Théorie algorithmique des anneaux arithmétiques, des anneaux de Prüfer et des anneaux de Dedekind

L. Ducos, H. Lombardi, C. Quitté, M. Salou

Avril 2003

Résumé

Nous développons la théorie constructive des anneaux de Prüfer et de Dedekind. Les résultats de base de cette théorie sont reformulés de manière algorithmique. Les preuves que nous obtenons sont souvent plus simples et plus générales que celles que l'on trouve dans la littérature classique. Pour réaliser ces objectifs, de nombreuses définitions classiques doivent être reformulées de façon constructive. Nous ne faisons en général pas d'hypothèse d'intégrité, d'où l'importance accordée aux anneaux arithmétiques, aux anneaux de Prüfer (anneaux arithmétiques réduits) et anneaux de Prüfer cohérents (souvent appelés anneaux semi-héréditaires). Nous nous situons dans un cadre, naturel pour les applications concrètes, où l'on ne prétend pas disposer d'un algorithme de factorisation complète pour les idéaux inversibles d'un anneau de Dedekind. La factorisation complète d'un idéal inversible (qui n'existe pas toujours d'un point de vue constructif) est remplacée par l'existence de bases de factorisation partielle pour les familles finies d'idéaux inversibles. De nombreux résultats sont en outre démontrés dans le cadre moins restrictif des anneaux de Prüfer cohérents ou dans celui des anneaux de Prüfer cohérents de dimension inférieure ou égale à 1.

Abstract

We give a basic constructive theory for Prüfer rings and Dedekind rings. All results are given in a direct algorithmic way. Our proofs are often more simple and more general than the ones we found in classical literature. Many definitions have to be reformulated in an equivalent but constructive way. We don't assume in general to deal with domains, whence the importance given to arithmetical rings, Prüfer rings (arithmetical reduced rings) and Prüfer coherent rings (semi-hereditary rings). Our general setting for Dedekind rings does not include complete factorisation of invertible ideals. We prefer to use partial factorisation bases for finite families of invertible ideals, since they always do exist constructively. Moreover many important results are obtained in the weaker setting of Prüfer coherent rings or of dimension one Prüfer coherent rings.

Introduction

Motivations générales

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 [23]).

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. Nous montrons en particulier que la possibilité de calculer des factorisations partielles se conserve par extensions algébriques, à condition bien sûr de passer aux idéaux.

Un rôle crucial et simplificateur est joué par les *anneaux arithmétiques* (conformément à une intuition de Gian Carlo Rota [26]), qui sont les anneaux dans lesquels le treillis des idéaux est distributif, et par les *matrices de localisation principale*, qui sont les matrices qui explicitent la machinerie calculatoire des idéaux de type fini localement principaux.

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* et qui est souvent désigné par le vocable peu suggestif de « anneau semi-héréditaire »).
- la dimension de Krull est inférieure ou égale à 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 $\mathbb{R}$). Depuis [7, 20] on dispose

d'une caractérisation constructive de la dimension de Krull. Cela permet d'obtenir des versions algorithmiques pour les théorèmes qui traitent des anneaux de dimension inférieure ou égale à 1, comme par exemple le célèbre théorème « un et demi ». Nous obtenons aussi le théorème de structure pour les modules projectifs de type fini sur un anneau de Prüfer cohérent de dimension inférieure ou égale à 1 (théorème 4.4). Les théorèmes que nous démontrons pour les anneaux de dimension inférieure ou égale à 1 étaient auparavant inconnus dans leur version constructive.

De même, nous avons été amenés à étudier les anneaux de Prüfer cohérents « à factorisation partielle » (dans le cas local, ce sont les 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 implique la factorisation partielle des idéaux de type fini, qui elle-même implique la dimension ≤ 1 sous forme constructive.

L'article que vous lisez fait suite à [19] et [27] et présente des simplifications et améliorations substantielles par rapport à ces deux travaux.

Dans un article à venir certains des auteurs développeront l'aspect proprement « Calcul Formel » de ce travail. Il est en effet désormais possible de répondre à nombre de questions que l'on se pose usuellement au sujet des anneaux d'entiers de corps de nombres de manière « paresseuse » c'est-à-dire sans chercher à factoriser le discriminant ni à calculer une base d'entiers.

Mathématiques classiques et mathématiques constructives

Dans la mesure où nous voulons un traitement réellement algorithmique de la théorie des anneaux de Dedekind nous ne pouvons pas utiliser toutes les facilités que donnent l'usage systématique du lemme de Zorn et du principe du tiers exclu en mathématiques classiques.

Sans doute le lecteur ou la lectrice comprend bien qu'il est difficile d'implémenter le lemme de Zorn en calcul formel.

Le refus du principe du tiers exclu doit par contre lui sembler plus dur à avaler. Ce n'est de notre part qu'une constatation pratique. Si dans une preuve classique vous trouvez un raisonnement qui conduit à un calcul du type : « si x est inversible, faire ceci, sinon faire cela », il est bien clair que cela ne se traduit directement sous forme d'un algorithme que dans le cas où on dispose d'un test d'inversibilité dans l'anneau en question.

C'est pour insister sur cette difficulté, que nous devons contourner en permanence, que nous sommes amenés à parler souvent des deux points de vue, classique et constructif, sur un même sujet.

Pour ce qui concerne les définitions nous donnons en premier une variante constructive, quitte à montrer en mathématiques classiques l'équivalence avec la définition usuelle.

1 Préliminaires

1.1 Quelques définitions constructives

Dans le but de développer une version algorithmique de thérèmes classiques, nous aurons souvent besoin de définitions qui sont d'une part équivalentes aux définitions classiques du point de vue des mathématiques classiques et d'autre part directement utilisables dans les algorithmes.

Par exemple la définition classique d'un anneau local est un anneau qui possède un seul idéal maximal. De même le radical de Jacobson est défini comme intersection des idéaux maximaux. Ces définitions sont inopérantes d'un point de vue algorithmique.

Voici des définitions équivalentes (en mathématiques classiques) et directement utilisables dans les algorithmes.

On notera $\mathcal{U}_{\mathbf{A}}$ le groupe des unités de l'anneau commutatif $\mathbf{A}$. Le *radical de Jacobson* de $\mathbf{A}$, est l'idéal $\mathrm{Rad}(\mathbf{A})$ défini par :

$$\mathrm{Rad}(\mathbf{A}) = \{x \in \mathbf{A} \ ; \ 1 + x\mathbf{A} \subseteq \mathcal{U}_{\mathbf{A}}\} \ .$$

L'axiome constructif des *anneaux locaux* est

$$\forall x \in \mathbf{A} \quad x \in \mathcal{U}_{\mathbf{A}} \text{ ou } (1+x) \in \mathcal{U}_{\mathbf{A}} \ .$$

dans lequel le « ou » doit avoir sa signification constructive (il doit être explicite). Tout quotient et tout localisé d'un anneau local est un anneau local.

L'anneau $\mathbf{A}/\mathrm{Rad}(\mathbf{A})$ est le *corps résiduel* de l'anneau local. C'est un anneau local dont le radical de Jacobson est réduit à zéro. Voici une définition qui ne prend son sens qu'en mathématiques constructives : un anneau local $\mathbf{A}$ est dit *résiduellement discret* lorsque l'on a de manière explicite $\forall x \in \mathbf{A}\ x \in \mathrm{Rad}(\mathbf{A}) \ \vee \ x \in \mathcal{U}_{\mathbf{A}}$ (en mathématiques classiques, tout anneau local est résiduellement discret).

Un élément x d'un anneau $\mathbf{A}$ est dit *régulier* ou *non diviseur de zéro* s'il vérifie : $\forall y \in \mathbf{A}\ (xy = 0 \Rightarrow y = 0)$. Voici maintenant une nouvelle nuance inconnue en mathématiques classiques. Un anneau est dit *sans diviseur de zéro* s'il vérifie : $\forall x, y \in \mathbf{A}\ (xy = 0 \ \Rightarrow \ x = 0 \ \vee \ y = 0)$. Un anneau sans diviseur de zéro est dit *intègre* si on dispose d'un test d'égalité à 0 dans l'anneau, ce qui permet d'affirmer que tout élément est nul ou régulier. La notion d'anneau intègre est souvent problématique du point de vue algorithmique parce qu'elle se comporte mal par localisation (contrairement à la notion d'anneau sans diviseur de zéro).

1.2 Localisations en des monoïdes comaximaux

Définition 1.1

1. *On appelle* monoïde d'un anneau $\mathbf{A}$ *une partie de* $\mathbf{A}$ *contenant* 1 *et stable pour la multiplication (un monoïde peut éventuellement contenir* 0*).*
2. *Des monoïdes* $S_1, \ldots, S_n$ *sont dits* comaximaux*, si et seulement si :*
$$\forall s_1 \in S_1, \ldots, \forall s_n \in S_n, \quad \exists a_1, \ldots, a_n \in \mathbf{A}, \quad \textstyle\sum_{i=1}^{n} a_i s_i = 1.$$
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.*

Théorème 1.2 (principe local-global pour la résolution des systèmes linéaires) *Soit $S_1, \ldots, S_n$ 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 les trois points suivants sont équivalents :*

1. *Le système linéaire $BX = C$ admet une solution dans $\mathbf{A}^p$;*
2. *$\forall i \in \{1, \ldots, n\}$ le système linéaire $BX = C$ admet une solution dans $\mathbf{A}^p_{S_i}$;*
3. *Pour tout idéal maximal $\mathfrak{m} \subset \mathbf{A}$, l'équation $BX = C$ admet une solution dans $\mathbf{A}^p_{\mathfrak{m}}$.*

Preuve : Il est clair que 1. implique 2. et 3.
Montrons que 2. implique 1. Pour chaque i on a $Y_i \in \mathbf{A}^p_{S_i}$ et $s_i \in S_i$ tels que $BY_i/s_i = C$ dans $\mathbf{A}^m_{S_i}$, c'est-à-dire on a $t_i \in S_i$ tel que $t_i\ BY_i = s_i t_i\ C$ dans $\mathbf{A}^m$. Si $\sum_i a_i s_i t_i = 1$ on a donc la solution $X = \sum_i a_i t_i Y_i$.
Montrons que 3. implique 1. (en mathématiques classiques). Pour chaque idéal maximal $\mathfrak{m}$ on a, en notant $S_{\mathfrak{m}}$ le complémentaire de $\mathfrak{m}$ dans $\mathbf{A}$, $Y_{\mathfrak{m}} \in \mathbf{A}^p_{\mathfrak{m}}$, $s_{\mathfrak{m}}, t_{\mathfrak{m}} \in S_{\mathfrak{m}}$ tels que $t_{\mathfrak{m}}\ BY_{\mathfrak{m}} = s_{\mathfrak{m}} t_{\mathfrak{m}}\ C$ dans $\mathbf{A}$. L'idéal engendré par les $s_{\mathfrak{m}} t_{\mathfrak{m}}$ ne coupe aucun idéal maximal et donc il contient 1. Cela donne (de manière pas du tout explicite) une somme finie $\sum_i a_{\mathfrak{m}_i} s_{\mathfrak{m}_i} t_{\mathfrak{m}_i} = 1$ et on termine comme précédemment. □

La preuve du lemme suivant est facile.

Lemme 1.3 *Soient $a_1, \ldots, a_k, u_1, \ldots, u_\ell \in \mathbf{A}$. On note $\mathcal{S}(a_1, \ldots, a_k; u_1, \ldots, u_\ell)$ le monoïde formé des éléments de la forme $u_1^{n_1} \cdots u_\ell^{n_\ell} + \sum_i x_i a_i$. Alors les monoïdes $S_1 = \mathcal{S}(0; a_1)$, $S_2 = \mathcal{S}(a_1; a_2)$, $S_3 = \mathcal{S}(a_1, a_2; a_3)$, $\ldots$, $S_k = \mathcal{S}(a_1, \ldots, a_{k-1}; a_k)$ et $S_{k+1} = \mathcal{S}(a_1, \ldots, a_k; 1)$ sont comaximaux.*

On peut montrer en mathématiques classiques que le saturé du monoïde $\mathcal{S}(a_1, \ldots, a_k; u)$ est l'intersection de tous les $\mathbf{A} \setminus \mathfrak{p}$ pour les idéaux premiers $\mathfrak{p}$ qui contiennent $a_1, \ldots, a_k$ mais ne contiennent pas u.

Notez que $a_1, \ldots, a_k \in \mathrm{Rad}(S^{-1}\mathbf{A})$ si $S = \mathcal{S}(a_1, \ldots, a_k; u_1, \ldots, u_\ell))$. Le lemme précédent est utile lorsqu'on veut décrypter une preuve en mathématiques classiques qui utilise un principe local global lorsque la preuve classique se fait selon les lignes suivantes : on a $a_1, \ldots, a_k \in \mathbf{A}$ et on localise en un idéal maximal $\mathfrak{m}$, si $a_1 \notin \mathfrak{m}$ un certain calcul marche, si $a_1 \in \mathfrak{m}$ et $a_2 \notin \mathfrak{m}$ un autre calcul fonctionne, si $a_1, a_2 \in \mathfrak{m}$ et $a_3 \notin \mathfrak{m}$ un autre calcul fonctionne encore, etc... En général, le premier calcul fonctionne alors dans $S_1^{-1}\mathbf{A}$, le second dans $S_2^{-1}\mathbf{A}$, le troisième dans dans $S_3^{-1}\mathbf{A}$, etc... D'autres systèmes de monoïdes comaximaux peuvent s'avérer utiles pour décrypter des preuves classiques qui utilisent des arbres de calcul plus compliqués. Pour plus de détails sur ce sujet on consultera [19, 22].

Les applications du principe local-global de base sont nombreuses. Par exemple :

Corollaire 1.4 *Soient $\mathfrak{i}$ et $\mathfrak{j}$ deux idéaux d'un anneau commutatif $\mathbf{A}$ et $S_1, \ldots, S_n$ des monoïdes comaximaux.*

1. *On a $\mathfrak{i} \subseteq \mathfrak{j}$ dans $\mathbf{A}$ si et seulement si $\mathfrak{i}_{S_i} \subseteq \mathfrak{j}_{S_i}$ dans chaque $\mathbf{A}_{S_i}$.*
2. *Si $\mathfrak{j}$ est de type fini, alors il y a équivalence entre les trois propriétés suivantes :*
   - *il existe un idéal de type fini $\mathfrak{l}$ de $\mathbf{A}$ tel que $\mathfrak{l}\,\mathfrak{i} = \mathfrak{j}$;*
   - *$(\mathfrak{j} : \mathfrak{i})\ \mathfrak{i} = \mathfrak{j}$;*

– *pour chaque i il existe un idéal de type fini $\mathfrak{l}_i$ de $\mathbf{A}_{S_i}$ tel que $\mathfrak{l}_i\ \mathfrak{i}_{S_i} = \mathfrak{j}_{S_i}$ dans $\mathbf{A}_{S_i}$.*

Corollaire 1.5 *Soit $\mathbf{A}$ un anneau commutatif. Les propriétés suivantes sont équivalentes :*

1. $\forall x, y \in \mathbf{A}, \quad (\ xy = 0 \quad \Longrightarrow \quad \operatorname{Ann} x + \operatorname{Ann} y = \mathbf{A}\ )$.
2. $\forall x, y \in \mathbf{A}, \quad \operatorname{Ann} xy = \operatorname{Ann} x + \operatorname{Ann} y$.
3. *Si $xy = 0$ il existe des monoïdes comaximaux S_i tels que dans chacun des localisés A_{S_i}, x ou y devient nul.*
4. *Les localisés $\mathbf{A}_{\mathfrak{m}}$ de $\mathbf{A}$ en tous les idéaux maximaux $\mathfrak{m}$ sont intègres.*

Preuve : On peut réécrire comme suit la propriété numéro 1 :

$$\forall x, y \in \mathbf{A}, \quad (\ xy = 0 \quad \Longrightarrow \quad \exists u, v \in \mathbf{A}, \quad ux = vy = u + v - 1 = 0\ ) \qquad (1)$$

Il est clair que 2. $\Rightarrow$ 1. $\Rightarrow$ 3.
Si on a 1. et si $zxy = 0$ on a u, v tels que $uzx = vy = u+v-1 = 0$ donc $z = zu+zv$ avec $zu \in \operatorname{Ann} x$ et $zv \in \operatorname{Ann} y$. Donc 1. $\Rightarrow$ 2.
On obtient 3. implique 1. par le principe local-global appliqué au système linéaire $ux = vy = u + v - 1 = 0$ avec u et v pour inconnues.
Il est clair que la propriété (1) est stable par localisation. Pour montrer que 4. implique 1. par le principe local-global (en mathématiques classiques), il suffit donc de vérifier qu'un anneau local qui vérifie (1) est intègre. Plus précisément on a constructivement : si $xy = 0$ alors x ou y est nul. En effet $ux = vy = 0$ avec u ou v inversible puisque $u + v = 1$. □

Le corollaire précédent justifie la définition constructive suivante :

Définition 1.6 *Un anneau $\mathbf{A}$ est dit* localement sans diviseur de zéro *s'il vérifie l'implication (1) du corollaire 1.5 de manière explicite.*

De manière équivalente : tout idéal principal est plat. Un anneau sans diviseur de zéro est localement sans diviseur de zéro. Un localisé d'un anneau localement sans diviseur de zéro est encore localement sans diviseur de zéro. Un anneau localement sans diviseur de zéro est réduit.

Propriété 1.7 *Dans un anneau localement sans diviseur de zéro, l'annulateur d'un élément est un idéal idempotent.*

Preuve : Soit $y \in \operatorname{Ann}(x)$. Alors il existe u tel que $(1 - u)y = ux = 0$. On voit clairement que $u \in \operatorname{Ann}(x)$ et $y = uy \in \operatorname{Ann}(x)^2$, d'où $\operatorname{Ann}(x) = \operatorname{Ann}(x)^2$. □

Lemme 1.8 *Soit $\mathbf{A}$ un anneau localement sans diviseur de zéro, $V \in \mathbf{A}^n$ et $x \in \mathbf{A}$ tel que $xV = 0$. Alors il existe $s \in \mathbf{A}$ tel que $sV = 0$ et $(1 - s)x = 0$.*

Preuve : Pour chaque composante v_i de V on écrit $u_i x = s_i v_i = 0$ avec $u_i + s_i = 1$. On pose $s = \prod_i s_i$ de sorte que $sV = 0$. En développant le produit $\prod_i (u_i + s_i) = u + s = 1$ on voit que, dans la somme égale à u, chacun des $2^n - 1$ termes annule x, et donc $ux = 0$. □

1.3 Dimension de Krull

La preuve du théorème 1.13 ci-dessous est une simplification de celles données dans [20] et [6]. Ce théorème ainsi que les lemmes 1.9, 1.10, 1.12 sont des théorèmes de mathématiques classiques. Le lemme 1.9 est parfois appelé « théorème de Krull ».

Lemme 1.9 *Dans un anneau commutatif* $\mathbf{A}$*, on considère un idéal* $\mathfrak{i}$ *et un monoïde multiplicatif* S*. Si* $\mathfrak{i} \cap S = \emptyset$*, alors il existe un idéal premier* $\mathfrak{p}$ *tel que* $\mathfrak{i} \subset \mathfrak{p} \subset \mathbf{A} \setminus S$*.*

Preuve : Considérer un idéal maximal de l'anneau non trivial $S^{-1}\mathbf{A}$ / $S^{-1}\mathfrak{i}$. □

Lemme 1.10 *Dans un anneau commutatif* $\mathbf{A}$*, on considère un monoïde multiplicatif* S'*, un idéal* $\mathfrak{i}$ *et un élément* $x \in \mathbf{A}$*. On construit le monoïde* $S = x^{\mathbb{N}}(S' + \mathbf{A}x)$*. Si* $\mathfrak{i} \cap S = \emptyset$*, alors il existe un idéal premier* $\mathfrak{p} \supset \mathfrak{i}$ *tel que* $x \notin \mathfrak{p}$ *et* $S' \cap (\mathfrak{p} + \mathbf{A}x) = \emptyset$*.*

Preuve : Il suffit en effet que $\mathfrak{i} \subset \mathfrak{p} \subset \mathbf{A} \setminus S$. □

Définition 1.11 *(cf. [20]) Soit une suite* $x = x_1, \ldots, x_\ell$ *(de longueur* ℓ*) dans un anneau* $\mathbf{A}$*. On considère le monoïde multiplicatif* $\mathcal{S}_0$ *défini par*

$$\mathcal{S}_\ell = \{1\} \qquad \text{et} \qquad \mathcal{S}_i = x_{i+1}^{\mathbb{N}}(\mathcal{S}_{i+1} + \mathbf{A}x_{i+1}) \quad \text{pour} \quad 0 \leq i < \ell$$

La suite $x_1, \ldots, x_\ell$ *est dite* pseudo-singulière *lorsque* $0 \in \mathcal{S}_0$*, c'est-à-dire lorsqu'il existe* $a_1, \ldots, a_\ell \in \mathbf{A}$*,* $m_1, \ldots, m_\ell \in \mathbb{N}$*, tels que :*

$$x_1^{m_1}(x_2^{m_2}(\cdots(x_\ell^{m_\ell}(1 + a_\ell x_\ell) + \cdots) + a_2 x_2) + a_1 x_1) = 0 \tag{2}$$

Elle est dite pseudo-régulière *lorsqu'il est absurde qu'elle soit pseudo-singulière.*

Noter qu'une égalité (2) du style ci-dessus avec certaines valeurs pour les exposants m_i en fournit d'autres pour n'importe quelles valeurs supérieures des exposants.

Lemme 1.12 *On considère une suite* $x_1, \ldots, x_\ell$ *d'un anneau commutatif* $\mathbf{A}$*. Les propriétés suivantes sont équivalentes :*

1. *La suite est pseudo-régulière, i.e.* $0 \notin \mathcal{S}_0$ *;*
2. *Il existe des idéaux premiers* $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_\ell$ *tels que* $x_i \in \mathfrak{p}_i \setminus \mathfrak{p}_{i-1}$ *pour* $1 \leq i \leq \ell$*.*

Preuve : Supposons qu'il existe des idéaux premiers $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_\ell$ tels que $x_i \in \mathfrak{p}_i \setminus \mathfrak{p}_{i-1}$ pour $1 \leq i \leq \ell$. Alors on voit de proche en proche pour $k = \ell, \ldots, 0$ que $\mathfrak{p}_k \cap \mathcal{S}_k = \emptyset$. En particulier $\mathcal{S}_0$ ne contient pas 0.
Supposons la suite pseudo-régulière. Posons $x_0 = 0$, $\mathfrak{i}_0 = (0)$ et appliquons le lemme 1.10 avec $\mathfrak{i} = \mathfrak{i}_0$, $S' = \mathcal{S}_1$ et $x = x_1$. Alors $S = \mathcal{S}_0$ et on a bien $\mathfrak{i} \cap S = \emptyset$: il existe un idéal premier $\mathfrak{p}_0$ contenant $\mathfrak{i}_0$ mais pas x_1 et tel que $\mathcal{S}_1 \cap (\mathfrak{p}_0 + \mathbf{A}x_1) = \emptyset$.
Si on a construit $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_k$ $(k < \ell - 1)$ tels que $x_i \in \mathfrak{p}_i$, $x_{i+1} \notin \mathfrak{p}_i$ et $\mathcal{S}_{i+1} \cap (\mathfrak{p}_i + \mathbf{A}x_{i+1}) = \emptyset$ pour $1 \leq i \leq k$, on applique le lemme 1.10 avec $\mathfrak{i} = \mathfrak{i}_{k+1} = \mathfrak{p}_k + \mathbf{A}x_{k+1}$, $S' = \mathcal{S}_{k+2}$ et $x = x_{k+2}$. Alors $S = \mathcal{S}_{k+1}$ et on a bien $\mathfrak{i} \cap S = \emptyset$: il existe un idéal premier $\mathfrak{p}_{k+1}$ contenant $\mathfrak{i}_{k+1}$ (donc $\mathfrak{p}_k$ et x_{k+1}) mais pas x_{k+2} et tel que $\mathcal{S}_{k+2} \cap (\mathfrak{p}_{k+1} + \mathbf{A}x_{k+2}) = \emptyset$.
À la dernière étape on a $\mathfrak{p}_{\ell-1}$ avec $x_\ell \notin \mathfrak{p}_{\ell-1}$ et $1 \notin \mathfrak{p}_{\ell-1} + \mathbf{A}x_\ell$. Il existe donc un idéal premier $\mathfrak{p}_\ell$ contenant $\mathfrak{p}_{\ell-1} + \mathbf{A}x_\ell$. □

Une conséquence immédiate est la caractérisation constructive suivante de la dimension de Krull.

Théorème 1.13 *Soit* $\mathbf{A}$ *un anneau commutatif. Les propositions suivantes sont équivalentes :*

1. *La dimension de Krull (longueur maximale des chaînes strictement croissantes d'idéaux premiers) est inféreure ou égale à* d *;*
2. *Toute suite d'éléments de* $\mathbf{A}$ *de longueur* $d+1$ *est pseudo-singulière.*

Le fait suivant, qui résulte du principe local-global de base, affirme que l'on a bien mis à jour une propriété de nature locale.

Fait 1.14 *Soient* $S_1, \ldots, S_n$ *des monoïdes comaximaux de* $\mathbf{A}$ *et* $\underline{x} = x_1, \ldots, x_k$ *une suite finie d'éléments de* $\mathbf{A}$*. Alors* $\underline{x}$ *est pseudo-singulière dans* $\mathbf{A}$ *si et seulement si elle est pseudo-singulière dans chacun des* $\mathbf{A}_{S_i}$*.*

Tout ceci justifie la définition constructive suivante :

Définition 1.15 *Un anneau* $\mathbf{A}$ *est de* dimension (de Krull) inférieure ou égale *à* $d \in \mathbb{N}$ *si et seulement si toute suite d'éléments de* $\mathbf{A}$ *de longueur* $d+1$ *est pseudo-singulière. Autrement dit pour tous* $x_0, \ldots, x_d \in \mathbf{A}$ *il existe* $n \in \mathbb{N}$ *tel que :*

$$(x_0 \cdots x_d)^n \in \ x_0^{n+1}(x_1 \cdots x_d)^n \ \mathbf{A} + x_1^{n+1}(x_2 \cdots x_d)^n \ \mathbf{A} + \cdots + x_d^{n+1} \ \mathbf{A} \qquad (3)$$

L'anneau est dit de dimension -1 *s'il est trivial, c'est-à-dire si* $1 = 0$*.*

Fait 1.16

1. *Si* N *est le nilradical de* $\mathbf{A}$*. Alors* $\mathbf{A}$ *est de dimension de Krull inférieure ou égale à* d *si et seulement si* $\mathbf{A}/N$ *est de dimension de Krull inférieure ou égale à* d*.*
2. *Soient* $S_1, \ldots, S_n$ *des monoïdes comaximaux de* $\mathbf{A}$*. Alors* $\mathbf{A}$ *est de dimension de Krull inférieure ou égale à* d *si et seulement si chacun des* $\mathbf{A}_{S_i}$ *est de dimension de Krull inférieure ou égale à* d*.*

Le lemme suivant est immédiat. Il était également immédiat avec la définition usuelle de la dimension de Krull en mathématiques classiques, mais maintenant il a un contenu algorithmique précis. Remarquer aussi que la convention pour la dimension -1 est bien pertinente.

Lemme 1.17 *Soit* $d \in \mathbb{N}$ *et* x *régulier dans* $\mathbf{A}$*. Si* $\mathbf{A}$ *est de dimension inférieure ou égale à* d *alors* $\mathbf{A}/\langle x \rangle$ *est de dimension inférieure ou égale à* $d-1$*.*

Plus généralement, la définition 1.15 a la conséquence suivante.

Lemme 1.18 *Soit* $d \geq 0$*. Pour* $x \in \mathbf{A}$*, notons* $S_x^{\mathbf{A}} = S_x = x^{\mathbb{N}}(1 + x\mathbf{A})$ *et* $\mathbf{A}^{\{x\}} = S_x^{-1}\mathbf{A}$*. Alors* $\mathbf{A}$ *est de dimension inférieure ou égale à* d *si et seulement si pour tout* $x \in \mathbf{A}$ $\mathbf{A}^{\{x\}}$ *est de dimension inférieure ou égale à* $d-1$*.*

Notez que la propriété précédente pourrait servir de définition récursive pour la dimension de Krull, avec l'« initialisation » : $\dim(\mathbf{A}) = -1 \Leftrightarrow 1 =_{\mathbf{A}} 0$.

En fait on peut encore raffiner le critère ci-dessus en tenant compte du principe local-global donné dans le fait 1.14.

Lemme 1.19 *Soit $d \geq 0$. Pour montrer que $\mathbf{A}$ est de dimension inférieure ou égale à d il suffit de trouver pour tout $x \in \mathbf{A}$ des monoïdes comaximaux $S_{x,1}, S_{x,2}, \ldots, S_{x,n_x}$ tels que, en posant $\mathbf{A}_{x,i} = S_{x,i}^{-1}\mathbf{A}$ on ait chacun des $\mathbf{A}_{x,i}{}^{\{x\}}$ de dimension inférieure ou égale à $d-1$.*

Anneaux zéro-dimensionnels

On dira *anneau zéro-dimensionnel* pour anneau de dimension inférieure ou égale à 0. Il s'agit d'un léger abus de langage car affirmer que la dimension est inférieure ou égale à 0 laisse ouverte la possibilité de dimension égale à -1, ce qui signifie que l'anneau est trivial.

Lemme 1.20 *Les propriétés suivantes sont équivalentes :*

1. *$\mathbf{A}$ est zéro-dimensionnel.*
2. *$\forall x \in \mathbf{A}\ \exists a \in \mathbf{A}\ \exists d \in \mathbb{N}$ tels que $x^d = ax^{d+1}$.*
3. *$\forall x \in \mathbf{A}\ \exists s \in \mathbf{A}\ \exists d \in \mathbb{N}$ tels que $x^d\mathbf{A} = s\mathbf{A}$ et s idempotent.*
4. *Pour tout idéal de type fini $\mathfrak{i}$ de $\mathbf{A}$, il existe $d \in \mathbb{N}^*$ tel que $\mathfrak{i}^d = s\mathbf{A}$ où s est un idempotent, et en particulier $\mathrm{Ann}(\mathfrak{i}^d) = (1-s)\mathbf{A}$ et $\mathfrak{i}^e = \mathfrak{i}^d$ pour $e \geq d$.*

Preuve : 2. est une simple réécriture de 1.
Montrons que 2. implique 3. Pour tout élément $x \in \mathbf{A}$, il existe $a \in \mathbf{A}$ et $d \in \mathbb{N}$ tels que $x^d = ax^{d+1}$. En multipliant d fois par ax, on obtient $x^d = ax^{d+1} = a^2x^{d+2} = \cdots = a^dx^{2d}$. On voit alors que $a^dx^d = s$ est un idempotent et $x^d = sx^d$, donc $x^d\mathbf{A} = s\mathbf{A}$ et $\mathrm{Ann}(x^d) = \langle 1-s\rangle$.
Montrons que 3. implique 2. Si $s = ax^d$ et $x^ds = x^d$, alors $x^d = ax^{2d} = (ax^{d-1})x^{d+1}$.
Montrons que 3. implique 4. Si $\mathfrak{i} = x_1\mathbf{A} + \cdots + x_n\mathbf{A}$, alors il existe des idempotents $s_1, \ldots, s_n \in \mathbf{A}$ et des entiers $d_1, \ldots, d_n \geq 1$ tels que $x_i^{d_i}\mathbf{A} = s_i\mathbf{A}$. Soit $d \geq d_1 + \cdots + d_n - (n-1)$ et $s = 1 - (1-s_1)\cdots(1-s_n)$ de sorte que $s\mathbf{A} = s_1\mathbf{A} + \cdots + s_n\mathbf{A}$. Il est clair que l'idempotent s appartient à $\mathfrak{i}$, donc à toutes les puissances de $\mathfrak{i}$. D'autre part,

$$\mathfrak{i}^d \subset x_1^{d_1}\mathbf{A} + \cdots + x_n^{d_n}\mathbf{A} = s_1\mathbf{A} + \cdots + s_n\mathbf{A} = s\mathbf{A}$$

Conclusion : $\mathfrak{i}^d = s\mathbf{A}$.
Enfin, 4. implique clairement 3. □

Noter que dans un anneau zéro-dimensionnel, tout élément régulier est inversible.

Lemme 1.21 (Anneaux zéro-dimensionnels réduits, ou absolument plats)
Les propriétés suivantes sont équivalentes :

1. *$\mathbf{A}$ est zéro-dimensionnel réduit ;*
2. *$\forall x \in \mathbf{A}\ \exists a \in \mathbf{A}$ tel que $x(1-ax) = 0$;*
3. *$\forall x \in \mathbf{A}\ \exists s \in \mathbf{A}$ tel que $s^2 = s$ et $\langle x\rangle = \langle s\rangle$, en particulier $\mathrm{Ann}(x) = \langle 1-s\rangle$;*
4. *Tout idéal de type fini $\mathfrak{i}$ est engendré par un idempotent s, en particulier $\mathrm{Ann}(\mathfrak{i}) = \langle 1-s\rangle$;*
5. *Pour tout idéal $\mathfrak{i}$ (de type fini ou non), on a $\mathfrak{i}^2 = \mathfrak{i}$.*

2 Idéaux localement principaux, projectifs, inversibles

2.1 Idéaux localement principaux

La définition suivante sera justifiée du point de vue des mathématiques classiques par le corollaire 2.5.

Définition 2.1 *Un idéal de type fini* $\mathfrak{i}$ *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* $\mathfrak{i}_{S_j}$ *est principal dans* $\mathbf{A}_{S_j}$. *Dans la suite l'expression « idéal localement principal » signifiera toujours idéal de type fini localement principal.*

En particulier, un idéal localement principal $\mathfrak{i}$ reste localement principal si on remplace $\mathbf{A}$ par un localisé ou un quotient de $\mathbf{A}$.

Matrices de localisation principale

Définition 2.2 *Soit* $x_1, \ldots, x_n$ *des éléments de* $\mathbf{A}$. *On appelle* matrice de localisation principale (dans $\mathbf{A}$) pour $(x_1, \ldots, x_n)$ *une matrice* $A = (a_{ij})_{1 \leq i,j \leq n}$ *d'éléments de* $\mathbf{A}$ *qui vérifie :*

$$\left\{ \begin{array}{lrcll} \alpha) & \sum a_{ii} & = & 1 & \\ \beta) & a_{\ell j} x_i & = & a_{\ell i} x_j & \forall i, j, \ell \in \{1, \ldots, n\} \end{array} \right. \tag{4}$$

Remarques :
1. L'idéal $\mathfrak{i} = \langle x_1, \ldots, x_n \rangle$ devient principal, égal à $\langle x_i \rangle$, après localisation en a_{ii}.
2. La condition $\beta)$ signifie que les lignes de la matrice A sont « proportionnelles » à $(x_1, \ldots, x_n)$.
3. Si l'anneau est local, l'un des a_{ii} est inversible et l'idéal $\mathfrak{i}$ est engendré par l'un des x_i.

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

Preuve : Si $\mathfrak{i} = \langle g \rangle$, on 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

$$g = \sum_{i=1}^n u_i x_i = \sum_{i=1}^n u_i y_i g = \left(\sum_{i=1}^n b_{ii} \right) g$$

Donc

$$\left(1 - \sum\nolimits_{i=1}^n b_{ii}\right) g = 0, \text{ et } 1 - \sum\nolimits_{i=1}^n b_{ii} \in \mathrm{Ann}(x_k) \text{ pour tout } k.$$

Prenons $\boxed{a_{ij} = u_i y_j}$ pour $(i,j) \neq (n,n)$ et $\boxed{a_{nn} = u_n y_n + (1 - \sum_{k=1}^n u_k y_k)}$, alors (a_{ij}) est bien une matrice de localisation principale pour $(x_1, \ldots, x_n)$. □

Proposition 2.4 *Soit* $\mathfrak{i} = \langle x_1, \ldots, x_n \rangle$ *un idéal de type fini. L'idéal* $\mathfrak{i}$ *est localement principal si et seulement si* $(x_1, \ldots, x_n)$ *admet une matrice de localisation principale. Si l'anneau est local,* $\mathfrak{i}$ *est localement principal si et seulement s'il est engendré par l'un des* x_i.

Preuve : La condition est clairement suffisante. Montrons qu'elle est nécessaire. Le système linéaire (4) qui définit la matrice de localisation principale a une solution localement, donc aussi globalement (principe local-global de base).
Voyons enfin le cas local. Dans les équations (4) l'un des a_{ii} est inversible donc $\mathfrak{i} = \langle x_i \rangle$. □

Ceci donne en mathématiques classiques.

Corollaire 2.5 *Un idéal de type fini* $\mathfrak{i}$ *est localement principal si et seulement s'il devient principal dans tout localisé* $\mathbf{A}_\mathfrak{m}$ *par un idéal maximal* $\mathfrak{m}$.

Preuve : A l'instar de la démonstration précédente, si le système d'équations (4) admet une solution en les (a_{ij}) dans tous les localisés $\mathbf{A}_\mathfrak{m}$, alors il en admet une globalement dans $\mathbf{A}$. □

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

(1) $(x_1, \ldots, x_n)A = (x_1, \ldots, x_n)$.
(2) x_i *annule tout mineur d'ordre 2 de* A, *et* $x_i(A^2 - A) = 0$ *pour tout* i, *donc* $\langle x_1, \ldots, x_n \rangle (A^2 - A) = 0$
(3) *Si* $\mathbf{A}_i = \mathbf{A}[1/a_{ii}]$ *est le localisé obtenu en rendant* a_{ii} *inversible, on a* $\mathfrak{i}\,\mathbf{A}_i = \langle x_i \rangle \mathbf{A}_i$.
(4) $\langle x_1, \ldots, x_n \rangle \langle a_{1j}, \ldots, a_{nj} \rangle = \langle x_j \rangle$.
(5) *Plus généralement, si* $a = \sum \alpha_i x_i$ *et* ${}^t(y_1, \ldots, y_n) = A\ {}^t(\alpha_1, \ldots, \alpha_n)$ *alors*
$$\langle x_1, \ldots, x_n \rangle \langle y_1, \ldots, y_n \rangle = \langle a \rangle$$
En outre si $\mathrm{Ann}(\mathfrak{i}) = 0$ *la matrice* ${}^tA$ *est une matrice de localisation principale pour* $(y_1, \ldots, y_n)$.
(6) *En particulier si* $\sum \alpha_i x_i = 0$ *et* ${}^t(y_1, \ldots, y_n) = A\ {}^t(\alpha_1, \ldots, \alpha_n)$, *alors*
$$\langle x_1, \ldots, x_n \rangle \langle y_1, \ldots, y_n \rangle = 0$$
(7) *On considère* $\underline{x} : (\alpha_i) \mapsto \sum_i \alpha_i x_i$ *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* $\{(\nu_1, \ldots, \nu_n) | \&_i(\nu_i \in N)\} \subset \mathbf{A}^n$, *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 :
$$\sum_{i=1}^n a_{ij} x_i = \sum_{i=1}^n a_{ii} x_j = x_j$$
(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
$$x_h(b_{ij} - a_{ij}) = x_h a_{ij}\left(\sum_{k=1}^n a_{kk}\right) - a_{ij}x_h = 0.$$
(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,

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

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 $\mathrm{Ann}(\mathfrak{i}) = 0$. 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 $\mathfrak{j} = \langle x_1, \ldots, x_i \rangle \cap \langle x_{i+1}, \ldots, x_n \rangle$ 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 $\mathfrak{j}$ 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 *Soit* $\mathfrak{i}$ *et* $\mathfrak{j}$ *deux idéaux localement principaux engendrés respectivement par* n *et* m *éléments. Alors* $\mathfrak{i}\,\mathfrak{j}$ *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* $\mathfrak{i}$ *et* $\mathfrak{j}$*, alors* $\mathfrak{i}\,\mathfrak{j}$ *est engendré par les coefficients du polynôme* $f = gh$*.*

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

$$c_{(ij)(k\ell)} x_m y_n = a_{ij} b_{k\ell} x_m y_n = a_{im} b_{kn} x_j y_\ell = c_{(im)(kn)} x_j y_\ell$$
$$\text{et} \sum\nolimits_{i,j} c_{(ii)(jj)} = \sum\nolimits_{i,j} a_{ii} b_{jj} = \Big(\sum\nolimits_{i=1}^{n} a_{ii}\Big)\Big(\sum\nolimits_{j=1}^{m} b_{jj}\Big) = 1$$

Donc $\mathfrak{i}\,\mathfrak{j}$ est localement principal.

Soit $(z_1, \ldots, z_p)$ le vecteur des coefficients de f. On veut montrer que $\mathfrak{i}\,\mathfrak{j} = \langle z_1, \ldots, z_p \rangle$. Si les S_i (resp. les S'_k) sont des monoïdes comaximaux tels que $\mathfrak{i}_{S_i} = \langle x_i \rangle_{S_i}$ (resp. $\mathfrak{j}_{S'_k} = \langle y_k \rangle_{S'_k}$), alors les $S_i S'_k$ sont des monoïdes comaximaux et on a $(\mathfrak{i}\,\mathfrak{j})_{S_i S'_k} = \langle x_i y_k \rangle_{S_i S'_k}$. 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[1] 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 $(\mathfrak{i}\,\mathfrak{j})_{S_i S'_k}$. L'égalité $\mathfrak{i}\,\mathfrak{j} = \langle z_1, \ldots, z_p \rangle$ a donc été prouvée dans tous les localisés et elle est vraie globalement. □

Puissances d'un idéal localement principal

Lemme 2.8 *Si* $\mathfrak{i} = \langle x_1, \ldots, x_k \rangle$ *est localement principal, alors* $\mathfrak{i}^n = \langle x_1^n, \ldots, x_k^n \rangle$*.*

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

[1] Voir [24] : pour deux polynômes F, G à une indéterminée, à coefficients dans un anneau commutatif, et $d \geq \deg(G)$, on a : $\mathrm{c}(F)^{d+1}\, \mathrm{c}(G) = \mathrm{c}(F)^d\, \mathrm{c}(FG)$ où $c(F)$, $c(G)$ et $c(FG)$ désignent respectivement les idéaux engendrés par les coefficients de F, G et FG.

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 $D \geq k(n-1)+1$. 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 $b_{\ell i} x_j^n = c_\ell (a_{\ell i} x_j)^n = c_\ell (a_{\ell j} x_i)^n = b_{\ell j} x_i^n$ 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 $x_1^{n_1} \cdots x_k^{n_k}$ en fonction des x_i^n lorsque $n = n_1 + \cdots + n_k$:

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

□

« Quotient » d'un idéal par un idéal localement principal qui le contient

Proposition 2.9 *Soit* $\mathfrak{i}$ *et* $\mathfrak{j}$ *deux idéaux tels que* $\mathfrak{i} \subset \mathfrak{j}$ *et* $\mathfrak{j}$ *localement principal (resp.* $\mathfrak{i}$ *de type fini). Alors il existe un idéal* $\mathfrak{l}$ *(resp. de type fini) tel que* $\mathfrak{i} = \mathfrak{j}\,\mathfrak{l}$.

Preuve : Si $\mathfrak{j} = \langle x_1, \dots, x_n \rangle$ et $y \in \mathfrak{i}$, on trouve $\mathfrak{l}_y$ tel que $\mathfrak{j}\,\mathfrak{l}_y = \langle y \rangle$ en appliquant la proposition 2.6, item (5). Ensuite $\mathfrak{l}$ est la somme des $\mathfrak{l}_{y_i}$ pour une famille (y_i) qui engendre $\mathfrak{i}$. □

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

Lemme 2.10 *Soit* $\mathfrak{i}$ *et* $\mathfrak{j}$ *deux idéaux de type fini avec* $\mathfrak{i}+\mathfrak{j}$ *localement principal. L'intersection* $\mathfrak{i} \cap \mathfrak{j}$ *est un idéal de type fini qui vérifie*

$$(\mathfrak{i} \cap \mathfrak{j})(\mathfrak{i}+\mathfrak{j}) = \mathfrak{i}\,\mathfrak{j}$$

Si de plus $\mathfrak{i}$ *et* $\mathfrak{j}$ *sont localement principaux alors* $\mathfrak{i} \cap \mathfrak{j}$ *est localement principal.*

Preuve : Soit $\mathfrak{i} = \langle x_1, \dots, x_n \rangle$ et $\mathfrak{j} = \langle y_1, \dots, y_m \rangle$. L'idéal $\mathfrak{i} \cap \mathfrak{j}$ est de type fini d'après la proposition 2.6, point (8). Considérons une localisation où $\mathfrak{i}+\mathfrak{j}$ est, par exemple, engendré par x_1. Alors $\mathfrak{j}_S \subset \langle x_1 \rangle = \mathfrak{i}_S$, $(\mathfrak{i} \cap \mathfrak{j})_S = \mathfrak{j}_S$ et $(\mathfrak{i}+\mathfrak{j})_S = \mathfrak{i}_S$. Ainsi l'égalité $(\mathfrak{i} \cap \mathfrak{j})(\mathfrak{i}+\mathfrak{j}) = \mathfrak{i}\,\mathfrak{j}$ est une égalité qui est vérifiée localement en des monoïdes comaximaux, donc globalement.
Enfin, avec le même raisonnement, si de plus $\mathfrak{i}$ et $\mathfrak{j}$ sont localement principaux, on voit que $\mathfrak{i} \cap \mathfrak{j}$ est localement 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).

Transporteurs [2] : quelques égalités

Propriété 2.11 *Soit* $\mathfrak{i}, \mathfrak{j}$ *deux idéaux de type fini dans un anneau commutatif. Si* $\mathfrak{i}+\mathfrak{j}$ *est localement principal alors* $(\mathfrak{j} : \mathfrak{i}) + (\mathfrak{i} : \mathfrak{j}) = \langle 1 \rangle$.

Démonstration Voir la démonstration du lemme 2.10 : si $\mathfrak{i}+\mathfrak{j}$ est localement principal alors $(\mathfrak{j} : \mathfrak{i}) + (\mathfrak{i} : \mathfrak{j}) = \langle 1 \rangle$ car il s'agit là d'un système linéaire que l'on résoud en appliquant le principe local-global de base. □

[2] On note classiquement $\mathfrak{j} : \mathfrak{i}$ l'idéal transporteur $\{x \in \mathbf{A} \mid x\mathfrak{i} \subset \mathfrak{j}\}$.

Proposition 2.12 *Soit* $\mathbf{A}$ *un anneau commutatif et* $\mathfrak{i},\mathfrak{j},\mathfrak{l}$ *trois idéaux (de type fini ou non). On a* $\mathfrak{i}:(\mathfrak{j}+\mathfrak{l})=(\mathfrak{i}:\mathfrak{j})\cap(\mathfrak{i}:\mathfrak{l})$ *et* $(\mathfrak{j}\cap\mathfrak{l}):\mathfrak{i}=(\mathfrak{j}:\mathfrak{i})\cap(\mathfrak{l}:\mathfrak{i})$. *Si* $(\mathfrak{j}:\mathfrak{l})+(\mathfrak{l}:\mathfrak{j})=\langle 1\rangle$ *(en particulier si* $\mathfrak{j}+\mathfrak{l}$ *est localement principal) alors on a :*

(0) $\forall\, j,k\in\mathbb{N},\ \mathfrak{j}^j.\mathfrak{l}^k\subset\mathfrak{j}^{j+k}+\mathfrak{l}^{j+k}$ *et* $\forall\, n\in\mathbb{N},\ (\mathfrak{j}+\mathfrak{l})^n=\mathfrak{j}^n+\mathfrak{l}^n$

(1) $(\mathfrak{j}+\mathfrak{l}):\mathfrak{i}=(\mathfrak{j}:\mathfrak{i})+(\mathfrak{l}:\mathfrak{i})$ (2) $\mathfrak{i}:(\mathfrak{j}\cap\mathfrak{l})=(\mathfrak{i}:\mathfrak{j})+(\mathfrak{i}:\mathfrak{l})$

(3) $(\mathfrak{j}+\mathfrak{l})(\mathfrak{j}\cap\mathfrak{l})=\mathfrak{j}\,\mathfrak{l}$ (4) $\mathfrak{i}\,(\mathfrak{j}\cap\mathfrak{l})=\mathfrak{i}\,\mathfrak{j}\cap\mathfrak{i}\,\mathfrak{l}$

(5) $\mathfrak{i}+(\mathfrak{j}\cap\mathfrak{l})=(\mathfrak{i}+\mathfrak{j})\cap(\mathfrak{i}+\mathfrak{l})$ (6) $\mathfrak{i}\cap(\mathfrak{j}+\mathfrak{l})=(\mathfrak{i}\cap\mathfrak{j})+(\mathfrak{i}\cap\mathfrak{l})$

En outre la suite exacte courte ci-après est scindée :

$$(0)\longrightarrow\mathfrak{j}\cap\mathfrak{l}\xrightarrow{\delta}\mathfrak{j}\times\mathfrak{l}\xrightarrow{\sigma}\mathfrak{j}+\mathfrak{l}\longrightarrow(0)$$

où $\delta(x)=(x,-x)$ *et* $\sigma(y,z)=y+z$.

Preuve : Nous laissons à la lectrice le soin de prouver les deux premières égalités de la proposition et les inclusions universelles suivantes où $\mathfrak{t}=(\mathfrak{j}:\mathfrak{l})+(\mathfrak{l}:\mathfrak{j})$.

(0) $\big((\mathfrak{j}:\mathfrak{l})^k+(\mathfrak{l}:\mathfrak{j})^j\big)\ \mathfrak{j}^j.\mathfrak{l}^k\subset\mathfrak{j}^{j+k}+\mathfrak{l}^{j+k}$

(1) $\mathfrak{t}\,\big((\mathfrak{j}+\mathfrak{l}):\mathfrak{i}\big)\subset(\mathfrak{j}:\mathfrak{i})+(\mathfrak{l}:\mathfrak{i})\subset(\mathfrak{j}+\mathfrak{l}):\mathfrak{i}$

(2) $\big(\mathfrak{i}:(\mathfrak{j}\cap\mathfrak{l})\big)\mathfrak{t}\subset(\mathfrak{i}:\mathfrak{j})+(\mathfrak{i}:\mathfrak{l})\subset\mathfrak{i}:(\mathfrak{j}\cap\mathfrak{l})$

(3) $\mathfrak{t}\,\mathfrak{j}\,\mathfrak{l}\subset(\mathfrak{j}+\mathfrak{l})(\mathfrak{j}\cap\mathfrak{l})\subset\mathfrak{j}\,\mathfrak{l}$

(4) $\mathfrak{t}\,(\mathfrak{i}\,\mathfrak{j}\cap\mathfrak{i}\,\mathfrak{l})\subset\mathfrak{i}\,(\mathfrak{j}\cap\mathfrak{l})\subset\mathfrak{i}\,\mathfrak{j}\cap\mathfrak{i}\,\mathfrak{l}$

(5) $\mathfrak{t}\,\big((\mathfrak{i}+\mathfrak{j})\cap(\mathfrak{i}+\mathfrak{l})\big)\subset\mathfrak{i}+(\mathfrak{j}\cap\mathfrak{l})\subset(\mathfrak{i}+\mathfrak{j})\cap(\mathfrak{i}+\mathfrak{l})$

(6) $\mathfrak{t}\,\big(\mathfrak{i}\cap(\mathfrak{j}+\mathfrak{l})\big)\subset(\mathfrak{i}\cap\mathfrak{j})+(\mathfrak{i}\cap\mathfrak{l})\subset\mathfrak{i}\cap(\mathfrak{j}+\mathfrak{l})$

Enfin, comme $(\mathfrak{j}:\mathfrak{l})+(\mathfrak{l}:\mathfrak{j})=\langle 1\rangle$, un scindage de σ est donné par :

$$\begin{cases}\mathfrak{j}+\mathfrak{l} & \longrightarrow & \mathfrak{j}\times\mathfrak{l}\\ x & \longmapsto & (jx,kx)\end{cases}$$

avec $j\in(\mathfrak{j}:\mathfrak{l})$, $k\in(\mathfrak{l}:\mathfrak{j})$, $j+k=1$. □

2.2 Idéaux projectifs de type fini

Rappelons sans démonstrations quelques points clés de la théorie constructive des modules projectifs de type fini (voir par exemple [22]).

– Un $\mathbf{A}$-module M est projectif de type fini s'il est isomorphe à un facteur direct dans un $\mathbf{A}$-module libre $\mathbf{A}^n$, autrement dit s'il est isomorphe à l'image d'une matrice de projection $P\in\mathbf{A}^{n\times n}$. D'autres caractérisations sont les suivantes :
  1. M est un module de type fini et pour tout homomorphisme surjectif $\varphi : M'\to M$, $\operatorname{Ker}\varphi$ est facteur direct dans M'.
  2. M est un module de présentation finie et plat.
– Le polynôme $R_M(X)=\sum_i r_iX^i$ défini par $\det(\mathrm{I}_n+XP)=R_M(1+X)$ ne dépend que de M et c'est un polynôme *multiplicatif* : il vérifie $R_M(XY)=R_M(X)R_M(Y)$ et $R_M(1)=1$. Cela signifie que les r_i forment un système fondamental d'idempotents orthogonaux (sfio). On a $r_0=\det(\mathrm{I}_n-P)$ et l'idéal $\langle r_0\rangle$ est l'annulateur de M.
– Le fait pour un module M d'être projectif de type fini se conserve par changement d'anneau de base, même chose pour le polynôme R_M.
– Le module est dit de rang k si $R_M(X)=X^k$. Il est dit de rang inférieur ou égal à k si $r_{k+1}=\cdots=r_n=0$ c'est-à-dire encore si tous les mineurs d'ordre $k+1$ de la matrice P sont nuls. S'il a un rang k le module M est dit de rang constant. Quand il existe, le rang d'un module projectif de type fini est bien défini dès que l'anneau n'est pas trivial.

– Le localisé $\mathbf{A}_{r_k} = \mathbf{A}[1/r_k]$ est isomorphe à $\mathbf{A}\,/\langle 1 - r_k\rangle$. Le localisé M_{r_k} est isomorphe au sous-module $r_k M$. Il est de rang k en tant que $\mathbf{A}_{r_k}$- module. Le module M est somme directe des « composantes » $r_k M$ $(k > 0)$.
– Si N est un sous-module projectif de type fini de M et si M est de rang inférieur ou égal à k alors N est de rang inférieur ou égal à k.
– Si $\varphi : M \to M'$ est un homomorphisme surjectif entre deux modules projectifs tels que $R_M = R_{M'}$, c'est un isomorphisme. C'est en particulier le cas si M et M' sont tous deux de rang k.

Lemme 2.13 *Soit M un $\mathbf{A}$-module engendré par $x_1, \ldots, x_n$. Notons $\underline{x} : (a_i)_i \mapsto \sum_{i=1}^n a_i x_i : \mathbf{A}^n \to M$. Alors M est projectif de rang inférieur ou égal à 1 si et seulement s'il existe une matrice $P = (p_{ij}) \in \mathbf{A}^{n\times n}$ vérifiant :*

1. *$P^2 = P$ et tout mineur d'ordre 2 de P est nul (donc le polynôme $R_{\operatorname{Im} P}$ est égal à $(1 - r_1) + r_1 X$ avec $r_1 = \operatorname{tr}(P)$) ;*
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 l'idempotent $1 - \operatorname{tr}(P) = \det(I_n - P)$.*

Une telle matrice est appelée une matrice de projection pour $(x_1, \ldots, x_n)$. *Dans ce cas on a* $\operatorname{Ker} P = \operatorname{Ker} \underline{x}$ *et $\underline{x}$ induit (par restriction) un isomorphisme de* $\operatorname{Im} P$ *sur M (cet isomorphisme associe la j-ème colonne de P à x_j).*

Lemme 2.14 *Soit $\underline{x} : (a_i)_i \mapsto \sum_{i=1}^n a_i x_i$ une forme linéaire $\mathbf{A}^n \to \mathbf{A}$. On suppose que $\mathfrak{i} = \langle x_1, \ldots, x_n\rangle$ est localement principal et que* $\operatorname{Ann} \mathfrak{i} = \langle r\rangle$ *avec r idempotent. Soit A une matrice de localisation principale pour $(x_1, \ldots, x_n)$, $s = 1 - r$ et $P = sA$. Alors* $\operatorname{Ker} P = \operatorname{Ker} \underline{x}$ *et P est une matrice de projection pour $(x_1, \ldots, x_n)$. En particulier, $\mathfrak{i}$ est projectif (de rang inférieur ou égal à 1).*

Preuve : Le point (2) de la proposition 2.6 montre que $A^2 - A$ est à coefficients dans $\operatorname{Ann} \mathfrak{i} = \langle r\rangle$, d'où $(sA)^2 = sA^2 = sA$, donc P est bien une matrice de projection.
Le point (1) de la proposition 2.6 et les égalités $sx_i = x_i$ montrent $\operatorname{Ker} P \subset \operatorname{Ker} \underline{x}$. L'inclusion inverse provient du point (6) de la proposition 2.6 : soit $\alpha \in \operatorname{Ker} \underline{x}$ et $y = A\alpha$, alors y est à coefficients dans $\operatorname{Ann} \mathfrak{i}$, donc $sy = 0$ et $\alpha \in \operatorname{Ker} P$.
Pour montrer que $P = sA$ est une matrice de projection pour $(x_1, \ldots, x_n)$, on utilise d'une part la définition 2.2 et d'autre part le point (2) de la proposition 2.6 : les mineurs d'ordre 2 de sA appartiennent à $\operatorname{Ann} \mathfrak{i} = \langle 1 - s\rangle$, donc sont nuls. □

Corollaire 2.15

1. *Un idéal de type fini $\mathfrak{i}$ est un module projectif si et seulement s'il est localement principal et son annulateur est engendré par un idempotent ;*
2. *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* $\operatorname{Ann} \langle x_1, \ldots, x_n\rangle = \langle r\rangle$ *(r idempotent), alors on peut prendre $A' = (1 - r)A$;*
   – *si la matrice A' est connue, alors* $\operatorname{Ann} \langle x_1, \ldots, x_n\rangle = \langle r\rangle$ *avec $r = 1 - \operatorname{tr}(A') = \det(\mathrm{I}_n - A')$ et une matrice de localisation principale A est obtenue en ajoutant r à l'un quelconque des coefficients diagonaux de A'.*

3. *Un idéal de type fini* $\mathfrak{i}$ *est un module projectif de rang* 1 *si et seulement s'il est localement principal et son annulateur est réduit à* $\langle 0\rangle$.

Remarque : Il n'y a pas de différence entre une matrice de localisation principale et une matrice de projection pour un système générateur fini d'un idéal projectif de rang 1.

Lemme 2.16 *Si* $\mathfrak{i}$ *et* $\mathfrak{j}$ *sont des idéaux projectifs de type fini d'un anneau* $\mathbf{A}$*, alors leur produit* $\mathfrak{i}\,\mathfrak{j}$ *l'est également, et il est isomorphe à* $\mathfrak{i}\otimes_{\mathbf{A}}\mathfrak{j}$.

Preuve : Voyons d'abord le cas où $\mathfrak{i}$ et $\mathfrak{j}$ sont de rang 1. On sait que $\mathfrak{i}\,\mathfrak{j}$ 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 $\mathfrak{i}\otimes_{\mathbf{A}}\mathfrak{j}\to\mathfrak{i}\,\mathfrak{j}\ : x\otimes y\mapsto xy$ est alors un homomorphisme surjectif entre modules projectifs de type fini de même rang. C'est donc un isomorphisme. Le cas général se ramène au cas précédent en localisant successivement par les idempotents du sfio $\{ab,\ (1-a)b,\ a(1-b),\ (1-a)(1-b)\}$ où $\mathrm{Ann}\,\mathfrak{i}=\langle a\rangle$ et $\mathrm{Ann}\,\mathfrak{j}=\langle b\rangle$. □

Le lemme de simplification

Lemme 2.17 (lemme de simplification) *Si* $\mathfrak{i}$ *est un idéal projectif de rang* 1*, et* $\mathfrak{j}$ *et* $\mathfrak{j}'$ *sont deux idéaux tels que* $\mathfrak{i}\,\mathfrak{j}\subset\mathfrak{i}\,\mathfrak{j}'$ *(resp.* $\mathfrak{i}\,\mathfrak{j}=\mathfrak{i}\,\mathfrak{j}'$*) alors* $\mathfrak{j}\subset\mathfrak{j}'$ *(resp.* $\mathfrak{j}=\mathfrak{j}'$*).*

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

Proposition 2.18 *Soit* k *idéaux stricts* $\mathfrak{i}_1,\dots,\mathfrak{i}_k$ *de* $\mathbf{A}$ *deux à deux comaximaux. On définit une application*

$$\phi\ :\ \left\{\begin{array}{ccc}\mathbb{N}^k & \longrightarrow & \{\text{idéaux de }\mathbf{A}\}\\ \alpha & \longmapsto & \mathfrak{i}_1^{\alpha_1}\cdots\mathfrak{i}_k^{\alpha_k}\end{array}\right.$$

Alors on a :

$$\phi(\alpha+\beta)=\phi(\alpha).\phi(\beta),\quad \phi(\sup(\alpha,\beta))=\phi(\alpha)\cap\phi(\beta),\quad \phi(\inf(\alpha,\beta))=\phi(\alpha)+\phi(\beta)$$

Si, de plus, les idéaux $\mathfrak{i}_1,\dots,\mathfrak{i}_k$ *sont projectifs de rang* 1*, alors* ϕ *est injective.*

Preuve : Pour trois idéaux quelconques $\mathfrak{i},\mathfrak{j},\mathfrak{l}\subset\mathbf{A}$, on a $\mathfrak{i}\,\mathfrak{j}+\mathfrak{i}\,\mathfrak{l}=\mathfrak{i}\,(\mathfrak{j}+\mathfrak{l})$. Soit $m,n,p\in\mathbb{N}$. Si $\mathfrak{i}+\mathfrak{j}=\mathbf{A}$ alors $\mathfrak{i}^m+\mathfrak{j}=\mathbf{A}$, $\mathfrak{i}\,\mathfrak{j}=\mathfrak{i}\cap\mathfrak{j}$, $\mathfrak{j}+\mathfrak{i}\,\mathfrak{l}=\mathfrak{j}+\mathfrak{l}$. Si $\mathfrak{i}+\mathfrak{j}=\mathfrak{i}+\mathfrak{l}=\mathbf{A}$ alors $\mathfrak{i}+\mathfrak{j}\,\mathfrak{l}=\mathfrak{i}+(\mathfrak{j}\cap\mathfrak{l})=\mathbf{A}$ et

$$\mathfrak{i}^n\mathfrak{j}\cap\mathfrak{i}^p\mathfrak{l}=(\mathfrak{i}^n\cap\mathfrak{j})\cap(\mathfrak{i}^p\cap\mathfrak{l})=\mathfrak{i}^{\max(n,p)}\cap(\mathfrak{j}\cap\mathfrak{l})=\mathfrak{i}^{\max(n,p)}(\mathfrak{j}\cap\mathfrak{l})$$

$$\mathfrak{i}^n\mathfrak{j}+\mathfrak{i}^p\mathfrak{l}=\mathfrak{i}^{\min(n,p)}(\mathfrak{i}^{n-\min(n,p)}\mathfrak{j}+\mathfrak{i}^{p-\min(n,p)}\mathfrak{l})=\mathfrak{i}^{\min(n,p)}(\mathfrak{j}+\mathfrak{l})$$

Ces dernières lignes prouvent (à l'aide d'une récurrence) les égalités de la propriété. Enfin, pour démontrer le caractére injectif de ϕ, on utilise (dans une récurrence) le lemme 2.17. □

Proposition 2.19 (« Quotient » d'un idéal par un idéal projectif) *Soit* $\mathfrak{i}$ *et* $\mathfrak{j}$ *deux idéaux tels que* $\mathfrak{i} \subset \mathfrak{j}$ *et* $\mathfrak{j}$ *projectif de type fini. Soit* r *l'idempotent annulateur de* $\mathfrak{j}$*. Si* $r = 0$*, c'est-à-dire si* $\mathfrak{j}$ *est de rang* 1*, il existe un idéal unique* $\mathfrak{l}$ *tel que* $\mathfrak{i} = \mathfrak{j}\,\mathfrak{l}$*. Plus généralement, il existe un idéal unique* $\mathfrak{l}$ *tel que* $\mathfrak{i} = \mathfrak{j}\,\mathfrak{l}$ *et* $r\mathfrak{l} = 0$*. On notera alors* $\mathfrak{l} = \mathfrak{i} \div \mathfrak{j}$*.*

Preuve : L'existence de $\mathfrak{l}$ provient de la proposition 2.9 (il existe $\mathfrak{l}'$ tel que $\mathfrak{i} = \mathfrak{j}\,\mathfrak{l}'$ et on pose $\mathfrak{l} = (1-r)\mathfrak{l}'$) et l'unicité du lemme 2.17. □

Remarque : Les idéaux $\mathfrak{l}'$ vérifiant $\mathfrak{j}\,\mathfrak{l}' = \mathfrak{i}$ sont tous les idéaux contenant $\mathfrak{l} = \mathfrak{i} \div \mathfrak{j}$ et contenus dans le transporteur $\mathfrak{i} : \mathfrak{j} = \{x \in \mathbf{A} \mid x\mathfrak{j} \subset \mathfrak{i}\} = \mathfrak{l} + \mathrm{Ann}(\mathfrak{j})$.

2.3 Idéaux inversibles

Définition 2.20 *Un idéal* $\mathfrak{i}$ *d'un anneau* $\mathbf{A}$ *est dit* inversible *s'il existe un idéal* $\mathfrak{j}$ *de* $\mathbf{A}$ *et un élément régulier* a *tels que* $\mathfrak{i}\,\mathfrak{j} = \langle a \rangle$*.*

NB : Si a est fixé, $\mathfrak{j}$ est unique car $\mathfrak{i}\,\mathfrak{j} = \mathfrak{i}\,\mathfrak{j}_1 = \langle a \rangle$ implique $\mathfrak{i}\,\mathfrak{j}\,\mathfrak{j}_1 = a\mathfrak{j} = a\mathfrak{j}_1$ et donc $\mathfrak{j} = \mathfrak{j}_1$ (a régulier). Par ailleurs, $a = a_1b_1 + \cdots + a_kb_k$ avec $a_1, \ldots, a_k \in \mathfrak{i}$, $b_1, \ldots, b_k \in \mathfrak{j}$. Posons $\mathfrak{i}' = \langle a_1, \ldots, a_k \rangle \subset \mathfrak{i}$ et $\mathfrak{j}' = \langle b_1, \ldots, b_k \rangle \subset \mathfrak{j}$. Alors $\langle a \rangle \subset \mathfrak{i}'\mathfrak{j}' \subset \mathfrak{i}\,\mathfrak{j} = \langle a \rangle$. Donc $\mathfrak{i}'\mathfrak{j}' = \mathfrak{i}\,\mathfrak{j} = \mathfrak{i}\,\mathfrak{j}' = \mathfrak{i}'\mathfrak{j}$ ce qui implique $\mathfrak{i} = \mathfrak{i}'$ et $\mathfrak{j} = \mathfrak{j}'$. En particulier tout idéal inversible est de type fini.

Proposition 2.21 *Un idéal* $\mathfrak{i}$ *est inversible si et seulement s'il est localement principal et contient un élément régulier. Un idéal inversible est un module projectif de rang 1.*

Preuve :
• Si $\mathfrak{i}$ est de type fini, localement principal, et contient un régulier a, alors il est inversible d'après le point (5) de la proposition 2.6. C'est un module projectif de rang 1 d'après le corollaire 2.15.
• Supposons $\mathfrak{i}$ inversible. On a vu juste avant que $\mathfrak{i}$ est de type fini. Reprenons les mêmes notations et montrons que $\mathfrak{i} = \langle a_1, \ldots, a_k \rangle$ 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 que l'on doit vérifier sont vraies après multiplication par a. □

Proposition 2.22 (« Quotient » d'un idéal par un idéal inversible) *Soit* $\mathfrak{i}$ *et* $\mathfrak{j}$ *deux idéaux tels que* $\mathfrak{i} \subset \mathfrak{j}$ *avec* $\mathfrak{i}$ *localement principal et* $\mathfrak{j}$ *inversible, engendrés respectivement par* n *et* m *éléments, alors* $\mathfrak{i} \div \mathfrak{j}$ *est engendré par* $n + m - 1$ *éléments.*

Preuve : Il existe un élément régulier $a \in \mathfrak{j}$, et $\mathfrak{j}_1 \subset \mathbf{A}$ tels que $\mathfrak{j}\,\mathfrak{j}_1 = \langle a \rangle$ ($\mathfrak{j}_1$ est engendré par m éléments, cf. proposition 2.6, point (5)). Or $\mathfrak{i} = \mathfrak{j}\,\mathfrak{l}$, donc $\mathfrak{i}\,\mathfrak{j}_1 = \mathfrak{j}\,\mathfrak{l}\,\mathfrak{j}_1 = a\mathfrak{l}$. Mais $\mathfrak{i}\,\mathfrak{j}_1$ est engendré par $n + m - 1$ éléments (proposition 2.7). Écrivons $\mathfrak{i}\,\mathfrak{j}_1 = \langle z_1, \ldots, z_k \rangle$ avec $k = n + m - 1$. On a $\mathfrak{i}\,\mathfrak{j}_1 \subset \langle a \rangle$. Pour tout $i \in \{1, ..., k\}$, il existe un élément b_i tel que $z_i = b_ia$. On a alors $a\langle b_1, \ldots, b_k \rangle = \mathfrak{i}\,\mathfrak{j}_1 = a\mathfrak{l}$, donc $\mathfrak{l} = \langle b_1, \ldots, b_k \rangle$ puisque a est régulier. □

Comportement des idéaux projectifs ou inversibles par changement d'anneau de base

Un idéal localement principal $\mathfrak{i} = \langle x_1, \ldots, x_n \rangle \subset \mathbf{A}$ reste localement principal par changement d'anneau de base $\varphi : \mathbf{A} \to \mathbf{B}$ puisqu'une matrice de localisation principale est transformée en une matrice de localisation principale. Par contre les choses sont plus délicates avec les idéaux projectifs ou inversibles. Cela tient à ce que le nouvel idéal $\mathfrak{i}^\varphi = \varphi(\mathfrak{i})\mathbf{B} = \langle \varphi(x_1), \ldots, \varphi(x_n) \rangle \subset \mathbf{B}$ n'est pas nécessairement isomorphe au module $\mathfrak{i} \otimes_{\mathbf{A}} \mathbf{B}$. Par exemple un idéal principal inversible reste principal mais son annulateur peut a priori devenir « n'importe quoi ».

Néanmoins, l'isomorphisme $\mathfrak{i}^\varphi \simeq \mathfrak{i} \otimes_{\mathbf{A}} \mathbf{B}$ est assuré si $\mathfrak{i}$ est de présentation finie et si l'extension est plate (i.e. $\mathbf{B}$ est un $\mathbf{A}$-module plat). Cela comprend en particulier les cas où $\mathbf{B}$ est un localisé de $\mathbf{A}$ et celui où il est libre sur $\mathbf{A}$.

Fait 2.23 *Soit $\mathfrak{i} = \langle x_1, \ldots, x_n \rangle$ un idéal de type fini de $\mathbf{A}$ et $\varphi : \mathbf{A} \to \mathbf{B}$ une extension plate. Si $\mathfrak{i}$ est projectif ou inversible alors il en va de même pour $\mathfrak{i}^\varphi$.*

Un exemple d'idéaux maximaux inversibles

Définition 2.24

1. *Une partie S d'un ensemble E est dite* détachable *si on a un test pour « $x \in S$? » lorsque $x \in E$;*
2. *Un anneau est dit* fortement discret *si les idéaux de type fini sont détachables ;*
3. *Un $\mathbf{A}$-module est dit* fortement discret *si les sous-modules de type fini sont détachables ;*
4. *Dans un anneau, on dit que* la relation de divisibilité est explicite *lorsque les idéaux principaux sont détachables.*

NB : La définition précédente doit être lue constructivement. Dans le premier point par exemple le test doit décider si $x \in S$ ou pas, et apporter la preuve constructive du fait correspondant. En particulier dans le dernier point le test décide si un élément x (arbitraire) divise un autre élément y, et en cas de réponse positive, il donne un élément c tel que $xc = y$.

Par exemple toute algèbre de présentation finie sur $\mathbb{Z}$ (ou sur un corps qui possède un test d'égalité à 0) est un anneau fortement discret (ce résultat n'est pas trivial, voir [23]).

Concernant les idéaux premiers, nous les supposerons toujours détachables pour simplifier les énoncés. Ceci donne les définitions constructives suivantes :
Un idéal premier détachable est un idéal $\mathfrak{p}$ tel que l'anneau quotient $\mathbf{A}/\mathfrak{p}$ soit intègre, il est minimal si le localisé $\mathbf{A}_\mathfrak{p}$ est zéro-dimensionnel. L'idéal $\mathfrak{p}$ est maximal détachable si $\mathbf{A}/\mathfrak{p}$ est un corps possédant un test d'égalité à 0.

En mathématiques classiques, tout anneau est fortement discret, tout idéal est détachable en vertu du principe du tiers exclu, qui donne en particulier : « $\forall x \in \mathbf{A},\ x \in \mathfrak{i} \ \vee \ x \notin \mathfrak{i}$ ». Donc en mathématiques classiques, la proposition suivante se lit en oubliant partout « détachable » : la preuve constructive vaut aussi, comme toujours, en mathématiques classiques.

Proposition 2.25 *Soit* $\mathbf{A}$ *un anneau intègre,* $\mathfrak{p}$ *un idéal maximal inversible détachable,* $\mathbf{K}$ *le corps de fractions de* $\mathbf{A}$ *et* $f(X) \in \mathbf{A}[X]$ *un polynôme irréductible unitaire de* $\mathbf{K}[X]$*. On suppose que sur le corps résiduel* $\mathbf{F}_\mathfrak{p} = \mathbf{A}/\mathfrak{p}$*, le polynôme* f *se factorise en un produit de polynômes unitaires deux à deux étrangers :* $f(X) = \prod_i g_i(X)$*. Soit* $\mathbf{B} = \mathbf{A}[x] = \mathbf{A}[X]/\langle f(X)\rangle$*. Alors dans* $\mathbf{B}$ *l'idéal* $\mathfrak{p}\ \mathbf{B}$ *est égal au produit des idéaux* $\langle g_i(x), \mathfrak{p}\rangle = \mathfrak{q}_i$*. Ces idéaux sont inversibles et détachables. En outre* g_i *est irréductible si et seulement si* $\mathfrak{q}_i$ *est maximal.*

Preuve : L'idéal $\mathfrak{q}_i$ est détachable en vertu de l'isomorphisme canonique $\mathbf{B}/\mathfrak{q}_i \simeq \mathbf{F}_\mathfrak{p}[X]/\langle g_i(X)\rangle$. On constate facilement que les $\mathfrak{q}_i$ sont deux à deux comaximaux. Donc $\prod_i \mathfrak{q}_i = \bigcap_i \mathfrak{q}_i$. Par ailleurs, en tant que treillis, le treillis des idéaux contenant $\mathfrak{p}\ \mathbf{B}$ est isomorphe au treillis des idéaux de $\mathbf{B}/\mathfrak{p}\ \mathbf{B} \simeq \mathbf{F}_\mathfrak{p}[X]/\langle f(X)\rangle$, donc $\bigcap_i \mathfrak{q}_i = \mathfrak{p}\ \mathbf{B}$. Enfin $\mathfrak{p}\ \mathbf{B}$ (et donc chaque facteur de $\mathfrak{p}\ \mathbf{B}$) est inversible d'après le fait 2.23 puisque $\mathbf{B}$ est un $\mathbf{A}$-module libre. □

Factorisation en produit d'idéaux maximaux inversibles

Lemme 2.26 *Soit* $\mathbf{A}$ *un anneau commutatif,* $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$*,* $\mathfrak{q}_1, \ldots, \mathfrak{q}_{k'}$ *des idéaux maximaux inversibles détachables avec* $\mathfrak{p}_i \neq \mathfrak{p}_j$ *et* $\mathfrak{q}_i \neq \mathfrak{q}_j$ *si* $i \neq j$*. Si* $\prod_{i=1}^{k} \mathfrak{p}_i^{n_i} = \prod_{i=1}^{k'} \mathfrak{q}_i^{m_i}$*, alors* $k = k'$ *et il existe* $\sigma \in \mathcal{S}_k$ *tel que* $\mathfrak{p}_i = \mathfrak{q}_{\sigma(i)}$ *et* $n_i = m_{\sigma(i)}$ *pour tout* i*.*

Preuve : En effet, $\mathfrak{p}_1$ (premier) contient $\prod_{i=1}^{k'} \mathfrak{q}_i^{m_i}$, donc il contient l'un des $\mathfrak{q}_j$ (maximal), donc $\mathfrak{p}_1 = \mathfrak{q}_j$. On simplifie par l'idéal inversible $\mathfrak{p}_1 = \mathfrak{q}_j$ et on termine par induction.
Autre preuve : puisqu'on a un test d'égalité pour les idéaux de type fini on se ramène au cas d'une égalité $\prod_{i=1}^{\ell} \mathfrak{p}_i^{n_i} = \prod_{i=1}^{\ell} \mathfrak{p}_i^{m_i}$, (avec $m_i, n_i \geq 0$) et on conclut par la proposition 2.18. □

Proposition 2.27 *Soit* $\mathfrak{i}, \mathfrak{p}_1, \ldots, \mathfrak{p}_n$ *des idéaux de type fini d'un anneau fortement discret* $\mathbf{A}$*, les* $\mathfrak{p}_i$ *étant maximaux inversibles, et des entiers positifs* m_i*. Supposons* $\prod_i \mathfrak{p}_i^{m_i} \subset \mathfrak{i}$*. Alors il existe des entiers* $n_i \leq m_i$ *tels que* $\mathfrak{i} = \prod_i \mathfrak{p}_i^{n_i}$*. En particulier,* $\mathfrak{i}$ *est inversible.*

Preuve : Si $\mathfrak{i} = \mathbf{A}$, le résultat est clair. Si ce n'est pas le cas, alors $\mathfrak{i}$ ne peut pas être comaximal à tous les $\mathfrak{p}_i$, donc $\mathfrak{i}$ est inclus dans l'un des $\mathfrak{p}_i$, par exemple, dans $\mathfrak{p}_1$. On considère $\mathfrak{l} = \mathfrak{i} \div \mathfrak{p}_1$. Par le lemme de simplification 2.17, $\mathfrak{l}$ contient $\mathfrak{p}_1^{m_1-1} \prod_{i>1} \mathfrak{p}_i^{m_i}$. On termine par induction. □

Remarque : En mathématiques classiques, il n'est pas nécessaire de supposer $\mathfrak{i}$ de type fini, et tout anneau est fortement discret.

Proposition 2.28 *Soit* $\mathbb{Z}[x] \simeq \mathbb{Z}[X]/\langle f(X)\rangle$ *avec* f *un polynôme irréductible unitaire. Si pour tout nombre premier* p *qui divise le dicriminant de* f *et tout* $g \in \mathbb{Z}[x]$ *unitaire, facteur irréductible de* f *dans* $\mathbb{F}_p[X]$*, l'idéal* $\langle p, g(x)\rangle$ *est inversible dans* $\mathbb{Z}[x]$*, alors tout idéal de type fini non nul est inversible et, s'il est distinct de* $\langle 1\rangle$*, il se décompose en produit d'idéaux maximaux inversibles.*

Preuve : Un idéal de type fini non nul de $\mathbb{Z}[x]$ ou bien est égal à $\langle 1\rangle$, ou bien contient un entier > 1. Un tel entier se factorise en produit d'entiers premiers. En appliquant la proposition 2.27, il suffit de montrer que tout nombre premier p engendre un idéal contenant un produit d'idéaux maximaux inversibles. Les idéaux maximaux de $\mathbb{Z}[x]$ sont les idéaux $\langle p, g(x)\rangle$ où $g \in \mathbb{Z}[X]$ est facteur irréductible de f dans $\mathbb{F}_p[X]$ (cf. la proposition 2.25). 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 2.25. Dans le cas restant, supposons que $f(X) = \prod_i g_i^{n_i}(X)$ modulo p. Alors on voit que $\prod_i \langle g_i(x), p\rangle^{n_i} \subset \prod_i \langle g_i^{n_i}(x), p\rangle \subset \langle p\rangle$. Ceci termine la preuve car les idéaux maximaux $\langle g_i(x), p\rangle$ sont inversibles par hypothèse. □

Remarque : Dans le « cas restant », avec la proposition 2.27, on obtient $\langle p\rangle = \prod_i \langle g_i(x), p\rangle^{m_i}$ $(m_i \leq n_i)$. Ceci implique $\prod_i g_i^{m_i}(x) = 0 \mod p$, donc $f(X)$ divise $\prod_i g_i(X)^{m_i}$ modulo p, et enfin $m_i = n_i$. Conclusion : $\langle p\rangle = \prod_i \langle g_i(x), p\rangle^{n_i}$.

2.4 Le théorème un et demi

Définition 2.29 *Un anneau est dit* quasi intègre *si l'annulateur de tout élément est engendré par un idempotent.*

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

Lemme 2.30 *On considère $x_1, \ldots, x_n$ des vecteurs d'un module sur un anneau commutatif. Si on a $\mathrm{Ann}(x_i) = \langle r_i\rangle$ où r_i est un idempotent pour $1 \leq i \leq n$, alors il existe des idempotents orthogonaux $t_2, \ldots, t_n$ tels que l'élément $x = x_1 + t_2x_2 + \cdots + t_nx_n$ vérifie $\mathrm{Ann}(x_1, \ldots, x_n) = \mathrm{Ann}(x) = \langle r_1 \cdots r_n\rangle$.*
En particulier dans un anneau quasi intègre tout idéal de type fini i a pour un annulateur un idéal $\langle r\rangle$ avec r idempotent, et il contient un élément x ayant le même annulateur.

Preuve : Soit s_i tel que $s_i + r_i = 1$, on a :

$$\begin{aligned} 1 = \;& s_1 + r_1 = s_1 + r_1(s_2 + r_2) = s_1 + r_1s_2 + r_1r_2(s_3 + r_3) = \cdots \\ = \;& s_1 + r_1s_2 + r_1r_2s_3 + \cdots + r_1r_2 \cdots r_{n-1}s_n + r_1r_2 \cdots r_n \end{aligned}$$

Posons $t_1 = s_1$, $t_2 = r_1s_2$, $t_3 = r_1r_2s_3, \ldots, t_{n+1} = r_1r_2 \cdots r_n$ $(t_1, \ldots, t_{n+1}$ est un sfio) et $x = t_1x_1 + t_2x_2 + \cdots + t_nx_n$. Il est clair que $\langle t_{n+1}\rangle \subset \mathrm{Ann}(x_1, \ldots, x_n) \subset \mathrm{Ann}(x)$. Inversement, soit $z \in \mathrm{Ann}(x)$. Alors $zx = 0$, donc $zt_ix_i = zt_ix = 0$ pour $1 \leq i \leq n$, donc $zt_i \in \mathrm{Ann}(x_i) = \langle r_i\rangle$, donc $zt_i = zt_ir_i = 0$. Mais $z = \sum_{i=1}^{n+1} zt_i$, donc $z = zt_{n+1} \in \langle t_{n+1}\rangle$.
Enfin, on remarque que $t_1x_1 = s_1x_1 = x_1$ donc $x = 1.x_1 + t_2x_2 + \cdots + t_nx_n$. □

Lemme 2.31 *Tout module projectif de rang 1 sur un anneau zéro-dimensionnel est libre*[3].

[3] Cas particulier du résultat suivant : si $\mathbf{A}/\mathrm{Rad}(\mathbf{A})$ est zéro-dimensionnel tout $\mathbf{A}$-module projectif de rang constant est libre (voir par exemple [22]).

Preuve : Soit P une matrice de projection dont l'image est le module projectif. Appelons P_j la j-ème colonne de $P = (p_{ij})$. Par le lemme 1.20, pour chaque p_{ii}, il existe un entier $d_i \geq 0$ et un idempotent s_i tels que $\langle s_i \rangle = \langle p_{ii}^{d_i} \rangle = \langle p_{ii}^{d_i+1} \rangle$. Comme $\mathrm{tr}(P) = 1$, on a $\langle p_{11}^{d_1+1}, \ldots, p_{nn}^{d_n+1} \rangle = \mathbf{A}$ donc $\mathrm{Ann} \langle p_{11}^{d_1+1}, \ldots, p_{nn}^{d_n+1} \rangle = \langle 0 \rangle$. Notons $r_i = 1 - s_i$: on a alors $\langle r_i \rangle = \mathrm{Ann}(p_{ii}^{d_i+1})$. D'après le lemme 2.30, il existe un sfio, précisément $t_1 = s_1$, $t_2 = r_1 s_2$, $t_3 = r_1 r_2 s_3, \ldots$, $t_{n+1} = r_1 r_2 \cdots r_n$, et $x = t_1 p_{11}^{d_1+1} + \cdots + t_n p_{nn}^{d_n+1}$ dont l'annulateur est nul (remarquer que $t_{n+1} = 0$). Donc x est régulier, donc inversible (dimension nulle). On en déduit que le vecteur $V = t_1 P_1 + \cdots + t_n P_n = {}^t(v_1, \ldots, v_n)$ est unimodulaire : $t_1 p_{11}^{d_1} v_1 + \cdots + t_n p_{nn}^{d_n} v_n = x$ car $t_i v_i = t_i p_{ii}$. Conclusion : $\{V\}$ est une base de $\mathrm{Im}\, P$. □

Théorème 2.32 (théorème un et demi) *Soit* $\mathbf{A}$ *un anneau commutatif de dimension inférieure ou égale à* 1 *et* $\mathfrak{i}$ *un idéal inversible. Soit* $x \in \mathfrak{i}$ *un élément régulier. Alors il existe* $y \in \mathfrak{i}$ *tel que pour tout* $n \geq 1$, $\mathfrak{i} = x^n \mathfrak{i} + y\mathbf{A}$. *En particulier* $\mathfrak{i} = \langle x^n, y \rangle$.

Preuve : Comme x est régulier, l'anneau $\mathbf{A}/x\mathbf{A}$ est zéro-dimensionnel. Le module $\mathfrak{i} \otimes_{\mathbf{A}} \mathbf{A}/x\mathbf{A} \simeq \mathfrak{i}/x\mathfrak{i}$ est projectif de rang 1, si bien qu'il est libre sur $\mathbf{A}/x\mathbf{A}$ (lemme 2.31), donc engendré par un élément. Il existe donc $y \in \mathfrak{i}$ tel que $\mathfrak{i}/x\mathfrak{i} = (y\mathbf{A} + x\mathfrak{i})/x\mathfrak{i}$. Ceci implique $\mathfrak{i} = x\mathfrak{i} + y\mathbf{A}$, et par suite $\mathfrak{i} = x(x\mathfrak{i} + y\mathbf{A}) + y\mathbf{A} = x^2\mathfrak{i} + y\mathbf{A}$ ... □

La preuve que nous avons présentée ici est nettement plus simple et plus générale que celle que l'on trouve usuellement dans le cadre des anneaux de Dedekind. Elle nous a été inspirée par la lecture de [28], avec un résultat et une technique de preuve légèrement différentes. Elle est totalement constructive car elle est basée sur une définition constructive de la dimension de Krull.

Le théorème un et demi admet une extension remarquable due à O. Forster [10] dans le cas noethérien et à R. Heitmann [12, 13] dans le cas général : un idéal inversible sur un anneau de dimension inférieure ou égale à d peut toujours être engendré par $d + 1$ éléments. Plus généralement un module de type fini qui peut être engendré localement par r éléments est engendré par $r + d$ éléments. Pour une preuve constructive voir [8].

Le théorème suivant qui est un corollaire du théorème un et demi, aura une application intéressante pour les anneaux de Prüfer cohérents.

Théorème 2.33 *Soit* $\mathbf{A}$ *un anneau de dimension inférieure ou égale à* 1, *dont le radical de Jacobson* $\mathrm{Rad}(\mathbf{A})$ *contient un élément régulier, et* $\mathfrak{i}$ *un idéal inversible. Alors* $\mathfrak{i}$ *est principal.*

Preuve : Soient $y \in \mathrm{Rad}(\mathbf{A})$ et $x \in \mathfrak{i}$ tous deux réguliers. Alors $\mathfrak{i} \cap \mathrm{Rad}(\mathbf{A})$ contient $a = xy$ qui est régulier. Par le théorème un et demi, il existe $z \in \mathfrak{i}$ tel que $\mathfrak{i} = \langle a^2, z \rangle$. Donc $a = ua^2 + vz$ ce qui donne $a(1 - ua) = vz$ et puisque a est dans le radical $a \in \langle z \rangle$ donc $\mathfrak{i} = \langle z \rangle$. □

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

Théorème 2.34 *Soit $n \geq 3$ et $(x_1, \ldots, x_n)$ un vecteur unimodulaire sur un anneau quasi intègre $\mathbf{A}$ de dimension inférieure ou égale à 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 on peut par manipulations élémentaires transformer le vecteur (colonne) $v = (x_1, \ldots, x_n)$ en $(y_1, x_2, \ldots, x_n)$ unimodulaire où y_1 est régulier (cf. lemme 2.30). Considérons l'anneau $\mathbf{B} = \mathbf{A}/\langle y_1\rangle$. Cet anneau est zéro-dimensionnel et le vecteur v est transformé en $(0, x_2, \ldots, x_n)$ toujours unimodulaire. Puisque $n \geq 3$, on peut transformer dans $\mathbf{B}$ par manipulations élémentaires $(x_2, \ldots, x_n)$ en $(1, 0, \ldots, 0)$. Regardons dans $\mathbf{A}$ ce que l'on obtient alors : $(y_1, 1 + ay_1, z_3, \ldots, z_n)$, d'où ensuite, toujours par manipulations élémentaires $(y_1, 1, z_3, \ldots, z_n)$, puis $(1, 0, \ldots, 0)$. □

Ce théorème admet une généralisation importante, due à H. Bass dans le cas noethérien et à R. Heitmann [13] dans le cas général : la conclusion est valable si $n \geq 2 + \dim(\mathbf{A})$ pour n'importe quel anneau commutatif. En outre on peut utiliser une meilleure notion de dimension, introduite par Heitmann (en généralisation de la dimension du j-spectrum, qui ne fonctionne que pour le cas noethérien). Pour une preuve constructive voir [8].

3 Anneaux arithmétiques et anneaux de Prüfer

3.1 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 :*

$$\begin{cases} ux_2 &= vx_1 \\ wx_2 &= (1-u)x_1 \end{cases} \tag{5}$$

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

Fait 3.2 *La définition implique que $\langle x_1, x_2\rangle \langle u, w\rangle = \langle x_1\rangle$. Inversement si on a un idéal $\mathfrak{j}$ tel que $\langle x_1, x_2\rangle \mathfrak{j} = \langle x_1\rangle$ on en déduit facilement des éléments u, v, w convenables.*

Il y a de nombreuses autres propriétés qui peuvent caractériser les anneaux arithmétiques, en particulier le fait que les idéaux (ou encore les idéaux de type fini) forment un treillis distributif : voir [15, 18, 19].

Fait 3.3 – *Tout quotient et tout localisé d'un anneau arithmétique est un anneau arithmétique.*

– *Un anneau est arithmétique si et seulement s'il a la même propriété après localisation en des monoïdes comaximaux.*
– *Un idéal de type fini contenant un élément régulier dans un anneau arithmétique est un idéal inversible.*

Lemme 3.4 (anneaux arithmétiques locaux)
1. Un anneau $\mathbf{A}$ *est local et arithmétique si et seulement si pour tous* $a, b \in \mathbf{A}$, $a \in b\mathbf{A}$ *ou* $b \in a\mathbf{A}$. *De manière équivalente, tout idéal de type fini est principal et l'ensemble des idéaux de type fini est totalement ordonné pour l'inclusion.*
2. Soit $\mathbf{A}$ *un anneau arithmétique local. Pour deux idéaux arbitraires,* $\mathfrak{i} \not\subset \mathfrak{j}$ *implique* $\mathfrak{j} \subset \mathfrak{i}$. *Donc en mathématiques classiques, l'ensemble de tous les idéaux est totalement ordonné pour l'inclusion.*

Preuve : 1. Dans un anneau local un idéal localement principal $\mathfrak{i} = \langle x_1, \ldots, x_n\rangle$ est engendré par l'un des x_i (proposition 2.4). Ceci donne l'implication directe. Voyons la réciproque. Tout d'abord tout idéal de type fini est clairement principal donc localement principal. Ensuite l'anneau est local : soit $x \in \mathbf{A}$, si x divise $1+x$, $1+x = xy$ et x est inversible, si $1+x$ divise x, $x = (1+x)-1 = (1+x)y$ et $1+x$ est inversible.
2. Si $\mathfrak{i} \not\subset \mathfrak{j}$, soit $x \in \mathfrak{i}$ et $x \notin \mathfrak{j}$. Pour tout $y \in \mathfrak{j}$, on a nécessairement $y \in x\mathbf{A}$, donc $\mathfrak{j} \subset x\mathbf{A} \subset \mathfrak{i}$. □

Ces anneaux sont les « valuation rings » de Kaplansky [17]. Nous prendrons cependant nos « anneaux de valuation » (voir la définition 3.11) sans diviseur de zéro conformément à la terminologie de Bourbaki.

Construction de la matrice de localisation principale

Proposition 3.5 *Dans un anneau arithmétique* $\mathbf{A}$, *tout idéal de type fini est localement principal. Plus précisément pour tout* $(x_1, ..., x_n) \in \mathbf{A}^{1\times n}$, *il existe une matrice de localisation principale* $A = (a_{ij})$.

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

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

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 :

$$\begin{cases} u_i x_n &= v_i x_i \\ w_i x_n &= t_i x_i \\ u_i + t_i &= 1 \end{cases}$$

• Nous avons

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

Posons $\boxed{a_{ii} = s_i u_i = S_i}$ et $\boxed{a_{nn} = S_n = \sum_{i=1}^{n-1} s_i t_i}$, de sorte que $\sum_{i=1}^{n} S_i = 1$.
• D'autre part, pour $i \neq j \in \{1, \ldots, n-1\}$

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

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 $\boxed{a_{ni} = \sum_{j=1}^{n-1} b_{ji} w_j}$.

• 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

$$a_{nj} x_i = \left(\sum_{\ell=1}^{n-1} b_{\ell j} w_\ell\right) x_i = \left(\sum_{\ell=1}^{n-1} b_{\ell i} x_j\right) w_\ell = \left(\sum_{\ell=1}^{n-1} b_{\ell i} w_\ell\right) x_j = a_{ni} x_j. \qquad \square$$

Propriété 3.6 *Dans un anneau arithmétique, les idéaux de type fini vérifient les relations de la proposition 2.12 (page 14).*

Anneaux de Bezout

Définition 3.7 *Un* anneau de Bezout *est un anneau dans lequel les idéaux de type fini sont principaux.*

Par exemple, tout anneau arithmétique local et donc tout localisé d'un anneau arithmétique par un idéal premier[4] est un anneau de Bezout.

Le lemme 2.3 donne immédiatement.

Proposition 3.8 *Tout anneau de Bezout est un anneau arithmétique.*

Test d'appartenance à un idéal de type fini

Dans un anneau fortement discret, la relation de divisibilité est explicite. On a la réciproque (remarquable) pour les anneaux arithmétiques.

Proposition 3.9 *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 $LX = c$ avec $L = (b_1, \dots, b_n)$: soit $A = (a_{ij})$ une matrice de localisation principale pour $(b_1, \dots, b_n)$, l'équation $LX = c$ admet une solution si et seulement si pour tout i on peut trouver c_i tel que $a_{ii} c = b_i c_i$, 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}.*

[4] Pour qu'un localisé $\mathbf{A}_\mathfrak{p}$ soit local au sens constructif la localisation en l'idéal $\mathfrak{p}$ doit être définie via le monoïde complémentaire S, qui doit vérifier de manière explicite : $\forall x \in \mathbf{A}\ x \in S \vee (1+x) \in S$. Ceci est vérifié dans le cas des idéaux premiers détachables.

Idéaux premiers projectifs de rang 1

Proposition 3.10 *Dans un anneau arithmétique, un idéal premier détachable projectif de rang* 1 *est maximal.*

Preuve : Soit $\mathfrak{p}$ un idéal premier projectif de rang 1 et $y \notin \mathfrak{p}$. Alors $\mathfrak{p} \subset \mathfrak{p} + \langle y \rangle$. Comme l'anneau est arithmétique, il existe un idéal $\mathfrak{j}$ tel que $\mathfrak{j} \cdot (\mathfrak{p} + \langle y \rangle) = \mathfrak{p}$. Mais $\mathfrak{p}$ est premier et $y \notin \mathfrak{p}$, donc $\mathfrak{j} \subset \mathfrak{p}$. En multipliant par $\mathfrak{p}+\langle y \rangle$, on obtient $\mathfrak{p} \subset \mathfrak{p} \cdot (\mathfrak{p}+\langle y \rangle)$. Grâce au lemme de simplification 2.17, on a $\langle 1 \rangle \subset \mathfrak{p} + \langle y \rangle$. Conclusion : y est inversible dans $\mathbf{A}/\mathfrak{p}$. □

3.2 Anneaux de Prüfer et anneaux cohérents

Définition 3.11 *Un anneau arithmétique* $\mathbf{A}$ *est appelé* anneau de Prüfer *s'il est réduit, ou de manière équivalente, s'il est localement sans diviseur de zéro.*
On dit que $\mathbf{A}$ *est un* anneau de valuation *s'il est un anneau de Prüfer local, ou de manière équivalente, s'il est un anneau sans diviseur de zéro vérifiant* $\forall a, b,\ a \in b\mathbf{A}$ *ou* $b \in a\mathbf{A}$ *(voir le lemme 3.4).*

Justification :
— Pour tous $x, y \in \mathbf{A}$, il existe $u \in \mathbf{A}$ tel que $uy \in \mathbf{A}x$ et $(1-u)x \in \mathbf{A}y$ ($\mathbf{A}$ arithmétique), si bien que l'égalité $xy = 0$ implique $\mathbf{A}xy = \langle 0 \rangle$, $uy^2 = 0$ et $(1-u)x^2 = 0$, et ($\mathbf{A}$ réduit) $uy = (1-u)x = 0$.
— Pour un anneau $\mathbf{A}$ commutatif, être localement sans diviseur de zéro implique être réduit : si $x.x = 0$ alors il existe $u \in \mathbf{A}$ tel que $ux = (1-u)x = 0$, donc en sommant, $x = 0$. □

Fait 3.12 *Tout quotient réduit et tout localisé d'un anneau de Prüfer est un anneau de Prüfer. Un anneau est de Prüfer si et seulement s'il a la même propriété après localisation en des monoïdes comaximaux.*

Définition 3.13 *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.*

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

Fait 3.14 *Un anneau est cohérent si et seulement si l'intersection de deux idéaux de type fini est un idéal de type fini et l'annulateur de tout élément est un idéal de type fini (cf. par exemple [23]).*

3.3 Anneaux de Prüfer cohérents

Nous aurons besoin du lemme classique suivant :

Lemme 3.15 *Si un idéal de type fini* $\mathfrak{j}$ *est idempotent (c'est-à-dire* $\mathfrak{j}^2 = \mathfrak{j}$*) il est engendré par un idempotent, et cet idempotent est déterminé de manière unique.*

Preuve : C'est un « determinant trick ». Supposons $\mathfrak{j} = \langle x_1, \dots, x_n \rangle$. Puisque $\mathfrak{j}^2 = \mathfrak{j}$, il existe une matrice carrée M à coefficients dans $\mathfrak{j}$ telle que $(x_1, \dots, x_n) = (x_1, \dots, x_n)M$, donc $(x_1, \dots, x_n)(\mathrm{I}_n - M) = 0$. On multiplie cette égalité à droite par la transposée de la comatrice de $\mathrm{I}_n - M$ et on obtient : $(x_1, \dots, x_n) \det(\mathrm{I}_n - M) = 0$. Or $\det(\mathrm{I}_n - M) = 1 - e$ avec $e \in \mathfrak{j}$. Il vient finalement $(x_1, \dots, x_n) = (x_1, \dots, x_n).e$, c'est-à-dire que e fixe $x_1, \dots, x_n$ par multiplication, donc $\mathfrak{j} = \langle e \rangle$ et $e = e^2$. □

Rappelons que l'annulateur d'un élément d'un anneau localement sans diviseur de zéro (comme un anneau de Prüfer) est un idéal idempotent (cf. propriété 1.7) et, par ailleurs, qu'un anneau est dit quasi intègre si l'annulateur de tout élément est engendré par un élément idempotent.

Proposition 3.16 *Pour un anneau* $\mathbf{A}$ *les propriétés suivantes sont équivalentes :*

1. $\mathbf{A}$ *est un anneau de Prüfer cohérent ;*
2. $\mathbf{A}$ *est un anneau de Prüfer quasi intègre ;*
3. $\mathbf{A}$ *est un anneau de Prüfer et l'annulateur d'un idéal de type fini* $\mathfrak{i}$ *est toujours un idéal* $\langle r \rangle$ *avec* r *idempotent ;*
4. *Tout idéal de type fini de* $\mathbf{A}$ *est projectif.*

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

Preuve :
1. implique 2. Soit $\mathfrak{j} = \mathrm{Ann}(x)$. Alors pour tout $y \in \mathfrak{j}$, il existe $u \in \mathbf{A}$ tel que $uy = (1-u)x = 0$ (voir la définition 1.6). Ainsi, $y = uy + (1-u)y = (1-u)y \in \mathfrak{j}^2$. Donc $\mathfrak{j} = \mathfrak{j}^2$. On applique le lemme 3.15.
2. implique 3. d'après le lemme 2.30.
3. implique 4. d'après le corollaire 2.15 (point 1).
4. implique 1. clair. □

Proposition 3.17 *Tout anneau de Prüfer zéro-dimensionnel est cohérent.*

Preuve : Résulte immédiatement du lemme 1.21. □

Exemple 3.18 *Un anneau de Prüfer (Bezout) non cohérent de dimension* 1 *(inspiré d'un exemple de Sarah Glaz).*
On considère une indéterminée x sur $\mathbb{Q}$, puis $\alpha = (0, x, 0, x, 0, x, \dots) \in \mathbb{Q}[x]^{\mathbb{N}}$ et $\mathbf{A} = \left\{ \left(P_i(\alpha_i)\right)_i \mid P \in \mathbb{Q}[x]^{\mathbb{N}} \text{ stationnaire} \right\}$. Alors $\mathbf{A}$ est un anneau de Bezout réduit car $\mathbb{Q}[x]$ l'est. De plus, l'annulateur de $\alpha \in \mathbf{A}$ est la réunion strictement croissante des idéaux engendrés par les idempotents $(1, 0, 1, 0, \dots, 1, 0, 1, 0, 0, 0, 0, 0, \dots)$. Ainsi l'annulateur de α n'est pas de type fini et $\mathbf{A}$ est un anneau de Prüfer non cohérent. Enfin, $\mathbf{A}$ est de dimension 1 car $\mathbb{Q}[x]$ l'est.

Fait 3.19

1. *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 est de Prüfer cohérent si et seulement s'il a la même propriété après localisation en des monoïdes comaximaux ;*
2. *Soit un idéal de type fini* $\mathfrak{i}$ *dans un anneau de Prüfer cohérent. Alors* $\mathfrak{i}$ *est inversible si et seulement si* $\mathrm{Ann}(\mathfrak{i}) = 0$ *si et seulement si* $\mathfrak{i}$ *est projectif de rang* 1 *;*
3. *Un anneau arithmétique intègre est un anneau de Prüfer cohérent, tout idéal de type fini non nul est inversible.*

Pour le point 2. on applique le lemme 2.30.

Anneaux de valuation cohérents

Le résultat suivant, inconnu en mathématiques classiques, a une signification algorithmique cruciale. Rappelons qu'un anneau de valuation est sans diviseur de zéro, donc, en mathématiques classiques, intègre.

Proposition 3.20 *Un anneau de valuation non trivial est cohérent si et seulement s'il est intègre (i.e. s'il possède un test d'égalité à* 0*).*

Preuve : Si $\mathbf{A}$ est intègre l'annulateur d'un élément est $\langle 0\rangle$ ou $\langle 1\rangle$ donc la condition 2. dans la proposition 3.16 est vérifiée. Inversement si cette condition est vérifiée, soit r l'idempotent tel que $\mathrm{Ann}(x) = \langle r\rangle$. Puisque l'anneau est local on a $r = 0$ (si $1 - r$ est inversible) ou $r = 1$ (si r est inversible). Comme $0 \neq 1$, on a donc un test d'égalité à 0 dans $\mathbf{A}$. □

Par ailleurs l'anneau trivial est un anneau de valuation intègre et cohérent.

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

Lemme 3.21 *Soit* $\mathfrak{i}$ *et* $\mathfrak{j}$ *deux idéaux de type fini engendrés respectivement par* n *et* m *éléments dans un anneau de Prüfer cohérent avec* $\mathfrak{i} \subset \mathfrak{j}$*. Alors on peut construire* $n + m - 1$ *générateurs pour* $\mathfrak{i} \div \mathfrak{j}$*.*

Preuve : Soit r l'idempotent annulateur de $\mathfrak{j}$. En considérant les localisés $\mathbf{A}_r$ et $\mathbf{A}_{1-r}$, on est ramené aux cas extrêmes $r = 1$ et $r = 0$. Le premier cas est clair. Pour le second, on applique la proposition 2.22. □

Lemme 3.22 *Soit* $\mathfrak{i}$ *et* $\mathfrak{j}$ *deux idéaux de type fini dans un anneau de Prüfer cohérent. Alors* $\mathfrak{i} \cap \mathfrak{j} = (\mathfrak{i}\ \mathfrak{j}) \div (\mathfrak{i} + \mathfrak{j})$*. D'autre part, on peut déterminer un système générateurs de* $\mathfrak{i} \cap \mathfrak{j}$ *à* $n + m$ *éléments.*

Preuve : Il est clair que si $\langle r\rangle = \mathrm{Ann}(\mathfrak{i} + \mathfrak{j})$ alors $r(\mathfrak{i} \cap \mathfrak{j}) = 0$, donc la première affirmation résulte immédiatement du lemme 2.10 et de la proposition 2.19. Pour obtenir un système générateurs à $n + m$ éléments, on utilise la proposition 2.6, item (8), avec les générateurs de $\mathfrak{i} + \mathfrak{j}$. □

Noyau, image et conoyau d'une matrice

Le théorème suivant donne des informations précises sur la structure d'un module de présentation finie (point 3.), sur celle d'un sous-module de type fini d'un module libre (point 1.) et sur celle d'un module projectif de type fini général. La preuve du point 1. est déjà, constructive, dans [4] chapitre 1 proposition 6.1.

Théorème 3.23 *Soit* $\mathbf{A}$ *un anneau de Prüfer cohérent et soit un homomorphisme* $\varphi : \mathbf{A}^m \to \mathbf{A}^n$.

1. *L'image de* φ *est un module projectif de type fini, isomorphe à une somme directe de* n *idéaux de type fini ;*
2. *Le noyau de* φ *est facteur direct ;*
3. *Le conoyau de* φ *est somme directe de son sous-module de torsion (les éléments dont l'annulateur contient un élément régulier) et d'un sous-module projectif de type fini ;*
4. *Tout module projectif de rang* k *est isomorphe à une somme directe de* k *idéaux inversibles ;*
5. *Tout module projectif de rang inférieur ou égale à* k *est isomorphe à une somme directe de* k *idéaux de type fini.*

Preuve : 1. Considérons $M = \operatorname{Im}\varphi \subseteq \mathbf{A}^n$ et $\pi_n : \mathbf{A}^n \to \mathbf{A}$ la dernière forme coordonnée. L'idéal $\pi_n(M) = \mathfrak{i}_n$ est de type fini donc projectif, et la restriction surjective $\pi'_n : M \to \mathfrak{i}_n$ de π_n est scindée, et

$$M \simeq \operatorname{Ker}\pi'_n \oplus \operatorname{Im}\pi'_n = (M \cap \mathbf{A}^{n-1}) \oplus \mathfrak{i}_n \ .$$

On termine la preuve par induction sur n : $M \cap \mathbf{A}^{n-1}$ est de type fini puisque isomorphe à un quotient de M. On a donc écrit $M \simeq \mathfrak{i}_1 \oplus \cdots \oplus \mathfrak{i}_n$.
2. Conséquence immédiate de 1.
3. Technique « locale-globale ». Voir [19].
4. Si M est de rang constant $k \geq 1$, alors son dual M^* l'est également, leurs annulateurs sont nuls, et il existe $\mu \in M^*$ tel que $\operatorname{Ann}(\mu) = \langle 0\rangle$ (cf. lemme 2.30). Alors $\mu(M)$ est un idéal inversible de $\mathbf{A}$ car son annulateur est également nul. De plus, $M \simeq \operatorname{Ker}\mu \oplus \operatorname{Im}\mu$, ce qui prouve que $\operatorname{Ker}\mu$ est projectif de type fini de rang constant $k-1$ ...
5. On considère M comme somme directe de ses composantes de rang $1, \ldots, k$ et on applique le point 4. à chacune d'elles. □

Idéaux de type fini premiers

Proposition 3.24 *Soit* $\mathfrak{p}$ *un idéal premier détachable de type fini dans un anneau de Prüfer cohérent. Soit* r *l'idempotent qui engendre l'annulateur de* $\mathfrak{p}$*, et* $s = 1-r$*. On a* $r = 0$ *ou* $\mathfrak{p} = \langle s\rangle$*. Si* $r = 0$ *alors* $\mathfrak{p}$ *est inversible et maximal. Si* $\mathfrak{p} = \langle s\rangle$*,* $\mathbf{A}_r$ *est un anneau intègre et* $\mathbf{A}_\mathfrak{p}$ *est isomorphe au corps des fractions de* $\mathbf{A}_r$ *(donc* $\mathfrak{p}$ *est minimal).*

Preuve : On a $\mathbf{A} = r\mathbf{A} \oplus s\mathbf{A}$ avec $\mathfrak{p} \subset s\mathbf{A}$ donc $\mathbf{A}/\mathfrak{p} \simeq \mathbf{A}_r \times (\mathbf{A}_s/\mathfrak{p})$. L'idempotent r, vu dans $\mathbf{A}/\mathfrak{p}$ est égal à 0 ou 1 puisque $\mathbf{A}/\mathfrak{p}$ est intègre.

Dans le premier cas $\mathbf{A}_r$ est trivial donc $r = 0$ dans $\mathbf{A}$. On conclut avec la proposition 3.10 et le fait 3.19 point 2.
Dans le deuxième cas, $\mathbf{A}_s/\mathfrak{p}$ est trivial donc $\mathfrak{p} = s\mathbf{A}$. En outre $\mathbf{A}_r \simeq \mathbf{A}/\mathfrak{p}$ est intègre et on vérifie que $\mathrm{Frac}(\mathbf{A}_r) \simeq \mathbf{A}_{\mathfrak{p}}$. □

On a en mathématiques classiques le résultat suivant.

Corollaire 3.25 *Dans un anneau arithmétique* $\mathbf{A}$*, un idéal premier de type fini est maximal ou minimal. En particulier tout anneau arithmétique noethérien est de dimension inférieure ou égale à* 1*.*

Preuve : On note $\sqrt{\langle 0\rangle}$ le nilradical de $\mathbf{A}$. Les idéaux premiers de $\mathbf{A}$ sont en bijection avec ceux du quotient $\mathbf{A}/\sqrt{\langle 0\rangle}$. On se ramène donc au cas d'un anneau de Prüfer $\mathbf{B}$. Soit un idéal maximal $\mathfrak{m}$ de $\mathbf{B}$. Les idéaux premiers de $\mathbf{B}$ contenus dans $\mathfrak{m}$ sont en bijection avec ceux du localisé $\mathbf{B}_{\mathfrak{m}}$. On peut donc se ramener au cas d'un anneau de Prüfer local (anneau de valuation) donc intègre et cohérent. On conclut alors avec la proposition 3.24. □

4 Anneaux de Prüfer cohérents de dimension ≤ 1

4.1 Théorème un et demi

Le théorème 2.32 (un et demi) admet la variante (pour le cas intègre voir [14]) :

Théorème 4.1 *Soit* $\mathbf{A}$ *un anneau de Prüfer cohérent de dimension inférieure ou égale à* 1 *et* $\mathfrak{i}$ *un idéal de type fini. Il existe* $x \in \mathfrak{i}$ *tel que* $\mathrm{Ann}(x) = \mathrm{Ann}(\mathfrak{i})$*. Pour un tel* x*, il existe* $y \in \mathfrak{i}$ *tel que pour tout* $n \geq 1$*,* $\mathfrak{i} = x^n\mathfrak{i} + y\mathbf{A}$*. En particulier* $\mathfrak{i} = \langle x^n, y\rangle$*. En outre on peut construire un* y *tel que* $\mathrm{Ann}(y) = \mathrm{Ann}(\mathfrak{i})$*.*

Preuve : Soit r l'idempotent annulateur de $\mathfrak{i}$. En considérant les localisés $\mathbf{A}_r$ et $\mathbf{A}_{1-r}$, on est ramené aux cas extrêmes $r = 1$ et $r = 0$. Le premier cas est clair. Pour le second, on applique le théorème un et demi car x est régulier. Si $\mathrm{Ann}(y) = \langle e\rangle$, $e^2 = e$ et $f = 1 - e$, on considère $y' = y + ex \in \mathfrak{i}$. On a $y = fy'$ et donc $\mathfrak{i} = x^n\mathfrak{i} + y'\mathbf{A}$. □

Nous généralisons maintenant un résultat classique souvent formulé ainsi : *un anneau de Dedekind* [5] *intègre ayant un nombre fini d'idéaux maximaux est un anneau principal.* Pour le cas d'un anneau de Prüfer intègre voir [14].

Théorème 4.2 *Soit* $\mathbf{A}$ *un anneau de Prüfer cohérent de dimension inférieure ou égale à* 1*, dont le radical de Jacobson* $\mathrm{Rad}(\mathbf{A})$ *contient un élément régulier. Alors* $\mathbf{A}$ *est un anneau de Bezout.*

Preuve : Soit $\mathfrak{i}'$ un idéal de type fini. Son annulateur est engendré par un idempotent e. Alors $\mathfrak{i} = \mathfrak{i}' + \langle e\rangle$ est inversible et $\mathfrak{i}' = (1 - e)\mathfrak{i}$. Il suffit de montrer que $\mathfrak{i}$ est principal. Or cela résulte du théorème 2.33. □

[5] Voir la définition constructive d'un anneau de Dedekind, section 5.

4.2 Structure des idéaux de type fini et des modules de présentation finie

Nous revisitons le résultat classique suivant, dans lequel nous allons nous débarrasser de l'hypothèse noethérienne : *si* $\mathbf{A}$ *est un anneau noethérien intègre de dimension inférieure ou égale à* 1 *et* $\mathfrak{i}, \mathfrak{j}$ *deux idéaux avec* $\mathfrak{i}$ *inversible et* $\mathfrak{j} \neq 0$, *alors il existe* $u \in \mathrm{Frac}(\mathbf{A})$ *tel que l'idéal* $u\,\mathfrak{i}$ *est entier et étranger à* $\mathfrak{j}$.

Dans la preuve, nous considérons le monoïde multiplicatif des idéaux fractionnaires de l'anneau $\mathbf{A}$, formé par les sous-$\mathbf{A}$-modules de type fini de l'anneau total des fractions $\mathrm{Frac}(\mathbf{A})$. Il est clair qu'un idéal de type fini de $\mathbf{A}$ est inversible dans ce monoïde si et seulement s'il est inversible au sens de la définition 2.20.

Lemme 4.3 *Soit* $\mathbf{A}$ *un anneau quasi intègre (par exemple un anneau de Prüfer cohérent) de dimension inférieure ou égale à* 1. *Soit* $\mathfrak{i}$ *un idéal inversible de* $\mathbf{A}$ *et* $\mathfrak{j}$ *un idéal contenant un élément régulier. Alors il existe un élément* u *inversible dans* $\mathrm{Frac}(\mathbf{A})$ *tel que l'idéal* $u\,\mathfrak{i}$ *est entier (contenu dans* $\mathbf{A}$*) et étranger à* $\mathfrak{j}$.

Preuve : On cherche a et b réguliers tels que $\frac{b}{a}\,\mathfrak{i} \subseteq \mathbf{A}$, c'est-à-dire encore $b\,\mathfrak{i} \subseteq a\mathbf{A}$, et $\mathbf{A} = \frac{b}{a}\,\mathfrak{i} + \mathfrak{j}$. Si c est un élément régulier de $\mathfrak{j}$, comme la condition devrait être aussi réalisée lorsque $\mathfrak{j}$ est l'idéal $c\mathbf{A}$, on doit trouver a et b réguliers tels que $b\,\mathfrak{i} \subseteq a\mathbf{A}$ et $\mathbf{A} = \frac{b}{a}\,\mathfrak{i} + c\mathbf{A}$. Si on s'arrange pour que $a \in \mathfrak{i}$, on a $b \in a\,\mathfrak{i}$ et il suffit donc de réaliser les conditions $b\,\mathfrak{i} \subseteq a\mathbf{A}$ et $\mathbf{A} = \langle b, c\rangle$. C'est ce que nous allons faire.
Soit e régulier $\in \mathfrak{j}$, f régulier $\in \mathfrak{i}$. Posons $c = ef \in \mathfrak{i} \cap \mathfrak{j}$. D'après le théorème un et demi, il existe $a \in \mathfrak{i}$ tel que $\mathfrak{i} = \langle a, c^2\rangle = \langle a, c\rangle$. Puisque $\mathbf{A}$ est quasi intègre, en raisonnant comme au théorème 4.1 on peut supposer a régulier.
Puisque $c \in \mathfrak{i}$ on a une égalité $c = \alpha a + \beta c^2$ ce qui donne $c(1 - \beta c) = \alpha a$. Posons $b = 1 - \beta c$ de sorte que $\mathbf{A} = \langle b, c\rangle$. On obtient $b\,\mathfrak{i} = b\,\langle a, c\rangle = \langle ba, bc\rangle = a\,\langle b, \alpha\rangle \subseteq a\mathbf{A}$.
Si b est régulier on a donc gagné.
Si b n'est pas régulier ou plus généralement lorsqu'on ignore si b est régulier on considère l'idempotent r annulateur de b et $s = 1 - r$. Alors les conditions voulues sont réalisées pour a et $b' = b + ra = sb + ra$: b' est régulier, $sb' = b$ donc $\mathbf{A} = \langle b', c\rangle$ et $b'\,\mathfrak{i} = (b + ra)\,\mathfrak{i} \subseteq b\,\mathfrak{i} + ra\,\mathfrak{i} \subseteq a\mathbf{A}$. □

Le résultat suivant est classique (théorème de Steinitz) pour les anneaux de Dedekind. Il a été généralisé pour les domaines de Prüfer possédant la propriété un et demi par Kaplansky [16] et Heitman&Levy [14]. Ici aussi l'inspection de la preuve montrerait que l'hypothèse « de dimension inférieure ou égale à 1 » pourrait être affaiblie en « possédant la propriété un et demi ».

Théorème 4.4 *Soit* $\mathbf{A}$ *un anneau de Prüfer cohérent de dimension inférieure ou égale à* 1. *Tout module projectif* M *de rang constant* $k \geq 1$ *est isomorphe à* $\mathbf{A}^{k-1} \oplus \mathfrak{i}$, *où* $\mathfrak{i}$ *est un idéal inversible. En particulier, il est engendré par* $k+1$ *éléments. Enfin puisque* $\mathfrak{i} \simeq \wedge^k M$ *la classe d'isomorphisme de* M *comme* $\mathbf{A}$*-module détermine celle de* $\mathfrak{i}$.

Preuve : D'après le théorème 3.23, M est une somme directe de k idéaux inversibles. Il suffit donc de traiter le cas $M \simeq \mathfrak{i} \oplus \mathfrak{j}$, avec des idéaux inversibles $\mathfrak{i}$ et $\mathfrak{j}$.

Par le lemme 4.3, on peut trouver un idéal $\mathfrak{i}_1$ tel que $\mathfrak{i}_1 \simeq \mathfrak{i}$ (comme $\mathbf{A}$-modules) et $\mathfrak{i}_1 + \mathfrak{j} = \langle 1 \rangle$ (comme idéaux). On a alors la suite exacte courte

$$\langle 0 \rangle \longrightarrow \mathfrak{i}_1\mathfrak{j} = \mathfrak{i}_1 \cap \mathfrak{j} \xrightarrow{\delta} \mathfrak{i}_1 \oplus \mathfrak{j} \xrightarrow{\sigma} \mathfrak{i}_1 + \mathfrak{j} = \mathbf{A} \longrightarrow \langle 0 \rangle$$

où $\delta(x) = (x, -x)$ et $\sigma(x, y) = x + y$. Cette suite est scindée (cf. la proposition 2.12) donc $M \simeq \mathfrak{i} \oplus \mathfrak{j} \simeq \mathfrak{i}_1 \oplus \mathfrak{j} \simeq \mathbf{A} \oplus (\mathfrak{i}_1 \cap \mathfrak{j}) = \mathbf{A} \oplus (\mathfrak{i}_1\mathfrak{j})$. □

On en déduit immédiatement :

Corollaire 4.5 *Soit* $\mathbf{A}$ *un anneau de Prüfer cohérent de dimension inférieure ou égale à* 1. *Tout module projectif* M *est isomorphe à une somme directe* $r_1\mathbf{A} \oplus r_2\mathbf{A}^2 \oplus \cdots \oplus r_n\mathbf{A}^n \oplus \mathfrak{i}$, *où les* r_i *sont des idempotents orthogonaux (certains peuvent être nuls) et* $\mathfrak{i}$ *est un idéal de type fini.*

Théorème 4.6 *Soit* $\mathbf{A}$ *un anneau de Prüfer cohérent de dimension inférieure ou égale à* 1 *et* $x_1, \ldots, x_n \in \mathbf{A}$. *Il existe une matrice inversible* M *qui transforme* $(x_1, \ldots, x_n)$ *en* $(y_1, y_2, 0, \ldots, 0)$.

Preuve : Il suffit de traiter le cas où $n = 3$. Si e est un idempotent, alors $\mathbf{GL}_n(\mathbf{A}) \simeq \mathbf{GL}_n(\mathbf{A}_e) \oplus \mathbf{GL}_n(\mathbf{A}_{1-e})$. Quitte à localiser par l'annulateur de $\langle x_1, x_2, x_3 \rangle$ et par son complémentaire, on peut supposer que $\operatorname{Ann}\langle x_1, x_2, x_3 \rangle = \langle 0 \rangle$.
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 4.4, on 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 2.34, ce vecteur est la première ligne d'une matrice inversible M, et la première coordonnée de XM est nulle. □

Le théorème précédent donne une forme réduite des matrices lignes. Il semblerait utile de le généraliser de façon à obtenir des formes réduites de matrices arbitraires.

4.3 Factorisations partielles

Définition 4.7 *Soit* $F = \{\mathfrak{i}_1, \ldots, \mathfrak{i}_n\}$ *une famille d'idéaux inversibles dans un anneau* $\mathbf{A}$. *On dit que* F *admet une* factorisation partielle *s'il existe une famille* $P = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\}$ *d'idéaux inversibles deux à deux étrangers telle que tout idéal* $\mathfrak{i}_j$ *de* F *peut s'écrire sous la forme :* $\mathfrak{i}_j = \mathfrak{p}_1^{m_{1j}} \cdots \mathfrak{p}_k^{m_{kj}}$ *(certains des* m_{ij} *peuvent être nuls). On dit alors que* $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\}$ *est une base de factorisation partielle pour la famille* F.

Définition 4.8 *Un anneau est appelé* anneau de Prüfer à factorisation partielle *si c'est un anneau de Prüfer cohérent fortement discret*[6] *et si toute famille finie d'idéaux inversibles admet une factorisation partielle.*

[6] D'après la proposition 3.9 un anneau arithmétique est fortement discret si et seulement si la relation de divisibilité est explicite.

Lemme 4.9 *Soit* $\mathbf{A}$ *est un anneau de Prüfer à factorisation partielle local. On note* $\mathfrak{m} = \mathrm{Rad}(\mathbf{A})$. *Si* $a, b \in \mathfrak{m}$ *non nuls, alors il existe* $p \in \mathfrak{m}$, *deux entiers strictement positifs* m *et* n *et deux éléments inversibles* u *et* v *tels que* $a = up^m$ *et* $b = vp^n$. *En conséquence, un anneau de valuation à divisibilité explicite avec un élément non nul dans* $\mathrm{Rad}(\mathbf{A})$ *est à factorisation partielle si et seulement si son groupe de valuation est isomorphe à un sous-groupe de* $\mathbb{Q}$.

Preuve : Voyons l'implication directe. Comme les idéaux de type fini sont principaux et totalement ordonnés pour l'inclusion, une base de factorisation partielle pour $(\langle a\rangle, \langle b\rangle)$ ne peut contenir qu'un seul élément, du type $\langle p\rangle$ d'où la décomposition de a et b. 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 a supposé qu'il en existait au moins un) dont on donne l'image dans $\mathbb{Q}$ en posant $v(a) = 1$, de manière purement conventionnelle. La réciproque est immédiate car $\mathbb{Z}$ est principal. □

Remarque : Un anneau de Prüfer à factorisation partielle n'est donc pas nécessairement noethérien, bien que la réciproque soit vraie (voir le théorème 5.2).

Théorème 4.10 *Un anneau de Prüfer à factorisation partielle est de dimension inférieure ou égale à* 1.

Preuve : – Pour tous $m, n \in \mathbb{N}$, et pour $t \in \mathbb{N}$ assez grand on a :

$$\begin{array}{rll} & mt + nt \geq m(t+1) + nt & (\text{si } m = 0) \\ \text{ou} & mt + nt \geq n(t+1) & (\text{si } m > 0) \end{array}$$

– Considérons $x, y \in \mathbf{A}$ deux éléments réguliers. Ces deux éléments engendrent deux idéaux inversibles, qui se factorisent dans une base de factorisation partielle $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\}$: $\quad x\mathbf{A} = \prod_i \mathfrak{p}_i^{m_i} \qquad y\mathbf{A} = \prod_i \mathfrak{p}_i^{n_i} \qquad n_i, m_i \in \mathbb{N},\ \forall\ i$
On cherche un t tel que $x^t y^t \in x^{t+1} y^t \mathbf{A} + y^{t+1}\mathbf{A}$. Par la proposition 2.18 cela revient à demander : $\prod_i \mathfrak{p}_i^{m_i t + n_i t} \subset \prod_i \mathfrak{p}_i^{m_i(t+1)+n_i t} + \prod_i \mathfrak{p}_i^{n_i(t+1)} = \prod_i \mathfrak{p}_i^{\min(m_i(t+1)+n_i t,\ n_i(t+1))}$, c'est-à-dire encore pour tout i : $m_i t + n_i t \geq \min(m_i(t+1) + n_i t,\ n_i(t+1))$. Par le point précédent ceci est vérifié pour $t \in \mathbb{N}$ assez grand.

– Soit $x, y \in \mathbf{A}$ deux éléments quelconques et e_x, e_y deux idempotents engendrant leurs annulateurs respectifs. Dans les quatre localisés $\mathbf{A}_{e_x e_y}$, $\mathbf{A}_{e_x(1-e_y)}$, $\mathbf{A}_{(1-e_x)e_y}$, $\mathbf{A}_{(1-e_x)(1-e_y)}$, les éléments x, y sont réguliers ou nuls. La suite (x, y) est alors pseudo-singulière dans chacune des 4 composantes de l'anneau, et donc dans l'anneau lui-même. □

4.4 Factorisations moins poussées en dimension inférieure à 1

Théorème 4.11 *Dans un anneau de Prüfer cohérent de dimension inférieure ou égale à* 1, *on considère deux idéaux de type fini* $\mathfrak{i}$ *et* $\mathfrak{j}$ *avec* $\mathfrak{i}$ *inversible. Alors on peut écrire* $\mathfrak{i} = \mathfrak{i}_1\mathfrak{i}_2$ *avec* $\mathfrak{i}_1 + \mathfrak{j} = \langle 1\rangle$ *et* $\mathfrak{j}^n \subset \mathfrak{i}_2$ *pour un entier* n *convenable. Cette écriture est unique et on a* $\mathfrak{i}_1 + \mathfrak{i}_2 = \langle 1\rangle$, $\mathfrak{i}_2 = \mathfrak{i} + \mathfrak{j}^n = \mathfrak{i} + \mathfrak{j}^{n+1}$.

Preuve :

– Unicité du couple $(\mathfrak{i}_1, \mathfrak{i}_2)$: soit deux couples $(\mathfrak{i}_1, \mathfrak{i}_2)$ et $(\mathfrak{i}'_1, \mathfrak{i}'_2)$ satisfaisant $\mathfrak{i} = \mathfrak{i}_1\mathfrak{i}_2 = \mathfrak{i}'_1\mathfrak{i}'_2$ avec $\mathfrak{i}_1 + \mathfrak{j} = \mathfrak{i}'_1 + \mathfrak{j} = \langle 1\rangle$ et $\mathfrak{j}^n \subset \mathfrak{i}_2$, $\mathfrak{j}^m \subset \mathfrak{i}'_2$. On peut imposer $m = n$. Vérifions alors que $\mathfrak{i}_2 = \mathfrak{j}^n + \mathfrak{i} = \mathfrak{i}'_2$:

$$\mathfrak{i}_1 + \mathfrak{j} = \langle 1\rangle \;\Rightarrow\; \mathfrak{i}_1 + \mathfrak{j}^n = \langle 1\rangle \;\Rightarrow\; \mathfrak{i}_1 + \mathfrak{i}_2 = \langle 1\rangle$$
$$\text{donc} \quad \mathfrak{i}_2 = \mathfrak{i}_2 \cap (\mathfrak{i}_1 + \mathfrak{j}^n) = \mathfrak{i}_2 \cap \mathfrak{i}_1 + \mathfrak{i}_2 \cap \mathfrak{j}^n = \mathfrak{i}_2\mathfrak{i}_1 + \mathfrak{j}^n = \mathfrak{i} + \mathfrak{j}^n$$

Maintenant, nécessairement $\mathfrak{i}_1 = \mathfrak{i}'_1 = \mathfrak{i} \div (\mathfrak{j}^n + \mathfrak{i})$.
– Existence du couple $(\mathfrak{i}_1, \mathfrak{i}_2)$: cherchons $\mathfrak{i}_2$ sous la forme $\mathfrak{i}+\mathfrak{j}^n$. Alors on aura $\mathfrak{i}_1 = \mathfrak{i}\div\mathfrak{i}_2$ et

$$(\mathfrak{i}_1 + \mathfrak{j})(\mathfrak{i} + \mathfrak{j}^n) = (\mathfrak{i}_1 + \mathfrak{j})\mathfrak{i}_2 = \mathfrak{i}_1\mathfrak{i}_2 + \mathfrak{j}\ \mathfrak{i}_2 = \mathfrak{i} + \mathfrak{j}\ (\mathfrak{i} + \mathfrak{j}^n) = \mathfrak{i} + \mathfrak{j}^{n+1}$$

Donc $\mathfrak{i}_1 + \mathfrak{j} = \langle 1\rangle \;\Leftrightarrow\; \mathfrak{i} + \mathfrak{j}^n = \mathfrak{i} + \mathfrak{j}^{n+1}$. Ainsi, il suffit de trouver $n \in \mathbb{N}$ tel que $\mathfrak{i} + \mathfrak{j}^n = \mathfrak{i} + \mathfrak{j}^{n+1}$. Pour cela, il suffit de raisonner dans le quotient $\mathbf{A}/\mathfrak{i}$ de dimension inférieure ou égale à zéro : voir le lemme 1.20. □

Remarque : On n'a pas eu besoin de supposer les idéaux détachables.

Théorème 4.12 *Soit dans un anneau de Prüfer cohérent de dimension inférieure ou égale à* 1*, des idéaux de type fini deux à deux étrangers* $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ *et un idéal inversible* $\mathfrak{i}$*. Alors on peut écrire* $\mathfrak{i} = \mathfrak{i}_0 \cdot \mathfrak{i}_1 \cdots \mathfrak{i}_n$ *avec les idéaux de type fini* $\mathfrak{i}_0, \ldots, \mathfrak{i}_n$ *deux à deux étrangers et, pour* $j \geq 1$*,* $\mathfrak{p}_j^{m_j} \subset \mathfrak{i}_j$ *avec* m_j *entier convenable. Cette écriture est unique et on a* $\mathfrak{i}_j = \mathfrak{i} + \mathfrak{p}_j^{m_j} = \mathfrak{i} + \mathfrak{p}_j^{1+m_j}$.

Preuve : Par récurrence en utilisant le théorème 4.11 avec $\mathfrak{j} \in \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$. □

5 Anneaux de Dedekind

Une définition constructive de la noetheriannité est « toute suite croissante d'idéaux de type fini contient deux termes consécutifs égaux », d'autres définitions un peu plus fortes sont parfois utiles (cf. [23, 25]).

Définition 5.1 *On appelle* anneau de Dedekind *un anneau de Prüfer cohérent noethérien et fortement discret (intègre ou non).*

En mathématiques classiques, tout anneau est fortement discret et tout anneau noethérien est cohérent, ce qui raccourcit la définition.

Du point de vue algorithmique un quotient de $\mathbb{Z}$ par un idéal arbitraire $\mathfrak{i}$ est toujours noethérien mais il n'est pas nécessairement cohérent : il n'y a pas d'algorithme qui calcule un système générateur fini pour l'annulateur d'un élément dans $\mathbb{Z}/\mathfrak{i}$ si on ne dispose pas d'informations suffisantes sur $\mathfrak{i}$.

5.1 Les anneaux de Dedekind sont à factorisation partielle

Le corollaire 3.25 donne en mathématiques classiques qu'un anneau de Dedekind est de dimension inférieure ou égale à 1. Nous obtiendrons constructivement le résultat en montrant qu'un anneau de Dedekind est à factorisation partielle.

Théorème 5.2 *Soit* **A** *un anneau de Dedekind. Alors toute famille* $\mathfrak{F}$ *finie d'idéaux inversibles de* **A** *admet une factorisation partielle. Autrement dit, tout anneau de Dedekind est un anneau de Prüfer à factorisation partielle.*

Preuve : Le monoïde des idéaux inversibles de **A** est un monoïde à pgcd au sens de [23]. Le théorème résulte donc du théorème de factorisation partielle pour les monoïdes à pgcd dans lesquels toute suite décroissante pour la divisibilité admet deux termes consécutifs égaux ([23] chapitre 4, théorème 1.8 page 111). □

5.2 Anneaux de Dedekind à factorisation complète

Un anneau de Prüfer cohérent fortement discret dans lequel tout idéal inversible se décompose en produit d'idéaux maximaux inversibles est noethérien, et il est aussi à factorisation partielle. Nous l'appelerons *anneau de Dedekind à factorisation complète*. Dans le cas intègre ce sont les anneaux de Dedekind étudiés dans [23]. En mathématiques classiques, tout anneau de Dedekind est à factorisation complète.

L'anneau $\mathbb{Z}[x]$ dans la proposition 2.28 est un anneau de Dedekind est à factorisation complète. Le lemme suivant est facile (voir par exemple [27]).

Lemme 5.3 *Un anneau de Dedekind est à factorisation complète si et seulement s'il vérifie la propriété suivante : on a un test qui décide si un idéal de type fini* $\mathfrak{i}$ *est maximal ou non, et en cas de réponse négative, fournit un* x *tel que* $x \notin \mathfrak{i}$, $1 \notin \mathfrak{i}+\langle x\rangle$.

6 Anneaux normaux, extensions entières

6.1 Idéaux intégralement clos et anneaux normaux

Définition 6.1 *Soit* $\mathfrak{i}$ *un idéal d'un anneau* **A** *contenu dans un anneau* **B**.

1. *Un élément* $x \in \mathbf{B}$ *est dit* entier sur $\mathfrak{i}$ *s'il vérifie une relation de dépendance intégrale* $x^{n+1} = a_1x^n + a_2x^{n-1} + \cdots + a_nx + a_{n+1}$ *avec* $\forall h,\ a_h \in \mathfrak{i}^h$;
2. *L'anneau* **B** *est dit* entier sur **A** *si tout* $x \in \mathbf{B}$ *est entier sur* **A** ;
3. *L'idéal* $\mathfrak{i}$ *est dit* intégralement clos (dans **A**) *si tout* $x \in \mathbf{A}$ *entier sur* $\mathfrak{i}$ *est dans* $\mathfrak{i}$;
4. *L'anneau* **A** *est dit* intégralement clos dans **B** *si tout* $x \in \mathbf{B}$ *entier sur* **A** *est dans* **A** ;
5. *L'anneau* **A** *est dit* normal *lorsque tout idéal principal est intégralement clos (voir la proposition 6.4).*

Fait 6.2

1. *Un anneau est normal si et seulement s'il a la même propriété après localisation en des monoïdes comaximaux ;*
2. *Un anneau normal est intégralement clos dans son anneau total des fractions ;*
3. *Un élément* $x \in \mathbf{A}$ *est entier sur l'idéal* $\mathfrak{i} \subseteq \mathbf{A}$ *si et seulement si* $\mathfrak{i}\,(\mathfrak{i}+\langle x\rangle)^n = (\mathfrak{i}+\langle x\rangle)^{n+1}$;

4. *Un idéal* $\mathfrak{i}$ *est intégralement clos (dans* $\mathbf{A}$*) si et seulement s'il vérifie la propriété de simplification* $\quad \forall x \in \mathbf{A},\ \mathfrak{i}\,(\mathfrak{i}+\langle x\rangle)^n = (\mathfrak{i}+\langle x\rangle)^{n+1} \Longrightarrow \mathfrak{i} = \mathfrak{i}+\langle x\rangle$

Proposition 6.3 *Un anneau normal est réduit et localement sans diviseur de zéro.*

Preuve : L'idéal $\langle 0\rangle$ est intégralement clos veut dire que l'anneau est réduit. Mais en fait, si $xy = 0$, alors $x^2 = xz$ avec $z = x + y$, donc x entier sur $\langle z\rangle$, donc $x \in \langle z\rangle$, i.e. $x = a(x + y)$. En multipliant par y, on voit que $ay^2 = 0$, donc $ay = 0$ (anneau réduit). Ainsi on a bien $ay = (1 - a)x = 0$: l'anneau est localement sans diviseur de zéro. □

Nous faisons maintenant le lien avec la définition classique usuelle d'anneau normal. Il est facile de voir qu'un anneau intègre est normal si et seulement s'il est intégralement clos dans son corps de fractions. On parle alors d'anneau (intègre et) intégralement clos.

Proposition 6.4 *Un anneau commutatif* $\mathbf{A}$ *est normal si et seulement si le localisé de* $\mathbf{A}$ *en n'importe quel idéal maximal est (intègre et) intégralement clos.*

Preuve : Considérons un anneau $\mathbf{A}$ dont chaque localisé $\mathbf{A}_\mathfrak{p}$ en un idéal maximal $\mathfrak{p}$ est (intègre et) intégralement clos (dans son corps de fractions). Si $a \in \mathbf{A}_\mathfrak{p}$ est entier sur $b\mathbf{A}_\mathfrak{p}$ alors $a \in b\mathbf{A}_\mathfrak{p}$. Ceci ayant lieu pour tous les idéaux maximaux, par le principe local-global, $a \in b\mathbf{A}$, donc $b\mathbf{A}$ est intégralement clos.
Réciproquement, si $\mathbf{A}$ est normal au sens de la définition 6.1, alors $\mathbf{A}$ est localement sans diviseur de zéro, donc tout localisé $\mathbf{A}_\mathfrak{p}$ en un idéal maximal $\mathfrak{p}$ est intègre. De plus, l'anneau $\mathbf{A}_\mathfrak{p}$ est normal (car localisé d'un anneau normal) donc intégralement clos. □

Lemme 6.5 *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 $\mathfrak{i}$. Puisque l'anneau $\mathbf{A}$ est arithmétique, il existe un idéal de type fini $\mathfrak{j}$ tel que $(\mathfrak{i}+\langle x\rangle)\,\mathfrak{j} = \langle x\rangle$. De plus, pour un $n \geq 0$, on a $\mathfrak{i}\,(\mathfrak{i}+\langle x\rangle)^n = (\mathfrak{i}+\langle x\rangle)^{n+1}$ car x est entier sur $\mathfrak{i}$. En multipliant cet égalité par $\mathfrak{j}^n$, on obtient $x^n\mathfrak{i} = x^n(\mathfrak{i}+\langle x\rangle)$, ce qui signifie qu'il existe $y \in \mathfrak{i}$ tel que $x^{n+1} = x^n y$ c'est-à-dire $x^n(y - x) = 0$. Puisque l'anneau $\mathbf{A}$ est localement sans diviseur de zéro, il existe s tel que $sx = 0$ et $(1-s)(y-x) = 0$, et donc $x = (1-s)y \in \mathfrak{i}$.
□

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

Lemme 6.6 *Soit* M *un* $\mathbf{A}$*-module de type fini dont l'annulateur est réduit à* 0*,* $\mathfrak{j}$ *un idéal de type fini et* $x \in \mathrm{Frac}(\mathbf{A})$ *vérifiant* $xM \subseteq \mathfrak{j}M$*. Alors* x *est entier sur* $\mathfrak{j}$*.*

Preuve : Si $M = a_1\mathbf{A}+\cdots+a_n\mathbf{A}$, la matrice $A \in \mathfrak{j}^{n\times n}$ est telle que $x^t(a_1,\ldots,a_n) = A^t(a_1,\ldots,a_n)$. Par suite $\det(x\mathrm{I}_n - A)$ annule ${}^t(a_1,\ldots,a_n)$ donc est nul. □

6.2 Transfert de la dimension 0

Théorème 6.7 *Soit* $\mathbf{A}$ *un anneau zéro-dimensionnel et* $\mathbf{B}$ *un sur-anneau entier sur* $\mathbf{A}$*. Alors* $\mathbf{B}$ *est zéro-dimensionnel.*

Preuve : Soit $x \in \mathbf{B}$: il existe $a_0, \ldots, a_n \in \mathbf{A}$ $(a_n = 1)$ tels que

$$a_n x^n + \cdots + a_1 x + a_0 = 0 \tag{6}$$

Comme $\mathbf{A}$ est zéro-dimensionnel, pour tout $i \leq n$, il existe $d_i \in \mathbb{N}^*$ et $s_i \in \mathbf{A}$ idempotent tels que $s_i\mathbf{A} = a_i^{d_i}\mathbf{A}$ (cf. lemme 1.20). Soit $r_i = 1 - s_i$ (engendrant l'annulateur de $a_i^{d_i}$) et $t_i = r_0 \cdots r_{i-1} s_i$ pour tout $i \leq n$. On note $t_{n+1} = r_0 \cdots r_n$; on a déjà vu que $(t_i)_{i=0..n+1}$ forme un sfio de $\mathbf{A}$, mais on constate que $t_{n+1} = 0$ car $1 = a_n = s_n = 1 - r_n$. Nous allons montrer que $t_i x^{e_i} \in x^{1+e_i}\mathbf{B}$ pour tout $0 \leq i \leq n$. Comme $\sum_{i=0}^{n} t_i = 1$, on obtiendra finalement $x^e \in x^{1+e}\mathbf{B}$ pour $e = \max(e_i)_i$, ce qui montrera que la dimension de $\mathbf{B}$ est inférieure à 0.
Fixons $0 \leq i \leq n$. L'égalité (6) montre que

$$a_n x^n + \cdots + a_i x^i = -(a_{i-1}x^{i-1} + \cdots + a_1 x + a_0)$$

Dans le localisé $\mathbf{B}_{t_i} \simeq \mathbf{B}/\langle 1 - t_i \rangle$, les éléments $a_0, \ldots, a_{i-1}$ sont nilpotents, donc $a_n x^n + \cdots + a_i x^i$ l'est aussi, disons d'indice k_i. De plus, a_i est inversible dans $\mathbf{B}_{t_i}$, disons d'inverse f_i. Ainsi, dans $\mathbf{B}_{t_i}$,

$$0 = \left(f_i(a_n x^n + \cdots + a_{i+1}x^{i+1}) + x^i\right)^{k_i} \in \left\langle x^{ik_i+1} \right\rangle + x^{ik_i}$$

Ceci traduit finalement que $t_i x^{ik_i}$ est multiple de $t_i x^{ik_i+1}$ dans $\mathbf{B}$. □

6.3 Transfert de la dimension pour le cas des anneaux de Prüfer

Nous ne donnons pas ici la preuve constructive, trop longue, que la dimension de Krull se conserve par extensions entières (voir à ce sujet [7]).

Nous donnons une preuve simple pour le cas particulier suivant, celui qui nous intéresse dans cet article. Le théorème s'étendrait facilement au cas des anneaux arithmétiques.

Théorème 6.8 *Soit* $\mathbf{A}$ *un anneau de Prüfer de dimension inférieure ou égale à* d *et* $\mathbf{B}$ *un localisé d'un anneau entier sur* $\mathbf{A}$*. Alors* $\mathbf{B}$ *est de dimension inférieure ou égale à* d*.*

Preuve : On procéde par récurrence sur d, le cas $d = -1$ étant clair. On suppose le résultat vrai pour la dimension $d-1$ et on suppose $\mathbf{A}$ de dimension inférieure ou égale à d.

Nous faisons d'abord la preuve dans le cas où l'anneau $\mathbf{A}$ est local résiduellement discret. Puisque la dimension ne peut que diminuer par localisation, on peut supposer $\mathbf{B}$ entier sur $\mathbf{A}$. Soit $x \in \mathbf{B}$, $S_x^{\mathbf{B}} = x^{\mathbb{N}}(1 + x\mathbf{B})$ et $\mathbf{B}^{\{x\}} = (S_x^{\mathbf{B}})^{-1}\mathbf{B}$. D'après le lemme 1.18 il suffit de montrer que $\mathbf{B}^{\{x\}}$ est de dimension inférieure ou égale à $d-1$. Soit $\widetilde{S_x^{\mathbf{B}}}$ le saturé de $S_x^{\mathbf{B}}$ (qui donne le même localisé), $S = \widetilde{S_x^{\mathbf{B}}} \cap \mathbf{A}$ et $\mathbf{A}' = S^{-1}\mathbf{A}$. L'anneau $\mathbf{B}^{\{x\}}$ est un localisé de $\varphi(\mathbf{B})$, où φ est l'homomorphisme canonique de $\mathbf{B}$ dans $\mathbf{B}^{\{x\}}$, et $\varphi(\mathbf{B})$ est entier sur $\varphi(\mathbf{A})$ donc a fortiori sur $\psi(\mathbf{A}')$, où $\psi : \mathbf{A}' \to \mathbf{B}^{\{x\}}$

est aussi un homomorphisme canonique. Et $\psi(\mathbf{A}')$ est un quotient de $\mathbf{A}'$. Il suffit donc de montrer que $\mathbf{A}'$ est de dimension inférieure ou égale à $d-1$.
Considérons une équation de dépendance intégrale pour x :

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0 \qquad (*)$$

Posons $a_n = 1$. Si a_0 est une unité, x est inversible dans $\mathbf{B}$ et $\mathbf{B}^{\{x\}}$ est l'anneau trivial ($\mathbf{A}'$ aussi d'ailleurs). Sinon soit k le plus petit indice tel que a_k soit une unité. L'égalité $(*)$ s'écrit

$$a_k\, x^k \left(1 + \frac{a_{k+1}}{a_k}x + \cdots + \frac{1}{a_k}x^{n-k}\right) = -\left(a_{k-1}x^{k-1} + \cdots + a_0\right) \qquad (**)$$

Le premier membre est clairement dans $\widetilde{S_x^{\mathbf{B}}}$. Puisque $\mathbf{A}$ est un anneau de valuation soit alors $j \in \{0, \ldots, k-1\}$ tel que a_j divise $a_0, \ldots, a_{k-1}$. Il est clair que $a = a_j$ est dans $S = \widetilde{S_x^{\mathbf{B}}} \cap \mathbf{A}$ et puisque $a \in \mathrm{Rad}(\mathbf{A})$, $1 + a\mathbf{A}$ est formé d'unités, donc $S_a^{\mathbf{A}} \subset S$. Par suite $\mathbf{A}'$ est un localisé de $\mathbf{A}^{\{a\}}$, et donc de dimension inférieure ou égale à $d-1$.

La preuve dans le cas général consiste à transformer la preuve donnée dans le cas local en utilisant le principe local-global donné au lemme 1.19.
En vertu du lemme 1.3 on considère les monoïdes comaximaux $S_0 = \mathcal{S}(0; a_0)$, $S_1 = \mathcal{S}(a_0; a_1)$, $S_2 = \mathcal{S}(a_0, a_1; a_2)$, $\ldots$, $S_{n-1} = \mathcal{S}(a_0, \ldots, a_{n-2}; a_{n-1})$ et $S_n = \mathcal{S}(a_0, \ldots, a_{n-1}; 1)$.
D'autre part, puisque $\mathbf{A}$ est un anneau de Prüfer, il existe pour chaque k des éléments $c_{k,0}, \ldots, c_{k,k-1}$ de somme 1 tels que a_j divise $c_{k,j}a_0, \ldots, c_{k,j}a_{k-1}$ dans $\mathbf{A}$.
La preuve donnée dans le cas local nous montre que la considération des monoïdes $S_{k,j} = \mathcal{S}(a_0, \ldots, a_{k-1}; a_k, c_{k,j})$ permet d'appliquer le lemme 1.19. □

6.4 Anneaux normaux de dimension inférieure ou égale à 1

Propriété 6.9 *Si $\mathbf{A}$ est un anneau de dimension inférieure ou égale à 1, pour des éléments réguliers $a_1, \ldots, a_n \in \mathbf{A}$, on note $\widetilde{a_i}$ le produit $\prod_{j\neq i} a_j$.*
Si $\widetilde{a_1}\mathbf{A} \cap \cdots \cap \widetilde{a_n}\mathbf{A} = a_1 \ldots a_n\mathbf{A}$ alors $a_1\mathbf{A} + \cdots + a_n\mathbf{A} = \mathbf{A}$.

Preuve : Nous démontrons le résultat pour $n = 2$. Le cas général, plus lourd, se traite à l'identique.

Posons $\mathfrak{i} = a_1\mathbf{A} + a_2\mathbf{A}$ et montrons que $\mathfrak{i} = \mathbf{A}$. Soit $S = 1 + \mathfrak{i}$. Il suffit de montrer que le localisé $\mathbf{B} = S^{-1}\mathbf{A}$ est trivial, c'est-à-dire encore que $\mathfrak{J} = \mathfrak{i}\,\mathbf{B} = \mathbf{B}$. Notez que $\mathfrak{J} = a_1\mathbf{B} + a_2\mathbf{B}$ est inclus dans le radical de Jacobson de $\mathbf{B}$, qui reste de dimension inférieure ou égale à 1.

En particulier si z est régulier dans $\mathbf{B}$, il existe d_i et b_i tels que $a_i^{d_i}(1 + a_i b_i) \in z\mathbf{B}$, ce qui implique $a_i^{d_i} \in z\mathbf{B}$. Donc il existe un entier d tel que $\mathfrak{J}^d \subset z\mathbf{B}$. Prenons $z = a_1a_2$. Si $d \geq 1$, on a $\mathfrak{J}^{d-1}(a_1\mathbf{B} + a_2\mathbf{B}) \subset a_1a_2\mathbf{B}$. En particulier $a_1\,\mathfrak{J}^{d-1} \subset a_1a_2\mathbf{B}$, et puisque a_1 est régulier, $\mathfrak{J}^{d-1} \subset \widetilde{a_1}\mathbf{B}$. De même $\mathfrak{J}^{d-1} \subset \widetilde{a_2}\mathbf{B}$, donc $\mathfrak{J}^{d-1} \subset \widetilde{a_1}\mathbf{B} \cap \widetilde{a_2}\mathbf{B} = a_1a_2\mathbf{B}$. Par induction sur d, on obtient $\mathbf{B} = \mathfrak{J}^0 \subset a_1a_2\mathbf{B}$ donc a_1a_2 inversible et $\mathfrak{J} = \mathbf{B}$. □

Théorème 6.10 *Soit $\mathbf{A}$ un anneau normal de dimension inférieure ou égale à 1. Pour des éléments réguliers $a_1, \ldots, a_n \in \mathbf{A}$, on note $\widetilde{a_i}$ le produit $\prod_{j\neq i} a_j$.*
Si l'idéal $\widetilde{a_1}\mathbf{A} \cap \cdots \cap \widetilde{a_n}\mathbf{A}$ est de type fini, alors $a_1 \ldots a_n\mathbf{A} = (a_1\mathbf{A} + \cdots + a_n\mathbf{A})(\widetilde{a_1}\mathbf{A} \cap \cdots \cap \widetilde{a_n}\mathbf{A})$. En particulier, l'idéal $a_1\mathbf{A} + \cdots + a_n\mathbf{A}$ est inversible.

Preuve (calquée sur celle de la propriété 6.9) : Nous démontrons le résultat pour $n = 2$. Le cas général se traite à l'identique.

On a toujours $(a_1\mathbf{A} + a_2\mathbf{A})(\widetilde{a_1}\mathbf{A} \cap \widetilde{a_2}\mathbf{A}) \subset a_1a_2\mathbf{A}$, autrement dit il existe un idéal de type fini $\mathfrak{i}$ tel que $(a_1\mathbf{A} + a_2\mathbf{A})(\widetilde{a_1}\mathbf{A} \cap \widetilde{a_2}\mathbf{A}) = a_1a_2\,\mathfrak{i}$. On va démontrer que $\mathfrak{i} = \mathbf{A}$. Soit $S = 1 + \mathfrak{i}$. Il suffit de montrer que le localisé $\mathbf{B} = S^{-1}\mathbf{A}$ est trivial, c'est-à-dire encore que $\mathfrak{I} = \mathfrak{i}\mathbf{B} = \mathbf{B}$. Notez que $\mathfrak{I}$ est inclus dans le radical de Jacobson de $\mathbf{B}$, qui reste de dimension inférieure ou égale à 1 et normal, et qu'on a $(a_1\mathbf{B} + a_2\mathbf{B})(\widetilde{a_1}\mathbf{B} \cap \widetilde{a_2}\mathbf{B}) = a_1a_2\,\mathfrak{I}$.

Comme dans la preuve de la propriété 6.9, si $z \in \mathbf{B}$ est régulier, puisque $\mathfrak{I}$ est de type fini et dans le radical de Jacobson, il existe un entier d tel que $\mathfrak{I}^d \subset z\mathbf{B}$. Cela implique que $(a_1a_2)^d\,\mathfrak{I}^d \subset (a_1a_2)^d z\mathbf{B}$, donc $(a_1\mathbf{B} + a_2\mathbf{B})^d(\widetilde{a_1}\mathbf{B} \cap \widetilde{a_2}\mathbf{B})^d \subset (a_1a_2)^d z\mathbf{B}$.

Si $d \geq 1$, notons $\mathfrak{J} = (a_1\mathbf{B} + a_2\mathbf{B})^{d-1}(\widetilde{a_1}\mathbf{B} \cap \widetilde{a_2}\mathbf{B})^{d-1}$ et $z' = (a_1a_2)^{d-1}$. Montrons que $\mathfrak{J} \subset z'z\mathbf{B}$. On a $\mathfrak{J}\,(\widetilde{a_1}\mathbf{B} \cap \widetilde{a_2}\mathbf{B})(a_1\mathbf{B} + a_2\mathbf{B}) \subset (a_1a_2)z'z\mathbf{B}$. Comme dans la preuve de la propriété 6.9, on en déduit l'inclusion $\mathfrak{J}\,(\widetilde{a_1}\mathbf{B} \cap \widetilde{a_2}\mathbf{B}) \subset z'z\,(\widetilde{a_1}\mathbf{B} \cap \widetilde{a_2}\mathbf{B})$ (car a_1, a_2, z, z' sont réguliers). Le lemme 6.6 nous dit alors que tout élément de $\mathfrak{J}$ est entier sur $z'z\mathbf{B}$. Et puisque $\mathbf{B}$ est normal, $\mathfrak{J} \subset z'z\mathbf{B}$.

Une induction sur d donne alors $\mathbf{B} \subset z\mathbf{B}$. Autrement dit, tout élément z régulier est inversible. En particulier a_1 et a_2, donc $\mathfrak{I} = (a_1\mathbf{B} + a_2\mathbf{B})(\widetilde{a_1}\mathbf{B} \cap \widetilde{a_2}\mathbf{B}) = \mathbf{B}$. □

Théorème 6.11 *Un anneau* $\mathbf{A}$ *normal, cohérent, de dimension inférieure ou égale à* 1*, est un anneau de Prüfer. En particulier un anneau* $\mathbf{A}$ *normal, cohérent, noethérien, fortement discret et de dimension inférieure ou égale à* 1*, est un anneau de Dedekind.*

Preuve : Il suffit de montrer que $\mathbf{A}$ est arithmétique car un anneau normal est localement sans diviseur de zéro. L'annulateur d'un élément de $\mathbf{A}$ est un idéal idempotent (proposition 6.3 et propriété 1.7) et de type fini ($\mathbf{A}$ cohérent), donc engendré par un idempotent (lemme 3.15).

Soit $a, b \in \mathbf{A}$ et e, f les idempotents engendrant leurs annulateurs respectifs. On découpe : $\mathbf{A} = e\mathbf{A} \oplus (1-e)f\mathbf{A} \oplus (1-e)(1-f)\mathbf{A}$.

Dans $e\mathbf{A}$ et $(1-e)f\mathbf{A}$, l'idéal $\langle a, b\rangle$ est monogène ($a = 0 \in e\mathbf{A}$ ou $b = 0 \in (1-e)f\mathbf{A}$) donc on peut y déterminer une matrice de localisation principale pour (a, b).

Dans $(1-e)(1-f)\mathbf{A}$ (normal, cohérent, de dimension inférieure ou égale à 1), les éléments a, b sont réguliers donc l'idéal $\langle a, b\rangle$ est inversible (théorème 6.10). On peut déterminer dans cette dernière composante une matrice de localisation principale pour (a, b). □

6.5 Extensions entières d'anneaux de Prüfer

Le cas intègre

Il ne faut pas croire[7] qu'un anneau $\mathbf{B}$ intercalé entre un anneau intégralement clos $\mathbf{A}$ et son corps des fractions est obligatoirement intégralement clos. Voici un contre-exemple avec un anneau factoriel non principal : $\mathbf{A} = \mathbf{K}[x, y]$ un anneau de polynômes sur un corps et $\mathbf{B} = \mathbf{A}[z]$ où $z = x/y + y/x$. Alors $x/y \in \mathrm{Frac}(\mathbf{B}) = \mathbf{K}(x, y)$ est entier sur $\mathbf{B}$ (racine de $T^2 - zT + 1$), mais $x/y \notin \mathbf{B}$ pour des raisons d'homogénéité.

[7] Bien que le résultat soit vrai si $\mathbf{B}$ est un localisé de $\mathbf{A}$.

Le théorème 6.13 (où l'hypothèse de noethériannité est absente) est relié[8] aux deux théorèmes classiques suivants (cf. [11], page 17) :

Krull-Akizuki : Si $\mathbf{A}$ est un anneau de Dedekind et $\mathbf{L}$ une extension finie du corps des fractions de $\mathbf{A}$, alors la fermeture intégrale de $\mathbf{A}$ dans $\mathbf{L}$ est un anneau de Dedekind.

Grell-Noether : Si $\mathbf{A}$ est un anneau de Dedekind alors tout anneau compris entre $\mathbf{A}$ et son corps des fractions est de Dedekind.

Nous rappelons sans preuve le théorème suivant dû à Kronecker (cf. [9] chapitre 0, ou [5])

Théorème 6.12 (Kronecker) *Soit $\mathbf{B}$ un anneau commutatif, $f, g \in \mathbf{B}[X]$, $h = fg$, et $\mathbf{A}$ le sous-anneau de $\mathbf{B}$ engendré par les coefficients de h. Si f_i et g_j sont des coefficients respectifs de f et g, alors leur produit $f_i g_j$ est entier sur l'idéal engendré par les coefficients de h dans $\mathbf{A}$.*

Théorème 6.13 *Soit $\mathbf{A}$ un anneau de Prüfer intègre de corps des fractions $\mathbf{K}$, $\mathbf{L}$ une extension algébrique de $\mathbf{K}$, $\mathbf{A}'$ la fermeture intégrale de $\mathbf{A}$ dans $\mathbf{L}$ et enfin un anneau $\mathbf{B}$ vérifiant $\mathbf{A}' \subset \mathbf{B} \subset \mathbf{L}$. Alors tout idéal de type fini de $\mathbf{B}$ est nul ou inversible, i.e. $\mathbf{B}$ est un anneau de Prüfer intègre.*

Preuve : Il suffit de traiter le cas d'un idéal $\mathfrak{i}$ engendré par deux éléments non nuls a, b. On remarque que $\mathbf{L}$ possède un test d'égalité à zéro ([23] th. 1.9 p. 141)) donc $\mathbf{B}$ est intègre. Comme $a \neq 0$ est algébrique sur $\mathbf{A}$, on peut trouver $\overline{a} \in \mathbf{B}$ tel que $\overline{a}a \in \mathbf{A} \setminus \{0\}$. Ainsi, quitte à remplacer (a, b) par $(\overline{a}a, \overline{a}b)$, on restreint l'étude au cas où $(a, b) \in \mathbf{A} \times \mathbf{B}$.
Soit $P \in \mathbf{A}[X]$ non nul s'annulant en b. On écrit $P(X) = (X-b)Q(X)$ où $Q \in \mathbf{B}[X]$. On a donc $P(aX) = (aX - b)Q(aX)$. On note $\mathfrak{i}$ le contenu de $P(aX)$ (dans $\mathbf{A}$) et $\mathfrak{i}'$ le contenu de $Q(aX)$ (dans $\mathbf{B}$). On a clairement $\mathfrak{i}\,\mathbf{B} \subset \langle a, b\rangle\ \mathfrak{i}'$. Comme $\mathfrak{i} \subset \mathbf{A}$ est inversible ($\mathbf{A}$ arithmétique intègre et $\mathfrak{i} \neq \langle 0\rangle$), il existe un idéal fractionnaire $\mathfrak{j}$ tel que $\mathbf{A} = \mathfrak{i}\,\mathfrak{j}$, et donc $\mathbf{B} = \mathfrak{i}\,\mathfrak{j}\,\mathbf{B} \subset \langle a, b\rangle\,\mathfrak{i}'\,\mathfrak{j}\,\mathbf{B}$.
Soit $j \in \mathfrak{j}$. Comme $jP(aX) = (aX - b)Q(aX)j$, on sait (cf. le théorème 6.12) que $\langle a, b\rangle\ \mathfrak{i}'\ \langle j\rangle\ \mathfrak{i} \subset \mathbf{A}$. Comme $\mathbf{B}$ contient $\mathbf{A}'$, on a $\langle a, b\rangle\ \mathfrak{i}'\ \langle j\rangle \subset \mathbf{A}' \subset \mathbf{B}$ pour tout $j \in \mathfrak{j}$. Par conséquent, $\langle a, b\rangle\,\mathfrak{i}'\,\mathfrak{j}\,\mathbf{B} \subset \mathbf{B}$.
Conclusion : $\langle a, b\rangle\,\mathfrak{i}'\mathfrak{j}\,\mathbf{B} = \mathbf{B}$, ce qui prouve que $\langle a, b\rangle$ est inversible dans $\mathbf{B}$. □

Le cas général

Lemme 6.14 *Soit $\mathbf{A}$ un anneau de Prüfer, $\mathbf{B}$ un sur-anneau normal et entier sur $\mathbf{A}$. Alors pour tout couple $(a, b) \in \mathbf{A} \times \mathbf{B}$, on peut construire une matrice de localisation principale pour (a, b).*

Preuve : Soit $P \in \mathbf{A}[X]$ unitaire s'annulant en b. On écrit $P(X) = (X - b)Q(X)$ où $Q \in \mathbf{B}[X]$. On a donc $P(aX) = (aX - b)Q(aX)$. On note $\mathfrak{i}$ le contenu de $P(aX)$ (dans $\mathbf{A}$) et $\mathfrak{i}'$ le contenu de $Q(aX)$ (dans $\mathbf{B}$). On a clairement $\mathfrak{i}\,\mathbf{B} \subset \langle a, b\rangle\,\mathfrak{i}'$.

[8] En particulier le théorème de Krull-Akizuki est une conséquence directe de 6.13 en mathématiques classiques.

Pour tout $i \in \mathfrak{i}$ (plus tard, on prendra pour i le coefficient dominant de $P(aX)$, i.e. une puissance de a), il existe un idéal $\mathfrak{j} \subset \mathbf{A}$ tel que $i\mathbf{A} = \mathfrak{i}\,\mathfrak{j}$ car $\mathbf{A}$ est arithmétique. Soit $j \in \mathfrak{j}$. Comme $jP(aX) = (aX - b)Q(aX)j$, on sait (cf. le théorème 6.12) que $\langle a, b\rangle\, \mathfrak{i}' j$ est entier sur $j\mathfrak{i}\ \mathbf{B} \subset \mathfrak{j}\ \mathfrak{i}\ \mathbf{B} = i\mathbf{B}$. Comme $\mathbf{B}$ est normal, $i\mathbf{B}$ est intégralement clos, on a donc $\langle a, b\rangle\, \mathfrak{i}' j \subset i\mathbf{B}$ pour tout $j \in \mathfrak{j}$. Par conséquent, $\langle a, b\rangle\, \mathfrak{i}'\mathfrak{j}\ \mathbf{B} \subset i\mathbf{B} = \mathfrak{i}\ \mathfrak{j}\ \mathbf{B} \subset \langle a, b\rangle\, \mathfrak{i}'\mathfrak{j}\ \mathbf{B}$. Conclusion : pour tout $i \in \mathfrak{i}$, il existe $\mathfrak{j} \subset \mathbf{A}$ tel que $\langle a, b\rangle\, \mathfrak{i}'\mathfrak{j}\ \mathbf{B} = i\mathbf{B}$.
Ainsi, il existe $u, v \in \mathbf{B}$ tels que $ua + vb = i$ et il existe $M \in M_2(\mathbf{B})$ tel que ${}^t(u, v).(a, b) = i.M$. On a alors $iM.{}^t(-b, a) = 0$ et $i(\mathrm{tr}(M) - 1) = ua + vb - i = 0$. Comme $\mathbf{B}$ est localement sans diviseur de zéro (cf. la proposition 6.3), grâce au lemme 1.8, il existe $z \in \mathbf{B}$ tel que $(zM)^t(-b, a) = 0$, $z(\mathrm{tr}(M)-1) = 0$, et $(1-z)i = 0$. On a donc $(zM)^t(-b, a) = 0$ mais $\mathrm{tr}(zM) = z$ différente de 1 *a priori*.
En particulier, pour $i = a^n \in \mathfrak{i}$ (le coefficient dominant de $P(aX)$), on a $(1-z)a^n = 0$. Comme $\mathbf{B}$ est réduit, on a simplement $(1 - z)a = 0$. On obtient enfin une matrice de localisation principale pour le couple (a, b) : $zM + \begin{pmatrix} 0 & 0 \\ 0 & 1 - z \end{pmatrix}$. □

Théorème 6.15 *Soit* $\mathbf{A}$ *un anneau de Prüfer,* $\mathbf{B}$ *un sur-anneau normal et entier sur* $\mathbf{A}$*. Alors* $\mathbf{B}$ *est un anneau de Prüfer.*

Preuve : Comme $\mathbf{B}$ est réduit (cf. la proposition 6.3), il reste à démontrer que $\mathbf{B}$ est arithmétique, i.e. que l'on peut construire une matrice de localisation principale pour tout couple $(x, y) \in \mathbf{B}^2$.
Soit $P = \sum_{i=0}^{n} p_i X^i \in \mathbf{A}[X]$ unitaire s'annulant en x. On écrit $P(X) = (X-x)Q(X)$ où $Q = \sum_{i=0}^{n-1} q_i X^i \in \mathbf{B}[X]$. On a alors $p_i = q_{i-1} - xq_i$ pour tout $0 \leq i \leq n$ (par convention $q_{-1} = 0$ et $q_n = 0$). On pose $b_i = -yq_i$ pour $0 \leq i \leq n - 1$, et grâce au lemme 6.14, on sait calculer des matrices de localisation principale M_i des couples $(p_i, b_i) \in \mathbf{A} \times \mathbf{B}$:

$$\forall\ i \in \{0, \ldots, n-1\}, \quad \begin{cases} \mathrm{tr}(M_i) = 1 \\ M_i.{}^t(-b_i, p_i) = 0 \end{cases}$$

Or $(-b_i, p_i) \equiv q_i(y, -x) \mod q_{i-1}\mathbf{B}^2$, si bien que

$$\forall\ i \in \{0, \ldots, n-1\}, \qquad q_i M_i.{}^t(y, -x) \equiv 0 \mod q_{i-1}\mathbf{B}^2 \tag{7}$$

Montrons par récurrence qu'il existe $z_0, \ldots, z_{n-1} \in \mathbf{B}$ et $\widetilde{M_0}, \ldots, \widetilde{M_{n-1}} \in M_2(\mathbf{B})$ tels que

$$\forall\ i \in \{0, \ldots, n-1\}, \quad \begin{cases} \mathrm{tr}(\widetilde{M_i}) = 1 - z_0 \cdots z_i \\ \widetilde{M_i}.{}^t(y, -x) = 0 \\ z_i q_i = 0 \end{cases}$$

En effet, le résultat est vrai pour $i = 0$: on prend $\widetilde{M_0} = M_0$ et le lemme 1.8 donne z_0 à partir de l'équation (7) car $\mathbf{B}$ est localement sans diviseur de zéro (cf. la proposition 6.3). Pour passer du rang i au rang $i+1$, on multiplie $q_{i+1}M_{i+1}.{}^t(y, -x) \equiv 0 \mod q_i\mathbf{B}^2$ par z_i, ce qui donne

$$q_{i+1}z_i M_{i+1}.{}^t(y, -x) = 0 \quad \text{et } \textit{a fortiori} \quad q_{i+1}z_0 \cdots z_i M_{i+1}.{}^t(y, -x) = 0$$

dans $\mathbf{B}$, qui est localement sans diviseur de zéro, donc (lemme 1.8), il existe $z_{i+1} \in \mathbf{B}$ tel que

$$0 = (1 - z_{i+1})z_0 \cdots z_i M_{i+1}.{}^t(y, -x) \quad \text{et} \quad 0 = z_{i+1}q_{i+1}$$

En posant $\widetilde{M_{i+1}} = \widetilde{M_i} + (1 - z_{i+1})z_0 \cdots z_i M_{i+1}$, on vérifie facilement que $\mathrm{tr}(\widetilde{M_{i+1}}) = 1 - z_0 \cdots z_{i+1}$ et $\widetilde{M_{i+1}}.{}^t(y, -x) = 0$. L'hypothèse de récurrence est donc vérifiée au rang $i + 1$.
Enfin, au rang $n-1$, on a $q_{n-1} = p_n = 1$, donc $z_{n-1} = z_{n-1}q_{n-1} = 0$, donc $\mathrm{tr}(\widetilde{M_{n-1}}) = 1$ et la matrice $\widetilde{M_{n-1}}$ est une matrice de localisation principale du couple (x, y). □

6.6 Les cas cohérent et fortement discret

Lemme 6.16 *Soit* **A** *un anneau intégralement clos dans son anneau total des fractions. Si* **A** *est quasi intègre, alors* **A** *est normal.*

Preuve : Tout d'abord remarquons que **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 $a'_i = sa_i$. On a $ry^n = 0$, donc puisque **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 **A** est normal. □

Proposition 6.17 *Soit* **A** *un anneau normal quasi intègre. Soit* $f(X) \in \mathbf{A}[X]$ *un polynôme unitaire dont le discriminant est régulier. Soit* $\mathbf{A}' = \mathbf{A}[X]\,/\langle f(X)\rangle$ *et* **B** *la clôture intégrale de* $\mathbf{A}'$ *dans son anneau total des fractions. Alors* **B** *est un anneau quasi intègre.*

Preuve : Notons **K** l'anneau total des fractions de **A** et **L** celui de $\mathbf{A}'$ (c'est aussi celui de **B**). On a $\mathbf{L} \simeq \mathbf{K}[X]\,/\langle f(X)\rangle$. Par le théorème 6.7 l'anneau **L** est zéro-dimensionnel et comme il est réduit, il est quasi intègre. Soit $x \in \mathbf{B}$ et r son annulateur idempotent dans **L**. Puisque $r^2 = r$, r est entier sur **A** donc $r \in \mathbf{B}$, et l'idéal annulateur de x dans **B** est $r\mathbf{B}$. □

Théorème 6.18 *Soit* **A** *un anneau de Prüfer cohérent. Soit* $f(X) \in \mathbf{A}[X]$ *un polynôme unitaire dont le discriminant est régulier. Soit* $\mathbf{A}' = \mathbf{A}[X]\,/\langle f(X)\rangle$ *et* **B** *la clôture intégrale de* $\mathbf{A}'$ *dans son anneau total des fractions. Alors* **B** *est un anneau de Prüfer cohérent. En outre si* **A** *est fortement discret (resp. noethérien), alors il en va de même pour* **B**.

Preuve : La première affirmation est conséquence de la proposition 6.17, du lemme 6.16 et du théorème 6.15. Pour les dernières voir [19]. □

Remarque : Nous ne savons pas si la variante suivante, qui serait bien utile, est vraie : *dans le théorème précédent, si* **A** *est à factorisation partielle, il en va de même pour* **B**. Par ailleurs en mathématiques classiques dans le cas noethérien, on sait que **B** est un **A**-module projectif de type fini. Cependant, il ne semble pas qu'on puisse expliciter un système générateur de **B** comme **A**-module sans décomposer le discriminant en produit d'idéaux maximaux inversibles de **A**. Dans [23] la variante « domaines de Dedekind à factorisation complète » du théorème 6.18 est prouvée constructivement sous certaines hypothèses restrictives (du point de vue constructif, mais toujours vraies en mathématiques classiques) concernant l'extension considérée.

Références

[1] Bernstein, D. *Factoring into coprimes in essentially linear time.* Journal of Algorithms **54** (2005), 1–30. 2

[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). 2

[3] Buchmann J., Lenstra H. *Approximating rings of integers in number fields.* J. Théor. Nombres Bordeaux **6** (2) (1994), 221–260. 2, 3

[4] Cartan H., Eilenberg S. *Homological algebra.* Princeton University Press (1956). 28

[5] Coquand T., Ducos L., Lombardi H., Quitté C. *L'idéal des coefficients du produit de deux polynomes.* Revue des Mathématiques de l'Enseignement Supérieur, **113** (3) (2003) 25–39. 39

[6] Coquand T., Lombardi H. *Hidden constructions in abstract algebra (3) Krull dimension of distributive lattices and commutative rings.* dans : Commutative ring theory and applications. Eds : Fontana M., Kabbaj S.-E., Wiegand S. Lecture notes in pure and applied mathematics vol 131. M. Dekker. (2002) 477–499. 7

[7] Coquand T., Lombardi H. *Krull dimension of distributive lattices and commutative rings : Going Up and Going Down.* En préparation. 2, 36

[8] Coquand T., Lombardi H., Quitté C. *Generating non noetherian modules constructively.* Preprint 2004. 21, 22

[9] Edwards H. *Divisor theory.* Birkhaüser. Boston MA. (1990) 39

[10] Forster O. *Über die Anzahl der Erzeugenden eines Ideals in einem Noetherschen Ring.* Math. Z. **84** (1964) 80–87. 21

[11] Freid M. D., Jarden M. *Field Arithmetic* Springer-Verlag, 11. (1986) 39

[12] Heitmann R. *Generating ideals in Prüfer domains.* Pacific J. Math. **62** (1) 117–126 (1976). 21

[13] Heitmann, R. *Generating non-Noetherian modules efficiently.* Michigan Math. **31** 2 (1984) 167–180. 21, 22

[14] Heitmann R., Levy L. *1 1/2 and 2 generator ideals in Prüfer domains.* Rocky Mountain J. Math. **5** (3) 361–673 (1975). 29, 30

[15] Jensen C. *Arithmetical rings.* Acta Mathematica Academiae Scientiarum Hungaricae **17**, (1-2), (1966) 115–123. 22

[16] Kaplansky I. *Modules over Dedekind Rings and Valuation Rings.* Trans. Amer. Math. Soc. **72**, (1952) 327–340. 30

[17] Kaplansky I. *Commutative Rings.* Allyn and Bacon, Mass. USA (1970). 23

[18] Larsen M., McCarthy P. *Multiplicative Theory of Ideals.* Academic Press (1971). 22

[19] Lombardi H. *Platitude, localisation et anneaux de Prüfer, une approche constructive.* Publications Mathématiques de Besançon. Théorie des nombres. Années 1998-2001. 3, 5, 22, 28, 41

[20] Lombardi H. *Dimension de Krull, Nullstellensätze, évaluation dynamique.* Mathematische Zeitschrift **242** (2002) 23–46. 2, 7

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

[22] Lombardi H., Quitté C. *Théorie constructive élémentaire des modules projectifs de type fini.* Preprint 2003. 5, 14, 20

[23] Mines R., Richman F., Ruitenburg W. *A Course in Constructive Algebra.* Springer-Verlag (1988). 2, 18, 25, 33, 34, 39, 41

[24] Northcott D. *A generalization of a theorem on the content of polynomials.* Proc. Cambridge Philos. Soc. **55** (1959), 282–288. 12

[25] Perdry H. *Strongly noetherain rings and constructive ideal theory.* A parître au Journal of Symbolic Computation. 33

[26] Rota Gian Carlo *The many lives of lattice theory.* Notices Amer. Math. Soc. **44** (11), (1997), 1440–1445. 2

[27] Salou M. *Théorie algorithmique des anneaux arithmétiques, des anneaux de Prüfer et des anneaux de Dedekind.* Thèse, avril 2002, Besançon, Université de Franche-Comté. 3, 34

[28] Vasconcelos W. *The rings of dimension 2.* M. Dekker. NY. 1976. 21

Lionel Ducos, Claude Quitté
Laboratoire de Mathématiques, SP2MI, Boulevard 3, Teleport 2, BP 179,
86960 FUTUROSCOPE Cedex, FRANCE,
emails : `lionel.ducos@mathlabo.univ-poitiers.fr`,
`quitte@mathlabo.univ-poitiers.fr`

Henri Lombardi
Laboratoire de Mathématiques, UMR CNRS 6623, UFR des Sciences et Techniques,
Université de Franche-Comté, 25030 BESANÇON cedex, FRANCE,
partiellement financé par le rseau européen RAAG CT-2001-00271
email : `henri.lombardi@univ-fcomte.fr`
page web : `http ://hlombardi.free.fr/`

Maimouna Salou
Laboratoire de Mathématiques, UMR CNRS 6623, UFR des Sciences et Techniques,
Université de Franche-Comté, 25030 BESANÇON cedex, FRANCE
email : `maimouna.salou@math.univ-fcomte.fr`

Table des matières

Introduction **2**

1 Préliminaires **4**
1.1 Quelques définitions constructives 4
1.2 Localisations en des monoïdes comaximaux 4
1.3 Dimension de Krull 7

2 Idéaux localement principaux, projectifs, inversibles **10**
2.1 Idéaux localement principaux 10
2.2 Idéaux projectifs de type fini 14
2.3 Idéaux inversibles 17
2.4 Le théorème un et demi 20
2.5 Pour $n \geq 3$, $\mathbf{SL}_n(\mathbf{A}) = \mathbf{E}_n(\mathbf{A})$ 22

3 Anneaux arithmétiques et anneaux de Prüfer **22**
3.1 Anneaux arithmétiques 22
3.2 Anneaux de Prüfer et anneaux cohérents 25
3.3 Anneaux de Prüfer cohérents 26

4 Anneaux de Prüfer cohérents de dimension ≤ 1 **29**
4.1 Théorème un et demi 29
4.2 Structure des idéaux de type fini et des modules de présentation finie 30
4.3 Factorisations partielles 31
4.4 Factorisations moins poussées en dimension inférieure à 1 32

5 Anneaux de Dedekind **33**
5.1 Les anneaux de Dedekind sont à factorisation partielle 33
5.2 Anneaux de Dedekind à factorisation complète 34

6 Anneaux normaux, extensions entières **34**
6.1 Idéaux intégralement clos et anneaux normaux 34
6.2 Transfert de la dimension 0 36
6.3 Transfert de la dimension pour le cas des anneaux de Prüfer 36
6.4 Anneaux normaux de dimension inférieure ou égale à 1 37
6.5 Extensions entières d'anneaux de Prüfer 38
6.6 Les cas cohérent et fortement discret 41

Références **42**