calculer "avec une grande probabilité de succès" comme suit : on tire au hasard un vecteur colonne unimodulaire dans $\mathbb{Z}^3$ et on considère la combinaison linéaire correspondante des colonnes de P, enfin, on teste l'unimodularité du vecteur obtenu. Nous cherchons ensuite M sous la forme :

$$M = \begin{bmatrix} u_1 & x & i \\ u_2 & y & j \\ u_3 & z & k \end{bmatrix}$$

On veut à déterminer (x, y, z), (i, j, k) pour que M soit de déterminant 1. En développant ce déterminant par rapport à (i, j, k), on obtient

$$a'i + b'j + c'k = (u_2 z - u_3 y)i + (u_3 x - u_1 z)j + (u_1 y - u_2 x)k = 1 \quad (\star)$$

Donc $\operatorname{Im} M$ contient le vecteur unimodulaire

$$V = \begin{bmatrix} a' \\ b' \\ c' \end{bmatrix} = x \begin{bmatrix} 0 \\ u_3 \\ -u_2 \end{bmatrix} + y \begin{bmatrix} -u_3 \\ 0 \\ u_1 \end{bmatrix} + z \begin{bmatrix} u_2 \\ -u_1 \\ 0 \end{bmatrix}$$

Donc V est aussi un vecteur unimodulaire dans l'image de la matrice

$$\begin{bmatrix} 0 & -u_3 & u_2 \\ u_3 & 0 & -u_1 \\ -u_2 & u_1 & 0 \end{bmatrix}$$

On cherche par la méthode probabiliste, "avec une grande probabilité de succès", un tel vecteur unimodulaire. On obtient ainsi (a', b', c') et (x, y, z), et puisque (a', b', c') est unimodulaire il existe des éléments i, j, k tels que $a'i + b'j + c'k = 1 = det(M)$. En fait le test d'unimodularité de (a', b', c') donne i, j, k et fonctionne comme suit : on considère la matrice de localisation principale $D = (d_{ij})$ de (a', b', c'), et ce vecteur est unimodulaire si et seulement si les trois éléments du corps de fractions $i = d_{11}/a'$, $j = d_{22}/b'$, $k = d_{33}/c'$, sont dans $\mathbf{A}$ (cf. proposition 3.6).

Conclusion

Nous avons dans ce travail établi des versions algorithmiques simples pour des théorèmes qui ont reçu récemment une preuve constructive dans [13]. Notamment nous avons mis en place la machinerie calculatoire des matrices de localisation principale comme un outil de base dans les anneaux arithmétiques et les anneaux de Prüfer qui permet de simplifier de nombreuses preuves dans [13], en particulier la question des extensions entières.

Nous avons également établi des versions constructives pour certains théorèmes classiques importants concernant les anneaux de Prüfer cohérents de dimension ≤ 1, à factorisation partielle ou de Dedekind (sections 6 et 7). Les versions classiques concernaient en général uniquement le cas intègre. La théorie constructive des anneaux de Dedekind dans [16] reposait sur une hypothèse de factorisation complète qui s'applique pour les corps de nombres mais qui n'est pas très naturelle (par exemple elle ne s'applique pas en toute généralité aux corps de fonctions algébriques).

Quelques résultats dont on aimerait donner une version algorithmique simple (une preuve constructive existe déjà).

Notamment :

La proposition 1.24 sur le fait qu'une extension entière d'un anneau de dimension ≤ 1 est encore un anneau de dimension ≤ 1.

La proposition 3.7 sur les propriétés de distributivité dans le treillis des idéaux de type fini d'un anneau arithmétique.

La proposition 4.10 sur la structure des modules de présentation finie sur un anneau de Prüfer cohérent.

Le lemme 5.3 sur le caractère intégralement clos des idéaux de type fini dans un anneau de Prüfer.

Quelques résultats de maths classiques dont on aimerait donner une version constructive.

Nous pensons particulièrement aux théorèmes suivants.

Le théorème de structure des modules de torsion de présentation finie pour les Dedekind : somme directe de modules $\mathbf{A}/I$.

Le théorème de Lequain-Simis [15] : tout module projectif de type fini M sur un $\mathbf{A}[X_1, \ldots, X_n]$ où $\mathbf{A}$ est un anneau de Prüfer cohérent, peut être obtenu par extension des scalaires à partir d'un $\mathbf{A}$-module projectif de type fini. Ceci est une généralisation remarquable (sans hypothèse noethérienne) du théorème de Quillen-Suslin, lequel répond positivement à la conjecture de Serre.

Le théorème qui affirme que les anneaux $\mathbf{A}[X_1, \ldots, X_n]$ comme ci-dessus sont cohérents et "réguliers" au sens suivant : tout module de présentation finie admet une résolution projective de longueur $\leq n$.

Quelques questions ouvertes (à notre connaissance).

Nous pensons notamment aux questions suivantes.

Une extension entière d'un anneau de Prüfer à factorisation partielle est-elle toujours un anneau de Prüfer à factorisation partielle ?

Un idéal de type fini projectif de rang 1 est-il toujours inversible sur un anneau arithmétique cohérent ? (cela permettrait d'étendre le théorème 6.3 au cas d'un anneau arithmétique cohérent de dimension quelconque : le nombre de générateurs d'un idéal inversible peut être ramené à $1 + \dim \mathbf{A}$).

Quels théorèmes de structure valables pour les Dedekind restent valables pour les anneaux de Prüfer à factorisation partielle, pour les anneaux de Prüfer cohérents de dimension ≤ 1 ? En particulier un anneau de Prüfer à factorisation partielle vérifie-t-il le théorème un et demi, le lemme 7.7 ?

On souhaiterait avoir une forme réduite agréable (après changement de bases à la source et au but) pour une matrice arbitraire sur un anneau de Dedekind (ce qui généraliserait le théorème 7.4), voire sur un anneau de Prüfer à factorisation partielle, voire sur un anneau de Prüfer cohérent de dimension ≤ 1.

Annexe 1 : Codes Axiom

Nous construisons d'abord les catégories des principaux anneaux sur lesquels nous travaillons. Puis nous definissons les domaines des extensions et des idéaux.

(1) La catégorie des anneaux arithmétiques : la matrice de localisation principale est construite par la procédure "distribute". En plus nous avons un test pour vérifier si la matrice obtenue vérifie les propriétés (8) de la définition d'une telle matrice.

)ab cat ARITRNG ArithmeticalRing

```
ArithmeticalRing : Category == CommutativeRing with

     distribute : (%,%) -> Record(local: %, coef1: %, coef2:%)
     ++ distribute(x1,x2) = (local=u, coef1=v, coef2=w) =>
     ++ u x2 = v x1
     ++ (1-u) x1 = w x2

     distribute : Vector(%) -> Matrix(%)

     distributeTest : Vector(%) -> Boolean

     Nonzerodivisor : Vector(%) -> %
      --- cette procedure nous donne le premier element non nul
      ---de la liste dans le cas integre, ou 0 si la liste est nulle


     modulo : (%,%) -> %
      --- pour simplifier nos calculs nous introduisons une procedure
      --- modulo(a,b) qui nous donne (si possible) une valeur "reduite"
      --- de a dans la classe mod(b)
      --- On l'utilisera surtout dans le "theo2" des ideaux


   add

     distribute(vect:Vector(%)) : Matrix(%)  ==
       n := #(vect)
       (n <= 1) => matrix([[1]])
       every?(zero?, vect) => (m : Matrix(%) := new(n,n,0) ; m(1,1) := 1 ; m)
       if member?(0$%, vect)
       then
         d : Matrix(%) := distribute( remove(zero?, vect) )
         b : Matrix(%) := scalarMatrix(n,0)
         I : List(NonNegativeInteger) := [i for i in 1..n | not(vect.i=0)]
         for j in 1..#(I) for j' in I repeat
            -- on a : j' = I.j
            for i in 1..#(I) for i' in I repeat
              -- on a : i' = I.i
              b(i',j') := d(i,j)
       else
         (u,v,w) := distribute(vect.1 , vect.2)
         b : Matrix(%) := matrix([[u,v],[w,1-u]])
         liste : List(%) := entries(vect)
         for j in 3..n for vj in liste(3..n) repeat
           -- on a : b = distribute(vect(1..j-1))
           -- et vj = b.j
```

```
        vin : List(Record(local:%, coef1: %, coef2: %)) :=
           [distribute(vi,vj) for vi in liste(1..j-1)]
           -- [distribute(vect.i,vect.j) for i in 1..j-1]
        a : Matrix(%) := new(j,j,0)
        for i in 1..j-1 repeat
          u := vin.i.local
          for k in 1..j-1 repeat
            a(i,k) := u * b(i,k)
          a(i,j) :=  vin.i.coef1 * b(i,i)
        for i in 1..j-1 repeat
          a(j,i) := "+"/[b(k,i) * vin.k.coef2 for k in 1..j-1]
        a(j,j) := 1 - "+"/[a(i,i) for i in 1..j-1]
        -- on obtient : a = distribute(vect(1..j))
        b := a
      b


    distributeTest(x) : Boolean  ==
      n := #(x)
      b : SquareMatrix(n,%) := squareMatrix(distribute(x))
      for i in 1..n repeat
        for j in 1..n repeat
          for k in 1..n repeat
            if not(b(i,j) * x.k = b(i,k) * x.j)
            then return(false)
      one?(trace(b))



    Nonzerodivizor(v) ==
      every?(zero?,v) => 0
      remove(zero?, v).1



    modulo(a,b) == a
```

(2) Catégorie des anneaux fortement discrets

)ab cat SDRING StronglyDiscreteRing

```
StronglyDiscreteRing : Category == CommutativeRing with

      exquo : (%,%) -> Union(Boolean,  %)
```

(3) Catégorie des anneaux arithmétiques fortement discrets

)ab cat ARITSDRNG ArithmeticalStronglyDiscreteRing

```
ArithmeticalStronglyDiscreteRing : Category ==
       Join(ArithmeticalRing , StronglyDiscreteRing) with

      oneSolLin: (Vector(%) , %)  ->  Vector(%)

    add

      oneSolLin(b : Vector(%) , c : %) : Vector(%) ==
        n := #(b)
        A : Matrix(%) := distribute(b)
```

```
        V : Vector(%) := vector([c*A(i,i) for i in 1..n])
        d : Vector(%) := vector([exquo(Vi,b.i)::%  for i in 1..n])
        d
```

(4) Catégorie des anneaux de Bezout

)ab cat BERNG BezoutRing

```
BezoutRing : Category == ArithmeticalRing with

      BezoutCoeff : Vector(%) -> Record(coef:Vector(%) , generator:%)
      +++ BezoutCoeff(x1,...xn) := ((u1,..un) , g)  avec
      +++ g = u1x1 +.....+unxn

      BezoutQuo : (Vector(%) , %) -> Vector(%)
      +++ BezoutQuo((x1,..xn) , g) : (y1,...yn)
      +++ tel que xi = g*yi

      distribute : Vector(%) -> Matrix(%)

    add

      distribute(v:Vector(%)) ==
        n := #v
        (n <= 1) => matrix([[1]])
        every?(zero?, v) => (m : Matrix(%) := new(n,n,0) ; m(1,1) := 1 ; m)
        p := BezoutCoeff(v)
        Y : Matrix(%) := matrix([(BezoutQuo(v , p.generator)])
        U : Matrix(%) := matrix([p.coef])
        A : Matrix(%) := transpose(U) * Y
        A(n,n) := 1 - "+"/[U.i * Y.i for i in 1..n]
        A
```

(5) Catégorie des anneaux réduits

)ab cat REDRING ReducedRing

```
ReducedRing : Category == CommutativeRing with

        reduced? : () -> Boolean
        ++ if  [ x**2 := 0 then x=0 ]

   add
        reduced?() == true
```

(6) Catégorie des anneaux de Prüfer

)ab cat PRURING PruferRing

```
PruferRing : Category == Join(ArithmeticalRing , ReducedRing)
```

(7) Catégorie des anneaux quasi intègres

)ab cat PPRING PPRing

```
--- anneaux quasi integre
PPRing  : Category ==  CommutativeRing with

       killer : % -> %
       ++ r = killer(a)  =>
       ++ a r = 0
```

```
      ++ r r = r
      ++ \forall x , x a = 0 => xr = x

      killer : Vector(%) -> %
      --- l'annulateur de tout ideal de type fini est aussi
      --- un idempotent
    add

      killer(V : Vector(%)) ==
        n := #(V)
        R : list(%) := [killer(V.i) for i in 1..n]
        r : % := */[R.i for i in 1..n]

        r
```

(8) Catégorie des anneaux de Prüfer quasi intègres

)ab cat PUPPRNG PruferPPRing

```
PruferPPRing  : Category == Join(PruferRing , PPRing) with

     projective : Vector(%) -> Matrix(%)
     --- On calcule une matrice de projection Q dont l'image est
     --- egale au noyau de L

    projectiveTest : Vector(%) -> Boolean
    --- on teste si la projective du vector est bien une matrice
    --- de projectionb qui annule le vector

    projectiveTest : (Matrix(%) , Vector(%)) -> Boolean
    --- Pour une matrice M et un vecteur v donnes, on verifie que
    --- M est bein une matrice de projection pour v.

  add

    projective(L : Vector(%)) : Matrix(%) ==
       every?(zero?, L) => scalarMatrix(#L, 1)
       scalarMatrix(#L,1) - (1 - killer(L))*distribute(L)


    projectiveTest(L:Vector(%)) : Boolean ==
      p := projective(L)
      q : SquareMatrix(#L, %) := squareMatrix(p)
      (p*p=p)::Boolean and every?(zero?,L*p)
            and ((trace(q)=(#L-1+killer(%))::%)::Boolean or every?(zero?, L))


    projectiveTest(M: Matrix(%) , L:Vector(%)) : Boolean ==
      not(nrows(M) = ncols(M) = #(L)) => error failed
      q : SquareMatrix(#L, %) := squareMatrix(M)
      (p*p=p)::Boolean and every?(zero?,L*p)
            and ((trace(q)=(#L-1+killer(%))::%)::Boolean or every?(zero?, L))
```

(9) Catégorie des anneaux cohérents
)ab cat COHERNG CoherentRing

```
CoherentRing  :  Category  ==  CommutativeRing  with

     homogenousLinSolve: Vector(%)  -> Record(matrice: Matrix(%),  vecteur :
Vector(%))
     --- LX = 0 <===> il existe une matrice G et un vecteur Y,  X = GY

     homogenousSysLinSolve: Matrix(%) ->
         Record(matrice: Matrix(%),  vecteur : Vector(%))

   add

     homogenousSysLinSolve(M: Matrix(%)): Record(matrice: Matrix(%), vecteur:
Vector(%)) ==
       n := nrows(M)
       p := ncols(M)
       V : Vector(%) := vector([M(1,j) for j in 1..p])
       X : Record(matrice: Matrix(%), vecteur : Vector(%))
                 := homogenousLinSolve(V)
       G : Matrix(%) :=  X.matrice
       for i in 2..n repeat
         V : Vector(%) := vector([M(i,j) for j in 1..p])
         X  :=  homogenousLinSolve(V*G)
         G : Matrix(%) := G*(X.matrice)
       [G , X.vecteur]
```

(10) Catégorie des anneaux cohérents fortement discrets
)ab cat SDCRNG StronglyDiscreteCoherentRing

```
StronglyDiscreteCoherentRing  : Category == CoherentRing  with

     oneSolLin : (Vector(%) , %) ->  Vector(%)
     ---- pour (L,c) donne, on calcule Z tel que LZ = c

     linSolve: (Vector(%) , %) ->
               Record(particuliere: Vector(%), generale: Matrix(%))

     sysLinsSolve: (Matrix(%), Vector(%)) ->
               Record(particuliere: Vector(%), generale: Matrix(%))

   add

     linSolve(b: Vector(%) , d:%) ==
       X0 : Vector(%) := oneSolLin(b , d)
       -- X0 est une solution particuliere de l'equation
       X : Record(matrice: Matrix(%),  vecteur : Vector(%))
                  :=  homogenousLinSolve(b)
       G : Matrix(%) := X.matrice
       [X0 , G]
       -- la solution generale de l'equation est de la forme
       -- X0 + GY ou Y est un Vector(%)

     sysLinSolve(B: Matrix(%), D: Vector(%)) :
      Record(particuliere: Vector(%), generale: Matrix(%)) ==
       n := nrows(B)
```

```
      p := ncols(B)
      not(n = #D) => error "Bad call in sysLinSolve"
      V : Vector(%) := vector([B(1,j) for j in 1..p])
      X := linSolve(V, D.1)
      X0 : Vector(%) := X.particuliere
      G : Matrix(%) := X.generale
      -- X est la solution de l'equation 1 : [X0,G]
      for i in 2..n repeat
        -- la solution des equations 1,...,i-1 est [X0,G]
        -- on reduit l'equation i : B'X = D'
        B': Vector(%) := vector([B(i,j) for j in 1..p])
        D' := D.i - (B' * (X0::Matrix(%))).1
        B' := B' * G
        Y := linSolve(B', D')
        X0 := X0 + G * Y.particuliere
        G := G * Y.generale
        -- la solution des equations 1,...,i est [X0,G]
      [X0,G]
```

(11) Catégorie des anneaux de Prüfer cohérents

)ab cat PUCORNG PruferCoherentRing

```
PruferCoherentRing : Category ==
           Join(PruferPPRing , CoherentRing) with

      homogenousLinsolve: Vector(%)  ->  Matrix(%)
      ++++ Ker L = Im P

    add

      homogenousLinSolve(V : Vector(%)): Matrix(%) ==
        projective(V)
```

(12) Catégorie des anneaux de Prüfer fortement discrets

)ab cat PUSDRNG PruferStronglyDiscreteCoherentRing

```
PruferStronglyDiscreteCoherentRing : Category ==
   Join(PruferCoherentRing , StronglyDiscreteCoherentRing) with

      exquo : (%,%) -> Union(Boolean  %)

      oneSolLin: (Vector(%) , %)  ->  Vector(%)

    add

      oneSolLin(b : Vector(%) , c : %) : Vector(%) ==
        n := #(b)
        A : Matrix(%) := distribute(b)
        V : Vector(%) := vector([c*A(i,i) for i in 1..n])
        d : Vector(%) := vector([exquo(Vi,b.i)::%  for i in 1..n])
        d
```

(13) Catégorie des domaines de Prüfer
Ici aussi les differentes procedures de la projective marche. Il suffit de definir un "killer" plus simple.

)ab cat PRDO PruferDomain

```
PruferDomain :  Category ==
          Join(PruferPPRing,IntegralDomain, StronglyDiscreteCoherentRing) with

       killer : % -> %

       oneSolLin: (Vector(%) , %)  ->  Vector(%)

     add

       killer(x : %) ==
         (x = 0)  => 1
         not(x = 0) => 0

       oneSolLin(b : Vector(%) , c : %) : Vector(%) ==
         n := #(b)
         A : Matrix(%) := distribute(b)
         V : Vector(%) := vector([c*A(i,i) for i in 1..n])
         d : Vector(%) := vector([exquo(Vi,b.i)::%  for i in 1..n])
         d
```

(14) Catégorie des Domaines de Bezout

)ab cat BEDO BezoutDomain

```
BezoutDomain :  Category == Join(BezoutRing, PruferDomain)

      distribute : (%,%) -> Record(local:%, coef1:%, coef2:%)

    add

      distribute(v:Vector(%)) ==
        n := #v
        (n <= 1) => matrix([[1]])
        every?(zero?, v) => (m : Matrix(%) := new(n,n,0) ; m(1,1) := 1 ; m)
        p := BezoutCoeff(v)
        Y : Matrix(%) := matrix([(BezoutQuo(v , p.generator)])
        U : Matrix(%) := matrix([p.coef])
        transpose(U) * Y
```

(15) Nous construisons ici un domaine dans lequel se feraient la plupart de nos calculs.

)ab domain BEUCDOM BezoutEuclideanDomain

```
BezoutEuclideanDomain(R : EuclideanDomain) :
            Join(EuclideanDomain, BezoutDomain) with

      BezoutCoeff : Vector(%) -> Record(coef:Vector(%) , generator:%)

      BezoutQuo : (Vector(%) , %) -> Vector(%)

      homogenousLinSolve: Vector(%)  ->
                       Record(matrice: Matrix(%),  vecteur : Vector(%))
```

```
    coerce : R -> %
      ++ Pour obtenir des elements de % a partir de ceux de R.
    coerce : % -> R
      ++ ...et reciproquement.

  == R add
    Rep := R

    coerce(x:%) == (x::Rep)::R
    coerce(x:R) == (x::Rep)::%

    BezoutCoeff(v:Vector(%)) ==
      l := entries(v)
      principalIdeal(l)


    BezoutQuo(v : Vector(%) , c : %) ==
      l := entries(v)
      expressIdealMember(l)


    homogenousLinSolve(L : Vector(%)) ==
       scalarMatrix(#L,1) - projective(L)


    modulo(a:%,b:%) : % == a rem b
```

(16) Soit Z un anneau de Prüfer, on peut construire dans certains cas une matrice de localisation principale pour des éléments de $Z[X]/\langle f\rangle$. La méthode proposée ici ne marche pas pour tous les polynômes f, dans le cas contraire on utilise la "distribute" implementée dans le paragraphe suivant qui marche dans tous les cas.

)ab domain NUMRNG NumberRing

```
NumberRing(X,Z,f) : PUB == PRIV where
   X : Symbol
   Z : BezoutEuclideanDomain
   ZX == UnivariatePolynomial(X, Z)
   f : ZX
   SAE == SimpleAlgebraicExtension(Z, ZX, f)
   PRS == PseudoRemainderSequence(Z, ZX)

   PUB == Join(PruferDomain, MonogenicAlgebra(Z, ZX)) with
     distribute : (%,%) -> Record(local:%, coef1:%, coef2:%)

   PRIV == SAE add
     Rep := SAE

     reduced?() == not zero?(discriminant(f))

     h:% exquo g:% ==
        p : Union(ZX, "failed")
        if retractIfCan(g) case Z then
          p := lift(h) exquo$ZX retract(g)
          --- lift(h) met h dans l'anneau des polynomes ZX
        else
          sr := semiResultantEuclidean2(f, lift(g))$PRS
```

```
        --- semiResultantEuclidean2(f,g) donne le deuxieme coefficient
        --- et la resultante dans l'equation de la resultante
        pp := monicDivide(lift(h) * sr.coef2, f).remainder
        ---- monocDivide = division par un polynome unitaire
        p := pp exquo$ZX sr.resultant
      p case "failed" => "failed"
      convert(p::ZX)
      --- convert permet de mettre un element de ZX dans Z

  Nonzerodivisor(v : Vector(%)) : % ==
      (#v = 0) => 0$%
      every?(zero?, v) => 0$%
      l : List(%) := entries(remove(zero?, v))
      E : List(Z) := [retract(i)::Z for i in l | retractIfCan(i) case Z]
      N : List(Z) := [norm(i) for i in l]
      x : Z := gcd(concat(E,N))
      x::%

  distribute(a,b) ==
      d := degree(f)
      m0 : Matrix(Z) := new(d,d,0)
      mb : Matrix(Z) := transpose regularRepresentation(b)
      --- regularRepresentation(b) donne la transposee de
      --- la matrice de multiplication par b
      ma : Matrix(Z) := transpose regularRepresentation(a)
      haut := horizConcat(horizConcat(mb,-ma),m0)
      bas := horizConcat(horizConcat(ma,m0),mb)
      M : Matrix(Z) := vertConcat(haut,bas)
      C : Vector(Z) := concat(coordinates(0$%), coordinates(a))
      sol := syslinsolve(M,C)
      sp := sol.particuliere
      u : % := represents(sp(1..d))
      --- represents(vector) donne l'element de Z[a] dont les
      --- coordonnees sont dans vector
      v : % := represents(sp(d+1..2*d))
      w : % := represents(sp(2*d+1..3*d))
      [u,v,w]

  modulo(a:%, b:%) : % ==
      (a exquo b) case % => 0$%
      retractIfCan(b) case "failed" => a
      bb : Z := retract(b)
      aa : Vector(Z) := coordinates(a)
      aa := map(#1 rem$Z bb, aa)
      --- rem donne le reste de la division
      convert(aa)  --- On remet aa dans ZX/f
```

(17) Ici nous implémentons les principaux resultats de la section 5, plus précisément le théorème 5.1 page 43.

)ab domain PRNUMRNG PruferNumberRing

```
--- on construit l'anneau des entiers O d'un anneau de prufer Z

PruferNumberRing(X,Z,f) : PUB == PRIV where
   X : Symbol
   Z : PruferDomain
   Q == Fraction(Z)
```

```
UP ==> UnivariatePolynomial
ZX == UP(X, Z)
f : ZX
QX == UP(X, Q)
UPCF2 == UnivariatePolynomialCategoryFunctions2(Z,ZX,Q,QX)
 ---- UPCF2 est un package qui permet de passer de ZX dans QX
SAE == SimpleAlgebraicExtension(Q, QX, map(coerce,f)$UPCF2)
PRS == PseudoRemainderSequence(Q, QX)

PUB == Join(PruferDomain, MonogenicAlgebra(Q, QX)) with
  "*" : (Z,%) -> %
  "+" : (Z,%) -> %
  entier? : % -> Boolean
  setControl : Boolean -> Boolean
  control? : () -> Boolean
  distribute : (%,%) -> Record(local:%, coef1:%, coef2:%)

PRIV == SAE add
  Rep := SAE
  z:Z * x:% == (z::Q)::Rep * x
  z:Z + x:% == (z::Q)::Rep + x

  control : Boolean := true
  control?() == control
  setControl(b) == control := b

  check?(y : Rep) : Boolean ==
     for i in coefficients(characteristicPolynomial(y)) repeat
       if retractIfCan(i) case "failed" then return(false)
     true

  entier?(y : %) == check?(y::Rep)

  reduced?() == not zero?(discriminant(f))
  --- on teste si l'anneau est reduit

  killer(g : %) : % ==
     G : QX := lift(g)
     F : QX := map(coerce,f)$UPCF2
     -- f est un polynome de ZX, on le met dans QX
     d : QX := gcd(F, G)
     d := (F exquo d)::QX
     p := semiSubResultantGcdEuclidean1(d, G)$PRS
     -- semiSubResultantGcdEuclidean1(d, G) donne u et gcd(d,g)
     --  dans la relation :   u*d + v*g : gcd(d,g)
     -- Attention : p.gcd est inversible mais <> 1 a priori...
     convert(((p.coef1 * d) exquo p.gcd)::QX)
     --convert permet de passer de QX dans QX/f

  Nonzerodivisor(v : Vector(%)) : % ==
      (#v = 0) => 0$%
      every?(zero?, v) => 0$%
      l : List(%) := entries(remove(zero?, v))
      E : List(Z) :=
         [retract(retract(i)::Q)::Z for i in l | retractIfCan(i) case Q]
      if Z has EuclideanDomain then
```

```
        N : List(Z) := [retract(norm(i))::Z for i in l]
        x : Z := gcd(concat(E,N))
        not zero?(x) => return((x::Q)::%)
      not(empty?(E)) => ((E.1)::Q)::%
      for i in l repeat
        ni := norm(i)::%
        if not zero?(ni) then return(ni)
      0

--a:% / b:% == (a exquo$% b)::%
--a:% quo b:% == (a exquo$% b)::%
--recip(a:%) == 1 exquo$% a
--inv(a:%) == (1 exquo$% a)::%
a:% exquo b:% ==
   x := a exquo$Rep b
   x case "failed" => "failed"
   y : Rep := x::Rep
   not(control) => y::%
   check?(y) => y::%
   "failed"

distribute(a:%,b:%) ==
  y : Rep := a /$Rep b
  n := degree(f)
  l : List(Q) := entries(vectorise(characteristicPolynomial(y), n+1))
   --- vectorise(P) donne sous forme de vecteur les coef du poly
  pdenom := "*"/[denom(i) for i in l]
  l2 : Vector(Z) := vector([retract(i * pdenom) for i in l])
  S : Matrix(Z) := distribute(l2)
  z : % := 1 ; A : List(%) := concat(1$%, [(z := z*a) for i in 1..n])
  z : % := 1 ; B : List(%) := concat(1$%, [(z := z*b) for i in 1..n])
  AB : List(%) := [A.(i+1) * B.(n-i+1) for i in 1..n]
  for k in 1..n repeat
    So := "+"/[S(i,k+i) for i in 1..n-k+1]
    som := som + So * AB.k
  u : % := -som / B.(n+1)
  v : % := (u * b) / a
  w : % := ((1-u) * a) / b
  [u,v,w]

modulo(a:%,b:%) : % ==
   (a exquo b) case % => 0$%
   if Z has EuclideanDomain then
     retractIfCan(b) case "failed" => return(a)
     bb : Z := retract(retract(b)::Q)
     aa : List(Q) := entries(coordinates(a))
     aa := [( numer(i) rem$Z (bb*denom(i)) ) /denom(i) for i in aa]
     return(convert(vector(aa)))
   a
```

(18) Domaine des idéaux de type fini avec les differentes opérations sur ces idéaux, dont le théorème deux générateurs (**"theo2"**), la factoristion partielle (**"baseFactor"**), et le théorème un et demi (**"twoGenerators"**)

)ab domain ID Ideals

```
-- nos ideaux sont definis par leur generateurs, et la distribute associee

Ideals(R) : PUB == PRIV where
   R : PruferDomain
   SUP == SparseUnivariatePolynomial(R)
   NNI ==> NonNegativeInteger

   PUB == Monoid with

     "+" : (%, %) -> %
     0 : () -> %
     "exquo" : (%, R) -> Union(%, "failed")
     "exquo" : (R, %) -> Union(%, "failed")
     "exquo" : (%, %) -> Union(%, "failed")
     uniMod? : () -> Integer
     setUniMod : Integer -> Integer
     ideal : List(R) -> %
     ideal : Vector(R) -> %
     generators : % -> Vector(R)
     distribute : % -> Matrix(R)
     intersection : (%, %) -> %
     partialFactors : (%, %) ->
      Record(basis : List(%), exponents1 : List(NNI), exponents2 : List(NNI))
     decomp : (a : % , F : List(%))  ->  List(%)
     baseFactor : List(%) ->
        Record(basis : List(%), exponents : List(List(NNI)))

     unimodulaireChoix : Matrix(R) ->
                    Record(coordinates : List(R), vect : Vector(R))
     theo2 : (Vector(R), R) -> Vector(R)
     removeMultiple : List(R) -> List(R)
     vectorToIdeal : Vector(R) -> %
     baseFactor1 : (%, List(%), List(List(NNI))) ->
                  Record(basis : List(%), exponents : List(List(NNI)))
     in? : (R, %) -> Boolean
     twoGenerators : (% , R) -> R

   PRIV == Record(gen : List(R), dist : Matrix(R)) add
     Rep := Record(gen : List(R), dist : Matrix(R))

     coerce(a : %) : OutputForm == coerce(a.gen)
       -- pour un affichage lisible, on ne sort que les generateurs
       -- sans la matrice distribute

     vectorToIdeal(l : Vector(R)) : % ==
        construct(entries(l), distribute(l))
        -- L'argument est un vecteur suppose "reduit"

     listToIdeal(l : List(R)) : % == vectorToIdeal(vector(l))
        -- L'argument est une liste supposee "reduite"

     1 == listToIdeal([1$R])
```

```
0 == listToIdeal([0$R])

one?(J) ==
   I : List(R) := J.gen
   every?(zero?, I) => false
   S : Matrix(R) := J.dist
   for i in 1..#I | not(I.i=0) repeat
      if (S(i,i) exquo$R I.i) case "failed" then return(false)
   true

uniMod := 10 ;
uniMod?() == uniMod
setUniMod(n) == uniMod := n

unimodulaireChoix(M) :
   Record(coordinates : List(R), vect : Vector(R)) ==
   --- M est une matrice, et on cherche
   --- un vecteur qui engendre l'anneau
   n := ncols(M)
   L : List(Vector(R)) := [column(M,i) for i in 1..n]
   for j in 2..uniMod repeat
     c : List(R) := [(random(j)$Integer)::R for i in 1..n]
     --I : Vector(R) := "+"/[c.i * L.i for i in 1..n]
     I : Vector(R) := new(#(L.1),0$R)
     for ci in c for Li in L repeat
        I := I + ci*Li
     one?(vectorToIdeal(I)) => return(construct(c, I))
   error "unimodulaireChoix$ID : tentatives infructueuses"


theo2(W : Vector(R), a : R) : Vector(R) ==
   -- calcule un systeme de 2 generateurs de W modulo a
   #W < 3 => map(modulo(#1,a), W)
   V : Vector(R) := W(1..2)
   for x in entries(W(3..)) repeat
     V := concat(V, x)
     V := map(modulo(#1,a), V)
     p : Matrix(R) := projective(V)$R
     u : Vector(R) := unimodulaireChoix(p).vect
     -- en esperant que...
     m : Matrix(R) :=
           matrix([[0$R,-u.3,u.2],[u.3,0$R,-u.1],[-u.2,u.1,0$R]])
     v := unimodulaireChoix(m)
     -- en esperant que...
     w : Vector(R) := v.vect
     d : Matrix(R) := distribute(w)
     i : R := if w.1=0 then 0 else (d(1,1) exquo w.1)::R
     j : R := if w.2=0 then 0 else (d(2,2) exquo w.2)::R
     k : R := if w.3=0 then 0 else (d(3,3) exquo w.3)::R
     m := matrix([entries(u), v.coordinates, [i,j,k]])
     V := (m*V)(2..3)
   map(modulo(#1,a), V)


removeMultiple(I : List(R)) : List(R) ==
   J := I
```

```
      for i in I repeat
         not member?(i, J) => "suivant"
         for j in J | not(i=j) repeat
            if (j exquo i) case R then J := remove!(j,J)
      J

   reductionListe(I : List(R)) : List(R) ==
      a : R := bonChoix(vector(I))$R
      I := concat(a, I)
      I := remove!(zero?$R, I)
      I := removeDuplicates!(I)
      empty?(I) => [0$R]
      I := removeMultiple(I)
      (#I = 1) => I
      R has EuclideanDomain => [gcd(I)]
      I := concat(a, entries(theo2(vector(I), a)))
      I := remove!(zero?$R, I)
      I := removeDuplicates!(I)
      I := removeMultiple(I)

   reductionIdeal(J : %) : % ==
      one?(J) => 1$%
      I : List(R) := J.gen
      I := reductionListe(I)
      I = J.gen => J
      listToIdeal(I)

   ideal(v:Vector(R)) == ideal(entries(v))
   ideal(v:List(R)) ==
      J := listToIdeal(reductionListe(v))
      one?(J) => 1$%
      J

   generators(a : %) == vector(a.gen)
   distribute(a : %) == (a.dist)::Matrix(R)

   I + J ==
       ideal(concat(I.gen, copy(J.gen)))

   A * B ==
      I := A.gen
      J := B.gen
      pI := "+"/[monomial(I.i,i)$SUP for i in 1..#I]
      pJ := "+"/[monomial(J.i,i)$SUP for i in 1..#J]
      ideal(coefficients(pI*pJ))

   J:% exquo a:R ==
      I := J.gen
      c := new(#I,0$R)
      for i in 1..#I repeat
         d := I.i exquo$R a
         d case "failed" => return("failed")
         c.i := d::R
      reductionIdeal(construct(c, J.dist))

   a:R exquo J:% ==
```

```
   -- lemme \vref{}
   I : List(R) := J.gen
   every?(zero?, I) => "failed"
   S : Matrix(R) := J.dist
   c : List(R) := new(#I,0)
   for i in 1..#I | not(I.i=0) repeat
      d := (S(i,i) * a) exquo$R I.i
      d case "failed" => return("failed")
      c.i := d::R
   ideal(c)

J:% exquo K:% ==
   -- lemme \vref{}
   a : R := bonChoix(vector(K.gen))$R
   C : % := (a exquo K)::% * J
   C exquo a

I:% = J:% ==
  -- egalite entre deux ideaux
  e := I exquo$% J
  e case "failed" => false
  one?(e)


intersection(I:%, J:%) : % == ((I*J) exquo (I+J))::%
    --- lemme 8 page 14



partialFactors(a:%,b:%) :
  Record(basis: List(%), exponents1: List(NNI), exponents2: List(NNI))==
  --- base de factorisations partielle pour deux elements
  L : List(%) := [a,b]
  Ea : List(NNI) := [1,0]
  Eb : List(NNI) := [0,1]
  i : NNI := 1
  repeat
    -- L(j) et L(k) premiers entre eux pour tout j < i et tout k <> j
    -- L(j) et L(k) premiers entre eux pour tout j >= i et tout k >= j+2
    -- ici, a = "*" / [L(j)^Ea(j) for j in 1..#L]
    -- ici, b = "*" / [L(j)^Eb(j) for j in 1..#L]
    (#L < i) => break
    one?(L(i)) =>
       (L := delete!(L,i) ; Ea := delete!(Ea,i) ; Eb := delete!(Eb,i))
    (#L <= i) => break
    d := L(i) + L(i+1)
    one?(d) => (i := i+1)
    L := insert!(d, L, i+1)
    Ea := insert!( Ea(i)+Ea(i+1) , Ea, i+1)
    Eb := insert!( Eb(i)+Eb(i+1) , Eb, i+1)
    L(i) := (L(i) exquo d)::%
    L(i+2) := (L(i+2) exquo d)::%
  empty?(L) => construct([1$%],[0],[0])
  construct(L, Ea, Eb)

decomp(a , F) ==
```

```
      --- Voir lemme 9 page 15
      --- on decompose a dans la famille F d'ideaux
      --- etrangers deux a deux
      n := #(F)
      L : List(%) := new(n+1, 1)
      -- on pose a0 := a
      for j in 1..n repeat
        -- ici, a0 = L.1 * L.2 * ... * L.n * a
        while not(one?(g := a + F.j)) repeat
          a := (a exquo g)::%
          L.j := L.j * g
      L.(n+1) := a
      L

baseFactor1(a : %, F : List(%), expo : List(List(NNI)) ) :
          Record(basis : List(%), exponents : List(List(NNI))) ==
    --- F est deja une base de factorisation pour certains elements
    --- avec ses exposants dans expo.
    --- baseFactor1 reecrit a et les elements de F dans la nouvelle
    --- base obtenue par decomp(a,F) avec de nouveaux exposants.
    m := #F
    q : List(%) := decomp(a, F)
    base : List(%) := []
    expon : List(List(NNI)) := [[] for j in expo]
    expoLast : List(NNI) := []
    for j in 1..m repeat
       p := partialFactors(q.j, F.j)
       base := concat(base, p.basis)
       v : Vector(NNI) := vector(p.exponents2)
       expon := [concat!(expon.i, entries(expo.i.j *v)) for i in 1..#expo]
       expoLast := concat!(expoLast, p.exponents1)
    base := concat(base, q.(m+1))
    expoLast := concat!(expoLast, 1)
    expon := [concat!(i, 0) for i in expon]
    construct(base, concat!(expon, [expoLast]))


baseFactor(F : List(%)) :
   Record(basis : List(%), exponents : List(List(NNI))) ==
   -- Voir proposition 9  fin de la preuve( k > 2 )
   -- factorisation partielle pour une famille F d'ideaux
   -- etrangers deux a deux
   #F = 0 => construct([], [])
   #F = 1 => construct(F, [[1]])
   pF := partialFactors(F.1,F.2)
   base : List(%) := pF.basis
   exposants : List(List(NNI)) := [pF.exponents1, pF.exponents2]
   for a in F(3..) repeat
      bF := baseFactor1(a, base, exposants)
      base := bF.basis
      exposants := bF.exponents
   construct(base, exposants)


in?(x : R, I : %) : Boolean == (ideal([x]) exquo I) case %
-- on teste si x est dans l'ideal I
```

```
twoGenerators(I,a) ==
  --- theoreme 3 (theoreme un et demi) page 19
  --- I est un ideal contenant un non diviseurs de zero a
  not in?(a, I) => error "l'element n'est pas dans l'ideal"
  p : List(%) := partialFactors(I, ideal([a])).basis
  ajout : Boolean := true
  while ajout repeat
    ajout := false
    J0 : % := I * ("*"/p)
    J : List(%) :=[(J0 exquo i)::% for i in p]
    liste : List(R) := []
    for i in J repeat
      l : Vector(R) := select(in?(#1, I), generators(i))
      liste := concat!(liste, l.1)
    b : R := "+"/liste
    C : % := (ideal([b]) exquo I)::%
    F : List(%) := []
    for pi in p repeat
      C' := C+pi
      if one?(C') then
        F := concat!(F, pi)
      else
        ajout := true
        q := partialFactors(pi , C').basis
        F := concat!(F, q)
    p := F
  b
```

Annexe 2 : Exemples et résultats expérimentaux

7.4 Clôture intégrale

Dans cette section, nous allons calculer en appliquant les recettes précédentes quelques matrices de localisation principale dans des extensions entières de $\mathbb{Z}$. Cela nous permettra de calculer certaines clotures intégrales de manière relativement facile et plus ou moins automatique.

Rappelons que si x est un entier algébrique, racine du polynôme unitaire irréductible $P(X) \in \mathbb{Z}[X]$, l'anneau $\mathbf{B} = \mathbb{Z}[x]$ est intégralement clos si et seulement si tous les idéaux de la forme $\langle p, G(x)\rangle$, où p est un nombre premier qui divise le discriminant de P et G un facteur irréductible de P modulo p, sont inversibles (c'est suffisant par la proposition 4.13 et le lemme 5.3, c'est nécessaire par le théorème 5.1). La procédure donnée au théorème 5.1 page 43 calcule explicitement l'inverse dans la clôture intégrale de $\mathbf{B}$ et il suffit de tester si les générateurs de cet inverse sont dans $\mathbf{B}$. S'il s'avère que $\mathbf{B}$ n'est pas intégralement clos, notre connaissance de la cloture intégrale $\mathbf{B}'$ de $\mathbf{B}$ s'est néanmoins améliorée puisque nous disposons de nouveaux éléments dans $\mathbf{B}'$. En fait, l'anneau $\mathbf{B}_1$ engendré par x et ces nouveaux éléments est un *ordre* de $\mathbb{Q}[x]$ (un sous-anneau qui est un $\mathbb{Z}$-module libre de rang $\deg(P)$) contenu dans $\mathbf{B}'$, et on peut calculer une base de $\mathbf{B}_1$ comme $\mathbb{Z}$-module. Si on arrive à trouver les idéaux maximaux de $\mathbf{B}_1$ contenant p on calcule de nouveau leurs inverses dans $\mathbf{B}'$ par la procédure du théorème 5.1. En itérant le processus on finit par obtenir une base $\mathbf{B}'$ comme $\mathbb{Z}$-module, c'est-à-dire à calculer $\mathbf{B}'$.

Soit $\mathbf{B} = \mathbb{Z}[\sqrt[3]{2}]$.

$P(X) = X^3 - 2$, et $\operatorname{disc}(P) = -3^3 2^2$.
Les idéaux de la forme $\langle p, G(x)\rangle$ sont donc $\langle 2, x\rangle$ et $\langle 3, x+1\rangle$.
En fait ces idéaux sont principaux, on a :
$\langle 2, x\rangle = \langle x\rangle$ et $\langle 3, x+1\rangle = \langle x+1\rangle$.
L'anneau $\mathbf{B}$ est donc intégralement clos.

Soit $\mathbf{B} = \mathbb{Z}[\sqrt[3]{175}]$

$P(X) = X^3 - 175$, et $\operatorname{disc}(P) = -27(175)^2 = -3^3 7^2 5^4$.
On a : $\langle 3, x-1\rangle . \langle 522, -36x^2 + 78x + 192, 424x^2 - 167x - 236\rangle = 3$,
$\langle 7, x\rangle . \langle 49, 2x^2\rangle = 7$, et $\langle 5, x\rangle . \left\langle 5, -\frac{2}{5}x^2 \right\rangle = 5$.
On voit apparaître ici un nouveau élément dans la clôture qui n'est pas dans $\mathbf{B}$, donc ce dernier n'est pas intégralement clos.

7.5 Exemples de calculs de la matrice de localisation principale, et de la matrice de projection

Dans $\mathbb{Z}$

$\text{distribute}(30, 5, 11, 7, 0) =$

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ -900 & -150 & -330 & -210 & 0 \\ -600 & 110 & 242 & 154 & 0 \\ -390 & -65 & -143 & -91 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

distributeTest$(30, 5, 11, 7, 0)$ = true

En calculant la matrice de localisation principale du même vecteur, mais avec la procédure "distribute" implémentée dans les anneaux de Bezout on obtient une matrice plus simplifiée :

distribute$(30, 5, 11, 7, 0)$ =

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 60 & 10 & 22 & 14 & 0 \\ -90 & -15 & -33 & -21 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

distributeTest$(30, 5, 11, 7, 0)$ = true

projective$(30, 5, 11, 7, 0)$ =

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ -60 & -10 & -21 & -14 & 0 \\ 90 & 15 & 33 & 22 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

projectiveTest$(30, 5, 11, 7, 0)$ = true

Dans $\mathbb{Z}[i]$

distribute$(4x^2, -21x^4 + 53, 33x + 83)$ =

$$\begin{bmatrix} +247682292x + 2984124 & -1981458336x - 23872992 & -5164026582x + 1981458336 \\ 0 & 0 & 0 \\ +10257786x + 4222210 & -82062288x - 33777680 & -247682292x - 2984123 \end{bmatrix}$$

Dans $\mathbb{Z}[x]$ **avec** $x^2 = 5$

Nous utilisons ici la " distribute" implementée dans les **NumberRing** au paragraphe 16 de l'Annexe 1.

distribute$(x, 2)$ =

$$\begin{bmatrix} 5 & 2x \\ -2x & -4 \end{bmatrix}$$

distribute$(1+x,2)$ = " Error detected within library code Bad call in LinearSolve"

L'idéal $\langle 1+x,2\rangle$ n'est pas inversible dans cet anneau.

7.6 Exemples de calculs sur les idéaux

Soit A $= \mathbb{Z}[\sqrt[2]{-1}]$

Soit $I = \langle 4x^2, -21x^4+53, 33x+83\rangle$
Nonzerodivisor$(I) = 2$, et theo$(I,2) = \langle x+1, x+1\rangle = \langle x+1\rangle$
twoGenerators$(I,2) = \langle -x+1\rangle$.

Soit A $= \mathbb{Z}[\sqrt[2]{-5}]$

Soit $J = \langle 4x^2+22, 11x+1, 33x+83, 33x+83, 2x, 66x+54\rangle$
Nonzerodivisor$(J) = 2$.
twoGenerators$(J,2) = \langle 2, x+1\rangle$.

Soit A $= \mathbb{Z}[\sqrt[2]{5}]$

$\langle x-33\rangle \cap \langle x+4\rangle = \langle -29x-127\rangle$

La factorisation partielle de $\{\langle 23x+59\rangle, \langle 8x+21\rangle\}$ nous donne comme base de factorisation partielle :

$$\{\langle 76, 23x+59, x+29\rangle, \langle 11, 4x+5\rangle\}$$

et on a :

$$\begin{aligned} \langle 23x+59\rangle &= \langle 76, 23x+59, x+29\rangle . \langle 11, 4x+5\rangle \\ \langle 8x+21\rangle &= \langle 11, 4x+5\rangle^2 \end{aligned}$$

On peut obtenir aussi une autre base :

$$\{\langle 3x+11\rangle, \langle x+4\rangle\}$$

Alors

$$\begin{aligned} \langle 23x+59\rangle &= \langle 3x+11\rangle . \langle x+4\rangle \\ \langle 8x+21\rangle &= \langle x+4\rangle^2 \end{aligned}$$

Soient les idéaux :
$I = \langle 23x+59\rangle$, $J = \langle 8x+21\rangle$
$K = \langle 9968464, 236992x+2133636, -4089564x-6622376\rangle$ et
$L = \langle -5764x-12496\rangle$.
On obtient comme base de factorisation partielle de $\{I,J,K,L\}$ la famille $\{P_1, P_2, P_3, P_4, P_5\}$ égale à :

$$\left\{\langle x+1\rangle, \langle 2x+1\rangle, \langle x+4\rangle, \langle 271, 152x-138, 224x+196\rangle, \left\langle 11, -x-7, -\frac{21}{2}x+\frac{7}{2}\right\rangle\right\}$$

avec

$$
\begin{aligned}
I &= \langle x+1\rangle . \langle 2x+1\rangle . \langle x+4;\rangle = P_1.P_2.P_3 \\
J &= \langle x+4\rangle^2 = P_3^2 \\
K &= \langle x+1\rangle^2 . \langle 2x+1\rangle . \langle x+4\rangle^2 . \langle 271, 152x-138, 224x+196\rangle = P_1^2.P_2.P_3^2.P_4 \\
L &= \langle x+1\rangle^2 . \langle 2x+1\rangle . \langle x+4\rangle . \langle 271, 152x-138, 224x+196\rangle . \left\langle 11, -x-7, -\frac{21}{2}x+\frac{7}{2}\right\rangle \\
&= P_1^2.P_2.P_3.P_4.P_5
\end{aligned}
$$

Références

[1] Bernstein, D. *Factoring into coprimes in essentially linear time.* Journal of Algorithms (à paraître) 1

[2] 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. n°1122, 27–34 (1996). 1

[3] Buchmann J., Lenstra H. *Approximating rings of integers in number fields.* J. Théor. Nombres Bordeaux **6** (2) (1994), 221– 260. 1, 2

[4] Bourbaki N. *Algèbre. Groupes ordonnés.* 55

[5] Coquand T., Lombardi H. *Constructions cachées en algèbre abstraite (3) Dimension de Krull, Going Up, Going Down.* preprint. 13, 16

[6] Della Dora J., Dicrescenzo C., Duval D. *About a new method for computing in algebraic number fields.* EUROCAL '85. Lecture Notes in Computer Science n°204, (Ed. Caviness B.F.) 289–290. Springer 1985. 10

[7] Jensen C. *Arithmetical rings.* Acta Mathematica Academiae Scientiarum Hungaricae **17**, (1-2), (1966) 115–123. 27

[8] Jacobsson C., Lofwall C. *Standard Bases for general coefficient rings and a new constructive proof of Hilbert's Basis Theorem* J. Symbolic Computation, **12**, (1991) 337–371 57

[9] Hallouin E. *Parcours intiatique à travers la théorie des valuations* Rapport technique n°115 du Dept. de Maths de l'Université de Poitiers. (1997) 42

[10] Hermida J., Sánchez-Giralda T. *Linear Equations over Commutative Rings and Determinantal Ideals.* Journal of Algebra **99**, (1986) 72–79. 2, 33

[11] Kaplansky I. *Commutative Rings.* Allyn and Bacon, Mass. USA (1970). 27

[12] Larsen M., McCarthy P. *Multiplicattive Theory of Ideals.* Academic Press (1971). 27

[13] Lombardi H. *Platitude, localisation et anneaux de Prüfer, une approche constructive.* Preprint 2000. 2, 27, 36, 37, 41, 44, 47, 63

[14] Lombardi H. *Dimension de Krull, Nullstellensätze et Évaluation dynamique.* Math. Zeitschrift, sous presse. 13

[15] Lequain, Y., Simis, A. *Projective modules over R[X1,... ,Xn], R a Prüfer domain.* J. Pure Appl. Algebra **18** (2) (1980), 165–171. 63

[16] Mines R., Richman F., Ruitenburg W. *A Course in Constructive Algebra.* Springer-Verlag (1988). 1, 6, 55, 59, 63

[17] Northcott D. *A generalization of a theorem on the content of polynomials.* Proc. Cambridge Philos. Soc. **55** (1959), 282–288. 20

[18] Perdry H. *Aspects constructifs de la théorie des corps valués* Thèse. Besançon (2001). 57

[19] Quentel, Y. *Sur une caractérisation des anneaux de valuation de hauteur 1* C. R. Acad. Sci., Paris, Ser. A **265**, 659–661 (1967). 52

[20] Richman F. *Non trivial uses of trivial rings.* Proc. Amer. Math. Soc., **103** (1988), 1012–1014. 53

[21] Rota Gian Carlo *The many lives of lattice theory.* Notices Amer. Math. Soc. **44** (11), (1997), 1440–1445. 1

[22] Vasconcelos W. *The rings of dimension 2.* M. Dekker. NY. 1976. 49, 50

Résumé

Le but de cette thèse est de donner des preuves algorithmiques des résultats connus sur les *anneaux de Dedekind*.

La plupart des définitions usuelles se prêtent mal à ce traitement.

En effet les questions de factorisation qui sont en théorie considérées comme résolues se heurtent à des problèmes de complexité ou même de décidabilité comme la factorisation du discriminant.

Une partie du travail a consisté à donner des preuves constructives plus simples sur les *anneaux arithmétiques*, en utilisant les *matrices de localisation principale*.

Nous traitons la factorisation des idéaux dans le cadre des *anneaux de Prüfer cohérents*, et des *anneaux de Dedekind*, et nous travaillons plus en detail la notion de *factorisation partielle* qui est plus facile du point de vue algorithmique.

Nous proposons des versions algorithmiques des théorèmes "deux générateurs" et "un et demi" générateur sur les anneaux de *Prüfer cohérents de dimension* ≤ 1, et *les anneaux de Dedekind*.

A la fin nous donnons quelques exemples d'implémentation de certains de nos algorithmes en Axiom.

Abstract

The deal of this thesis is to give algorithmic proof of classical results on *Dedekind rings*.

Most of the usual definitions can't have algorithmic treatement.

Indeed factorisation problems which are classicaly solved are often not feasible in practice .

In the first part we give constructive proofs on *arithmetical rings*, using *principal localisation matrices*.

The factorisation of ideals is studied in the *Prüfer coherents rings* and *Dedekind rings*.

And the notion of *partial factorisation* is deeply investigated in an algorithmic way.

We propose constructive proofs for theorems "two generators" and "one and half" generator on *Prüfer Coherents rings of dimension* ≤ 1 and *Dedekind rings*.

At the end we give examples of implementation of some algorithms in Axiom.

MSC 2000 : 13A15, 13C10, 13C11, 13F05, 13F30, 13B22, 03F65.

Mots clés : Mathématiques Constructives, Anneaux arithmétiques, anneaux de Prüfer, Anneaux de Dedekind, Calcul formel.

Key Words : Constructive Mathematics, Arithmetical rings, Prüfer rings, Dedekind rings, Computer Algebra.