THÉORIE DES NOMBRES
BESANÇON

Années 1998/2001

Platitude, localisation et anneaux de Prüfer : une approche constructive

H. LOMBARDI

Platitude, localisation et anneaux de Prüfer : une approche constructive

H. Lombardi([1])

Juin 2001

Résumé

Nous étudions par des méthodes élémentaires et constructives les modules plats et les anneaux de Prüfer. Nous adoptons la définition suivante lorsque l'on autorise des diviseurs de zéros : un anneau de Prüfer est un anneau pour lequel tout idéal de type fini est plat.

Dans les preuves classiques on utilise la localisation en n'importe quel idéal maximal, et on obtient un anneau de valuation. La preuve classique implique un nombre fini de calculs explicites sous l'hypothèse suivante : tout élément est dans l'idéal maximal ou est inversible. La relecture constructive consiste en la considération de localisations pour lesquelles tout élément pertinent dans le calcul est dans le radical (de l'anneau localisé) ou inversible (dans l'anneau localisé). Ainsi, au lieu d'utiliser des localisations en tous les idéaux maximaux, nous utilisons des localisations bien controlées, en des parties multiplicatives S_i que l'on peut décrire en termes finis, et telles que les ouverts U_{S_i} correspondants recouvrent le spectre de Zariski.

English abstract

We study by elementary and constructive methods the basic theory of Prüfer rings. We adopt the following definition in the case where zero divisors are allowed : a Prüfer ring is a ring for which any finitely generated ideal is flat.

In classical proofs, we deal with localizations at each maximal ideal, getting valuation rings. In order to get constructive proofs we use a close inspection of the classical proof for the case of valuation rings. We see that the proof involves some finite computations under the hypothesis : any element is in the maximal ideal or is invertible. The constructive rereading consists in considering localizations for which any relevant element is in the radical (of the localized ring) or is invertible (in the localized ring). Instead of localizations at maximal ideals we use well controlled localizations, at multiplicatively closed subsets S_i that are described in finite terms, the corresponding U_{S_i} being an open covering of the Zariski spectrum.

We think that we are showing in practice that many classical proofs are in fact constructive.

MSC 2000 : 13A15, 13C10, 13C11, 13F05, 13F30, 13B22, 03F65

Mots clés : Modules plats, Localisation, Principes local-global, Anneaux de Prüfer, Idéaux déterminantiels, Mathématiques constructives.

Key Words : Flat Modules, Localization, Local-global principles, Prüfer rings, Constructive Mathematics.

[1] Equipe de Mathématiques, UMR CNRS 6623, UFR des Sciences et Techniques, Université de Franche-Comté, 25030 BESANCON cedex, FRANCE, email: lombardi@math.univ-fcomte.fr

Table des matières

Introduction

Dans cet article, tous les anneaux considérés sont commutatifs, sauf mention expresse du contraire.

Notre but est de comprendre en termes constructifs les théorèmes classiques les plus importants concernant les anneaux de Prüfer.

Nous adoptons la définition (dans le cas non intègre) qu'un anneau est un anneau de Prüfer si ses idéaux de type fini sont plats. Cette définition a été proposée dans [14]. Un autre nom pour ces anneaux, dans la littérature est *anneau de dimension globale faible inférieure ou égale à un.*

A vrai dire, il y aurait au moins 3 autres definitions possibles. La première (plus forte) où on demanderait que les idéaux de type fini soient projectifs, dans la littérature, ces anneaux sont souvent appelés semihéréditaires. La seconde (plus faible) où on demanderait que les idéaux de type fini soient localement principaux : ce sont les anneaux arithmétiques. La dernière (encore un peu plus faible) où on demanderait que les idéaux de type fini contenant un non diviseur de zéro soient inversibles, ces anneaux sont appelés anneaux de Prüfer dans [19]. Les quatre notions coïncident dans le cas intègre. Pour des contre-exemples dans le cas non intègre voir remarque 4.7.2 page 47 et exemples 4.4.4 page 36 et 4.8.1 page 49.

Les résultats que nous obtenons de manière élémentaire et constructive ont des preuves connues en mathématiques classiques au moins pour le cas intègre.

Cependant, tant la manière de présenter la théorie que les résultats eux-mêmes, en tant que résultats proprement algorithmiques sont en bonne partie nouveaux. Nous rappelons que l'auteur du traité Al Jabr (ce qui a donné Algèbre) s'appelait Al Khwarizmi (ce qui a donné algorithme).

En outre notre méthode d'attaque est basée sur quelques idées simples exploitées de manière systématique, notamment la machinerie constructive des preuves par localisation, exposée section 1.1, qui est une manière constructive d'interpréter les preuves par localisation abstraites usuelles. Le fait de pouvoir mettre en oeuvre de manière systématique une méthode générale qui interprète à la fois des définitions abstraites et leur utilisation classique, sous forme de définitions puis de preuves de nature algorithmique, nous semble mériter une attention particulière. C'est en fait un morceau d'un "programme de Hilbert" pour l'algèbre abstraite, que nous entendons développer de manière plus large (cf. [8, 9, 20, 21, 22, 23, 24, 25, 26]).

Voici maintenant une description des résultats démontrés de manière élémentaire et constructive dans cet article.

Nous donnons des versions constructives pour les théorèmes suivants concernant la platitude.

Théorème P.1 (caractérisation locale des modules plats, voir section 3.1) *Un module M sur un anneau $\mathbf{A}$ est plat si et seulement si il est* localement plat.

Théorème P.2 (modules plats de type fini, voir propositions 3.2.7 et 3.2.8) *Soit M un $\mathbf{A}$-module plat de type fini. Si $\mathbf{A}$ est un anneau local, M est libre. Si $\mathbf{A}$ est intègre, M est projectif de type fini.*

Les versions constructives des théorèmes précédents diffèrent légèrement des versions classiques. Concernant le théorème P.2 elles impliquent les versions classiques en mathématiques classiques.

Les théorèmes qui suivent sont donnés dans leur version constructive. Nous devons pour cela préciser certaines définitions dans le cadre constructif.

Des éléments $x_1, \ldots, x_n$ de $\mathbf{A}$ sont dits *comaximaux* dans $\mathbf{A}$ si $\langle x_1, \ldots, x_n \rangle = \mathbf{A}$. Un idéal de type fini est dit *localement principal* lorsqu'il devient principal après localisation en des éléments comaximaux convenables. Un anneau est dit *arithmétique* lorsque tout idéal de type fini est localement principal.

Un idéal I d'un anneau $\mathbf{A}$ est dit *intégralement clos* si tout $x \in \mathbf{A}$ vérifiant une relation de dépendance intégrale $x^{n+1} = a_1 x^n + a_2 x^{n-1} + \cdots + a_n x + a_{n+1}$ avec $\forall h\ a_h \in I^h$, est dans I. Un anneau est dit *normal* lorsque tout idéal principal est intégralement clos.

Une partie S d'un ensemble E est dite *détachable* si il y a un test explicite d'appartenance à S pour les éléments de E. Un $\mathbf{A}$-module est dit *cohérent* si tout sous-module de type fini est de présentation finie, *fortement discret* si tout sous-module de type fini est détachable. Un anneau est dit cohérent ou fortement discret s'il est cohérent ou fortement discret en tant que $\mathbf{A}$-module.

Un anneau est dit *localement sans diviseur de zéro* si ses idéaux principaux sont plats. Un **A**-module est dit *sans torsion* s'il est réunion de sous modules plats. Si M est un **A**-module, le *sous-module de torsion* de M est l'ensemble des $x \in M$ dont l'annulateur contient un élément non diviseur de zéro. Un module est appelé un *module de torsion* s'il est égal à son sous-module de torsion.

Rappelons aussi qu'un idéal principal $\langle x \rangle$ est projectif si et seulement si l'annulateur de x est un idéal principal $\langle r \rangle$ avec r idempotent. Nous dirons qu'un anneau **A** est *quasi intègre* lorsque tout idéal principal est projectif.

Nous obtenons les théorèmes de structure suivants.

Théorème S.1 (voir théorème 4 section 4.3 et propositions 4.3.1, 4.8.5, 4.7.3 et 4.8.6) *Soit* **A** *un anneau de Prüfer cohérent.*

(1) *Tout noyau d'un homomorphisme entre modules projectifs de type fini est facteur direct.*

(2) *Soit P un* **A***-module projectif de type fini engendré par n éléments.*
   - *Le module P est somme directe de n sous modules isomorphes à des idéaux de type fini.*
   - *Lorsque P de rang ℓ il est somme directe de ℓ modules de rang* 1.

(3) *Tout module de présentation finie est somme directe de son sous-module de torsion et d'un sous module projectif (tous deux de type fini).*

Théorème S.2 (voir propositions 4.4.6, 4.8.4 et corollaire 4.5.2)

- *Un anneau arithmétique* **A** *est fortement discret si et seulement si la relation de divisibilité est explicite.*
- *Sur un anneau de Prüfer où la divisibilité est explicite tout module de présentation finie est fortement discret.*
- *Un anneau de Prüfer cohérent est discret si et seulement si l'ensemble de ses idempotents est discret.*
- *Un anneau de Prüfer cohérent et discret* **A** *est fortement discret si et seulement si* **A** *est une partie détachable de son anneau total de fractions.*

Théorème S.3 (voir proposition 4.4.12) *Soient $I_1, \ldots, I_n$ des idéaux de type fini d'un anneau arithmétique* **A**. *Posons $J_1 = \sum_{k=1}^{n} I_k$, $J_2 = \sum_{1 \leq j < k \leq n} (I_j \cap I_k)$, $\ldots$, $J_r = \sum_{1 \leq j_1 < \cdots < j_r \leq n} (I_{j_1} \cap \cdots \cap I_{j_r})$, $\ldots$, $J_n = \cap_{k=1}^{n} I_k$. Alors on a $J_n \subseteq \cdots \subseteq J_1$ avec un isomorphisme*

$$\bigoplus_{k=1}^{n} A/I_k \simeq \bigoplus_{k=1}^{n} A/J_k$$

Théorème S.4 (propriétés du monoïde multiplicatif des idéaux de type fini d'un anneau arithmétique, cf. théorème 6 section 4.4) *Soit* **A** *un anneau arithmétique. Notons $I \cdot J$ le produit de deux idéaux et T le monoïde multiplicatif des idéaux de type fini. On a les propriétés suivantes :*

- *la relation de préordre " I divise J dans T ", notée $I \leq_T J$, définie par $\exists L \in T \;\; J = I \cdot L$ est une relation d'ordre, équivalente à $J \subseteq I$.*
- *Avec cette relation d'ordre, T est un treillis distributif. On note $\wedge$ et $\vee$ les lois* min *et* max. *On a :* $\max(I, J) = I \cap J$ *et* $\min(I, J) = I + J$.
- $\forall I, J \;\; I \cdot J = (I \wedge J) \cdot (I \vee J)$
- $\forall I, J, K \;\; (\, I \cdot (J \wedge K) = (I \cdot J) \wedge (I \cdot K) \qquad \text{et} \qquad I \cdot (J \vee K) = (I \cdot J) \vee (I \cdot K)\,)$
- $\forall I, J \in T \; \forall n \in \mathbb{N} \;\; (I^n \wedge J^n = (I \wedge J)^n \;\; \text{et} \;\; I^n \vee J^n = (I \vee J)^n)$
- *Tout idéal de type fini I contenant un non diviseur de zéro est inversible, c'est un module projectif de type fini de rang 1, et il est simplifiable ($IJ = IK \Rightarrow J = K$).*
- *Si* **A** *est un anneau de Prüfer, on a la propriété de simplifiabilité locale suivante.*
  Si I, J_1, J_2 sont trois idéaux de type fini avec $J_1 \leq_T I$, $J_2 \leq_T I$ et $I \cdot J_1 = I \cdot J_2$ alors $J_1 = J_2$.

- *Si* $\mathbf{A}$ *est un anneau de Prüfer cohérent, on a la propriété de factorisation suivante. Soient des éléments* I_i *et* J_j *de* T *tels que* $I_1 \cdot I_2 \cdot \cdots \cdot I_n = J_1 \cdot J_2 \cdot \cdots \cdot J_m$ *alors on peut trouver des éléments* $K_{h\ell}$ $(h = 1, \ldots, n$ *et* $\ell = 1, \ldots, m)$ *tels que chaque* I_h *est produit des* $K_{h\ell}$ *correspondants et chaque* J_ℓ *est produit des* $K_{h\ell}$ *correspondants.*

Concernant les caractérisations des anneaux arithmétiques, des anneaux de Prüfer, des anneaux de Prüfer cohérents et des domaines de Prüfer, nous avons les résultats suivants.

Théorème C.1 (caractérisation des anneaux arithmétiques, voir proposition 3.3.3 et théorèmes 5 et 7 section 4.4) *Pour un anneau* $\mathbf{A}$*, les propriétés suivantes sont équivalentes:*

(1.1) *Tout idéal de type fini est localement principal.*

(1.2) *Tout idéal* $I = \langle x_1, x_2 \rangle$ *est localement principal.*

(1.3) *Pour tout idéal de type fini* $I = \langle x_1, \ldots, x_n \rangle$ *il existe* n *éléments* s_i $(i = 1, \ldots, n)$ *et* $n^2 - n$ *éléments* $a_{i,j}$ $(i \neq j \in \{1, \ldots, n\})$ *vérifiant les équations suivantes.*

$$\begin{array}{rcl} \sum_{i=1}^{n} s_i & = & 1 \\ a_{i,j}x_i - s_i x_j & = & 0 \quad i \neq j \in \{1, \ldots, n\} \end{array}$$

(2.1) *Pour tous idéaux de type fini* $J \subseteq I$*, il existe un idéal de type fini* L *tel que* $IL = J$

(2.2) *Pour tout idéal* $I = \langle x_1, x_2 \rangle$*, il existe un idéal de type fini* L *tel que* $IL = \langle x_1 \rangle$*, (i.e.* $\mathbf{A}$ *est arithmétique).*

(2.3) $\forall x_1, x_2 \in \mathbf{A}$ *le système linéaire suivant admet une solution :*

$$(B|C) = \left(\begin{array}{ccc|c} x_1 & x_2 & 0 & x_1 \\ x_2 & 0 & x_1 & 0 \end{array}\right)$$

(2.4) $\forall x_1, x_2 \in \mathbf{A}$ *il existe* $u \in \mathbf{A}$ *tel que :*

$$\langle x_1 \rangle \cap \langle x_2 \rangle = \langle (1-u)x_1, ux_2 \rangle$$

(3.1) *Pour tous idéaux de type fini* I *et* J *la suite exacte courte ci-après est scindée :*

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

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

(3.2) *Même chose en se limitant à des idéaux principaux.*

(4.1) *Pour tous idéaux de type fini* I *et* J*,* $(I : J) + (J : I) = \langle 1 \rangle$.

(4.2) *Même chose en se limitant à des idéaux principaux.*

(5.1) (Théorème chinois) *Si* $(J_k)_{k=1,\ldots,n}$ *est une famille finie d'idéaux de* $\mathbf{A}$ *et* $(x_k)_{k=1,\ldots,n}$ *est une famille d'éléments de* $\mathbf{A}$ *vérifiant* $x_k \equiv x_\ell \bmod J_k + J_\ell$ *pour tous* k, ℓ*, alors il existe un* $x \in \mathbf{A}$ *tel que* $x \equiv x_k \bmod J_k$ *pour tout* k.

(5.2) *Même chose en se limitant au cas de trois idéaux principaux.*

(6.1) *Pour tous idéaux* I*,* J *et* K *on a* $I \cap (J + K) = (I \cap J) + (I \cap K)$.

(6.2) *Même chose en se limitant au cas* $I = \langle x \rangle = \langle y + z \rangle$*,* $J = \langle y \rangle$ *et* $K = \langle z \rangle$

(7.1) *Pour tous idéaux* I*,* J *et* K *on a* $I + (J \cap K) = (I + J) \cap (I + K)$.

(7.2) *Même chose en se limitant au cas* $I = \langle x \rangle$*,* $J = \langle y \rangle$ *et* $K = \langle x + y \rangle$

(8.1) *Pour tous idéaux de type fini* I*,* J *et* K *on a* $(J + K) : I = (J : I) + (K : I)$.

(8.2) *Même chose avec* J *et* K *idéaux principaux et* $I = J + K$.

(9.1) *Pour tout idéal* I *et tous idéaux de type fini* J *et* K *on a* $I : (J \cap K) = (I : J) + (I : K)$.

(9.2) *Même chose avec* J *et* K *idéaux principaux et* $I = J \cap K$.

Théorème C.2 (caractérisations des anneaux de Prüfer, voir théorèmes 3 section 4.3, 8 section 4.5 et 9 section 4.6) *Pour un anneau* $\mathbf{A}$, *les propriétés suivantes sont équivalentes:*

(1.1) $\mathbf{A}$ *est un anneau de Prüfer (tout idéal de type fini est plat).*

(1.2) *Tout idéal est plat.*

(1.3) *Tout idéal* $\langle x_1, x_2\rangle$ *est plat.*

(2.1) *Tout sous-module d'un module plat est plat.*

(2.2) $\mathbf{A}$ *est localement sans diviseur de zéro et tout module sans torsion est plat.*

(3.1) $\mathbf{A}$ *est réduit et arithmétique.*

(3.2) $\mathbf{A}$ *est localement sans diviseur de zéro et arithmétique.*

(4.1) *Un système linéaire* $BX = C$ *arbitraire, dès que les idéaux déterminantiels de* $(B|C)$ *sont égaux à ceux de* B, *admet une solution.*

(4.2) *Même chose en se limitant à* $B \in \mathbf{A}^{2\times 3}$ *et* $C \in \mathbf{A}^{2\times 1}$.

(5.1) *Tout idéal est intégralement clos.*

(5.2) *Tout idéal de type fini est intégralement clos.*

(5.3) *Tout idéal à deux générateurs est intégralement clos.*

(5.4) $\mathbf{A}$ *vérifie les deux propriétés,*

$$\forall x, y \in \mathbf{A}\ \ xy \in \langle x^2, y^2\rangle \quad \text{et} \quad \forall x, y \in \mathbf{A}\ \ (x^2 \in \langle xy, y^2\rangle \ \Rightarrow\ \ x \in \langle y\rangle)$$

c'est-à-dire encore

$$\forall x, y \in \mathbf{A}\ \ \langle x, y\rangle^2 = \langle x^2, y^2\rangle \quad \text{et} \quad \forall x, y \in \mathbf{A}\ \ (\langle x, y\rangle^2 = \langle y\rangle\langle x, y\rangle \ \Rightarrow\ \ \langle x, y\rangle = \langle y\rangle)$$

(5.5) $\mathbf{A}$ *est normal et vérifie la propriété suivante.*
$\forall x, y \in \mathbf{A}\ \ \exists h, k \in \mathbb{N}\ : h + k > 0$ *et* $x^h y^k$ *est dans l'idéal engendré par les* $x^i y^j$ *tels que* $i + j = h + k$ *et* $i \neq h$.

(5.6) $\mathbf{A}$ *est normal et* $\forall x, y \in \mathbf{A}\ \forall h, k > 0\ \exists a, b \in \mathbf{A}\ \ x^h y^k = ax^{h+k} + by^{h+k}$, *c'est-à-dire encore* $\forall x, y \in \mathbf{A}\ \forall m > 1\ \langle x^m, y^m\rangle = \langle x, y\rangle^m$

(5.7) $\mathbf{A}$ *est normal et* $\forall x, y \in \mathbf{A}\ \ xy \in \langle x^2, y^2\rangle$.

(6.1) *Si* I, J_1, J_2 *sont trois idéaux de type fini de* $\mathbf{A}$ *avec* $J_1 \subseteq I$, $J_2 \subseteq I$ *et* $IJ_1 = IJ_2$, *alors* $J_1 = J_2$.

(6.2) *Si* I, J_1, J_2 *sont trois idéaux de type fini de* $\mathbf{A}$ *avec* $\mathrm{Ann}(I) \subseteq \mathrm{Ann}(J_1)$, $\mathrm{Ann}(I) \subseteq \mathrm{Ann}(J_2)$ *et* $IJ_1 \subseteq IJ_2$, *alors* $J_1 \subseteq J_2$.

Le *contenu* d'un polynome $f \in \mathbf{A}[X]$ est l'idéal $\mathrm{c}(f)$ engendré par les coefficients de f.

Théorème C.3 (caractérisations des anneaux de Prüfer cohérents, cf. section 4.3 théorème 4, section 4.8 théorème 14 et proposition 4.8.3) *Pour un anneau* $\mathbf{A}$, *les propriétés suivantes sont équivalentes:*

(1.1) $\mathbf{A}$ *est un anneau de Prüfer cohérent.*

(1.2) $\mathbf{A}$ *est un anneau arithmétique quasi intègre.*

(2.1) *Tout idéal de type fini est projectif.*

(2.2) *Tout sous-module de type fini d'un module projectif de type fini est projectif de type fini.*

(2.3) *Tout noyau d'un homomorphisme entre modules projectifs de type fini est facteur direct.*

(2.4) *Tout noyau d'une forme linéaire sur un module* $\mathbf{A}^n$ *est facteur direct.*

(3.1) $\mathbf{A}$ *est quasi intègre et tout idéal de type fini contenant un non diviseur de zéro est inversible.*

(3.2) $\mathbf{A}$ *est quasi intègre et tout idéal* $I = \langle x_1, x_2\rangle$ *avec* x_1 *et* x_2 *non diviseurs de zéro est inversible.*

(3.3) $\mathbf{A}$ *est quasi intègre et pour tous* $a, b \in \mathbf{A}$, *on a :* $\langle a, b\rangle^2 = \langle a^2, b^2\rangle = \langle a^2 + b^2, ab\rangle$.

(3.4) $\mathbf{A}$ *est quasi intègre et pour tous* $f, g \in \mathbf{A}[X]$, *on a :* $\mathrm{c}(f)\mathrm{c}(g) = \mathrm{c}(fg)$.

(4.1) **A** *est quasi intègre et tout sous anneau* $\mathbf{A}[a/b]$ *de l'anneau total des fractions de* **A** *(*$a \in \mathbf{A}$ *et* b *non diviseur de zéro dans* **A***) est normal.*

(4.2) **A** *est quasi intègre et tout anneau compris entre* **A** *et son anneau total des fractions est un anneau de Prüfer cohérent.*

Dans le théorème concernant les domaines de Prüfer nous ne répétons pas les caractérisations des anneaux arithmétiques ni des anneaux de Prüfer, qui interviennent dans les points (1.2) et (1.3).

Théorème C.4 (cf. lemme 4.7.5 et théorème 11 section 4.7) *Pour un anneau* **A** *non trivial, les propriétés suivantes sont équivalentes:*

(1.1) **A** *est un domaine de Prüfer (c'est-à-dire un anneau de Prüfer intègre).*

(1.2) **A** *est un anneau arithmétique intègre.*

(1.3) **A** *est anneau de Prüfer cohérent sans diviseur de zéro.*

(2) **A** *est intègre et tout module sans torsion est plat.*

(3) *Tout idéal à deux générateurs est un module de rang constant.*

(4) **A** *est intègre et les idéaux de type fini non nuls forment un monoïde multiplicatif simplifiable.*

(5) **A** *est intègre et les idéaux fractionnaires de type fini non nuls de* **A** *forment un groupe réticulé.*

(6) **A** *est intègre et si* I, J *sont deux idéaux principaux, on a* $(I+J)(I\cap J) = IJ$.

Les quatre théorèmes suivants concernent les extensions algébriques d'anneaux de Prüfer. Le dernier est particulièrement intéressant lorsqu'on cherche à construire une extension algébrique d'un anneau de Prüfer intègre pour lequel on ne dispose pas d'algorithme de factorisation pour les polynomes sur le corps des fractions.

Théorème E.1 (cf. théorème 10 section 4.6) *Soit* **A** *un sous anneau de* **B**. *Supposons que* **A** *soit un anneau de Prüfer, que* **B** *soit normal et que* **B** *soit entier sur* **A**. *Alors* **B** *est un anneau de Prüfer.*

Théorème E.2 (cf. théorème 12 section 4.7) *Soit* **A** *un domaine de Prüfer,* **K** *son corps de fraction,* **L** *une extension algébrique de* **K** *et* **B** *la cloture intégrale de* **A** *dans* **L**. *Alors* **B** *est un domaine de Prüfer.*
En outre si **A** *est fortement discret et si on sait calculer le polynome minimal dans* $\mathbf{K}[X]$ *d'un élément de* **L** *alors* **B** *est fortement discret.*

Théorème E.3 (cf. théorème 13 section 4.7) *Soit* **A** *un domaine de Prüfer et* **K** *son corps de fractions. Soit* $f(X) \in \mathbf{A}[X]$ *un polynome unitaire irréductible dans* $\mathbf{K}[X]$ *de discriminant non nul.*
Soit $\mathbf{A}' = \mathbf{A}[X]/f(X)$ *et* **B** *la cloture intégrale de* $\mathbf{A}'$ *dans son corps de fractions. Alors* **B** *est un domaine de Prüfer.*
En outre si **A** *est fortement discret ou noethérien, alors il en va de même pour* **B**.

Théorème E.4 (cf. théorème 15 section 4.8) *Soit* **A** *un anneau de Prüfer cohérent. Soit* $f(X) \in \mathbf{A}[X]$ *un polynome unitaire dont le discriminant est non diviseur de zéro.*
Soit $\mathbf{A}' = \mathbf{A}[X]/f(X)$ *et* **B** *la cloture intégrale de* $\mathbf{A}'$ *dans son anneau total des fractions. Alors* **B** *est un anneau de Prüfer cohérent.*
En outre si **A** *est noethérien ou fortement discret, alors il en va de même pour* **B**.

Dans la section 1 nous donnons quelques préliminaires, la section 2 est consacrée aux principes local-globals, la section 3 à la platitude et la section 4 aux anneaux arithmétiques et aux anneaux de Prüfer. Les annexes I, II III et IV contiennent des résultats constructifs dont on peut trouver par ailleurs des preuves constructives (cf. [9, 17, 20, 21, 22, 30, 31]). Dans l'annexe V nous donnons quelques lemmes qui peuvent faciliter les calculs dans les domaines de Prüfer et les anneaux de Prüfer.

Les références générales pour ce travail sont les suivantes. Dans [30] on trouve une approche constructive des bases de l'algèbre. Les théorèmes cités ci-dessus peuvent être trouvés, avec des preuves non constructives, et au moins pour le cas intègre, dans [12, 14, 19] et dans les exercices de [5, 6]. Quatre autres articles dans le même esprit que celui-ci sont [8, 23, 25, 24]. Les allusions dans le

texte à l'évaluation dynamique peuvent être sautées : le lecteur intéressé peut consulter sur ce sujet [9, 20, 21, 22].

Remerciements : Merci à Fred Richman pour ses suggestions et commentaires pertinents.

1 Préliminaires

1.1 La machinerie constructive des preuves par localisation

Nous donnons ici quelques explications sur le fonctionnement constructif de nos preuves. En général, nos preuves sont issues de preuves classiques qui utilisent des arguments de localisation.

L'argument de localisation classique fonctionne comme suit. Lorsque l'anneau est local une certaine propriété P est vérifiée en vertu d'une preuve assez concrète. Lorsque l'anneau n'est pas local, la même propriété est encore vraie car il suffit de la vérifier localement.

Nous examinons avec un peu d'attention la première preuve. Nous voyons alors apparaître certains calculs qui sont faisables en vertu du principe : $\forall x \in \mathbf{A}$, x est une unité ou x est dans l'idéal maximal. Principe qui est appliqué à des éléments x provenant de la preuve elle-même. Dans le cas d'un anneau non nécessairement local, nous répétons la même preuve, en remplaccant chaque disjonction "x est une unité ou x est dans l'idéal maximal", par la considération des deux anneaux $\mathbf{B}_x$ et $\mathbf{B}_{1+x\mathbf{B}}$, où $\mathbf{B}$ est la localisation "courante" de l'anneau $\mathbf{A}$ de départ, à l'endroit de la preuve où on se trouve. Lorsque la preuve initiale est ainsi déployée, on a construit à la fin un certain nombre, fini parce que la preuve est finie, de localisés $\mathbf{A}_{S_i}$, pour lesquels la propriété est vraie. En outre les ouverts de Zariski U_{S_i} correspondants recouvrent $\mathrm{Spec}(\mathbf{A})$ et cela implique que la propriété P est vraie avec $\mathbf{A}$ (cf. définition 2.1.1 et principes local-global concrets 2, 3 (section 2.2), 4 (section 4.1), 5 (section 4.6), 6, 7 (annexe IV)). Nous redisons ceci sous une forme plus précise dans le principe local-global concret général 1 page 17.

1.2 Du bon usage de l'anneau trivial

Pour pouvoir appliquer ce principe de constructivisation de preuves plus agréablement, nous faisons un traitement "sans négation" qui offre un plus grand confort pour l'uniformité des preuves. Plus précisément, nous affaiblissons légèrement la formulation de certaines définitions usuelles de manière à ce que l'anneau trivial (celui où $1 = 0$) puisse satisfaire ces définitions.

Nous nous situons dans le cadre de l'algèbre constructive développée dans le livre [30]. Dans ce livre le théorème usuellement énoncé sous la forme : *si* $\mathbf{A}$ *est un anneau non trivial et si* $m < n$ *il est impossible d'avoir une application linéaire surjective de* $\mathbf{A}^m$ *vers* $\mathbf{A}^n$, est donné sous la forme suivante "sans négation" qui est plus générale, et surtout plus confortable du point de vue constructif (en l'absence de tiers exclu) : *si* $m < n$ *et si on a une application linéaire surjective de* $\mathbf{A}^m$ *vers* $\mathbf{A}^n$ *alors l'anneau est trivial.*

Signalons aussi que le "bon usage" de l'anneau trivial tel que nous le développons systématiquement dans cet article se situe dans la philosophie de l'article [33].

Un *anneau local* est un anneau où est vérifié l'axiome suivant :

$$\forall x \in \mathbf{A} \qquad x \text{ ou } 1-x \text{ est inversible}$$

Il revient au même de dire

$$\forall x, y \in \mathbf{A} \quad [x+y \text{ inversible} \implies (x \text{ ou } y \text{ inversible})]$$

L'anneau trivial est local.

Un *corps-discret* (en un seul mot) est un anneau où est vérifié l'axiome suivant :

$$\forall x \in \mathbf{A} \qquad x = 0 \text{ ou } x \text{ est inversible}$$

Un corps-discret est un anneau local, l'anneau trivial est un corps-discret.

Un élément x d'un anneau $\mathbf{A}$ est dit *noninversible* (en un seul mot) s'il vérifie

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

Dans l'anneau trivial 0 est à la fois inversible et noninversible.

Un *corps de Heyting*, ou simplement *un corps*, est par définition un anneau local qui vérifie l'axiome suivant :

$$\forall x \in \mathbf{A} \qquad (x \text{ noninversible}) \Rightarrow x = 0$$

En particulier un corps-discret, donc aussi l'anneau trivial, est un corps. Les nombres réels forment un corps qui *n'est pas* un corps-discret([1]).

L'axiome ci-dessus pour les corps n'est pas un axiome facilement utilisable en algèbre. Cela tient à ce que l'axiome n'est pas dynamique au sens de [9, 20, 21, 22]. Dans le même ordre d'idées, dans l'article [29], les auteurs préfèrent voir le corps des nombres complexes comme un anneau local et réduit en vue de traiter ses propriétés purement algébriques.

Rappelons qu'un ensemble M est dit *discret* lorsque l'axiome suivant est vérifié

$$\forall x, y \in M \qquad x =_M y \text{ ou } \neg(x =_M y)$$

Tout corps qui est discret est un corps-discret, mais la réciproque *n'est pas* vraie. Par exemple tout quotient $\mathbf{K}$ d'un corps-discret est un corps-discret, mais ce n'est un ensemble discret que si on a $1 =_{\mathbf{K}} 0$ ou non.

Dans un anneau local, les éléments noninversibles forment un idéal. Le quotient de l'anneau par cet idéal est un corps de Heyting, appelé *corps résiduel de l'anneau local* $\mathbf{A}$.

Un *anneau local résiduellement discret* est un anneau local dont le corps résiduel est un corps-discret : il peut être caractérisé comme un anneau qui vérifie l'axiome suivant

$$\forall x \in \mathbf{A} \qquad x \in \mathbf{A}^\times \text{ ou } (1 + x\mathbf{A}) \subseteq \mathbf{A}^\times.$$

Par exemple l'anneau des entiers p-adiques, quoique *non* discret, est résiduellement discret.

Dans cet article nous n'utilisons pas les corps de Heyting, mais seulement les corps-discrets.

Une partie P d'un ensemble M est dite *détachable* lorsque la propriété suivante est vérifiée

$$\forall x \in M \qquad x \in P \text{ ou } \neg(x \in P)$$

Un $\mathbf{A}$-module M est *fortement discret* (dans [30], les auteurs disent "M a des sous-modules détachables", mais depuis ils ont adopté cette nouvelle terminologie qui est plus simple) si les sous-modules de type fini de M sont détachables. Un anneau est dit discret ou fortement discret s'il est discret ou fortement discret en tant que $\mathbf{A}$-module.

Les monoïdes S que nous considérons dans un anneau $\mathbf{A}$ ne sont pas astreints à la condition $0 \notin S$. Cela tient à ce que nous avons en vue le localisé $\mathbf{A}_S$. Or l'anneau trivial vérifie "toutes" les propriétés (en vertu de nos conventions). Cela nous facilite la vie parce qu'en général, on n'a pas de test pour savoir si 0 est dans un monoïde S qui débarque au cours d'une preuve.

Nous disons qu'un élément a de $\mathbf{A}$ est *non diviseur de zéro*[2] si la suite

$$0 \longrightarrow \mathbf{A} \xrightarrow{a.} \mathbf{A}$$

est exacte. Autrement dit, on a :

$$\forall b \in \mathbf{A} \quad (ba = 0 \Rightarrow b = 0)$$

[1] Nous utilisons la négation en italique pour indiquer que l'affirmation correspondante n'est pas prouvable en mathématiques constructives.

[2] Un élément a est un *diviseur de zéro* s'il existe $b \in \mathbf{A}$ vérifiant $ba = 0$ et $(b = 0 \Rightarrow 1 = 0)$. La notion est moins facile à manipuler constructivement que celle de "non diviseur de zéro", qui est à lire d'un seul trait, sans connotation négative.

C'est seulement dans l'anneau trivial que 0 est non diviseur de zéro.

Si M est un $\mathbf{A}$-module, le *sous-module de torsion* de M est l'ensemble des $x \in M$ dont l'annulateur contient un élément non diviseur de zéro. Un module est appelé un *module de torsion* s'il est égal à son sous-module de torsion. Lorsqu'il est de type fini cela revient à dire que son annulateur contient un élément non diviseur de zéro.

Un anneau $\mathbf{A}$ est dit *sans diviseur de zéro* si on a :

$$\forall a, b \in \mathbf{A} \quad (ba = 0 \Rightarrow (a = 0 \text{ ou } b = 0))$$

Notez que le corps des réels *n'est pas* sans diviseur de zéro : on ne sait pas réaliser explicitement l'implication ci-dessus avec $\mathbb{R}$.

Un anneau $\mathbf{A}$ est dit *intègre* s'il est discret et sans diviseur de zéro. Cela implique que tout élément est nul ou non diviseur de zéro. Un anneau intègre possède un corps de fractions, qui est discret.

Plus généralement un anneau $\mathbf{A}$ admet un corps-discret pour anneau total des fractions si et seulement si on a :

$$\forall a \in \mathbf{A} \quad (a = 0 \text{ ou } a \text{ non diviseur de zéro})$$

Dans ce cas $\mathbf{A}$ est intègre si et seulement si il est trivial ou non trivial, c.-à-d. si on a : $1 =_{\mathbf{A}} 0$ ou $\neg(1 =_{\mathbf{A}} 0)$.

Rappelons qu'un idéal principal $\langle x \rangle$ est un module projectif si et seulement si l'annulateur de x est un idéal principal $\langle r \rangle$ avec r idempotent (le $\mathbf{A}$-module $\langle x \rangle$ est alors isomorphe à $\mathbf{A}/\langle r \rangle$). Nous dirons qu'un anneau $\mathbf{A}$ est *quasi intègre* lorsque tout idéal principal est projectif. Un anneau est intègre si et seulement si il est quasi intègre et si les seuls idempotents sont 0 et 1, avec $(0 = 1) \vee \neg(0 = 1)$. Dans la littérature, un anneau quasi intègre est parfois appelé un anneau "faiblement Baer" ou encore, en anglais, un "pp-ring".

Dans un anneau quasi intègre on a une notion naturelle de *quotient exact d'un élément a par un élément b* lorsque b divise a : si $\langle r \rangle = \mathrm{Ann}(b)$ et $e = 1 - r$, l'élément b "vit dans $e\mathbf{A}$" et il existe un unique quotient c qui "vit au même endroit". En d'autres termes le quotient exact c de a par b est l'unique élément qui vérifie $bc = a$ et $ec = c$ (si $bq = a$ on peut remplacer q par $c = eq$ et si $bc = bc'$ alors $r(c - c') = c - c'$, et donc, si $ec = c$ et $ec' = c'$ cela donne $c - c' = re(c - c') = 0$).

Un $\mathbf{A}$-module est dit *libre de rang fini (ou encore de dimension finie)* s'il est isomorphe à un $\mathbf{A}^n$. D'un point de vue constructif, ceci est à distinguer d'un $\mathbf{A}$-module libre de type fini M, car la base de M peut être un ensemble non discret. Pour plus de précisions on pourra consulter [30].

1.3 Idéaux premiers et maximaux

Un idéal I d'un anneau $\mathbf{A}$ est appelé un *idéal premier* lorsque $1 \in I \Rightarrow 1 =_{\mathbf{A}} 0$ et l'anneau quotient est sans diviseur de zéro.

Rappelons que si $\mathcal{P}$ est un idéal premier, on note $\mathbf{A}_{\mathcal{P}}$ le localisé $\mathbf{A}_S$ où

$$S = \{x \in \mathbf{A} \; ; \; x \in \mathcal{P} \Rightarrow 1 =_{\mathbf{A}} 0\}$$

Si en outre $\mathcal{P}$ est détachable, $\mathbf{A}_{\mathcal{P}}$ est un anneau local résiduellement discret. La relation étroite qui existe entre les localisés locaux d'un anneau $\mathbf{A}$ et ses idéaux premiers est précisée par les deux lemmes suivants.

Fait 1.3.1 *Soit S un monoïde multiplicatif saturé détachable[3] d'un anneau non trivial $\mathbf{A}$, ne contenant pas 0 : alors $\mathbf{A}_S$ est un anneau local si et seulement si $S = \mathbf{A} \setminus \mathcal{P}$ où $\mathcal{P}$ est un idéal premier détachable.*

[3] Dans le cadre général où on ne suppose pas la détachabilité, la notion la plus pertinente semble être en fait celle de *coidéal*. Un coidéal d'un anneau $\mathbf{A}$ est une partie S vérifiant $xy \in S \Rightarrow x \in S$, $1 \in S$ et $(x + y \in S \Rightarrow x \in S \text{ ou } y \in S)$. De sorte que l'ensemble $P := \{x \in \mathbf{A} \; ; \; x \in S \Rightarrow 1 =_{\mathbf{A}} 0\}$ est un idéal de $\mathbf{A}$. Mais S *n'est pas toujours* égal à $S' = \{x \in \mathbf{A} \; ; \; x \in P \Rightarrow 1 =_{\mathbf{A}} 0\}$. On obtient alors l'équivalence pour un monoïde S entre : *être un coidéal* et *donner par localisation un anneau local*.

Fait 1.3.2 *Tout homomorhisme* $\mathbf{A} \to \mathbf{B}$ *d'un anneau* $\mathbf{A}$ *vers un anneau local résiduellement discret* $\mathbf{B}$ *se factorise de manière unique par* $\mathbf{A}_{\mathcal{P}}$ *où* $\mathcal{P}$ *est l'image réciproque du radical* $\mathcal{R}(\mathbf{B})$ *($\mathcal{P}$ est un idéal premier détachable de* $\mathbf{A}$*).*

Un idéal I d'un anneau $\mathbf{A}$ est appelé un *idéal maximal* lorsque $1 \in I \Rightarrow 1 =_{\mathbf{A}} 0$ et l'anneau quotient est un corps. En pratique d'un point de vue constructif on est souvent plus à l'aise avec les idéaux premiers qu'avec les idéaux maximaux, et ces derniers *ne sont pas toujours* premiers.

Contrairement aux preuves en mathématiques classiques, nous n'utilisons en règle générale pas d'idéaux premiers ni maximaux en tant que tels, car nous n'avons pas en général de moyen explicite pour construire un idéal premier $\mathcal{P}$ contenant un idéal I et ne coupant pas un monoïde S (lorsque la condition de compatibilité $0 \notin S + I$ est vérifiée.)

Le nilradical $\mathcal{N}(\mathbf{A})$ et le radical (de Jacobson) $\mathbf{Rad}(\mathbf{A}) = \mathcal{R}(\mathbf{A})$ de $\mathbf{A}$ sont définis sans recours aux idéaux premiers ou maximaux en posant

$$\mathcal{N}(\mathbf{A}) = \{x \in \mathbf{A} \,;\, \exists n \;\; x^n =_{\mathbf{A}} 0\} \quad \text{et} \quad \mathcal{R}(\mathbf{A}) = \{x \in \mathbf{A} \,;\, \forall y \in \mathbf{A} \;\; 1 + xy \text{ est inversible}\}$$

Lorsque $\mathbf{A}$ est un anneau local, $\mathcal{R}(\mathbf{A})$ est l'ensemble des éléments noninversibles (pour le cas non commutatif voir théorème III.6.5 dans [30]).

Par ailleurs, nous remplaccons la considération de la localisation en n'importe quel idéal premier, par la considération de localisations en une famille finie de monoïdes comaximaux (cf. section 2).

1.4 Systèmes d'équations linéaires

Les anneaux cohérents

Un anneau $\mathbf{A}$ est dit *cohérent* si toute équation linéaire $LX = 0$ ($L \in \mathbf{A}^{1\times n}$, $X \in \mathbf{A}^{n\times 1}$) admet pour solutions les éléments d'un sous-$\mathbf{A}$-module de type fini de $\mathbf{A}^{n\times 1}$. Autrement dit

$$\forall L \in \mathbf{A}^{1\times n} \;\; \exists m \in \mathbb{N} \;\; \exists G \in \mathbf{A}^{n\times m} \;\; (LX = 0 \Leftrightarrow \exists Y \in \mathbf{A}^{m\times 1} \; X = GY)$$

On peut exprimer cette propriété de manière un peu plus abstraite en disant qu'un anneau est cohérent si tout idéal de type fini est de présentation finie (en tant que $\mathbf{A}$-module). De même, un $\mathbf{A}$-module est dit *cohérent* si tout sous-module de type fini est de présentation finie. Dans un anneau cohérent, tout système linéaire "sans second membre" $BX = 0$ ($B \in \mathbf{A}^{k\times n}$, $X \in \mathbf{A}^{n\times 1}$) admet pour solutions les éléments d'un sous-$\mathbf{A}$-module de type fini de $\mathbf{A}^{n\times 1}$: par exemple si $k = 2$ et B est constitué des lignes L et L' on a une matrice G telle que $LX = 0 \Leftrightarrow \exists Y \in \mathbf{A}^{m\times 1} \; X = GY$, et il reste à résoudre $L'GY = 0$ qui équivaut à $\exists Z \; Y = G'Z$ pour une matrice G' convenable. Donc $BX = 0$ si et seulement si X peut s'écrire sous forme $GG'Z$. En langage un peu plus abstrait :

Proposition 1.4.1 *Si un anneau* $\mathbf{A}$ *est cohérent, tout module* $\mathbf{A}^m$ *est cohérent.*

On en déduit immédiatement que tout $\mathbf{A}$-module de présentation finie est lui-même cohérent.

Dans un anneau cohérent et fortement discret, on sait résoudre toute équation linéaire $LX = c$ au sens suivant : on est capable de décider s'il y a une solution, et lorsqu'il y a une solution, décrire l'ensemble des solutions sous la forme $X_0 + GY$ (Y arbitraire dans $\mathbf{A}^{m\times 1}$). On en déduit, comme dans le cas homogène, qu'on sait résoudre tout système linéaire $BX = C$ (avec la même signification). En langage un peu plus abstrait :

Proposition 1.4.2 *Si un anneau* $\mathbf{A}$ *est cohérent et fortement discret, tout module* $\mathbf{A}^m$ *est cohérent et fortement discret.*

On en déduit immédiatement que tout $\mathbf{A}$-module de présentation finie est lui-même cohérent et fortement discret.

Les idéaux déterminantiels et le lemme de la liberté

On essaie souvent de ramener les questions concernant les solutions de systèmes d'équations linéaires sur un anneau arbitraire à des questions concernant des déterminants. C'est la base de la théorie de l'élimination.

Pour étudier un système linéaire qui s'écrit sous forme matricielle $GX = C$, un outil fondamental est la considération des idéaux déterminantiels de la matrice G et de ceux de la matrice $(G|C)$.

Définition 1.4.3 *Si G est une matrice arbitraire $\in \mathbf{A}^{q\times m}$, les* idéaux déterminantiels *de la matrice G sont les idéaux*

$$\mathcal{D}_n(G) := \textit{idéal engendré par les mineurs d'ordre } n \textit{ de la matrice } G$$

où n est un entier arbitraire. Pour $n \leq 0$ les mineurs sont par convention égaux à 1, pour $n > \min(m,q)$ ils sont par convention égaux à 0.

Les idéaux déterminantiels d'une matrice ne changent pas lorsqu'on modifie une ligne (resp. une colonne) en lui rajoutant une combinaison linéaire des autres lignes (resp. colonnes), ou encore si on rajoute ou supprime une ligne (resp. une colonne) nulle. Des faits essentiels sont les suivants.

Fait 1.4.4

- *Pour toute matrice $G \in \mathbf{A}^{q\times m}$ on a les inclusions*

$$\{0\} = \mathcal{D}_{1+\min(m,q)}(G) \subseteq \cdots \subseteq \mathcal{D}_1(G) \subseteq \mathcal{D}_0(G) = \mathbf{A}$$

- *Les idéaux déterminantiels ne dépendent que de la classe d'équivalence de la matrice*[4].
- *Si G et H sont des matrices telles que GH est définie, alors, pour tout $n \geq 0$ on a*

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

On parlera aussi des idéaux déterminantiels d'une application linéaire entre $\mathbf{A}$-modules libres de rangs finis, puisque ces idéaux ne dépendent pas de la matrice qui represente l'application linéaire.

L'égalité suivante est immédiate :

$$\mathcal{D}_n(\varphi \oplus \psi) = \mathcal{D}_n(\varphi) + \mathcal{D}_{n-1}(\varphi)\mathcal{D}_1(\psi) + \cdots + \mathcal{D}_1(\varphi)\mathcal{D}_{n-1}(\psi) + \mathcal{D}_n(\psi)$$

Le lemme facile suivant est très utile. Il donne une condition suffisante pour qu'un système linéaire donné se comporte exactement comme dans le cas où l'anneau est un corps-discret.

Lemme de la liberté *Soit M un module de présentation finie, (isomorphe au) conoyau d'une matrice G de type $q \times m$ (i.e. le module est donné par q générateurs soumis à m relations). Si la matrice G contient un mineur d'ordre k inversible et si $\mathcal{D}_{k+1}(G) = 0$, alors elle est équivalente à la matrice canonique*

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

En particulier, le module M est libre de rang $q-k$. En fait, dans ce cas, l'image, le noyau et le conoyau de G sont libres, respectivement de rangs k, $m-k$ et $q-k$. En outre l'image et le noyau possèdent des supplémentaires libres.

Preuve Supposons que le mineur d'ordre k inversible soit en position nord-ouest. La matrice extraite correspondante est inversible. En multipliant (à droite ou à gauche au choix) par une matrice inversible on est ramené à une matrice

$$\begin{pmatrix} \mathrm{I}_k & M \\ N & P \end{pmatrix}$$

Par manipulations élémentaires on se ramène à une matrice

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

Et comme l'idéal déterminantiel $\mathcal{D}_{k+1}$ n'a pas changé on a $Q = 0$. □

[4] En fait la relation d'équivalence qui intervient ici est un peu plus large, puisqu'on a aussi le droit de rajouter ou supprimer une ligne ou une colonne nulle.

Les identités de Cramer

Une identité fondamentale est le développement d'un déterminant selon une ligne ou une colonne, et ses nombreuses conséquences.

Une première conséquence, ce sont les *identités de Cramer* : si F est une matrice $\in \mathbf{A}^{n\times(n+1)}$, si C_j désigne la j-ème colonne et si δ_j est le mineur obtenu en supprimant la colonne C_j, on a $\sum_j (-1)^j \delta_j C_j = 0$.

Ces identités fournissent par exemple le Nullstellensatz de Hilbert et donc les premiers "théorèmes d'élimination" en géométrie algébrique.

Une autre conséquence, c'est pour une matrice carrée $G \in \mathbf{A}^{n\times n}$, l'identité $G\widetilde{G} = \det(G)\mathrm{I}_n$ où $\widetilde{G}$ désigne la matrice cotransposée de G. D'où le "truc du déterminant" (determinant trick), le théorème de Cayley-Hamilton et le lemme de Nakayama.

Les identités de Cramer admettent la forme généralisée suivante.

Lemme 1.4.5 (identités de Cramer) *Si F est une matrice $\in \mathbf{A}^{n\times(m+1)}$, avec $n \geq m$ et $\mathcal{D}_{m+1}(F) = 0$, si C_j désigne la j-ème colonne et si δ_j est le mineur obtenu sur les m premières lignes en supprimant la colonne C_j, on a*

$$\sum_j (-1)^j \delta_j C_j = 0.$$

Deux propositions célèbres sont contenues dans la suivante. Le point (1) décrit dans quelles conditions un système linéaire admet toujours une solution (quel que soit le second membre), le point (2) décrit dans quelles conditions un système linéaire admet au plus une solution (quel que soit le second membre).

Proposition 1.4.6 *Soit $\varphi : \mathbf{A}^m \to \mathbf{A}^q$ une application $\mathbf{A}$-linéaire de matrice $G \in \mathbf{A}^{q\times m}$.*

(1) *φ est surjectif si et seulement si $\mathcal{D}_q(G) = \mathbf{A}$ ([5]) (on dit alors que G est unimodulaire).*

(2) *φ est injectif si et seulement si $\mathcal{D}_m(G)$ ne divise pas zéro, c.-à-d. si l'annulateur de $\mathcal{D}_m(G)$ est réduit à $\{0\}$ ([6]).*

Preuve

(1) Si φ est surjectif, il admet un inverse à droite ψ de matrice H : $GH = \mathrm{I}_q$ et le fait 1.4.4 page ci-contre donne $\mathbf{A} \subseteq \mathcal{D}_q(G)\mathcal{D}_q(H)$, donc $\mathcal{D}_q(G) = \mathbf{A}$. Supposons maintenant $\mathcal{D}_q(G) = \mathbf{A}$. Notons $(u_1, \ldots, u_m)$ la première ligne de G et $C_1, \ldots, C_m$ les colonnes de G. En écrivant la combinaison linéaire des mineurs d'ordre q égale à 1 et en développant chacun de ces mineurs selon la première ligne, on obtient une relation $u_1v_1 + \cdots + u_mv_m = 1$. On rajoute à la matrice G une première colonne égale à $u_1C_1 + \cdots + u_mC_m$. On obtient une matrice G' qui a la même image que G. Par manipulations élémentaires de colonnes, on ramène la première ligne de G' à la forme $(1, 0, \ldots, 0)$. Par manipulations élémentaires de lignes, on ramène ensuite la première colonne de G' à la forme ${}^t(1, 0, \ldots, 0)$. La matrice $G_1 \in \mathbf{A}^{(q-1)\times m}$ dans le coin inférieur droit vérifie $\mathcal{D}_{q-1}(G_1) = \mathcal{D}_q(G') = \mathcal{D}_q(G) = \mathbf{A}$. On termine donc par récurrence sur q.

(2) Supposons que $\mathcal{D}_m(G)$ ne divise pas zéro. Notons e_i les vecteurs de la base canonique de $\mathbf{A}^m$. L'annulateur du vecteur $(\wedge^m\varphi)(e_1 \wedge \cdots \wedge e_m)$ (dont les coordonnées sont les mineurs d'ordre m de G) est donc réduit à 0. Soit $x = \sum_{1\leq i\leq m} \alpha_i e_i$. Si $\varphi(x) = 0$ alors

$$0 = \varphi(x) \wedge \varphi(e_2) \wedge \cdots \wedge \varphi(e_m) = \alpha_1 (\wedge^m\varphi)(e_1 \wedge \cdots \wedge e_m)$$

donc $\alpha_1 = 0$. Même raisonnement pour les autres α_i.

Supposons maintenant que φ soit injectif. Nous voulons montrer que l'annulateur de $(\wedge^m\varphi)(e_1 \wedge \cdots \wedge e_m) = f_1 \wedge \cdots \wedge f_m$ est nul ($f_i = \varphi(e_i)$). Nous savons que toute relation de dépendance linéaire entre les f_i est triviale (si $\sum_i \lambda_i f_i = 0$ alors $\sum_i \lambda_i e_i = 0$ donc les λ_i sont nuls). Il suffit donc de montrer par récurrence sur k la propriété suivante : si k vecteurs colonnes $x_1, \ldots, x_k$ de $A^{q\times 1}$ sont indépendants (i.e., toute relation de dépendance linéaire est triviale), alors l'annulateur du vecteur $x_1 \wedge \cdots \wedge x_k$

[5] Cela ramène le cas $q\times m$ au cas $1\times\binom{q}{m}$. En particulier, si φ est surjectif et $m < q$ alors $1 =_{\mathbf{A}} 0$.

[6] Cela ramène le cas $q\times m$ au cas $\binom{m}{q}\times 1$. En particulier, si φ est injectif et $m > q$ alors $1 =_{\mathbf{A}} 0$.

est réduit à 0. Pour $k = 1$ c'est trivial. Pour passer de k à $k+1$ nous raisonnons comme suit. Soit α un scalaire annulant $x_1 \wedge \cdots \wedge x_{k+1}$. Soit $I \subseteq \{1, \ldots, q\}$ un ensemble de k indices, nous notons $d_I(y_1, \ldots, y_k)$ le mineur extrait sur les lignes indexées par I pour des vecteurs colonnes $y_1, \ldots, y_k$ de $\mathbf{A}^{q\times 1}$. Puisque $\alpha(x_1 \wedge \cdots \wedge x_{k+1}) = (\alpha x_1) \wedge x_2 \wedge \cdots \wedge x_{k+1} = 0$, et vu le lemme 1.4.5 page précédente, on a

$$\alpha \cdot \left[-d_I(x_2, \ldots, x_k, x_{k+1}) \cdot x_1 + d_I(x_1, x_3, \ldots, x_{k+1}) \cdot x_2 - \cdots + (-1)^{k+1} d_I(x_1, \ldots, x_k) \cdot x_{k+1}\right] = 0$$

Or les x_i sont linéairement indépendants donc $\alpha \cdot d_I(x_1, \ldots, x_k) = 0$. Comme ceci est vrai pour tout I, cela donne $\alpha(x_1 \wedge \cdots \wedge x_k) = 0$. Et par l'hypothèse de récurrence $\alpha = 0$.

□

On déduit facilement du résultat précédent que, si φ est injective, les puissances extérieures de φ sont toutes injectives (en particulier $m > q \Rightarrow 1 =_{\mathbf{A}} 0$).

Le lemme de l'image libre donne une condition suffisante pour que les seconds membres pour lesquels un système linéaire donné admet au moins une solution soient exactement les combinaisons linéaires d'une famille de vecteurs indépendants.

Lemme de l'image libre *Soit* $\mathbf{A}$ *un anneau, soit* B *une matrice* $\in \mathbf{A}^{q\times m}$. *Supposons qu'il existe un mineur* δ_k *d'ordre* k *non diviseur de zéro qui engendre* $\mathcal{D}_k(B)$ *et que l'idéal déterminantiel* $\mathcal{D}_{k+1}(B)$ *soit nul. Alors la matrice* B *a pour image le sous-module* librement engendré *par les* k *colonnes correspondant au mineur* δ_k.

Preuve Les identités de Cramer où figure le mineur δ_k peuvent être simplifiées par δ_k puisque δ_k divise tout mineur d'ordre k et qu'il est non diviseur de zéro. Cela montre que le module image est engendré par les k colonnes de B correspondant au mineur δ_k.
Par ailleurs si $XC = 0$ est une relation de dépendance linéaire entre les k vecteurs colonnes de la sous matrice carrée X correspondant à ce mineur, alors $\delta_k C = 0$, or δ_k est non diviseur de zéro, donc $C = 0$. □

Le lemme suivant donne un système de conditions suffisant pour qu'un système linéaire donné admette au moins une solution (la dernière condition est clairement nécessaire).

Lemme 1.4.7 *Soit* $\mathbf{A}$ *un anneau arbitraire. Soit* B *une matrice* $\in \mathbf{A}^{m\times n}$ *et* C *un vecteur colonne* $\in \mathbf{A}^{m\times 1}$. *Le système linéaire* $BX = C$ *admet une solution dans* $\mathbf{A}^{n\times 1}$ *lorsque les conditions suivantes sont réalisées :*

- *Chaque idéal déterminantiel* $\mathcal{D}_k(B)$ *est de la forme* $\delta_k \mathbf{A}$, *où* δ_k *est un mineur d'ordre* k.
- *Chaque* δ_k *vérifie la condition :* $\forall y \in \mathbf{A}\ \ (y\delta_k = 0 \Rightarrow (\delta_k = 0 \vee y = 0))$.
- *Les idéaux déterminantiels de* $(B|C)$ *sont égaux à ceux de* B.

Preuve On commence avec $k = \inf(m, n)$. On écrit l'identité à la Cramer

$$\delta_k \times C = \delta_k \times (\text{une combinaison linéaire des colonnes de } B)$$

qui résulte de la nullité des idéaux déterminantiels d'indice $k+1$ et du fait que $\mathcal{D}_k(B|C)$ est engendré par δ_k. Vu le deuxième item, on est dans l'un des deux cas suivants :
— on peut simplifier la combinaison linéaire en divisant tout par δ_k, donc on a gagné,
— $\delta_k = 0$, mais alors on a gagné par induction.

Traitons un exemple avec $m = 5$, $n = 3$. On a un système linéaire

$$\left(\begin{array}{ccc|c} a_1 & b_1 & c_1 & d_1 \\ a_2 & b_2 & c_2 & d_2 \\ a_3 & b_3 & c_3 & d_3 \\ a_4 & b_4 & c_4 & d_4 \\ a_5 & b_5 & c_5 & d_5 \end{array}\right)$$

avec par hypothèse $\mathcal{D}_4(B|C) = 0$. Supposons que $\mathcal{D}_3$ est engendré par le mineur principal

$$\delta_3 = \begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix}$$

Explicitions le lemme 1.4.5. On a l'égalité de Cramer

$$\delta_3 \begin{pmatrix} d_1 \\ d_2 \\ d_3 \end{pmatrix} = \begin{vmatrix} d_1 & b_1 & c_1 \\ d_2 & b_2 & c_2 \\ d_3 & b_3 & c_3 \end{vmatrix} \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} + \begin{vmatrix} a_1 & d_1 & c_1 \\ a_2 & d_2 & c_2 \\ a_3 & d_3 & c_3 \end{vmatrix} \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix} + \begin{vmatrix} a_1 & b_1 & d_1 \\ a_2 & b_2 & d_2 \\ a_3 & b_3 & d_3 \end{vmatrix} \begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix}$$

et aussi en développant le déterminant 4×4 (nul) sur les 4 premières lignes selon la dernière ligne

$$\delta_3 d_4 = \begin{vmatrix} d_1 & b_1 & c_1 \\ d_2 & b_2 & c_2 \\ d_3 & b_3 & c_3 \end{vmatrix} a_4 + \begin{vmatrix} a_1 & d_1 & c_1 \\ a_2 & d_2 & c_2 \\ a_3 & d_3 & c_3 \end{vmatrix} b_4 + \begin{vmatrix} a_1 & b_1 & d_1 \\ a_2 & b_2 & d_2 \\ a_3 & b_3 & d_3 \end{vmatrix} c_4$$

La même chose se produit avec la cinquième ligne et on a bien (ce que dit le lemme 1.4.5)

$$\delta_3 \begin{pmatrix} d_1 \\ d_2 \\ d_3 \\ d_4 \\ d_5 \end{pmatrix} = \begin{vmatrix} d_1 & b_1 & c_1 \\ d_2 & b_2 & c_2 \\ d_3 & b_3 & c_3 \end{vmatrix} \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \end{pmatrix} + \begin{vmatrix} a_1 & d_1 & c_1 \\ a_2 & d_2 & c_2 \\ a_3 & d_3 & c_3 \end{vmatrix} \begin{pmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \end{pmatrix} + \begin{vmatrix} a_1 & b_1 & d_1 \\ a_2 & b_2 & d_2 \\ a_3 & b_3 & d_3 \end{vmatrix} \begin{pmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \end{pmatrix}$$

c'est-à-dire

$$\delta_3 \begin{pmatrix} d_1 \\ d_2 \\ d_3 \\ d_4 \\ d_5 \end{pmatrix} = \delta_3\alpha \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \end{pmatrix} + \delta_3\beta \begin{pmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \end{pmatrix} + \delta_3\gamma \begin{pmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \end{pmatrix}$$

Vue la condition que vérifie δ_3 on obtient l'alternative

$$\begin{pmatrix} d_1 \\ d_2 \\ d_3 \\ d_4 \\ d_5 \end{pmatrix} = \alpha \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \end{pmatrix} + \beta \begin{pmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \end{pmatrix} + \gamma \begin{pmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \end{pmatrix} \qquad \text{ou} \qquad \delta_3 = 0$$

Dans le deuxième cas, $\mathcal{D}_3 = 0$. On suppose alors que $\mathcal{D}_2$ est engendré par le mineur principal $\delta_2 = \begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix}$. On oublie la troisième colonne de la matrice (qui n'est plus utile). Les mêmes calculs conduisent alors à une égalité

$$\delta_2 \begin{pmatrix} d_1 \\ d_2 \\ d_3 \\ d_4 \\ d_5 \end{pmatrix} = \delta_2\alpha' \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \end{pmatrix} + \delta_2\beta' \begin{pmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \end{pmatrix}$$

Vue la condition que vérifie δ_2 on obtient l'alternative

$$\begin{pmatrix} d_1 \\ d_2 \\ d_3 \\ d_4 \\ d_5 \end{pmatrix} = \alpha' \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \end{pmatrix} + \beta' \begin{pmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \end{pmatrix} \qquad \text{ou} \qquad \delta_2 = 0$$

Etc... □

Le même raisonnement avec une modification mineure donne le lemme suivant.

Lemme 1.4.8 *Soit* $\mathbf{A}$ *un anneau arbitraire. Soit* B *une matrice* $\in \mathbf{A}^{n\times(n+1)}$. *On suppose que les conditions suivantes sont réalisées :*

- *Chaque idéal déterminantiel* $\mathcal{D}_k(B)$ *est de la forme* $\delta_k\mathbf{A}$, *où* δ_k *est un mineur d'ordre* k.
- *Chaque* δ_k *vérifie la condition :* $\forall y \in \mathbf{A}\ \ (y\delta_k = 0 \ \Rightarrow\ (\delta_k = 0 \ \vee\ y = 0))$.

Alors il existe une colonne de B *qui est combinaison linéaire des autres.*

2 Principes local-globals

2.1 Monoïdes comaximaux

Dans la suite, lorsqu'on parle d'un monoïde d'un anneau, on entend toujours une partie contenant 1 et stable pour la multiplication. Un monoïde S d'un anneau $\mathbf{A}$ est dit *saturé* lorsqu'on a l'implication

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

On note $\mathbf{A}_S$ le localisé $S^{-1}\mathbf{A}$ de $\mathbf{A}$ en S. Si S est engendré par $s \in \mathbf{A}$, on note $\mathbf{A}_s$ ou $\mathbf{A}[1/s]$ le localisé, qui est isomorphe à $\mathbf{A}[T]/(sT-1)$. Si on sature un monoïde, on ne change pas la localisation. Deux monoïdes sont dits *équivalents* s'ils ont même saturé.

Définition 2.1.1

(1) *Des monoïdes* $S_1,\dots,S_n$ *de l'anneau* $\mathbf{A}$ *sont dits* comaximaux *si un idéal de* $\mathbf{A}$ *qui coupe chacun des* S_i *contient toujours* 1, *autrement dit si on a :*

$$\forall s_1 \in S_1\ \cdots\ \forall s_n \in S_n\ \ \exists a_1,\dots,a_n \in \mathbf{A}\quad \sum_{i=1}^{n} a_i s_i = 1$$

(2) *On dit que* les monoïdes $S_1,\dots,S_n$ de l'anneau $\mathbf{A}$ recouvrent le monoïde S *si* S *est contenu dans les* S_i *et si un idéal de* $\mathbf{A}$ *qui coupe chacun des* S_i *coupe toujours* S, *autrement dit si on a :*

$$\forall s_1 \in S_1\ \cdots\ \forall s_n \in S_n\ \ \exists a_1,\dots,a_n \in \mathbf{A}\quad \sum_{i=1}^{n} a_i s_i \in S$$

En algèbre classique (avec l'axiome de l'idéal premier) cela revient à dire dans le premier cas que les ouverts de Zariski $\mathbf{U}_{S_i}$ recouvrent $\mathrm{Spec}(\mathbf{A})$ et dans le deuxième cas que les ouverts de Zariski $\mathbf{U}_{S_i}$ recouvrent l'ouvert $\mathbf{U}_S$. Du point de vue constructif, $\mathrm{Spec}(\mathbf{A})$ est un espace topologique connu via ses ouverts $\mathbf{U}_S$ mais dont les points sont souvent difficilement accessibles.

Un recouvrement de recouvrements est un recouvrement (calculs immédiats) :

Lemme 2.1.2 (1) *(associativité) Si les monoïdes* $S_1,\dots,S_n$ *de l'anneau* $\mathbf{A}$ *recouvrent le monoïde* S *et si chaque* S_ℓ *est recouvert par des monoïdes* $S_{\ell,1},\dots,S_{\ell,m_\ell}$, *alors les* $S_{\ell,j}$ *recouvrent* S.

(2) *(transitivité) Soit* S *un monoïde de l'anneau* $\mathbf{A}$ *et* $S_1,\dots,S_n$ *des monoïdes comaximaux de l'anneau* $\mathbf{A}_S$. *Pour* $\ell = 1,\dots,n$ *soit* V_ℓ *le monoïde de* $\mathbf{A}$ *formé par les numérateurs des éléments de* V_ℓ. *Alors les monoïdes* $V_1,\dots,V_n$ *recouvrent* S.
Plus généralement soient $S_0,\dots,S_n$ *des monoïdes de l'anneau* $\mathbf{A}_S$ *tels que* $S_1,\dots,S_n$ *recouvre* S_0 *dans* $\mathbf{A}_S$. *Pour* $\ell = 0,\dots,n$ *soit* V_ℓ *le monoïde de* $\mathbf{A}$ *formé par les numérateurs des éléments de* S_ℓ. *Alors les monoïdes* $V_1,\dots,V_n$ *recouvrent* V_0.

Définition et notation 2.1.3 *Nous noterons* $\mathcal{M}(U)$ *le monoïde engendré par l'élément ou la partie* U *de* $\mathbf{A}$, $\mathcal{I}_{\mathbf{A}}(I)$ *ou* $\mathcal{I}(I)$ *ou* $\langle I\rangle$ *l'idéal de* $\mathbf{A}$ *engendré par* I, *et* $\mathcal{S}(I;U)$ *le monoïde :*

$$\mathcal{S}(I;U) = \{v\ ;\ \exists u \in \mathcal{M}(U)\ \exists a \in \mathcal{I}(I)\ \ v = u + a\ \}$$

et de la même manière :

$$\mathcal{S}(a_1,\dots,a_k;u_1,\dots,u_\ell) = \{v\ ;\ \exists u \in \mathcal{M}(u_1,\dots,u_\ell)\ \exists a \in \mathcal{I}(a_1,\dots,a_k)\ \ v = u + a\ \}.$$

Nous disons qu'un tel monoïde admet une description finie.

Il est clair que si u est égal au produit $u_1 \cdots u_\ell$, les monoïdes $\mathcal{S}(a_1, \ldots, a_k; u_1, \ldots, u_\ell)$ et $\mathcal{S}(a_1, \ldots, a_k; u)$ sont équivalents.

Notez que lorsqu'on localise en $S_1 = \mathcal{S}(I; U)$, les éléments de U deviennent inversibles et ceux de I se retrouvent dans le radical de $\mathbf{A}_{S_1}$.

Notre sentiment est que la "bonne catégorie" serait celle dont les objets sont les couples $(\mathbf{A}, I)$ où $\mathbf{A}$ est un anneau commutatif et I un idéal contenu dans le radical de $\mathbf{A}$, et les flèches de $(\mathbf{A}, I)$ vers $(\mathbf{A}', I')$ sont les homomorphismes $f : \mathbf{A} \to \mathbf{A}'$ tels que $f(I) \subseteq I'$. On retrouve les anneaux usuels en prenant $I = 0$ et les anneaux locaux (avec la notion de morphisme local) en prenant I égal à l'idéal maximal. Pour "localiser" un objet $(\mathbf{A}, I)$ dans cette catégorie, on utilise un monoïde U et un idéal J de manière à former le nouvel objet $(\mathbf{A}_{\mathcal{S}(J;U)}, (I+J)\mathbf{A}_{\mathcal{S}(J;U)})$.

Le lemme fondamental suivant récupère la mise constructivement lorsqu'on relit avec un anneau arbitraire une preuve donnée dans le cas d'un anneau local.

Lemme 2.1.4 *Soit U et I des parties de l'anneau $\mathbf{A}$ et $a \in \mathbf{A}$, alors les monoïdes $\mathcal{S}(I; U, a)$ et $\mathcal{S}(I, a; U)$ recouvrent le monoïde $\mathcal{S}(I; U)$. En particulier les monoïdes $S = \mathcal{M}(a) = \mathcal{S}(0; a)$ et $S' = \mathcal{S}(a; 1) = 1 + a\mathbf{A}$ sont comaximaux.*

Preuve Pour $x \in \mathcal{S}(I; U, a)$ et $y \in \mathcal{S}(I, a; U)$ on doit trouver une combinaison linéaire $x_1 x + y_1 y \in \mathcal{S}(I; U)$ $(x_1, y_1 \in \mathbf{A})$. On écrit $x = u_1 a^k + j_1$, $y = (u_2 + j_2) - (az)$ avec $u_1, u_2 \in \mathcal{M}(U)$, $j_1, j_2 \in \mathcal{I}(I)$, $z \in \mathbf{A}$. L'identité fondamentale $c^k - d^k = (c-d) \times \cdots$ donne un $y_2 \in \mathbf{A}$ tel que $y_2 y = (u_2 + j_2)^k - (az)^k = (u_3 + j_3) - (az)^k$ et on écrit $z^k x + u_1 y_2 y = u_1 u_3 + u_1 j_3 + j_1 z^k = u_4 + j_4$. □

Principe local-global concret général 1 *Lorsqu'on relit une preuve explicite, donnée dans le cas où $\mathbf{A}$ est un anneau local résiduellement discret, avec un anneau $\mathbf{A}$ arbitraire, selon la méthode indiquée à la section 1.1, on considère au départ $\mathbf{A}$ comme $\mathbf{A} = \mathbf{A}_{\mathcal{S}(0;1)}$ et à chaque disjonction (pour un a qui se présente au cours du calcul dans le cas local)*

a est inversible ou a est dans le radical de $\mathbf{A}$,

on remplace l'anneau "en cours" $\mathbf{A}_{\mathcal{S}(I;U)}$ par les deux anneaux $\mathbf{A}_{\mathcal{S}(I;U,a)}$ et $\mathbf{A}_{\mathcal{S}(I,a;U)}$ (dans chacun desquels le calcul peut se poursuivre). Alors on obtient à la fin de la relecture, une famille finie d'anneaux $\mathbf{A}_{\mathcal{S}(I_j;U_j)}$ avec les monoïdes $\mathcal{S}(I_j; U_j)$ comaximaux qui admettent une description finie.
On remarquera que si $b = a/(u+i)$ avec $u \in \mathcal{M}(U)$ et $i \in \mathcal{I}(I)$ et si la disjonction porte sur " b est inversible ou b est dans le radical de $\mathbf{A}$ ", alors il faut considérer les localisés $\mathbf{A}_{\mathcal{S}(I;U,a)}$ et $\mathbf{A}_{\mathcal{S}(I,a;U)}$.

Les exemples suivants sont fréquents et résultent immédiatement des lemmes 2.1.2 et 2.1.4, sauf le premier qui se fait par un petit calcul simple.

Exemples 2.1.5 Soit $\mathbf{A}$ un anneau, U et I des parties de $\mathbf{A}$, $S = \mathcal{S}(I; U)$.

(1) Soient $s_1, \ldots, s_n \in \mathbf{A}$ des éléments comaximaux (c'est-à-dire tels que $\langle s_1, \ldots, s_n \rangle = \mathbf{A}$). Les monoïdes $S_i = \mathcal{M}(s_i)$ sont comaximaux.
Plus généralement, si $t_1, \ldots, t_n \in \mathbf{A}$ sont des éléments comaximaux dans $\mathbf{A}_S$, les monoïdes $\mathcal{S}(I; U, t_i)$ recouvrent le monoïde S.

(2) Soient $s_1, \ldots, s_n \in \mathbf{A}$. Les monoïdes $S_1 = \mathcal{S}(0; s_1)$, $S_2 = \mathcal{S}(s_1; s_2)$, $S_3 = \mathcal{S}(s_1, s_2; s_3)$, ..., $S_n = \mathcal{S}(s_1, \ldots, s_{n-1}; s_n)$ et $S_{n+1} = \mathcal{S}(s_1, \ldots, s_n; 1)$ sont comaximaux.
Plus généralement, les monoïdes $V_1 = \mathcal{S}(I; U, s_1)$, $V_2 = \mathcal{S}(I, s_1; U, s_2)$, $V_3 = \mathcal{S}(I, s_1, s_2; U, s_3)$, ..., $V_n = \mathcal{S}(I, s_1, \ldots, s_{n-1}; U, s_n)$ et $V_{n+1} = \mathcal{S}(I, s_1, \ldots, s_n; U)$ recouvrent le monoïde $\mathcal{S}(I; U)$.

(3) Si $S, S_1, \ldots, S_n \subseteq \mathbf{A}$ sont des monoïdes comaximaux et si $b = a/(u+i) \in \mathbf{A}_S$ alors $\mathcal{S}(I; U, a), \mathcal{S}(I, a; U), S_1, \ldots, S_n \in \mathbf{A}$ sont comaximaux.

2.2 Principes local-globals concrets

La notion de monoïdes comaximaux est intéressante en vertu des nombreux principes de recollement concret dans lesquels ils interviennent. Citons en deux particulièrement utiles

Principe local-global concret 2 *Soient $S_1, \ldots, S_n$ des monoïdes comaximaux de $\mathbf{A}$ et soit $a, b \in \mathbf{A}$. Alors on a les équivalences suivantes :*

(1) *Recollement concret des égalités :*

$$a = b \quad \text{dans} \quad \mathbf{A} \qquad \Longleftrightarrow \qquad \forall i \in \{1, \ldots, n\} \;\; a/1 = b/1 \quad \text{dans} \quad \mathbf{A}_{S_i}$$

(2) *Recollement concret des non diviseurs de zéro :*

$$\begin{array}{c} a \text{ est non diviseur de zéro dans } \mathbf{A} \qquad \Longleftrightarrow \\ \forall i \in \{1, \ldots, n\} \;\; a/1 \text{ est non diviseur de zéro dans } \mathbf{A}_{S_i} \end{array}$$

(3) *Recollement concret des inversibles :*

$$\begin{array}{c} a \text{ est inversible dans } \mathbf{A} \qquad \Longleftrightarrow \\ \forall i \in \{1, \ldots, n\} \;\; a/1 \text{ est inversible dans } \mathbf{A}_{S_i} \end{array}$$

(4) *Recollement concret des solutions de systèmes linéaires : soit B une matrice $\in \mathbf{A}^{m\times p}$ et C un vecteur colonne $\in \mathbf{A}^{m\times 1}$.*

$$\begin{array}{c} \text{Le système linéaire } BX = C \text{ admet une solution dans } \mathbf{A}^{p\times 1} \\ \Longleftrightarrow \\ \forall i \in \{1, \ldots, n\} \text{ le système linéaire } BX = C \text{ admet une solution dans } \mathbf{A}_{S_i}^{p\times 1} \end{array}$$

(5) *Recollement concret des solutions de systèmes linéaires sous conditions homogènes : soit B une matrice et C un vecteur colonne dont les entrées sont des indéterminées, soit enfin (φ_ℓ) une famille de polynomes homogènes (à coefficients dans $\mathbf{A}$) en les entrées de B et C. Dans chacune des deux implications ci-dessous, les entrées de B et C sont spécialisées dans l'anneau $\mathbf{A}$, et un $\forall$ est implicite devant l'implication.*

$$\begin{array}{c} (\wedge_\ell \, \varphi_\ell(B, C) =_{\mathbf{A}} 0) \;\Rightarrow \text{ le système } BX = C \text{ admet une solution dans } \mathbf{A}^{p\times 1} \\ \Longleftrightarrow \\ \forall i \in \{1, \ldots, n\} \;\; \left((\wedge_\ell \, \varphi_\ell(B, C) =_{\mathbf{A}_{S_i}} 0) \;\Rightarrow \text{ le système } BX = C \text{ admet une solution dans } \mathbf{A}_{S_i}^{p\times 1} \right) \end{array}$$

(6) *Recollement concret de facteurs directs : soit M un sous module de type fini d'un module de présentation finie N.*

$$\begin{array}{c} M \text{ est facteur direct dans } N \\ \Longleftrightarrow \\ \forall i \in \{1, \ldots, n\} \; M_{S_i} \text{ est facteur direct dans } N_{S_i} \end{array}$$

Preuve Nous prouvons que les conditions locales sont suffisantes. Le point (3) est un cas particulier de (4).

(1) Supposons que $a/1 = 0$ dans les $\mathbf{A}_{S_i}$. Pour des $s_i \in S_i$ convenables on a donc $s_i a = 0$ dans $\mathbf{A}$. Comme $\sum_{i=1}^n a_i s_i = 1$ on obtient $a = 0$ dans $\mathbf{A}$.

(2) Supposons que $a/1$ soit non diviseur de zéro dans les $\mathbf{A}_{S_i}$. Soit $b \in \mathbf{A}$ avec $ab = 0$ dans $\mathbf{A}$ donc aussi $ab/1 = 0$ dans les $\mathbf{A}_{S_i}$. On a donc $b/1 = 0$ les $\mathbf{A}_{S_i}$, donc aussi dans $\mathbf{A}$.

(4) Supposons que le système d'équations $BX = C$ admette une solution X_i dans chaque $\mathbf{A}_{S_i}^{p\times 1}$. On peut écrire $X_i = Y_i/s_i$ avec $Y_i \in \mathbf{A}^{p\times 1}$ et $s_i \in S_i$. On a donc $s_i' BY_i = s_i s_i' C$ dans $\mathbf{A}$ avec $s_i' \in S_i$. Comme $\sum_{i=1}^n b_i s_i s_i' = 1$ on obtient $B(\sum_{i=1}^n b_i s_i' Y_i) = C$ dans $\mathbf{A}$.

Commentaire sur le point (5) : le fait que la condition locale est suffisante est simplement un cas particulier de (4). Par contre l'homogénéité intervient pour montrer que la condition locale est nécessaire. Notez aussi que (1), (2), (3), (4) peuvent être vus comme des cas particuliers de (5).

(6) Soit $C = N/M$ et $\rho : N \to C$ la projection canonique. Le module C est également un module de présentation finie. Le module M est facteur direct dans N si et seulement si il existe une application linéaire $\psi : C \to N$ telle que $\rho\psi = \mathrm{Id}_C$. Si on considère les entrées des matrices qui représentent ψ comme des inconnues, cela donne un système linéaire dont les coefficients sont donnés en fonction des matrices qui représentent N et M (pour plus de précisions voir l'annexe II, paragraphe "Catégorie des modules de présentation finie" page 55). On peut donc appliquer le point (4). □

Certaines preuves des principes qui suivent sont dans l'annexe. Pour la notion constructive de module noethérien voir [30] III.2.

Principe local-global concret 3 (recollement concret de propriétés de finitude pour les modules) *Soient $S_1, \ldots S_n$ des monoïdes comaximaux de $\mathbf{A}$ et soit M un $\mathbf{A}$-module. Alors on a les équivalences suivantes :*

(1) *M est de type fini si et seulement si chacun des M_{S_i} est un $\mathbf{A}_{S_i}$-module de type fini.*

(2) *M est de présentation finie si et seulement si chacun des M_{S_i} est un $\mathbf{A}_{S_i}$-module de présentation finie.*

(3) *M est plat si et seulement si chacun des M_{S_i} est un $\mathbf{A}_{S_i}$-module plat.*

(4) *M est projectif de type fini si et seulement si chacun des M_{S_i} est un $\mathbf{A}_{S_i}$-module projectif de type fini.*

(5) *M est projectif de rang k si et seulement si chacun des M_{S_i} est un $\mathbf{A}_{S_i}$-module projectif de rang k.*

(6) *M est cohérent si et seulement si chacun des M_{S_i} est un $\mathbf{A}_{S_i}$-module cohérent.*

(7) *M est noethérien si et seulement si chacun des M_{S_i} est un $\mathbf{A}_{S_i}$-module noethérien.*

2.3 Premiers exemples

Rappelons que deux matrices carrées $m \times m$ sont dites *semblables* lorsqu'elles représentent le même endomorphisme de $\mathbf{A}^m$ sur deux bases (distinctes ou non).

Nous donnons une preuve "matricielle" du lemme de la liberté locale et lui faisons subir ensuite la machinerie de relecture locale-globale.

Lemme de la liberté locale *Soit $\mathbf{A}$ un anneau local. Tout module projectif de type fini sur $\mathbf{A}$ est libre de dimension finie. De manière équivalente : toute matrice de projection F de type $n \times n$ est semblable à une* matrice de projection standard, *c.-à-d. de la forme :*

$$\mathrm{I}_{k,n,n} = \begin{pmatrix} \mathrm{I}_k & 0_{k,n-n} \\ 0_{n-k,k} & 0_{n-k} \end{pmatrix}$$

Preuve par Azumaya Cette preuve ne suppose pas le corps résiduel discret. Elle est extraite de la preuve du théorème d'Azumaya III.6.2 dans [30], pour le cas qui nous occupe ici. Autrement dit, nous donnons le contenu "matriciel" de la preuve du lemme de la liberté locale dans [30]. Nous allons diagonaliser la matrice F. La preuve fonctionne avec un anneau local non nécessairement commutatif. Appelons f_1 le vecteur colonne $f_{1..n,1}$ de la matrice F, et $e_1, \ldots, e_n$ la base canonique de $\mathbf{A}^n$.
– Premier cas, $f_{1,1}$ est inversible. Alors $f_1, e_2, \ldots, e_n$ est une base de $\mathbf{A}^n$. Par rapport à cette base l'endomorphisme φ a une matrice :

$$G := \begin{pmatrix} 1 & li \\ 0_{n-1,1} & F_1 \end{pmatrix}$$

En écrivant $G^2 = G$ on obtient $F_1^2 = F_1$ et $F_1 li = 0$. On a alors :

$$LGL^{-1} := \begin{pmatrix} 1 & li \\ 0_{n-1,1} & \mathrm{I}_{n-1} \end{pmatrix} \begin{pmatrix} 1 & li \\ 0_{n-1,1} & F_1 \end{pmatrix} \begin{pmatrix} 1 & -li \\ 0_{n-1,1} & \mathrm{I}_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & 0_{1,n-1} \\ 0_{n-1,1} & F_1 \end{pmatrix}$$

– Deuxième cas, $1 - f_{1,1}$ est inversible. Alors $e_1 - f_1, e_2, \ldots, e_n$ est une base de $\mathbf{A}^n$. Par rapport à cette base, $\mathrm{Id}_n - \varphi$ a une matrice :

$$G := \begin{pmatrix} 1 & li \\ 0_{n-1,1} & F_1 \end{pmatrix}$$

avec $G^2 = G$. Avec le même calcul que dans le cas précédent, $\mathrm{I}_n - F$ est donc semblable à une matrice :

$$\begin{pmatrix} 1 & 0_{1,n-1} \\ 0_{n-1,1} & F_1 \end{pmatrix}$$

avec $F_1^2 = F_1$, ce qui signifie que F est semblable à une matrice :

$$\begin{pmatrix} 0 & 0_{1,n-1} \\ 0_{n-1,1} & H_1 \end{pmatrix}$$

avec $H_1^2 = H_1$.
On termine la preuve par induction sur n. □

Lorsqu'on relit la preuve précédente avec un anneau arbitraire **A** en employant la méthode indiquée dans la section 1.1 et explicitée dans le principe local-global concret général 1 page 17 on obtient le résultat suivant.

Théorème 1 *Soit* **A** *un anneau. Si M est un module projectif de type fini sur* **A** *il existe des éléments comaximaux s_i, tels que pour chaque i, le module M_{s_i} est libre sur l'anneau $\mathbf{A}_{s_i}$, avec une base finie explicite.*
De manière plus précise : pour toute matrice de projection F de type $n \times n$, il existe 2^n éléments comaximaux s_i, tels que pour chaque $i = 1, \ldots, 2^n$ la matrice F est semblable dans l'anneau $\mathbf{A}_{s_i}$ à une matrice de projection standard $\mathrm{I}_{k,n,n}$. *En outre, le nombre de s_i correspondant à un module libre de rang k est égal à $\binom{n}{k}$.*

Ceci donne donc une version renforcée du principe de recollement concret des modules projectifs de type fini : on peut s'arranger pour que les localisations en des monoïdes comaximaux convenables soient libres. Nous explicitons maintenant la preuve.

Preuve On reprend la preuve du lemme de la liberté locale. A la première étape, on considère deux localisés de **A** : $\mathbf{A}_{f_{11}}$ et $\mathbf{A}_{1-f_{11}}$. Pour chacun de ces deux anneaux, le premier pas de la diagonalisation de F fonctionne. En suivant la preuve pas à pas, on crée 2^n monoïdes comaximaux S_j de **A** (appliquer l'associativité et la transitivité des recouvrements ou le point (1) dans les exemples 2.1.5). La matrice F est diagonalisable sur chacun des $\mathbf{A}_{S_j}$ et le nombre des j pour lesquels il y a k fois 1 et $n-k$ fois 0 sur la diagonale est égal à $\binom{n}{k}$. Enfin on remarque que si F est diagonalisable sur $\mathbf{A}_{S_j}$ elle est aussi diagonalisable sur $\mathbf{A}_{s_j}$ pour un s_j convenable dans S_j. □

Remarquez qu'il est tout à fait possible que, dans la preuve précédente, la plupart des localisés $\mathbf{A}_{S_j}$ soient triviaux. Néanmoins, la preuve foinctionne sans qu'on ait besoin de savoir pour quels S_j cela se produit.

Lemme de l'équivalence locale *Soit* **A** *un anneau local résiduellement discret. Une matrice G de type $q \times m$ à coefficients dans* **A** *est équivalente (sur* **A***) à une matrice :*

$$\begin{pmatrix} \mathrm{I}_k & 0_{k,m-k} \\ 0_{q-k,k} & G' \end{pmatrix}$$

où G' a tous ses coefficients dans l'idéal maximal de **A**.
Tout module de présentation finie sur **A** *peut être présenté par (i.e., est isomorphe au conayau d') une matrice G' de ce type.*

Preuve On considère un mineur résiduellement inversible d'ordre maximum k dans G : la matrice G contient un mineur d'ordre k inversible et tous les mineurs d'ordre $(k+1)$ sont noninversibles. Alors elle est équivalente à une matrice de la forme

$$\begin{pmatrix} \mathrm{I}_k & 0_{k,m-k} \\ 0_{q-k,k} & G' \end{pmatrix}$$

Et tous les coefficients de G' sont des combinaisons linéaires de mineurs d'ordre $k+1$ de G.
Notez que les matrices de passage P et Q se calculent explicitement à partir de G une fois qu'on a repéré un mineur d'ordre k inversible, tous les mineurs d'ordre $k+1$ étant noninversibles. □

Lorsqu'on relit la preuve précédente avec un anneau arbitraire **A** en employant la méthode indiquée dans la section 1.1 et explicitée dans le principe local-global concret général 1 page 17 on obtient le résultat suivant.

Corollaire 2.3.1 (Lemme de l'equivalence locale, version globale) *Soit* $\mathbf{A}$ *un anneau arbitraire et* G *une matrice* $\in \mathbf{A}^{q\times m}$. *Il existe une famille finie* (S_j) *de monoïdes comaximaux* $\mathcal{S}(I_j;U_j)$ *(avec* I_j *et* U_j *finis) vérifiant : pour chaque* j, *la matrice* G *est équivalente sur* $\mathbf{A}_{S_j}$ *à une matrice :*

$$\begin{pmatrix} \mathrm{I}_{k_j} & 0_{k_j,m-k_j} \\ 0_{q-k_j,k_j} & G_j \end{pmatrix}$$

où G_j *a tous ses coefficients dans le radical de* $\mathbf{A}_{S_j}$.
En outre les monoïdes comaximaux S_j *et les matrices* G_j *dépendent de manière uniforme de la matrice* G, *i.e., ils et elles peuvent être calculé(e)s dans* $\mathbb{Z}[g_{ij}]$ *avec des indéterminées* $g_{i,j}$ *comme entrées de la matrice* G, *puis le calcul se spécialise dans n'importe quel anneau commutatif.*

Preuve Sans détailler la machinerie de relecture constructive, on peut fournir directement une famille (S_j) sous la forme suivante. On range les mineurs $s_1,\dots,s_r$ de G par ordre de taille décroissante. On considère alors les monoïdes comaximaux $S_1 = \mathcal{S}(0;s_1)$, $S_2 = \mathcal{S}(s_1;s_2)$, $S_3 = \mathcal{S}(s_1,s_2;s_3)$, ..., $S_r = \mathcal{S}(s_1,\dots,s_{r-1};s_r)$ et $S_{r+1} = \mathcal{S}(s_1,\dots,s_r;1)$. Notez que l'entier r qui intervient ici est très grand. Il serait intéressant de savoir si la disjonction peut être réalisée avec beaucoup moins de monoïdes comaximaux. □

3 Premiers résultats concernant les modules plats

3.1 Définition et caractère local de la platitude

Définition 3.1.1 *Un* $\mathbf{A}$*-Module* M *est appelé un* module plat *si, pour toute relation de dépendance linéaire* $LX = 0$ *(où* $L \in \mathbf{A}^{1\times n}$ *et* $X \in M^{n\times 1}$*), on peut trouver un entier* m, *un élément* $Y \in M^{m\times 1}$ *et une matrice* $G \in \mathbf{A}^{n\times m}$ *qui vérifient :*

$$GY = X \quad \text{et} \quad LG = 0$$

(en langage intuitif, si il y a une relation de dépendance linéaire entre éléments de M *ce n'est pas la faute au module.)*

On peut noter que la définition ci-dessus ne correspond pas à un axiome dynamique au sens de [9, 20, 21, 22], à cause du $\exists m \in \mathbb{N}$, c'est-à-dire parce qu'on ne prévoit pas d'avance une borne pour l'entier m. Il serait utile de donner l'exemple d'un anneau pour lequel m peut être arbitrairement grand (selon le module plat considéré) pour un n fixé. Nous pensons que les méthodes de constructivisation des preuves classiques de [9, 20, 21, 22] s'appliquent aussi avec un axiome tel que celui qui gouverne la définition des modules plats.

Une première importante remarque est que l'explication qui est donnée pour la relation de dépendance linéaire $LX = 0$ dans la définition d'un module plat s'étend à un nombre fini de relation de dépendance linéaires.

Proposition 3.1.2 *Soit* M *un* $\mathbf{A}$*-module plat et une famille de* k *relations de dépendance linéaires écrites sous la forme* $LX = 0$ *où* $L \in \mathbf{A}^{k\times n}$ *et* $X \in M^{n\times 1}$. *Alors on peut trouver un entier* m, *un élément* $Y \in M^{m\times 1}$ *et une matrice* $G \in \mathbf{A}^{n\times m}$ *qui vérifient :*

$$GY = X \quad \text{et} \quad LG = 0$$

Preuve Notons $L_1,\dots,L_k$ les lignes de L. La relation de dépendance linéaire $L_1X = 0$ est expliquée par deux matrices G_1 et Y_1 et par deux égalités $X = G_1Y_1$ et $L_1G_1 = 0$. La relation de dépendance linéaire $L_2X = 0$ se réécrit $L_2G_1Y_1 = 0$ c'est-à-dire $L_2'Y_1 = 0$. Cette relation de dépendance linéaire s'explique sous la forme $Y_1 = G_2Y_2$ et $L_2'G_2 = 0$.
Donc $X = G_1Y_1 = G_1G_2Y_2$. Avec $L_1G_1G_2 = 0$ et $L_2G_1G_2 = L_2'G_2 = 0$. Le vecteur colonne Y_2 et la matrice $H_2 = G_1G_2$ expliquent donc les deux relations de dépendance linéaires $L_1X = 0$ et $L_2X = 0$. Il ne reste qu'à itérer le processus. □

Nous analysons maintenant du point de vue constructif le principe suivant en mathématiques classiques : un module est plat si et seulement si il l'est après localisation en n'importe quel idéal maximal.

Tout d'abord nous avons un principe de recollement concret des modules plats directement formulable en langage usuel, qui est donné en point (3) dans le principe local-global concret 3 page 18. Plus généralement, on a l'interprétation constructive suivante du caractère local de la platitude, un peu plus déroutante, car il ne semble pas qu'on puisse la formuler sans mettre au premier plan la notion de preuve. Nous en profitons pour donner aussi une preuve du point (3) dans le principe local-global concret 3.

Principe local-global dynamique 1 (Principe de preuve de la platitude par localisation) *Soit M un $\mathbf{A}$-module. Soit $LX = 0$ une relation de dépendance linéaire entre éléments de M (où $L \in \mathbf{A}^{1\times n}$ et $X \in M^{n\times 1}$). Pour trouver $m \in \mathbb{N}$, $Y \in M^{m\times 1}$ et une matrice $G \in \mathbf{A}^{n\times m}$ qui vérifient :*

$$X = GY \quad \text{et} \quad LG = 0 \qquad (*)$$

il suffit de le faire en évaluant dynamiquement $\mathbf{A}$ comme un anneau local résiduellement discret.

Preuve Supposons que l'évaluation dynamique ait donné le résultat souhaité. On a donc construit des monoïdes comaximaux $S_1, \ldots, S_r$ de $\mathbf{A}$ (avec une description finie) tels que l'on ait une solution (m_i, Y_i, G_i) pour $(*)$ avec chaque localisé $\mathbf{A}_{S_i}$.
Prouvons donc le point (3) dans le principe local-global concret 3. On peut écrire $Y_i = Z_i/s_i$, $G_i = H_i/s_i$ avec $Z_i \in M^{m_i\times 1}$, $G_i \in \mathbf{A}^{n\times m_i}$ et des s_i convenables $\in S_i$. On a alors $s_i' Z_i H_i = s_i'' X$ dans M et $s_i' L H_i = 0$ dans $\mathbf{A}$ pour certains s_i' et $s_i'' \in S_i$. On écrit $\sum_{i=1}^r b_i s_i'' = 1$ dans $\mathbf{A}$. On prend pour G la matrice obtenue en juxtaposant en ligne les matrices $b_i s_i' H_i$, et pour Y le vecteur obtenu en superposant en colonne les vecteurs Z_i. On obtient $GY = \sum_{i=1}^r b_i s_i'' X = X$ et $LG = 0$ dans M et $\mathbf{A}$. □

Notre thèse est que le principe classique qui affirme le caractère local de la platitude ne contient rien d'autre que la proposition ci-dessus. Il s'agit d'une thèse, qui se vérifie tous les jours en pratique, comme cela sera illustré dans les sections suivantes. Nous ne chercherons pas à formuler cette thèse de manière plus rigoureuse.

Notons en tout cas qu'on peut déduire, *en mathématiques classiques*, le principe local-global abstrait correspondant. Pour bien comprendre la preuve qui suit, il est préférable d'avoir lu [9]. Notez aussi que nous n'utiliserons pas ce principe abstrait dans la suite.

Principe local-global abstrait 1 *Un $\mathbf{A}$-module M est plat si et seulement si il est plat après localisation en n'importe quel idéal premier.*

Preuve Il faut montrer que la condition est suffisante. On considère une relation de dépendance linéaire $LX = 0$. Le couple $(\mathbf{A}, M)$ constitue un projet pour un couple (Anneau local, Module sur cet anneau). Puisque M est plat après localisation en n'importe quel idéal premier, le théorème de complétude de Gödel implique qu'il y a une preuve du fait que l'égalité $LX = 0$ peut être analysée via une matrice G vérifant $LG = 0$ et $GY = X$ dans la théorie formelle correspondante (pour laquelle il suffit de considérer les modèles où l'anneau est remplacé par un localisé local arbiraire de $\mathbf{A}$). Comme les axiomes des anneaux locaux résiduellement discrets (et ceux des modules) sont dynamiques, et comme ce qui doit être prouvé est formulable de manière dynamique, la preuve peut être transformée en une évaluation dynamique qui prouve l'existence de G. Cela signifie exactement que nous sommes ramenés dans les conditions d'utilisation du principe local-global dynamique 1. □

Ce genre de preuve peut être répété dans des situations très variées. Cela montre que l'utilisation du tiers exclu et du lemme de Zorn en algèbre classique peut souvent être comprise comme une manière de cacher (inconsciemment) des calculs explicites dans des théorèmes abstraits en utilisant judicieusement le théorème de complétude de Gödel.

Notons enfin qu'en mathématiques classiques, puisque tout idéal premier est contenu dans un idéal maximal, on peut remplacer sans dommage "idéal premier" par "idéal maximal" dans le principe local-global abstrait précédent. Il serait intéressant d'avoir un exemple où cette restriction de l'hypothèse

sert à simplifier vraiment une preuve d'un fait concret, de manière à essayer d'analyser ce qui se passe alors du point de vue constructif.

3.2 Modules plats de type fini

Généralités

Dans le cas où le module est de type fini, la platitude devient une propriété purement dynamique (cf. [9, 20, 21]) comme le montre le point (1) du lemme suivant.

Lemme 3.2.1 *On considère un* $\mathbf{A}$*-module* M *de type fini, et* $X \in M^{n\times 1}$ *un vecteur colonne ayant pour entrées un système générateur* $x_1, \ldots, x_n$ *de* M.

(1) *Le module* M *est plat si et seulement si pour toute relation de dépendance linéaire* $LX = 0$ *(où* $L \in \mathbf{A}^{1\times n}$*), on peut trouver deux matrices* $G, H \in \mathbf{A}^{n\times n}$ *qui vérifient :*

$$H + G = \mathrm{I}_n, \quad LG = 0 \quad \text{et} \quad HX = 0$$

(2) *Si* $\mathbf{A}$ *est un anneau local, si* M *est plat et si* $LX = 0$*, on obtient l'alternative :* $L = 0$ *ou l'un des* x_i *dépend linéairement des autres (il peut donc être supprimé sans changer* M*.)*

(3) *Si* $\mathbf{A}$ *est un anneau arbitraire, si* M *est plat et si* $LX = 0$*, il existe* $n+1$ *éléments* $s_0, \ldots, s_n$ *tels que* $s_0 + \cdots + s_n = 1$*,* $L = 0$ *dans* $\mathbf{A}_{s_0}$ *et* x_k *dépend linéairement des autres* x_j *dans* $\mathbf{A}_{s_k}$ *pour* $k = 1, \ldots, n$.

(4) *Si* $\mathbf{A}$ *est un anneau arbitraire, si* M *est plat et si* $LX = 0$*, il existe* $n+1$ *éléments* $s_0, \ldots, s_n$ *et* $n^2 - n$ *éléments* a_{ij} *(*$i \neq j \in \{1, \ldots, n\}$*) tels que* $s_0 + \cdots + s_n = 1$*,* $s_0 L = 0$ *et* $s_k x_k = \sum_{j\neq k} a_{kj} x_j$ $(k = 1, \ldots, n)$.

Preuve (1) On ramène une relation de dépendance linéaire arbitraire $L'X' = 0$ à une relation de dépendance linéaire $LX = 0$ en exprimant X' en fonction de X. A priori on devrait écrire X sous forme $G_1 Y$ avec $LG_1 = 0$. Comme $Y = G_2 X$ on prend $G = G_1 G_2$, $H = \mathrm{I}_n - G$.
(2) C'est un "determinant trick". On dit que $\det(G) = \det(\mathrm{I}_n - H)$ s'écrit $1 + \sum_{i,j} b_{i,j} h_{i,j}$. Donc $\det(G)$ ou l'un des $h_{i,j}$ est inversible. Dans le premier cas $Y = 0$, dans le deuxième, un des vecteurs x_i s'exprime en fonction des autres : puisque $HX = 0$ chaque ligne de H est une relation de dépendance linéaire entre les x_i.
Montrons (4), qui implique clairement (3). La preuve précédente prouve également (avec un anneau arbitraire) qu'il existe $n^2 + 1$ éléments comaximaux v_i tels qu'après localisation en l'un quelconque des v_i on ait $L = 0$ ou l'un des x_i dépend linéairement des autres.
Nous allons voir qu'on peut se ramener à seulement $n + 1$ localisations en des éléments comaximaux. On pose $s_0 = \det(G) = \det(\mathrm{I}_n - H)$ et les $h_{i,j}$ sont les v_ℓ, $\ell \in \{1, \ldots, n^2\}$. Puisque $GL = 0$ on a $s_0 L = 0$ dans $\mathbf{A}$.
Soit $I_1 \subseteq \{1, \ldots, n^2\}$ l'ensemble des indices ℓ pour lesquels on a : x_1 dépend linéairement de $x_2, \ldots, x_n$ dans $\mathbf{A}_{v_\ell}$. Cela donne pour chacun de ces indices une relation $v_\ell x_1 = \lambda_{2,\ell} x_2 + \cdots + \lambda_{n,\ell} x_n$([7]). On a de même $I_2, \ldots, I_n \subseteq \{1, \ldots, n^2\}$ et $\{1, \ldots, n^2\}$ est la réunion disjointe des I_k. On a la relation de comaximalité $1 = s_0 + v_1 u_1 + \cdots + v_{n^2} u_{n^2}$. On écrit pour chaque k

$$\left(\sum_{\ell\in I_k} v_\ell u_\ell\right) x_k = \left(\sum_{\ell\in I_k} u_\ell \lambda_{1,\ell}\right) x_1 + \cdots + \left(\sum_{\ell\in I_k} u_\ell \lambda_{n,\ell}\right) x_n$$

(sans terme en x_k dans le second membre) donc en posant (pour $k > 0$) $s_k = \sum_{\ell\in I_k} v_\ell u_\ell$ on a : $\sum_{k=0}^{n} s_k = 1$ et $s_k x_k$ est une combinaison linéaire des x_j $(j \neq k)$. □

[7] Nous n'avons pas besoin de mettre un exposant à v_ℓ vue la preuve du point (2). Mais s'il avait fallu en mettre un, cela marcherait quand même, avec une petite modification.

La preuve que nous venons de faire pour remplacer un grand nombre d'éléments comaximaux par un petit nombre d'autres éléments comaximaux est tout à fait générale, et c'est pratiquement la même que la preuve du principe de recollement concret des solutions de systèmes linéaires (principe local-global concret 2 (4)). Ici, au lieu de recoller (en une solution globale) les solutions locales d'un seul système linéaire, on recolle les solutions d'un système linéaire parmi $n+1$ (dans chaque localisation, un au moins de ces systèmes linéaires admet une solution) et on obtient $n+1$ localisations. Ceci pourrait faire l'objet d'une formulation un peu plus générale du principe local-global concret 2.

Nous pouvons donner une généralisation du point (1) du lemme précédent exactement dans le style de la proposition 3.1.2.

Proposition 3.2.2 *On considère un* $\mathbf{A}$*-module* M *plat de type fini, et* $X \in M^{n\times 1}$ *un vecteur colonne ayant pour entrées un système générateur* $x_1, \ldots, x_n$ *de* M*. Soit une famille de* k *relations de dépendance linéaires écrites sous la forme* $LX = 0$ *où* $L \in \mathbf{A}^{k\times n}$ *et* $X \in M^{n\times 1}$*. Alors on peut trouver une matrice* $G \in \mathbf{A}^{n\times n}$ *qui vérifie :*

$$GX = X \quad \text{et} \quad LG = 0$$

Preuve Faire à la proposition 3.1.2 ce que le lemme 3.2.1 (1) a fait à la définition 3.1.1. □

Modules plats de présentation finie

Rappelons d'abord un lemme sur les idéaux de type fini idempotents.

Lemme 3.2.3 *Si* J *est un idéal de type fini idempotent (i.e.,* $J = J^2$*) dans un anneau* $\mathbf{A}$*, alors* $J = \langle r\rangle$ *avec* $r^2 = r$ *entièrement déterminé par* J*.*

Preuve Pour l'existence, (cf. [31] chap. 4 exercice 11, p. 129) c'est encore un "determinant trick". On considère un système générateur $(a_1, \ldots a_q)$ de J et le vecteur $\mathbf{a} = (a_1, \ldots a_q)^T$. Puisque $a_j \in J^2$ pour $j = 1, \ldots, q$, il y a une matrice C de type $q \times q$ à coefficient dans J telle que $\mathbf{a} = C\mathbf{a}$, donc $(\mathrm{I}_q - C)\mathbf{a} = 0$. Si $d = \det(\mathrm{I}_q - C)$ on a $d\mathbf{a} = 0$ et $d = 1 - \delta$ avec $\delta \in J$. Donc $\mathbf{a} = \delta\mathbf{a}$, $J = \delta J$ et $d\delta = \delta - \delta^2 = 0$. Ainsi J est engendré par l'idempotent δ.
L'unicité est simple : si r et r' sont deux idempotents tels que $\langle r\rangle = \langle r'\rangle$, on a $r = r'x$ donc $rr' = r'^2x = r'x = r$, et pareillement $r'r = r'$. □

Le lemme de l'équivalence locale admet pour corollaire.

Proposition 3.2.4 *Soit* $\mathbf{A}$ *un anneau local résiduellement discret. Tout module de présentation finie plat est libre de rang fini*[8]*.*

Preuve D'après le lemme de l'équivalence locale page 20 le module est présenté par une matrice G' dont tous les coefficients sont dans $\mathcal{R}(\mathbf{A})$. Soit $I = \mathcal{D}_1(G')$ l'idéal engendré par les coefficients de G'. Le lemme 3.2.1, appliqué avec les relations de dépendance linéaires données par les colonnes de G', implique que $I^2 = I$. D'après le lemme 3.2.3 on a donc $I = \langle r\rangle$ avec $r^2 = r$. Puisque r est dans le radical $\mathcal{R}(\mathbf{A})$, $r = 0$ et G' est nulle. Le module est donc libre et son rang est égal au nombre de lignes de G'. □

Lorsqu'on relit la preuve de la proposition précédente avec un anneau arbitraire $\mathbf{A}$ en employant la méthode indiquée dans le principe local-global concret général 1 page 17 on obtient le résultat suivant. On notera, que dans le cas local, on obtient la proposition précédente dans une version renforcée puisqu'on supprime l'hypothèse que le $\mathbf{A}$ est résiduellement discret.

Théorème 2

(1) *Soit* $\mathbf{A}$ *un anneau commutatif arbitraire. Tout* $\mathbf{A}$*-module de présentation finie plat* M *est projectif de type fini.*

(2) *En outre, si* G *est une matrice de présentation de* M*, pour être certain que le module est plat, il suffit de tester la condition de platitude pour des combinaisons linéaires des colonnes en nombre fini qui ne dépendent que de la taille de* G *et qu'on peut préciser a priori.*

[8] Le rang k est un entier uniquement déterminé au sens suivant : $\mathbf{A}^k \simeq \mathbf{A}^h$ et $k \neq h$ impliquent $1 =_{\mathbf{A}} 0$.

Preuve On peut appliquer le principe de recollement concret des modules projectifs de type fini et il suffit donc de trouver des monoïdes comaximaux S_j tels que la localisation en chacun des S_j fasse de Coker(G) un module libre. Or c'est exactement ce que fait la relecture de la preuve de la proposition 3.2.4. Nous pouvons expliciter cette affirmation sous la forme suivante.
D'après le corollaire 2.3.1 il existe une famille finie (S_j) de monoïdes comaximaux qui admettent une description finie et qui vérifient : pour chaque j, la matrice G est équivalente sur $\mathbf{A}_{S_j}$ à une matrice :

$$\begin{pmatrix} \mathrm{I}_{k_j} & 0_{k_j,m-k_j} \\ 0_{q-k_j,k_j} & G_j \end{pmatrix}$$

où G_j a tous ses coefficients dans $\mathcal{R}(\mathbf{A}_{S_j})$. Soit $I_j = \mathcal{D}_1(G_j)$. Vue la platitude de Coker(G_j), le lemme 3.2.1, appliqué avec les relations de dépendance linéaires données par les colonnes de G_j, implique que $I_j^2 = I_j$. Donc I_j est engendré par un idempotent r_j qui est dans le radical de $\mathbf{A}_{S_j}$. Donc $r_j = 0$ et $G_j = 0$ dans $\mathbf{A}_{S_j}$.
On remarque enfin pour prouver le point (2) que la platitude de M n'a été utilisée qu'avec des relations de dépendance linéaires prédéfinies correspondant aux colonnes des G_j. □

On a le corollaire suivant.

Fait 3.2.5 *Si* **A** *est un anneau cohérent, un idéal principal* $\langle x \rangle$ *est plat si et seulement si il est projectif c'est-à-dire si et seulement si son annulateur* $J = \mathrm{Ann}(x)$ *est engendré par un idempotent.*

Remarque 3.2.6 Nous indiquons dans cette remarque une autre preuve du point (1) du théorème 2 page précédente. C'est la forme matricielle de la preuve proposée en exercice dans [30] (III.5 exercice 4 p.96).
Supposons que le $\mathbf{A}$-module M, engendré par $x_1, \ldots, x_q$, soit isomorphe au conoyau d'une matrice ${}^tL \in \mathbf{A}^{q\times m}$. Notons $X \in M^{m\times 1}$ le vecteur colonne ayant pour entrées les x_i. On a $LX = 0$ et toute relation de dépendance linéaire entre les x_i est une combinaison linéaire des lignes de L. En appliquant la proposition 3.2.2 on obtient une matrice G avec $X = GX$ et $LG = 0$. Cela donne $(\mathrm{I}_n - G)X = 0$. Donc chaque ligne de $\mathrm{I}_n - G$ est une combinaison linéaire des lignes de L : $\mathrm{I}_n - G = G_1 L$. Et $L(\mathrm{I}_n - G_1 L) = LG = 0$, c'est-à-dire $L = LG_1 L$. Cela donne $LG_1 = (LG_1)^2$ et le conoyau de ${}^tL$ est égal au conoyau du projecteur ${}^t(LG_1)$.
Cette preuve fonctionne aussi dans le cas non commutatif, et elle est en un certain sens plus simple que celle que nous avons donnée dans le cas commutatif, mais elle ne donne pas le point (2) du théorème 2.

Modules plats de type fini sur un anneau local et sur un anneau intègre

Classiquement, on a les résultats suivants : tout module plat de type fini sur un anneau local est libre, tout module plat de type fini sur un anneau intègre est projectif. Nous allons en donner des versions constructives. Comme d'habitude, le résultat classique découle du résultat constructif moyennant un appel simple au principe du tiers exclu.

Proposition 3.2.7 *Soit* **A** *un anneau local. Soit M module de type fini plat engendré par $x_1, \ldots, x_n$. Supposons que M soit fortement discret ou que l'existence de relations de dépendance linéaires non triviales soit explicite dans M. Alors M est librement engendré par une suite finie $x_{i_1}, \ldots, x_{i_k}$ (avec $k \geq 0$).*

Preuve Supposons d'abord que M soit fortement discret, on peut alors trouver une suite finie d'entiers $1 \leq i_1 < \cdots < i_k \leq n$ (où $k \geq 0$) tels que aucun des x_{i_ℓ} ne soit une combinaison linéaire des autres et tels que $x_{i_1}, \ldots, x_{i_k}$ engendrent M. Pour simplifier les notations, on suppose donc désormais que $k = n$, i.e., aucun des x_i n'est combinaison linéaire des autres. Le lemme 3.2.1 (2) nous dit alors que toute relation de dépendance linéaire entre les x_i est triviale.
Supposons maintenant que l'existence de relations de dépendance linéaires non triviales soit explicite dans M, c'est-à-dire que pour toute famille d'éléments de M, on sache dire s'il y a une relation de dépendance linéaire non triviale entre ces éléments et en fournir une le cas échéant. Alors en utilisant le lemme 3.2.1 (2) on peut supprimer un à un les éléments superflus dans la famille (x_i) sans changer

le module M, jusqu'à ce qu'il ne reste qu'une sous famille sans relation de dépendance linéaire non triviale. □

Notez que la preuve utilise l'hypothèse "M est fortement discret", ou "l'existence de relations de dépendance linéaires non triviales est explicite dans M" uniquement avec des familles extraites du système générateur (x_i). Par ailleurs chacune de ces hypothèses est trivialement vraie en mathématiques classiques.

Proposition 3.2.8 *Soit* $\mathbf{A}$ *un anneau intègre et* $\mathbf{K}$ *son corps de fractions. Soit* M *un* $\mathbf{A}$*-module plat de type fini engendré par* $x_1, \ldots, x_n$ *et* M' *l'espace vectoriel obtenu par extension des scalaires à* $\mathbf{K}$*. Supposons que l'on connaisse une base finie de* M' *(c'est-à-dire encore que* M' *soit fortement discret). Alors* M *est projectif.*

Preuve On applique la machinerie de preuve par localisation à la preuve du cas local analogue dans la proposition 3.2.7, c'est-à-dire essentiellement au lemme 3.2.1 (2). On obtient un nombre fini d'éléments comaximaux s_i, et la localisation en chaque s_i rend le module M libre. On applique ensuite le recollement concret des modules projectifs de type fini.
Prenons par exemple le cas où $n = 4$ et M' de dimension 2. On considère une relation de dépendance linéaire non triviale $LX = 0$. Puisque le module est plat, on a deux matrices $G, H \in \mathbf{A}^{4\times 4}$ avec $LG = 0$, $HX = 0$, $G + H = \mathrm{I}_4$. Si on localise en $\det(G)$, on obtient $L = 0$ donc $0 = 1$. Si on localise en une entrée h_{ij} de H, le module est engendré par les 3 éléments x_k avec $k \neq j$. On considère alors une relation de dépendance linéaire non triviale $L'X' = 0$ entre ces trois x_i. On applique la même technique, et on obtient après de nouvelles localisations, que le module est maintenant engendré par deux des x_i. Comme tous les anneaux construits par localisation sont triviaux ou des sous-anneaux de $\mathbf{K}$, il n'y a pas de relation de dépendance linéaire non triviale entre les deux x_i qui engendrent M après localisation. Donc le module est libre après chaque localisation. □

Platitude pour les sous modules de type fini d'un module libre

Nous donnons une petite variante de la proposition 3.2.7. Nous allons voir que du point de vue constructif, le résultat est maintenant assuré si l'anneau local $\mathbf{A}$ est discret.

Proposition 3.2.9 *Soit un anneau local discret* $\mathbf{A}$*, une matrice* $F \in \mathbf{A}^{n\times m}$ *et* M *le module image de* F*. Considérons les propriétés suivantes :*

(1) *M est plat.*

(2) *M est librement engendré par certaines colonnes de F.*

(3) *Il existe un entier $k \geq 0$ et un mineur s d'ordre k non diviseur de zéro tel que $\mathcal{D}_k(F) = s\mathbf{A}$ et $\mathcal{D}_{k+1}(F) = 0$.*

(4) *Il existe un entier $k \geq 0$ tel que $\mathcal{D}_{k+1}(F) = 0$ et $\mathcal{D}_k(F)$ est plat et non nul.*

On a

$$(1) \iff (2), \quad (3) \iff (4), \quad (3) \implies (2)$$

Preuve On a évidemment (2) $\Rightarrow$ (1) et (3) $\Rightarrow$ (4).
Montrons que (4) $\Rightarrow$ (3). Puisque l'anneau est local, l'idéal déterminantiel $\mathcal{D}_k(F)$ plat est engendré par un mineur s_k d'ordre k. Puisque $\mathbf{A}$ est discret et $s_k\mathbf{A}$ plat, s_k est nul ou non diviseur de zéro, or il est non nul par hypothèse.
On a (3) $\Rightarrow$ (2) d'après le lemme de l'image libre.
Montrons que (1) $\Rightarrow$ (2). Puisque $\mathbf{A}$ est discret, considérons un entier k tel qu'il existe un mineur s d'ordre k non nul et $\mathcal{D}_{k+1}(F) = 0$. Si $k < m$ appelons $C_1, \ldots, C_k$ les colonnes de F correspondant à s et soit C une autre colonne de F. On a une identité de Cramer

$$sC = \sum_i a_i C_i$$

Puisque $\mathcal{D}_{k+1}(F) = 0$, d'après le lemme 3.2.1 (2) et puisque $s \neq_{\mathbf{A}} 0$, cette relation de dépendance linéaire implique qu'une des colonnes de F peut être supprimée, après quoi on a de nouveau $\mathcal{D}_k(F) \neq 0$

et $\mathcal{D}_{k+1}(F) = 0$. On est ainsi ramené par induction au cas où $k = m$. Le module est alors librement engendré par les colonnes de F, car une relation de dépendance linéaire non triviale impliquerait (d'après le lemme 3.2.1 (2)) qu'une colonne s'exprime en fonction des autres, donc que $\mathcal{D}_k(F) = 0$. □

Si tous les idéaux déterminantiels de F sont plats, la condition (4) est vérifée puisque $0 = \mathcal{D}_{m+1}(F) \subseteq \mathcal{D}_m(F) \subseteq \cdots \subseteq \mathcal{D}_1(F) \subseteq \mathcal{D}_0(F) = 1$. La réciproque n'est pas vraie en général : si a est non diviseur de zéro dans $\mathbf{A}$, le module engendré par un vecteur colonne $C = \begin{pmatrix} a \\ b \end{pmatrix}$ est libre mais $\mathcal{D}_1(C)$ n'est pas nécessairement engendré par un seul élément. Ceci montre également que (3) est en général strictement plus fort que (1), et qu'une matrice peut avoir une image plate sans que cela soit vrai pour la matrice transposée. La platitude de l'image ne dépend donc pas seulement des idéaux déterminantiels de la matrice.

3.3 Idéaux plats de type fini et idéaux localement principaux

On étudie maintenant la platitude pour les idéaux de type fini. En mathématiques classiques, la proposition suivante est un corollaire immédiat de la proposition 3.2.7. En mathématiques constructives, il est nécessaire de fournir une nouvelle preuve, qui donne des informations algorithmiques de nature différente de celles données dans la preuve de la proposition 3.2.7. En effet, on ne fait plus les mêmes hypothèses concernant le caractère discret des choses.

Proposition 3.3.1 (Idéaux de type fini plats sur un anneau local) *Soit* $\mathbf{A}$ *un anneau local.*

(0) *Soit* $I = \langle x_1, \ldots, x_n \rangle$. *Si* I *est principal il est engendré par l'un des* x_j. *(Bezout toujours trivial sur un anneau local)*

(1) *Soit* $I = \langle x_1, \ldots, x_n \rangle$. *Si* I *est plat, il est principal, engendré par l'un des* x_j.

(2) *Un idéal principal* $\langle x \rangle$ *est plat si et seulement si* x *vérifie la propriété suivante*

$$\forall y \in \mathbf{A} \ \ (yx = 0 \ \Rightarrow \ (x = 0 \ \vee \ y = 0))$$

(3) *Supposons que* $\mathbf{A}$ *soit discret ou qu'on ait un test pour répondre à la question "*x *est-il non diviseur de zéro ?". Alors un idéal* $\langle x \rangle$ *est plat si et seulement si* x *est nul ou non diviseur de zéro, donc un idéal de type fini* I *est plat si et seulement si il est libre de rang* 0 *ou* 1.

Preuve (0) On a $I = \langle x_1, \ldots, x_n \rangle = z\mathbf{A}$, $z = a_1x_1 + \cdots + a_nx_n$, $zb_j = x_j$, donc $z(1 - \sum_j a_jb_j) = 0$. Si $1 - \sum_j a_jb_j$ est inversible, $I = 0 = \langle x_1 \rangle$. Si a_jb_j est inversible $I = \langle x_j \rangle$.

(1) On considère la relation de dépendance linéaire $x_2x_1 + (-x_1)x_2 = 0$. Soit $G = \begin{pmatrix} a_1 & \ldots & a_n \\ b_1 & \ldots & b_n \end{pmatrix}$ une matrice telle que $G \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ et $(x_2, -x_1)G = (0, 0)$. Si a_1 est inversible, l'égalité $a_1x_2 = b_1x_1$ montre que $I = \langle x_1, x_3, \ldots, x_n \rangle$. Si $1 - a_1$ est inversible, l'égalité $a_1x_1 + \cdots + a_nx_n = x_1$ montre que $I = \langle x_2, x_3, \ldots, x_n \rangle$. On termine par induction sur n.

(2) Une relation de dépendance linéaire concernant x est une égalité $yx = 0$. Si $\langle x \rangle$ est plat, il existe donc z vérifiant $xz = 0$ et $zy = y$. Si z est inversible $x = 0$, si $1 - z$ est inversible $y = 0$. Inversement si l'implication est vérifiée, étant donnée une relation de dépendance linéaire $yx = 0$ on prend $z = 1$ si $x = 0$ et $z = 0$ si $y = 0$. □

Lorsqu'on relit la preuve précédente du point (1) avec un anneau arbitraire $\mathbf{A}$ en employant la méthode indiquée dans le principe local-global concret général 1 page 17 on obtient le corollaire suivant.

Corollaire : On considère un anneau $\mathbf{A}$ *et un idéal* I *de type fini, engendré par* $x_1, \ldots, x_n, x_{n+1}$. *L'idéal* I *est un module plat si et seulement si il existe* 2^n *éléments comaximaux* s_i, *tels que pour chaque* $i = 1, \ldots, 2^n$ *il y a un entier* j *pour lequel* $I_{s_i} = I\mathbf{A}_{s_i} = x_j\mathbf{A}_{s_i}$ *et* $x_j\mathbf{A}_{s_i}$ *est plat (sur* $\mathbf{A}_{s_i}$*).*

En fait, en raisonnant comme au lemme 3.2.1 on peut améliorer ce résultat (voir la proposition 3.3.3 (3) et le corollaire 3.3.4 (3)).

En mathématiques classiques un idéal est dit *localement principal* s'il devient principal après localisation en n'importe quel idéal premier. Il semble difficile de fournir un énoncé équivalent qui fasse sens en mathématiques constructives. Néanmoins lorsqu'on se limite aux idéaux de type fini il n'y a pas de problème.

Définition 3.3.2 *Un idéal de type fini I d'un anneau $\mathbf{A}$ est dit* localement principal *s'il existe des monoïdes comaximaux $S_1, \ldots, S_n$ de $\mathbf{A}$ tels que I_{S_j} est principal dans $\mathbf{A}_{S_j}$.*

La propriété locale concrète dans la définition précédente, sans l'hypothèse que I est un idéal de type fini, implique évidemment que I est de type fini.

Proposition 3.3.3 (idéaux de type fini localement principaux) *Soit $I = \langle x_1, \ldots, x_n\rangle$ un idéal de type fini de $\mathbf{A}$. Les propriétés suivantes sont équivalentes:*

(1) *L'idéal I est localement principal.*

(2) *Il existe une famille d'éléments comaximaux (t_i) de $\mathbf{A}$ tels que pour tout i il existe $j \in \{1, \ldots, n\}$ $I_{t_i} = x_j \mathbf{A}_{t_i}$.*

(3) *Il existe n éléments s_i $(i = 1, \ldots, n)$ et $n^2 - n$ éléments $a_{i,j}$ $(i \neq j \in \{1, \ldots, n\})$ vérifiant les équations suivantes.*

$$\begin{array}{rcl} \sum_{i=1}^{n} s_i & = & 1 \\ s_i x_j & = & a_{i,j} x_i \quad i \neq j \in \{1, \ldots, n\} \end{array}$$

Preuve On a clairement (3) $\Rightarrow$ (2) $\Rightarrow$ (1).
Montrons qu'un idéal principal vérifie la condition (3). Supposons qu'on ait $\langle x_1, \ldots, x_n\rangle = \langle g\rangle$. On a $\sum b_i x_i = g$ et $g y_i = x_i$. Donc $y_i x_j = y_j x_i = g y_i y_j$. On a aussi $(\sum b_i y_i - 1)g = 0$. Posons $s = 1 - \sum b_i y_i$. On a $s x_i = s g y_i = 0$ pour tout i. On prend alors $s_i = b_i y_i$ pour $i < n$ et $s_n = b_n y_n + s$. Donc $\sum s_i = 1$, $s_i x_j = b_i y_j x_i$ pour $i < n$ et $s_n x_j = (b_n y_n + s) x_j = b_n y_j x_n$.
Montrons enfin qu'un idéal localement principal vérifie la condition (3). Cette propriété peut être vue comme l'existence d'une solution pour un système linéaire dont les coefficients s'expriment en fonction des générateurs x_i. On applique donc le principe de recollement concret des solutions de systèmes linéaires. □

HUM *La propriété $\bigwedge^2 I = 0$ est clairement vérifiée pour un idéal localement principal. Est-elle suffisante pour qu'un idéal de type fini soit localement principal ?*

Corollaire 3.3.4 (Idéaux de type fini plats sur un anneau quelconque)

- *Soit $I = \langle x_1, \ldots, x_n\rangle$ un idéal de type fini de $\mathbf{A}$. Les propriétés suivantes sont équivalentes:*
  (1) *L'idéal I est un module plat.*
  (2) *Après localisation en des éléments comaximaux convenables, l'idéal I est plat et principal.*
  (3) *Après localisation en n éléments comaximaux convenables, l'idéal I est plat et principal, engendré par l'un des x_i.*
- *Pour un anneau $\mathbf{A}$ les propriétés suivantes sont équivalentes:*
  (4) *Tout idéal de type fini est plat*
  (5) *Tout idéal de type fini est localement principal et tout idéal principal est plat.*

Avec un anneau arbitraire, d'après le lemme 3.2.1 (1), un idéal principal $I = \langle x\rangle$ est plat si et seulement si x vérifie la propriété suivante

$$\forall y \in \mathbf{A} \ (yx = 0 \implies \exists z \in \mathbf{A} \ (yz = 0 \ \wedge \ zx = x))$$

ou sous une forme plus symétrique

$$\forall y \in \mathbf{A} \ (yx = 0 \implies \exists s, z \in \mathbf{A} \ (s + z = 1 \ \wedge \ yz = 0 \ \wedge \ sx = 0))$$

qui peut se réinterpréter comme suit en termes de localisation en appelant $J = \mathrm{Ann}(x)$ l'idéal annulateur de x

$$J\mathbf{A}_{1+J} = 0$$

Cela implique $J^2 = J$. Remarquons qu'un idéal $\langle r \rangle$ engendré par un idempotent r est projectif donc plat. Comme un idéal idempotent de type fini est engendré par un idempotent (lemme 3.2.3), on retrouve le corollaire 3.2.5.

Remarque 3.3.5 Signalons aussi à titre de curiosité le résultat suivant dans lequel on suppose l'anneau seulement noethérien (on omet cohérent). Soit **A** un anneau noethérien. Un idéal principal $\langle x \rangle$ est plat si et seulement si son annulateur $J = \mathrm{Ann}(x)$ est idempotent. Dans ce cas $J = \mathrm{Ann}(x)$ est engendré par des idempotents.

Preuve On a déjà vu la partie directe. Supposons maintenant J idempotent. Soit $y \in J$ i.e., tel que $yx = 0$. Soit $J_1 = \langle y \rangle$. Puisque J est idempotent, il existe un idéal de type fini $J_2 \subseteq J$ tel que $J_1 \subseteq J_2^2 \subseteq J_2$. On construit ainsi une suite J_n d'idéaux de type fini $J_n \subseteq J$ avec $J_n \subseteq J_{n+1}^2 \subseteq J_{n+1}$. Lorsque $J_{n+1} = J_n$, on a J_n idempotent et de type fini, donc engendré par un idempotent r. On a donc $yr = y$ et $rx = 0$, cela donne l'élément $z = 1 - r$ cherché. □

Idéaux projectifs de type fini et idéaux inversibles

Définition 3.3.6 *Un idéal d'un anneau* **A** *est dit* inversible *lorsque, multiplié par un idéal convenable il donne un idéal principal engendré par un élément non diviseur de zéro.*

Soit **K** l'anneau total des fractions de **A**. On appelle *idéal fractionnaire* d'un anneau **A** un sous-**A**-module de **K** qui est contenu dans un module $(1/s)\mathbf{A}$ où s est non diviseur de zéro dans **A**. Tout sous-**A**-module de type fini de **K** est un idéal fractionnaire. Le produit de deux idéaux fractionnaires I et J est défini comme le **A**-module engendré par les xy où $x \in I$ et $y \in J$ (en fait le sous-groupe engendré est suffisant). Un idéal usuel de **A** est alors parfois appelé un idéal entier. Un idéal entier est inversible au sens de la définition 3.3.6 si et seulement si il est inversible dans le monoïde multiplicatif des idéaux fractionnaires de **A**. Le monoïde multiplicatif des idéaux fractionnaires de **A** peut aussi être construit à partir du monoïde multiplicatif des idéaux entiers de **A** en rajoutant formellement les inverses des idéaux principaux engendrés par des non diviseurs de zéro : comme ces derniers sont des éléments simplifiables, le monoïde des idéaux entiers s'identifie alors bien à une partie du monoïde des idéaux fractionnaires.

Lemme 3.3.7

(1) *Soient I et J deux idéaux d'un anneau* **A**. *Si $IJ = \langle c \rangle$ avec c non diviseur de zéro, il existe un entier $n > 0$ et des éléments $a_1, a_2, ..., a_n, b_1, b_2, ..., b_n$ de* **A** *tels que :*

$$(*)\quad I = \langle a_1, \ldots, a_n \rangle\,,\ J = \langle b_1, \ldots, b_n \rangle\,,\ c = \sum a_i b_i \text{ divise les } a_i b_j$$

(2) *Sous les mêmes hypothèses les idéaux I et J sont des* **A***-modules projectifs de type fini.*

(3) *Première réciproque : (on ne fait pas d'hypothèse sur c) si la condition $(*)$ est vérifiée on a $\langle a_1, \ldots, a_n \rangle \langle b_1, \ldots, b_n \rangle = \langle c \rangle$.*

(4) *Deuxième réciproque : si un idéal de* **A** *contient un non diviseur de zéro et est un* **A***-module projectif de type fini, c'est un idéal inversible, et la condition $(*)$ peut être réalisée pour n'importe quel système générateur $(a_1, a_2, ..., a_n)$ de I et n'importe quel élément c de I.*

(5) *Troisième réciproque : si un idéal de type fini I de* **A** *est localement principal, la condition $(*)$ peut être réalisée pour n'importe quel système générateur $(a_1, a_2, ..., a_n)$ de I et n'importe quel élément c de I.*

Preuve (1) Il est clair que I contient des éléments a_i et J contient des éléments b_i tels que $c = \sum a_i b_i$. Et c divise tout élément de IJ. Il reste donc à voir que tout $x \in I$ est dans $\langle a_1, \ldots, a_n \rangle$. On a $cx = \sum_i a_i b_i x$, et chaque $b_i x$ est un élément de IJ donc s'écrit cx_i avec $x_i \in \mathbf{A}$. Ainsi $cx = c \sum_i a_i x_i$. On peut simplifier par c puisque c ne divise pas zéro.
(2) On vient juste de voir que les formes linéaires (sur I) $\alpha_i : x \mapsto x_i = b_i x / c$ vérifient

$$\forall x \in I \quad x = \sum_i \alpha_i(x) a_i \qquad (**)$$

(3) C'est immédiat (ici il n'est pas exclu que c divise zéro).
(4) Soient $a_1, a_2, ..., a_n$ des générateurs de I et α_i des formes linéaires sur I vérifiant (**). Posons $b_i = \alpha_i(c)$. On a $c = \sum_i a_i b_i$ et pour tout couple (i,j) on a

$$a_i b_j = a_i \alpha_j(c) = \alpha_j(ca_i) = c\alpha_j(a_i)$$

donc la condition (*) est vérifiée.
(5) Réaliser la condition (*) équivaut à résoudre un système linéaire dont les coefficients sont c et les générateurs $a_1, \ldots, a_n$ de I. Or après localisation (en des éléments comaximaux) l'idéal devient égal à $\langle a_i \rangle$ et la solution du système linéaire est alors évidente (avec les b_j nuls pour $j \neq i$). On conclut par le point (4) du principe local-global concret 2 page 17. □

On notera qu'en fait tout idéal inversible est de rang 1, parce qu'il est contenu dans **A** et que son annulateur est réduit à zéro.

Le lemme 3.3.7 admet le corollaire suivant.

Proposition 3.3.8 *Dans un anneau, pour un idéal de type fini I contenant un non diviseur de zéro, les propriétés suivantes sont équivalentes:*

(1) *I est localement principal.*

(2) *I est inversible.*

(3) *I est un module projectif de type fini.*

(4) *I est un module de rang constant* 1.

HUM *On peut se demander si tout idéal de type fini localement principal et dont l'annulateur est réduit à zéro contient un non diviseur de zéro.*

Nous donnons maintenant une preuve directe qu'un idéal de type fini localement principal est projectif de type fini lorsqu'il est engendré par des non diviseurs de zéro, en construisant la matrice de projection correspondante.

Proposition 3.3.9 *Soit* **A** *un anneau et $\varphi : \mathbf{A}^n \to \mathbf{A}$ une forme linéaire $(y_i)_{1\leq i\leq n} \mapsto \sum_i c_i y_i$. Supposons que les c_i sont tous non non diviseurs de zéro et que l'idéal $I = \operatorname{Im}\varphi$ est localement principal. Précisément (cf. proposition 3.3.3 (3)) soient s_i $(i = 1, \ldots, n)$ et $a_{i,j}$ $(i \neq j \in \{1, \ldots, n\})$ vérifiant les équations suivantes.*

$$\begin{array}{rcl} \sum_{i=1}^n s_i & = & 1 \\ s_i c_j & = & a_{i,j} c_i \quad i \neq j \in \{1, \ldots, n\} \end{array}$$

Posons $a_{ii} = s_i$, notons P la matrice $(a_{ij})_{1\leq i,j\leq n}$ et $Q = \mathrm{I}_n - P$. Alors la matrice Q est une projection dont l'image est égale à $\operatorname{Ker}\varphi$.
En particulier Q est une matrice de présentation de I.

Preuve Montrons d'abord $a_{i,j}a_{k,\ell} = a_{i,\ell}a_{k,j}$ (pour tous les indices possibles). En effet, si on multiplie par $c_i c_k$ on obtient dans les deux cas $s_i s_k c_j c_\ell$. Montrons $P^2 = P$. En effet, si nous calculons le coefficient en position (i,j) dans P^2 nous obtenons

$$\sum_k a_{i,k}a_{k,j} = \sum_k a_{i,j}a_{k,k} = a_{i,j}\sum_k s_k = a_{i,j}.$$

Notons π la projection dont la matrice est Q. Montrons que $\varphi \circ \pi = 0$, c'est-à-dire $(c_1, \ldots, c_n)Q = 0$ ou encore $(c_1, \ldots, c_n)P = (c_1, \ldots, c_n)$. La coordonnée n°$k$ du premier membre est $\sum_i a_{i,k}c_i = \sum_i c_k s_i = c_k$. Montrons enfin que $\operatorname{Ker}\varphi \subseteq \operatorname{Im}\pi$, c'est-à-dire que toute relation $\sum_j \alpha_j c_j = 0$ s'obtient avec ${}^t(\alpha_1, \ldots, \alpha_n)$ comme combinaison linéaire des colonnes de Q. On a en effet en multipliant par s_i : $\sum_j \alpha_j s_i c_j = c_i(\sum_j \alpha_j a_{i,j}) = 0$, donc $\sum_j a_{i,j}\alpha_j = 0$. Donc $P\,{}^t(\alpha_1, \ldots, \alpha_n) = 0$ et ${}^t(\alpha_1, \ldots, \alpha_n) = Q\,{}^t(\alpha_1, \ldots, \alpha_n)$. □

3.4 Anneaux localement sans diviseur de zéro et modules sans torsion

Pour un anneau local $\mathbf{A}$ on a l'équivalence :

tout idéal principal est plat $\iff$ l'anneau est sans diviseur de zéro

Par ailleurs, la propriété pour un anneau d'être sans diviseur de zéro se comporte mal par recollement et celle pour un module d'être plat se comporte bien par localisation et recollement. Cela justifie la définition suivante :

Proposition et définition 3.4.1 *Un anneau* $\mathbf{A}$ *est dit* localement sans diviseur de zéro *lorsqu'il vérifie les propriétés équivalentes suivantes.*

(1) *Tout idéal principal de* $\mathbf{A}$ *est plat.*

(2) $\forall x, y \in \mathbf{A}\ \ (yx = 0 \ \Rightarrow\ \exists z \in \mathbf{A}\ (yz = 0 \ \wedge\ zx = x))$

(3) $\forall x, y \in \mathbf{A}\ \ (yx = 0$ *il existe des monoïdes comaximaux* $S_1, \ldots, S_k$ *tels que pour chaque* $i = 1, \ldots, k$ *on ait* $x = 0$ *ou* $y = 0$ *dans* $\mathbf{A}_{S_i}$.*)*

Notez qu'un anneau localement sans diviseur de zéro est réduit. Dans la littérature de lanque anglaise, on trouve parfois l'appellation *pf*-ring (principal ideals are flat) pour un anneau localement sans diviseur de zéro.

D'après le fait 3.2.5 on a :

Fait 3.4.2 *Un anneau cohérent est localement sans diviseur de zéro si et seulement si il est quasi intègre.*

Lemme 3.4.3 *Soit* $\mathbf{A}$ *un anneau localement sans diviseur de zéro. Soit* M *un* $\mathbf{A}$*-module plat,* $a \in \mathbf{A}$, $y \in M$ *tels que* $ay = 0$. *Alors il existe* $s \in \mathbf{A}$ *tel que* $as = 0$ *et* $sy = y$. *Autrement dit, tout sous-module monogène* $\mathbf{A}y$ *de* M *est plat.*

Preuve On a des éléments x_i de M et une égalité $y = \sum_i b_i x_i$ dans M avec $ab_i = 0$.
Puisque $ab_i = 0$, il existe u_i tel que $au_i = a$ et $u_i b_i = 0$.
On pose $t = u_1 \cdots u_n$ et $s = 1 - t$. Puisque $ta = a$, on a $as = 0$. Puisque $tb_i = 0$, on a aussi $ty = 0$ et $sy = y$. □

Définition 3.4.4 *Un* module sans torsion *est par définition un module* M *qui est réunion de sous modules plats.*

Lemme 3.4.5 *Soit* $\mathbf{A}$ *un anneau localement sans diviseur de zéro et* M *un* $\mathbf{A}$*-module.*

- *Les conditions suivantes sont équivalentes.*
  (1) M *est sans torsion.*
  (2) *Pour tout* $y \in M$, *le module* $\mathbf{A}y$ *est plat.*
  (3) *Pour tous* $a \in \mathbf{A}$, $y \in M$ *tels que* $ay = 0$, *il existe* $s \in \mathbf{A}$ *tel que* $as = 0$ *et* $sy = y$.
- *En particulier si* M *est sans torsion, son sous-module de torsion est réduit à zéro.*
- *Si* $\mathbf{A}$ *est quasi intègre,* M *est sans torsion si et seulement si son sous-module de torsion est réduit à zéro.*

Preuve Voyons l'équivalence donnée en premier. On a (1) $\Rightarrow$ (3) d'après le lemme 3.4.3, (3) $\Rightarrow$ (2) d'après le lemme 3.2.1(1) et (2) $\Rightarrow$ (1) est trivial. Pour le deuxième point on applique le (3) avec a non diviseur de zéro. Dans le troisième point, pour la réciproque, supposons $ay = 0$. Soit s l'idempotent annulateur de a et $r = 1 - s$. On a $a = sa$, $a' = r + a = r + as$ qui est non diviseur de zéro, et $a'sy = ay = 0$ donc $sy = 0$ (il est dans le sous-module de torsion). □

4 Anneaux de valuation, anneaux de Prüfer

On trouve des équivalents classiques des résultats que nous allons démontrer dans cette section concernant les anneaux de Prüfer, au moins pour le cas intègre, dans les exercices de [5, 6], dans [12] et dans [19].

Nous donnons ici un traitement constructif aussi bien du cas intègre que du cas général. Même dans le cas intègre, nous pensons que c'est la première fois que la version algorithmique de ces résultats classiques est complètement explicitée.

Nous espérons que la mise en forme constructive de ces résultats semblera également intéressante à la lectrice classique pour la simplicité et la généralité des méthodes mises en oeuvre.

4.1 Principe local-global pour les anneaux de Prüfer

Dans le cas d'un anneau non intègre, il semble que la définition suivante soit souvent acceptée pour les anneaux de Prüfer (cf. [14]). C'est en tout cas celle qui nous a paru la plus naturelle, vue l'importance centrale du concept de platitude en algèbre commutative. Un autre nom pour ces anneaux, dans la littérature est *anneau de dimension globale faible inférieure ou égale à un.*

Définition 4.1.1 *Un* anneau de Prüfer *est un anneau dont tous les idéaux de type fini sont plats. Un* anneau de valuation *est un anneau de Prüfer local.*

Notez qu'un anneau de Prüfer est localement sans diviseur de zéro, donc réduit. Un anneau qui est réunion filtrante de sous-anneaux de Prüfer est un anneau de Prüfer. D'après le fait 3.4.2 un anneau de Prüfer est cohérent si et seulement si il est quasi intègre.

Le principe de recollement concret suivant résulte du principe de recollement concret des modules de type fini et de celui des modules plats.

Principe local-global concret 4 (recollement concret des anneaux de Prüfer) *Soient $S_1, \ldots S_n$ des monoïdes comaximaux d'un anneau* **A**. *Alors* **A** *est un anneau de Prüfer si et seulement si chacun des $\mathbf{A}_{S_i}$ est un anneau de Prüfer. En particulier un produit fini d'anneaux de Prüfer est un anneau de Prüfer.*

En fait le caractère local de la platitude (principe local-global dynamique 1 page 22) nous donne même

Principe local-global dynamique 2 *Un anneau est un anneau de Prüfer si et seulement si lorsqu'on l'évalue dynamiquemennt comme anneau local résiduellement discret on obtient un anneau de valuation.*

et donc, en mathématiques classiques, le résultat suivant (que nous n'utiliserons pas dans cet article)

Principe local-global abstrait 2 *Un anneau est un anneau de Prüfer si et seulement si son localisé en n'importe quel idéal premier est un anneau de valuation.*

4.2 Anneaux de valuation

Un *anneau de Bezout* est par définition un anneau dans lequel tout idéal de type fini est principal (il suffit de le supposer pour les idéaux à deux générateurs).

Proposition 4.2.1 *Pour un anneau* **A** *les propriétés suivantes sont équivalentes:*

(1) **A** *est un anneau de Bezout local*

(2) *Pour tous $x, y \in \mathbf{A}$, x divise y ou y divise x.*

(3) **A** *est un anneau local et tout idéal $I = \langle x_1, \ldots, x_n \rangle$ est engendré par l'un des x_j.*

Preuve La proposition 3.3.1(0) donne l'équivalence des points (1) et (3). Le point (2) résulte trivialement de (3). Enfin (2) implique que **A** est local : supposons $x + y = 1$, si $x = ay$, y est inversible, de même si $y = bx$, x est inversible. □

Dans [16] Kaplanski appelle "valuation ring" un anneau de Bezout local et "valuation domain" un anneau de valuation (selon la terminologie de Bourbaki qui est maintenant la plus courante).

Proposition 4.2.2 *Pour un anneau* **A** *les propriétés suivantes sont équivalentes:*

(0) **A** *est un anneau de valuation.*

(1) **A** *est un anneau de Bezout local sans diviseur de zéro.*

(2) **A** *est réduit et pour tous $x, y \in \mathbf{A}$, x divise y ou y divise x.*

(3) **A** *est un anneau local sans diviseur de zéro et tout idéal* $I = \langle x_1, \ldots, x_n \rangle$ *est engendré par l'un des* x_j.

Preuve La proposition 3.3.1 étudie les idéaux de type fini plats sur un anneau local et donne l'équivalence des points (0), (1) et (3). On a (3) $\Rightarrow$ (2) car un anneau sans diviseur de zéro est réduit. Voyons enfin (2) $\Rightarrow$ (1). On sait déjà que **A** est local. Montrons que **A** est sans diviseur de zéro. Si $xy = 0$ et si $x = ay$ alors $ay^2 = 0$ donc $x^2 = 0$ donc $x = 0$, de même si $y = bx$ on a $y = 0$. □

Commentaire 4.2.3 Il est facile de voir que $\mathbb{Z}_p$ est un anneau de valuation si et seulement si on a le mini principe d'omniscience **LLPO** (cf. [7]). Il est évidemment fort triste que les entiers p-adiques *ne forment pas* un anneau de valuation. Cela montre que nos définitions ne sont sans doute pas encore vraiment les bonnes. Ce défaut n'est cependant pas rédhibitoire. D'une part nous sommes d'accord avec les mathématiciens classiques pour dire que **LLPO** implique que $\mathbb{Z}_p$ est un anneau de valuation. D'autre part, la plupart du temps, on n'a besoin que des éléments algébriques de $\mathbb{Z}_p$, qui forment un anneau de valuation fortement discret.

Le lemme 1.4.8 s'applique à toute matrice $\in \mathbf{A}^{n\times(n+1)}$ sur un anneau de valuation. On obtient donc :

Lemme 4.2.4 *Soit* **A** *un anneau de valuation,* M *un* **A***-module de type fini engendré par* n *éléments, et* $x_1, \ldots, x_{n+1} \in M$, *alors l'un des* x_j *est combinaison linéaire des autres. En particulier, deux systèmes générateurs minimaux de* M *ont le même nombre d'éléments.*

Le caractère discret d'un anneau de valuation possède plusieurs caractérisations constructives intéressantes, ce qui donne la propriété suivante sans équivalent classique.

Proposition 4.2.5 *Pour un anneau* **A** *trivial ou non trivial, les propriétés* (1.1) *à* (2.6) *sont équivalentes. Pour un anneau* **A** *arbitraire les propriétés* (2.1) *à* (2.6) *sont équivalentes.*

(1.1) **A** *est un anneau de valuation, discret.*

(1.2) **A** *est intègre, et si* $x, y \in \mathbf{A}$ *alors* x *divise* y *ou* y *divise* x.

(2.1) **A** *est un anneau local et tout idéal de type fini de* **A** *est libre de rang* 1 *ou* 0.

(2.2) **A** *est un anneau de valuation et tout élément de* **A** *est nul ou non diviseur de zéro.*

(2.3) **A** *est un anneau de valuation et tout élément* x *de* **A** *vérifie* $x = 0 \vee (x = 0 \Rightarrow 1 = 0)$.

(2.4) **A** *est un anneau local et tout idéal de type fini de* **A** *est projectif.*

(2.5) **A** *est un anneau de valuation cohérent.*

(2.6) **A** *est un anneau local et tout sous-module de type fini d'un module libre de rang fini est libre de rang fini.*

Preuve Les implications (1.1) $\Rightarrow$ (2.1) $\Rightarrow$ (2.4) $\Rightarrow$ (2.5) et l'équivalence (1.1) $\Leftrightarrow$ (1.2) sont claires. L'implication (2.5) $\Rightarrow$ (2.4) vient de ce que tout module de présentation finie plat est projectif de type fini. On a (2.1) $\Leftrightarrow$ (2.2) puisque l'idéal $\langle x \rangle$ est libre de rang 1 (resp. 0) si et seulement si x est non diviseur de zéro (resp. nul). Voyons (2.2) $\Leftrightarrow$ (2.3). Dans tout anneau on a "x non diviseur de zéro implique $(x = 0 \Rightarrow 1 = 0)$". Par ailleurs, dans un anneau sans diviseur de zéro soit x qui vérifie $(x = 0 \Rightarrow 1 = 0)$. Montrons qu'il est non diviseur de zéro. Soit y avec $yx = 0$. On a $y = 0$ ou $x = 0$. Dans le deuxième cas puisque $1 = 0$ on a aussi $y = 0$. Montrons que (2.4) $\Rightarrow$ (2.1). Supposons (2.4). Puisque les modules projectifs sont plats, l'anneau est un anneau de valuation. Un idéal de type fini est donc principal et projectif. Si $\langle x \rangle$ est un tel idéal, son annulateur est donc un idéal $\langle r \rangle$, où r est un idempotent. Puisque l'anneau est local, $r = 0$ ou $r = 1$. Si $r = 0$, $\langle x \rangle$ est libre de rang 1, et si $r = 1$, $x = 0$. On a donc montré l'équivalence des points (2.1) à (2.5).
L'implication (2.6) $\Rightarrow$ (2.4) est triviale et on sait que (2.1) $\Rightarrow$ (2.6) d'après le lemme de l'image libre. Enfin, lorsque **A** est trivial les 6 propriétés sont vraies, et lorsque **A** est non trivial, il est clair que (2.3) $\Rightarrow$ (1.1). □

Commentaire 4.2.6 1) L'hypothèse selon laquelle l'anneau **A** est trivial ou non trivial n'est pas très naturelle. Si on veut s'en débarasser, il faut remplacer dans (1.1) et (1.2) l'hypothèse "**A** est discret", c'est-à-dire $\forall x \in \mathbf{A}\ \ (x = 0 \text{ ou } \neg(x = 0))$ par la variante légèrement affaiblie suivante : $\forall x \in \mathbf{A}\ \ (x = 0 \text{ ou } (x = 0 \Rightarrow 1 = 0))$. On obtient alors les équivalences des 8 items sans hypothèse bizarre concernant **A** (en fait (1.1) devient (2.3)).
2) On a des exemples naturels d'anneaux locaux réduits et *non* discrets, par exemple le corps des réels $\mathbb{R}$. Par contre il semble difficile de donner un exemple naturel d'anneau de valuation *non* discret. On peut obtenir des exemples semi-pathologiques : soit **A** un anneau de valuation discret et S un monoïde. Alors le localisé $\mathbf{A}_S$ est un anneau de valuation mais il est discret seulement si on sait tester $0 \in S$, c.-à-d. s'il est trivial ou non trivial. Dans cet exemple le caractère non discret semble inessentiel, car les propriétés (2.1) à (2.6) restent vérifiées. On pourrait aussi considérer, lorsque **A** est résiduellement discret, un quotient $\mathbf{A}/P$ où P un un idéal qui hésite entre 0 et l'idéal maximal.

Définition 4.2.7 *Un anneau* **A** *est appelé un* domaine de valuation *si c'est un anneau de valuation discret (donc intègre) c'est-à-dire s'il vérifie les conditions équivalentes données à la proposition 4.2.5.*

On a facilement le lemme suivant.

Lemme 4.2.8 *Soit* **A** *un anneau de valuation.* **A** *est fortement discret si et seulement si il est discret et résiduellement discret, et cela équivaut aussi au fait que la relation de divisibilité est explicite (i.e.,* $\forall a, b \in \mathbf{A}$ (*(a divise b)* ou $\neg$*(a divise b)*)*)*

Pour résoudre un système linéaire $FX = B$ sur un anneau de valuation on peut utiliser la méthode du pivot, en choisissant comme premier pivot dans F une entrée qui divise toutes les autres. Il est clair que cette méthode est complètement explicite (i.e., elle décide s'il y a une solution) lorsque la relation de divisibilité est explicite. Avec la seule hypothèse que **A** est un anneau de Bezout local, cette méthode fournit une réduction $F = LDC$ où D est en forme diagonale de Smith, et L et C sont des produits de matrices élémentaires (une matrice élémentaire admet des 1 sur la diagonale et tous ses autres coefficients, sauf un seul, nuls). On peut noter que le coût algorithmique n'est guère plus élevé que dans le cas d'un corps-discret. Cela fournit le résultat suivant.

Proposition 4.2.9 *Soit* **A** *un anneau de Bezout local. Soit* $\varphi : \mathbf{A}^m \to \mathbf{A}^n$ *un homomorphisme entre modules libres de rangs finis.*

(1) *Pour des bases convenables, la matrice de* φ *est en forme diagonale de Smith. En particulier, tout module de présentation finie est isomorphe à un produit* $\prod_{i=1}^{n} \mathbf{A}/\langle a_i\rangle$ *où* a_i *divise* a_{i+1} *pour* $1 \leq i < n$ *(pour l'unicité, voir [30] chap. V, th. 2.4).*

(2) *Supposons en outre que* **A** *est réduit et discret, c'est-à-dire que c'est un domaine de valuation. Alors* $\operatorname{Ker}\varphi$ *et* $\operatorname{Im}\varphi$ *sont libres,* $\operatorname{Ker}\varphi$ *est facteur direct dans* $\mathbf{A}^m$*, et tout module de présentation finie est somme directe de son sous-module de torsion et d'un sous-module libre.*

4.3 Anneaux de Prüfer et modules sans torsion

Rappelons (cf. section 3.4) qu'un module est dit sans torsion s'il est réunion de sous-modules plats. En outre sur un anneau localement sans diviseur de zéro un module est sans torsion si et seulement si tout sous module monogène $\mathbf{A}x$ est plat. Donc sur un anneau localement sans diviseur de zéro un sous module d'un module sans torsion est sans torsion. Ceci donne l'implication (4) $\Rightarrow$ (3) dans le théorème suivant.

Théorème 3 *Pour un anneau* **A***, les propriétés suivantes sont équivalentes:*

(1) **A** *est un anneau de Prüfer (c'est-à-dire tout idéal de type fini est plat).*

(2) *Tout idéal est plat.*

(3) *Tout sous-module d'un module plat est plat.*

(4) **A** *est localement sans diviseur de zéro et tout module sans torsion est plat.*

Preuve Les implications (3) $\Rightarrow$ (2) $\Rightarrow$ (1) sont triviales.
Il reste à montrer que (1) $\Rightarrow$ (4). Soit M un module sans torsion sur un anneau de Prüfer. Nous voulons montrer qu'il est plat.
Supposons tout d'abord l'anneau local. Soit $LX = 0$ une relation de dépendance linéaire avec $L = (a_1, \ldots, a_m) \in \mathbf{A}^{1\times m}$ et $X \in M^{m\times 1}$. Sans perte de généralité, on suppose que $a_i = b_i a_1$ pour $i > 1$. La relation de dépendance linéaire se réécrit $a_1 y = 0$ avec $y = x_1 + b_2 x_2 + \cdots + b_m x_m$. Le sous module monogène $\mathbf{A}y$ est plat et l'anneau est local donc $a_1 = 0$ ou $y = 0$. Dans le premier cas $L = 0$. Dans le deuxième cas $X = HX$ et $LH = 0$ avec la matrice triangulaire H suivante :

$$H = \begin{pmatrix} 0 & -b_2 & -b_3 & \ldots & -b_m \\ 0 & 1 & 0 & \ldots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \ldots & \ldots & 0 & 1 \end{pmatrix}$$

Dans le cas d'un anneau de Prüfer arbitraire, on reprend le raisonnement précédent en utilisant les localisations (en des éléments comaximaux) qui rendent l'idéal $\langle a_1, \ldots, a_m\rangle$ engendré par l'un des a_i, données dans le corollaire 3.3.4. □

Si on rajoute la cohérence on obtient.

Théorème 4 *Pour un anneau* $\mathbf{A}$, *les propriétés suivantes sont équivalentes:*

(1) $\mathbf{A}$ *est un anneau de Prüfer cohérent.*
(2) *Tout idéal de type fini est projectif.*
(3) *Tout sous-module de type fini d'un module projectif de type fini est projectif de type fini.*
(4) *Tout noyau d'un homomorphisme entre modules projectifs de type fini est facteur direct.*
(5) *Tout noyau d'une forme linéaire sur un module* $\mathbf{A}^n$ *est facteur direct.*

Preuve On a évidemment (4) $\Rightarrow$ (5) et (3) $\Rightarrow$ (2). L'équivalence (1) $\Leftrightarrow$ (2) résulte de l'équivalence "projectif de type fini $\Leftrightarrow$ plat et de présentation finie". On a (1) $\Rightarrow$ (3) à partir de l'implication analogue dans le théorème précédent. Pour montrer (1) $\Rightarrow$ (4), on remarque que dans le cas local le résultat est donné par la proposition 4.2.9, et on applique la machinerie locale-globale explicitée dans le principe local-global concret général 1 page 17, avec le principe de recollement concret 2 (6). Enfin (5) $\Rightarrow$ (2) puisqu'un idéal de type fini n'est rien d'autre que l'image d'une forme linéaire définie sur un module libre de rang fini. □

Dans la littérature, un anneau vérifiant la propriété (2) est souvent appelé un *anneau semi-héréditaire.*

La propriété (4) dans le théorème précédent implique la propriété de décomposition suivante.

Proposition 4.3.1 *Soit* $\mathbf{A}$ *un anneau de Prüfer cohérent, et* P *un* $\mathbf{A}$*-module projectif de type fini engendré par* n *éléments.*

(1) *Le module* P *est somme directe de* n *sous modules isomorphes à des idéaux de type fini.*
(2) *Lorsque* $\mathbf{A}$ *est intègre et* P *de rang* ℓ, P *est somme directe de* ℓ *modules de rang* 1.

Preuve (1) Supposons que $P \oplus N = \mathbf{A}^n$. Notons $\lambda_i : x \mapsto x_i$ la i-ème forme coordonnée de A^n. Notons μ_i la restriction de λ_i à P. Par le point (4) du théorème 4 on sait que $P_1 = \operatorname{Ker}\lambda_1$ est un facteur direct de P. Et $P \simeq P_1 \oplus \operatorname{Im}\lambda_1$. En outre $\operatorname{Im}\lambda_1$ est un idéal de type fini de $\mathbf{A}$, et P_1 est facteur direct dans $\mathbf{A}^{n-1}$ (considérer la projection π dont P est le noyau, P_1 est le noyau de la restriction de π à $\mathbf{A}^{n-1}$, appliquer de nouveau le théorème 4(4)). On gagne donc par induction sur n.
(2) Dans le processus précédent, P est écrit comme somme directe d'idéaux de type fini engendrés respectivement par n, $n-1$, ..., 1 éléments (certains peuvent être nuls, naturellement). Lorsque $\mathbf{A}$ est discret, on peut supprimer les idéaux de type fini nuls dans la somme directe, et lorsque $\mathbf{A}$ est intègre, il reste des idéaux de type fini qui sont projectifs de rang 1 □

Le résultat (2) s'étend au cas de tous les anneaux de Prüfer cohérents en utilisant le fait qu'il sont quasi intègres (cf. 4.4.9).

4.4 Anneaux arithmétiques

Nous commenccons par une remarque banale mais très efficace :

Fait 4.4.1 *Soient I et J deux idéaux de type fini d'un anneau $\mathbf{A}$. Alors l'existence d'un idéal de type fini L tel que $IL = J$ est équivalente à l'existence d'une solution pour un système linéaire dont la taille et les coefficients dépendent uniquement des générateurs de I et de J.*

Preuve Soient $x_1, \ldots, x_n$ des générateurs de I et $y_1, \ldots, y_m$ des générateurs de J. Si L existe, pour chaque $j = 1, \ldots, m$ il existe des éléments $a_{i,j} \in L$ tels que

$$\sum_i a_{i,j} x_i = y_j.$$

Par ailleurs, pour chaque i, i', j on doit avoir $a_{i,j} x_{i'} \in J$, ce qui s'exprime par l'existence d'éléments $b_{i,i',j,j'} \in \mathbf{A}$ vérifiant

$$\sum_{j'} b_{i,i',j,j'} y_{j'} = a_{i,j} x_{i'}$$

Réciproquement, si on peut trouver des $a_{i,j}$ et $b_{i,i',j,j'} \in \mathbf{A}$ vérifiant les équations linéaires ci-dessus (dans lesquelles les x_i et y_j sont des coefficients), alors l'idéal L engendré par les $a_{i,j}$ vérifie bien $IL = J$. □

Un cas particulier utile est le suivant. La vérification est immédiate.

Fait 4.4.2 *Si $I = \langle x_1, x_2 \rangle$ et $J = \langle x_1 \rangle$, le système linéaire à résoudre pour trouver un idéal L vérifiant $IL = J$ est :*

$$(B|C) = \left(\begin{array}{ccc|c} x_1 & x_2 & 0 & x_1 \\ x_2 & 0 & x_1 & 0 \end{array}\right)$$

ou sous forme plus symétrique

$$(B'|C') = \left(\begin{array}{cccc|c} 1 & 1 & 0 & 0 & 1 \\ x_1 & 0 & x_2 & 0 & 0 \\ 0 & x_2 & 0 & x_1 & 0 \end{array}\right)$$

Définition 4.4.3 *Un anneau est appelé un* anneau arithmétique *si ses idéaux de type fini sont localement principaux.*

Un anneau de Bezout est arithmétique (voir preuve de la proposition 3.3.3). Une autre terminologie raisonnable pour anneau arithmétique serait : *anneau localement de Bezout.*

Exemple 4.4.4 Si $\mathbf{K}$ est un corps-discret, $\mathbf{K}[x]/(x^5)$ est un anneau local arithmétique, mais ce n'est pas un anneau réduit, et donc ce n'est pas un anneau de Prüfer.

On a immédiatement.

Fait 4.4.5 *Un quotient ou un localisé d'un anneau arithmétique est un anneau arithmétique. Si un anneau est arithmétique après localisation en une famille finie de monoïdes comaximaux il est arithmétique.*

On rappelle la notation $(I : J)_{\mathbf{A}} = I : J = \{x \in \mathbf{A} \mid xJ \subseteq I\}$.

Théorème 5 *Pour un anneau $\mathbf{A}$, les propriétés suivantes sont équivalentes:*

(1.1) $\mathbf{A}$ *est un anneau arithmétique.*

(1.2) *Tout idéal $I = \langle x_1, x_2 \rangle$ est localement principal.*

(1.3) *Tout idéal $I = \langle x_1, x_2 \rangle$ devient principal, engendré par x_1 ou x_2, après localisation en deux éléments comaximaux convenables s et t de $\mathbf{A}$.*

(1.4) *Pour tout idéal de type fini $I = \langle x_1, \ldots, x_n \rangle$ il existe n éléments s_i $(i = 1, \ldots, n)$ et $n^2 - n$ éléments $a_{i,j}$ $(i \neq j \in \{1, \ldots, n\})$ vérifiant les équations suivantes.*

$$\begin{array}{rcll} \sum_{i=1}^n s_i & = & 1 & \\ a_{i,j} x_i - s_i x_j & = & 0 & i \neq j \in \{1, \ldots, n\} \end{array}$$

(2.1) *Pour tous idéaux de type fini $J \subseteq I$, il existe un idéal de type fini L tel que $IL = J$*

(2.2) *Pour tout idéal $I = \langle x_1, x_2\rangle$, il existe un idéal $L = \langle y_1, y_2\rangle$ tel que $IL = \langle x_1\rangle$.*

(2.3) $\forall x_1, x_2 \in \mathbf{A}$ *le système linéaire suivant admet une solution :*

$$(B|C) = \begin{pmatrix} x_1 & x_2 & 0 & | & x_1 \\ x_2 & 0 & x_1 & | & 0 \end{pmatrix}$$

(2.4) $\forall x_1, x_2 \in \mathbf{A}$ *il existe $u \in \mathbf{A}$ tel que :*

$$\langle x_1\rangle \cap \langle x_2\rangle = \langle (1-u)x_1, ux_2\rangle$$

(3.1) *Pour tous idéaux de type fini I et J la suite exacte courte ci-après est scindée :*

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

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

(3.2) *Même chose en se limitant à des idéaux principaux.*

(4.1) *Pour tous idéaux de type fini I et J, $(I : J) + (J : I) = \langle 1\rangle$.*

(4.2) *Même chose en se limitant à des idéaux principaux.*

(5.1) (Théorème chinois) *Si $(J_k)_{k=1,\dots,n}$ est une famille finie d'idéaux de $\mathbf{A}$ et $(x_k)_{k=1,\dots,n}$ est une famille d'éléments de $\mathbf{A}$ vérifiant $x_k \equiv x_\ell \bmod J_k + J_\ell$ pour tous k, ℓ, alors il existe un $x \in \mathbf{A}$ tel que $x \equiv x_k \bmod J_k$ pour tout k.*

(5.2) *Même chose en se limitant aux idéaux de type fini.*

(5.3) *Même chose en se limitant au cas de trois idéaux principaux.*

Preuve

Les implications (2.1) $\Rightarrow$ (2.2) et (1.1) $\Rightarrow$ (1.2) sont triviales, et (2.2) $\Leftrightarrow$ (2.3) est le fait 4.4.2.
Pour (1.1) $\Leftrightarrow$ (1.4) et (1.2) $\Leftrightarrow$ (1.3), voir la proposition 3.3.3.
(1.2) $\Rightarrow$ (1.1). Si on a un idéal de type fini avec n générateurs, des localisations successives (chaque fois en des éléments comaximaux) le rendent principal. On conclut par transitivité et associativité des recouvrements.
(1.1) $\Rightarrow$ (2.1). Dans une localisation en s_i qui rend l'idéal I principal, puisque $J_{s_i} \subseteq I_{s_i}$ on a trivialement un idéal de type fini L_i tel que $I_{s_i}L_i = J_{s_i}$. On conclut par recollement concret des solutions de systèmes linéaires puisqu'on a le fait 4.4.1.
(2.3) $\Rightarrow$ (1.3) : si u, v, w est la solution du système linéaire donné en (2.3), lorsqu'on localise en u on a $I_u = x_1\mathbf{A}_u$ et lorsqu'on localise en $s = 1-u$ on a $I_s = x_2\mathbf{A}_s$.
(2.3) $\Rightarrow$ (2.4) : si u, v, w est la solution du système linéaire donné en (2.3), on a $(1-u)x_1 = vx_2$ et $-wx_1 = ux_2$ donc $\langle (1-u)x_1, ux_2\rangle \subseteq \langle x_1\rangle \cap \langle x_2\rangle$. Inversement si $z \in \langle x_1\rangle \cap \langle x_2\rangle$ on a $z = ax_1 = bx_2$ et donc

$$z = (1-u)z + uz = a(1-u)x_1 + bux_2$$

(2.4) $\Rightarrow$ (2.3) : si $\langle (1-u)x_1, ux_2\rangle \subseteq \langle x_1\rangle \cap \langle x_2\rangle$ on a évidemment des éléments v, w tels que $(1-u)x_1 = vx_2$ et $-wx_1 = ux_2$.
Les implications (3.1) $\Rightarrow$ (3.2) et (4.1) $\Rightarrow$ (4.2) sont triviales. Pour un anneau arithmétique les propriétés (3.1) et (4.1) sont immédiates dans le cas local, donc elles résultent facilement de (1.4) dans le cas général. On remarque en effet que la propriété pour la suite exacte d'être scindée (resp. pour la somme des deux idéaux d'être égale à $\langle 1\rangle$) équivaut à l'existence d'une solution pour un système linéaire.
(3.2) $\Rightarrow$ (2.3) : considérer $I = \langle x_1\rangle$ et $J = \langle x_2\rangle$. Une section éventuelle α pour σ est donnée par $\alpha(\pi(1)) = (\tilde{a}, \bar{b})$ où les éléments a et b doivent vérifier $a(I+J) \subseteq I$, $b(I+J) \subseteq J$ et $a+b \equiv 1 \bmod (I+J)$. Les deux premières conditions se réécrivent $ax_2 \in I$, $bx_1 \in J$. Si $a+b = 1+a_0+b_0$ avec $a_0 \in I$, $b_0 \in J$ alors, pour $t = a - a_0$ et $s = b - b_0$ on a $s+t = 1$, $sx_1 = vx_2$, $tx_2 = wx_1$.

(4.2) $\Rightarrow$ (2.3) est immédiat : considérer $I = \langle x_1 \rangle$ et $J = \langle x_2 \rangle$.
Montrons qu'un anneau arithmétique vérifie (5.2). Supposons tout d'abord l'anneau local. Les idéaux de type fini considérés sont alors totalement ordonnés par inclusion. Par exemple $J_1 \subseteq \cdots \subseteq J_n$ et donc $x_1 \equiv x_\ell \bmod J_\ell$ pour tout ℓ. La solution est alors donnée par $x = x_1$. Dans le cas d'un anneau arithmétique général, on applique la machinerie locale-globale, car il s'agit de trouver la solution d'un système linéaire sous conditions homogènes.
On a facilement (5.2) $\Leftrightarrow$ (5.1), et il reste à voir que que (5.3) implique (1.2). Soient $a, b \in \mathbf{A}$ et posons $c = a+b$, $J_1 = \langle a \rangle$, $J_2 = \langle b \rangle$, $J_3 = \langle c \rangle$, $x_1 = c$, $x_2 = a$ et $x_3 = b$. On a $J_1+J_2 = J_1+J_3 = J_3+J_2 = \langle a, b \rangle$ et les congruences $x_i \equiv x_k \bmod J_i + J_k$ sont vérifiées. On obtient qu'il existe u, v, w dans $\mathbf{A}$ tels que

$$c + ua = a + vb = b + wc$$

d'où

$$wb = (1 + u - w)a,\ (1 - w)a = (1 + w - v)b$$

Donc l'idéal $\langle a, b \rangle$ est localement principal. □

Anneaux arithmétiques fortement discrets

Proposition 4.4.6 *Un anneau arithmétique* $\mathbf{A}$ *est fortement discret si et seulement si la relation de divisibilité est explicite.*

Preuve La condition est clairement nécessaire. Montrons qu'elle est suffisante. On cherche à résoudre une équation linéaire $BX = c$. On considère (proposition 3.3.3) des éléments s_i et $a_{i,j}$ qui vérifient

$$\begin{array}{rcl} \sum_{i=1}^n s_i & = & 1 \\ s_i b_j & = & a_{i,j} b_i \quad i \neq j \in \{1, \ldots, n\} \end{array}$$

Donc $s_i B = b_i B_i$ et si l'équation $BX = c$ a une solution il existe c_i tel que $s_i c = b_i c_i$. On détermine un tel c_i (puisque la divisibilité est explicite). L'équation $BX = s_i c = b_i c_i$ admet donc la solution $x_i = c_i$, $x_j = 0$ si $j \neq i$. Puisque $\sum_{i=1}^n s_i = 1$ l'équation $BX = c$ admet donc la solution $(x_i = c_i)_{i=1,\ldots,n}$. □

Produit et intersection de deux idéaux de type fini dans un anneau arithmétique

Le lemme suivant permet de limiter le nombre de générateurs pour le produit de deux idéaux de type fini dans un anneau arithmétique. C'est aussi une généralisation du lemme de Gauss concernant le contenu d'un produit de deux polynomes à coefficients entiers. Rappelons qu'en général, le *contenu* d'un polynome $f \in \mathbf{A}[X]$ est l'idéal $\mathrm{c}(f)$ engendré par les coefficients de f.

Lemme 4.4.7 *Si* $g, h \in \mathbf{A}[X]$ *et* $\mathrm{c}(g)$ *est localement principal, alors on a* $\mathrm{c}(g)\mathrm{c}(h) = \mathrm{c}(gh)$[9]. *En conséquence si* I *et* J *sont deux idéaux de type fini d'un anneau arithmétique* $\mathbf{A}$ *engendrés respectivement par* m *et* n *éléments,* IJ *est engendré par* $m + n - 1$ *éléments.*

Preuve Il faut démontrer pour chaque coefficient g_i de g et chaque coefficient h_j que $g_i h_j \in \mathrm{c}(f)$ où $f = gh$. Ceci revient à résoudre une équation linéaire. On peut donc procéder localement. Par ailleurs il est connu que $\mathrm{c}(g) = \langle 1 \rangle \Rightarrow \mathrm{c}(gh) = \mathrm{c}(h)$ (voir par exemple le lemme d'Artin dans [32]). Localement on a $\mathrm{c}(g) = \langle g_i \rangle$, on écrit $g = g_i G$ avec $\mathrm{c}(G) = \langle 1 \rangle$ et donc $\mathrm{c}(gh) = g_i \mathrm{c}(Gh) = g_i \mathrm{c}(h) = \mathrm{c}(g)\mathrm{c}(h)$. □

Le résultat suivant généralise le point (2.4) dans le théorème 5 page 36.

Proposition 4.4.8 *Dans un anneau arithmétique l'intersection de deux idéaux de type fini est un idéal de type fini.*

[9] Les polynomes g tels que $\mathrm{c}(g)\mathrm{c}(h) = \mathrm{c}(gh)$ pour tout polynome h ont fait l'objet d'une étude intensive, voir à ce sujet [13].

Preuve Montrons que

$$\langle x_1,\dots,x_n\rangle \cap \langle y_1,\dots,y_m\rangle = \sum_{i,k} \langle x_i\rangle \cap \langle y_k\rangle$$

Le second membre est évidemment inclus dans le premier. Soit maintenant $z = \sum_i c_i x_i = \sum_k d_k y_k$. Appliquons le théorème 5 (1.4) à $\langle x_1,\dots,x_n\rangle$. Cela nous donne n éléments s_i $(i = 1,\dots,n)$ et $n^2 - n$ éléments $a_{i,j}$ $(i \neq j \in \{1,\dots,n\})$ vérifiant les équations suivantes.

$$\begin{array}{rcl} \sum_{i=1}^n s_i & = & 1 \\ a_{i,j}x_i - s_i x_j & = & 0 \quad i \neq j \in \{1,\dots,n\} \end{array}$$

De même on obtient m éléments t_k $(k = 1,\dots,m)$ et $m^2 - m$ éléments $b_{k,\ell}$ $(k \neq \ell \in \{1,\dots,m\})$ vérifiant les équations suivantes.

$$\begin{array}{rcl} \sum_{k=1}^m t_k & = & 1 \\ b_{k,\ell}y_k - t_k y_\ell & = & 0 \quad k \neq \ell \in \{1,\dots,m\} \end{array}$$

Donc $s_i t_k z$ se réécrit comme un élément de $\langle x_i\rangle \cap \langle y_k\rangle$. Il reste à faire la somme de ces nm éléments pour récupérer $z \in \sum_{i,k} \langle x_i\rangle \cap \langle y_k\rangle$. □

Puisqu'un anneau est cohérent si et seulement si d'une part l'intersection de deux idéaux de type fini est de type fini, et d'autre part l'annulateur de tout élément est de type fini (cf. [30]), on obtient comme corollaire du fait 3.4.2 et de la proposition 4.4.8 :

Proposition 4.4.9 *Un anneau arithmétique est cohérent si et seulement si l'annulateur de tout élément est de type fini. Un anneau arithmétique est un anneau de Prüfer cohérent si et seulement si il est quasi intègre.*

Le monoïde des idéaux de type fini d'un anneau arithmétique

La structure du monoïde ordonné formé par les idéaux de type fini d'un anneau arithmétique est très agréable.

HUM *Nous ne connaissons pas la terminologie officielle correspondant à la définition suivante.*

Définition 4.4.10 *Un monoïde, c'est-à-dire un ensemble T muni d'une loi interne associative avec élément neutre (on les notera $x\cdot y$ et 1) est appelé un* monoïde distributif, *lorsqu'il vérifie les propriétés suivantes.*

(com) la loi $x \cdot y$ est commutative

(ord) la relation de préordre " y divise x dans T ", notée $y \leq_T x$, définie par $\exists z\ x = z \cdot y$ est une relation d'ordre

(trd) avec cette relation d'ordre, T est un treillis distributif (on note $\wedge$ et $\vee$ les lois min *et* max*)*

(mima) $\forall x, y \quad x \cdot y = (x \wedge y) \cdot (x \vee y)$

(dis) $\forall x, y, z \ (\ x \cdot (y \wedge z) = (x \cdot y) \wedge (x \cdot z) \qquad \text{et} \qquad x \cdot (y \vee z) = (x \cdot y) \vee (x \cdot z)\ )$

(pu) $\forall x, y \in T \ \forall n \in \mathbb{N} \quad (x^n \wedge y^n = (x \wedge y)^n \ \text{ et } \ x^n \vee y^n = (x \vee y)^n)$

Le monoïde $(\mathbb{N}, \times)$ est le prototype des monoïdes distributifs. Tout produit fini ou somme directe infinie de monoïdes distributifs est un monoïde distributif. Un groupe réticulé est la même chose que le symétrisé d'un monoïde distributif simplifiable. Un monoïde distributif simplifiable est l'ensemble des éléments ≥ 0 dans un groupe réticulé. La théorie constructive des groupes réticulés discrets est faite dans [4].

Lemme 4.4.11 *Soit T un monoïde commutatif. Si $\leq_T$ est une relation d'ordre total, le monoïde est distributif. Si en outre le monoïde est simplifiable, il vérifie la propriété suivante.*

(dec) Soient des éléments x_i et y_j de T tels que $x_1 \cdot x_2 \cdot \cdots \cdot x_n = y_1 \cdot y_2 \cdot \cdots \cdot y_m$ alors on peut trouver des éléments z_{ij} $(i = 1,\dots,n$ et $j = 1,\dots,m)$ tels que chaque x_i est produit des z_{ij} correspondants et chaque y_j est produit des z_{ij} correspondants.

Preuve Seule la propriété (*dec*) demande une preuve. Supposons $y_1 \leq x_1$. Il existe un indice j tel que $y_1 \cdot \cdots \cdot y_j \leq x_1 \leq y_1 \cdot \cdots \cdot y_{j+1}$. Si $x_1 = y_1 \cdot \cdots \cdot y_j \cdot a$ et $x_1 \cdot b = y_1 \cdot \cdots \cdot y_j \cdot y_{j+1}$ (donc $y_{j+1} = a \cdot b$ en simplifiant par $y_1 \cdot \cdots \cdot y_j$) on prend $z_{1,1} = y_1, \ldots, z_{1,j} = y_j$, $z_{i,1} = \ldots = z_{i,j} = 1$ pour $i \geq 2$, $z_{1,j+1} = a$, $z_{1,k} = 1$ pour $k \geq j+2$. On se retrouve avec un problème analogue (mais plus petit), concernant $x_2, \ldots, x_n$ et $b, y_{j+2}, \ldots, y_m$. □

Théorème 6 *Soit* **A** *un anneau arithmétique (en particulier* **A** *peut être un anneau de Prüfer). Alors le monoïde multiplicatif des idéaux de type fini de* **A** *est un monoïde distributif dans lequel I divise J équivaut à $J \subseteq I$, l'intersection de deux idéaux est leur borne supérieure (ou p.p.c.m.) et leur somme est leur borne inférieure (ou p.g.c.d.). Lorsque* **A** *est un anneau de Prüfer cohérent, le monoïde vérifie en outre la propriété (dec).*

Preuve Etant donné un nombre fini d'idéaux de type fini, on peut après localisation en des éléments comaximaux convenables, supposer qu'ils sont tous principaux et totalement ordonnés par inclusion. Toutes les propriétés sont alors vraies d'après le lemme 4.4.11. Il suffit ensuite d'en faire un recollement concret.
Supposons maintenant que **A** soit un anneau de Prüfer cohérent. On reprend la preuve de la propriété (*dec*) dans le lemme précédent. Il y a un petit problème au moment de simplifier par $u = y_1 \cdot \cdots \cdot y_j$. On considère l'idempotent r tel que $\langle r \rangle$ est l'annulateur de u. Si on localise en $1 - r$, l'annulateur de u devient nul et on peut simplifier par u, donc c'est OK. Si on localise en r, on obtient $u = 0$, donc $y_1 \cdot \cdots \cdot y_j = 0 = x_1$. On peut alors considérer dans $\mathbf{A}_r$ les idempotents annulateurs de $y_1, \ldots, y_j$. Leur pgcd est égal à 1 (l'annulateur du produit), donc ils sont comaximaux. Donc quitte à localiser un peu plus, on est ramené au cas où $y_i = x_1 = 0$, qui se règle facilement (on prend $z_{1,i} = 0$, $z_{1,k} = y_k$, $z_{j,i} = x_j$ et 1 ailleurs). □

La propriété suivante généralise la propriété (3.1) dans le théorème 5 page 36 :

Proposition 4.4.12 *Soient $I_1, \ldots, I_n$ des idéaux de type fini d'un anneau arithmétique* **A**. *Posons $J_1 = \sum_{k=1}^{n} I_k$, $J_2 = \sum_{1 \leq j < k \leq n} (I_j \cap I_k)$, $\ldots$, $J_r = \sum_{1 \leq j_1 < \cdots < j_r \leq n} (I_{j_1} \cap \cdots \cap I_{j_r})$, $\ldots$, $J_n = \cap_{k=1}^{n} I_k$. Alors on a $J_n \subseteq \cdots \subseteq J_1$ avec un isomorphisme*

$$\bigoplus_{k=1}^{n} A/I_k \simeq \bigoplus_{k=1}^{n} A/J_k$$

Preuve Lorsque $n = 2$ cela résulte de la propriété (3.1) dans le théorème 5. Ensuite, on procède par induction et on utilise la distributivité du treillis des idéaux de type fini. □

La plupart des propriétés des monoïdes distributifs, appliquées au monoïde des idéaux de type fini, sont des conditions nécessaires et suffisantes pour qu'un anneau soit arithmétique. C'est l'objet du théorème suivant. Pour les énoncés voir [19] chapitre VI exercices 18 et 19, [12] exercices pages 321 et 476. On trouve des preuves dans [15] et [4] §1 exercice 25. Nous en indiquons ici des plus simples.

Théorème 7 *Pour un anneau* **A**, *les propriétés suivantes sont équivalentes:*

(1) **A** *est un anneau arithmétique.*

(2.1) *Pour tous idéaux I, J et K on a $I \cap (J + K) = (I \cap J) + (I \cap K)$.*

(2.2) *Même chose en se limitant aux idéaux principaux.*

(2.3) *Même chose en se limitant au cas $I = \langle x \rangle = \langle y + z \rangle$, $J = \langle y \rangle$ et $K = \langle z \rangle$*

(3.1) *Pour tous idéaux I, J et K on a $I + (J \cap K) = (I + J) \cap (I + K)$.*

(3.2) *Même chose en se limitant aux idéaux principaux.*

(3.3) *Même chose en se limitant au cas $I = \langle x \rangle$, $J = \langle y \rangle$ et $K = \langle x + y \rangle$*

(4.1) *Pour tous idéaux de type fini I, J et K on a $(J + K) : I = (J : I) + (K : I)$.*

(4.2) *Même chose avec J et K idéaux principaux et $I = J + K$.*

(5.1) *Pour tout idéal I et tous idéaux de type fini J et K on a $I : (J \cap K) = (I : J) + (I : K)$.*

(5.2) *Même chose avec J et K idéaux principaux et $I = J \cap K$.*

Preuve Les propriétés (2), (3), (4), (5), sont trivialement vérifiées lorsque l'ensemble des trois idéaux considérés est totalement ordonné par inclusion. Dans un anneau de Bezout local, elles sont donc vérifiées si on se limite aux idéaux de type fini. Comme les calculs peuvent être faits localement, cela passe aux anneaux arithmétiques. De manière générale, il est facile de voir que la version $(x.2)$ implique la version $(x.1)$ pour $x = 2, 3, 4$. Il reste à vérifier que les versions les plus faibles impliquent chacune que l'anneau est arithmétique.
Supposons (2.3). On a donc a, b, c, d tels que $x_1 = ax = by$, $x_2 = cx = dz$ et $x_1 + x_2 = x$. D'où $az = (b-a)y$ et $(1-a)y = (d+a-1)z$ et $\langle y, z\rangle$ est localement principal.
Supposons (3.3). On a donc $y \in \langle x\rangle + (\langle y\rangle \cap \langle x+y\rangle)$, c'est-à-dire qu'il existe a, b, c tels que $y = ax + by$, $by = c(x+y)$. D'où $cx = (b-c)y$ et $(1-c)y = (a+c)x$ et $\langle x, y\rangle$ est localement principal.
Supposons (4.2). On a $(J+K) : I = \langle 1\rangle$, $J : I = J : K$ et $K : I = K : J$. On trouve donc la propriété (4.2) du théorème 5.
Supposons (5.2). On a $I : (J \cap K) = \langle 1\rangle$, $I : J = K : J$ et $I : K = J : K$. On trouve donc la propriété (4.2) du théorème 5. □

Anneaux arithmétiques et idéaux inversibles

La proposition 3.3.8 donne comme cas particulier.

Proposition 4.4.13 *Dans un anneau arithmétique tout idéal de type fini contenant un non diviseur de zéro est inversible.*

Proposition 4.4.14 *Soit* **A** *un anneau quasi intègre. Alors les propriétés suivantes sont équivalentes:*

(1) **A** *est un anneau de Prüfer.*

(2) *Tout idéal de type fini contenant un non diviseur de zéro est inversible.*

(3) *Tout idéal $I = \langle x_1, x_2\rangle$ avec x_1 et x_2 non diviseurs de zéro est inversible.*

(4) *Pour tous $a, b \in \mathbf{A}$, on a : $\langle a, b\rangle^2 = \langle a^2, b^2\rangle = \langle a^2 + b^2, ab\rangle$.*

(5) *Pour tous $f, g \in \mathbf{A}[X]$, on a : $\mathrm{c}(f)\mathrm{c}(g) = \mathrm{c}(fg)$.*

Preuve On sait déjà que (1) $\Rightarrow$ (2) $\Rightarrow$ (3) et (1) $\Rightarrow$ (5).
Montrons que (3) implique que l'anneau est arithmétique. Considérons un idéal à deux générateurs arbitraire $I = \langle y_1, y_2\rangle$ et soit r_i l'annulateur idempotent de y_i. Considérons les idempotents orthogonaux : $e = (1-r_1)(1-r_2)$, $f = r_1(1-r_2)$, et $g = r_2$. On a $e+f+g = 1$. Si on localise en f ou g, un des y_i est nul et l'idéal I devient principal. Pour voir ce qui se passe si on localise en e considérons $x_1 = (1-e)+ey_1$, $x_2 = (1-e)+ey_2$. Ce sont des non diviseurs de zéro : si $ax_1 = 0$, alors $a(1-e) = 0$ et $aey_1 = 0$, donc $ae = aer_1 = 0$, donc $a = 0$. Donc l'idéal $J = \langle x_1, x_2\rangle$ est inversible dans **A**. Soient alors u, v, w tels que $ux_1 = vx_2$ et $(1-u)x_2 = wx_1$. On multiplie par e et on obtient $uey_1 = vey_2$ et $(1-u)ey_2 = wey_1$, ce qui implique que $I\mathbf{A}_e = \langle ey_1, ey_2\rangle \mathbf{A}_e$ est localement principal.
On a (5) $\Rightarrow$ (4) : considérer d'abord $f = aX + b$, $g = aX - b$, puis $f = aX + b$, $g = bX + a$.
Montrons (4) $\Rightarrow$ (3). Soit $I = \langle a, b\rangle$, avec a et b non diviseurs de zéro. Soient α, β tels que $ab = \alpha a^2 + \beta b^2$, $u = \alpha a^2$, $v = \beta b^2$ et soit $J = \langle \alpha a, \beta b\rangle$. On a $ab \in IJ$, donc

$$\langle (ab)^2\rangle \subseteq I^2J^2 = \langle a^2, b^2\rangle \langle \alpha^2 a^2, \beta^2 b^2\rangle .$$

On va montrer l'égalité $\langle (ab)^2\rangle = I^2J^2$, ce qui impliquera que I est inversible puisque $(ab)^2$ est non diviseur de zéro. Pour cela il suffit de montrer que $u^2 = \alpha^2 a^4$ et $v^2 = \beta^2 b^4$ sont dans $\langle (ab)^2\rangle$. Par exemple avec u^2 : on utilise $u^2 \in \langle u^2 + v^2, uv\rangle$, c'est-à-dire

$$u^2 = \gamma(u^2+v^2) + \delta uv = \gamma(u+v)^2 + (\delta - 2)uv = \gamma(ab)^2 + (\delta-2)\alpha\beta(ab)^2 = \epsilon(ab)^2.$$

□

Remarque 4.4.15 Dans [19] un anneau de Prüfer est défini comme un anneau dans lequel tout idéal de type fini contenant un non diviseur de zéro est inversible. Il s'agit d'une propriété légèrement plus faible que celle d'être un anneau arithmétique (cf. proposition 4.4.13 et remarque 4.7.2).

4.5 Anneaux de Prüfer et solutions des systèmes linéaires

Dans le théorème suivant l'équivalence entre les points (1.1) et (2.1) a été établie en mathématiques classiques dans l'article [14]. La preuve que nous en donnons ici est complètement algorithmique.

Théorème 8 *Pour un anneau* **A** *les propriétés suivantes sont équivalentes:*

(1.1) **A** *est un anneau de Prüfer.*

(1.2) *Tout idéal* $\langle x_1, x_2\rangle$ *est plat.*

(1.3) **A** *localement sans diviseur de zéro et arithmétique.*

(1.4) **A** *est réduit et arithmétique.*

(2.1) *Un système linéaire* $BX = C$ *arbitraire, dès que les idéaux déterminantiels de* $(B|C)$ *sont égaux à ceux de* B*, admet une solution.*

(2.2) *Même chose en se limitant à* $B \in \mathbf{A}^{2\times 3}$ *et* $C \in \mathbf{A}^{2\times 1}$.

Preuve L'équivalence des $(1.i)$ résulte l'équivalence des points (1.1) et (1.2) dans le théorème 5 page 36 et de l'étude générale des idéaux plats de type fini (corollaire 3.3.4 équivalence des points (4) et (5)).
On a évidemment (2.1) $\Rightarrow$ (2.2) et (1.3) $\Rightarrow$ (1.4).
On a facilement (2.2) $\Rightarrow$ (1.3), en considérant des solutions des systèmes linéaires suivants :

$$(B|C) = \left(\begin{array}{ccc|c} x_1 & x_2 & 0 & x_1 \\ x_2 & 0 & x_1 & 0 \end{array}\right)$$

avec $\mathcal{D}_1 = \langle x_1, x_2\rangle$ et $\mathcal{D}_2 = {\mathcal{D}_1}^2$; et, lorsque $xy = 0$,

$$(B|C) = \left(\begin{array}{c|c} x & x \\ y & 0 \end{array}\right)$$

avec $\mathcal{D}_1 = \langle x, y\rangle$ et $\mathcal{D}_2 = 0$ (puisque (1.4) $\Rightarrow$ (1.3), on pourrait même se limiter au cas où $x = y$ avec $x^2 = 0$).
Montrons que (1.4) $\Rightarrow$ (1.3). Supposons $xy = 0$. Soient s, t, a, b tels que $sx = ay$, $ty = bx$ et $s+t = 1$. Donc $sxy = ay^2 = 0$, $(ay)^2 = 0$ et $sx = ay = 0$.De la même manière $ty = 0$.
Pour montrer (1.1) $\Rightarrow$ (2.1), *on commence par le cas où* **A** *est local.* C'est alors une conséquence immédiate du lemme 1.4.7. *Pour un anneau arithmétique quelconque,* on applique alors la machinerie de la preuve par localisation. □

Notez qu'un quotient réduit d'un anneau de Prüfer est donc un anneau de Prüfer.

Commentaire 4.5.1 Bien que cela soit inutile, donnons une preuve directe que (2.1) implique que l'anneau est arithmétique, en montrant la propriété (1.4) dans théorème 5. Cette preuve est instructive. On considère par exemple un idéal de type fini $\langle x_1, x_2, x_3\rangle$. On doit montrer que le système linéaire suivant a une solution :

$$(B|C) = \left(\begin{array}{ccccccccc|c} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ x_2 & 0 & 0 & x_1 & 0 & 0 & 0 & 0 & 0 & 0 \\ x_3 & 0 & 0 & 0 & x_1 & 0 & 0 & 0 & 0 & 0 \\ 0 & x_1 & 0 & 0 & 0 & x_2 & 0 & 0 & 0 & 0 \\ 0 & x_3 & 0 & 0 & 0 & 0 & x_2 & 0 & 0 & 0 \\ 0 & 0 & x_1 & 0 & 0 & 0 & 0 & x_3 & 0 & 0 \\ 0 & 0 & x_2 & 0 & 0 & 0 & 0 & 0 & x_3 & 0 \end{array}\right)$$

et on vérifie que les idéaux déterminantiels de $(B|C)$ sont égaux à ceux de B.
Un raisonnement du même style marche avec un idéal de type fini engendré par n éléments en considérant des matrices beaucoup plus grosses. Ce genre de calculs a conduit un mathématicien célèbre à lancer un anathème fameux : il faut éliminer l'élimination. Pour lire le magnifique poème d'Abhyankar où il proclame "Éliminons, éliminons, éliminons, les éliminateurs de l'élimination", on pourra consulter la préface du livre Mishra [28].

Ce qui suit est un corollaire de la proposition 4.4.6 et du point (2.1) dans le théorème précédent.

Corollaire 4.5.2 *Dans un anneau de Prüfer où la divisibilité est explicite, on peut décider si un système linéaire admet ou non une solution, et en calculer une en cas de réponse positive. Autrement dit, tout module libre de rang fini (et donc aussi tout module de présentation finie) est fortement discret.*

Il serait intéressant de déployer la preuve de (1.2) $\Rightarrow$ (2.1) dans le théorème 8 page précédente dans le cas d'un anneau de Prüfer quelconque. On verrait qu'en pratique, lorsqu'on dispose d'un test pour l'inclusion des idéaux de type fini, c'est-à-dire dans le cas où l'anneau est fortement discret, l'algorithme (sous-jacent à la preuve) qui teste si un système linéaire admet une solution, et en calcule une en cas de réponse positive, a un comportement exponentiel par rapport à la taille des matrices.

4.6 Anneaux de Prüfer et idéaux intégralement clos

Définition 4.6.1 *Soit un I idéal d'un anneau $\mathbf{A}$, sous anneau d'un anneau $\mathbf{B}$. Un $x \in \mathbf{B}$ est dit* entier sur I *si il vérifie une relation de dépendance intégrale $x^{n+1} = a_1x^n + a_2x^{n-1} + \cdots + a_nx + a_{n+1}$ avec $\forall h\ a_h \in I^h$.*

Cas particuliers :

- (cas où $x \in \mathbf{A}$) Si $x \in \mathbf{A}$ il revient au même de dire $\exists n \geq 0\ I(I + \langle x\rangle_{\mathbf{A}})^n = (I + \langle x\rangle_{\mathbf{A}})^{n+1}$
- (cas où $I = \mathbf{A}$) Un $x \in \mathbf{B}$ est entier sur $\mathbf{A}$ si et seulement si $\mathbf{A}[x]$ est un $\mathbf{A}$-module de type fini.

Typiquement, un polynome tel que celui dans la définition 4.6.1 est obtenu comme polynome caractéristique d'une matrice à coefficients dans I, en particulier le "determinant trick" donne le lemme suivant :

Lemme 4.6.2 *Soit J un idéal de type fini de $\mathbf{A}$ dont l'annulateur est réduit à zéro. Si $x \in \mathbf{A}$ vérifie $xJ \subseteq IJ$ alors x est entier sur I.*

Définition 4.6.3

(1) *Un idéal I d'un anneau $\mathbf{A}$ est dit* intégralement clos *si tout $x \in \mathbf{A}$ entier sur I est dans I. Cela revient donc à dire que chaque fois qu'on a une égalité $I(I + \langle x\rangle)^n = (I + \langle x\rangle)^{n+1}$ on peut simplifier par $(I + \langle x\rangle)$.*

(2) *Un anneau est dit* normal *lorsque tout idéal principal est intégralement clos.*

(3) *Un sous anneau $\mathbf{A}$ d'un anneau $\mathbf{B}$ est dit* intégralement clos dans $\mathbf{B}$ *si tout $x \in \mathbf{B}$ entier sur $\mathbf{A}$ est dans $\mathbf{A}$.*

(4) *Un anneau $\mathbf{B}$ contenant un anneau $\mathbf{A}$ est dit* entier sur $\mathbf{A}$ *si tout $x \in \mathbf{B}$ est entier sur $\mathbf{A}$.*

Un anneau normal est intégralement clos dans son anneau total des fractions. Lorsque l'anneau est intègre, la notion d'anneau normal coïncide avec la notion usuelle d'anneau intégralement clos dans son corps des fractions. La définition ci-dessus d'un anneau normal est équivalente, en mathématiques classiques, à celle donnée le plus fréquemment (cf. [27]) : tout localisé en un idéal premier est intègre et intégralement clos dans son corps des fractions.

Lemme 4.6.4 *Tout anneau normal est localement sans diviseur de zéro. Plus précisément, on a pour tout anneau $\mathbf{A}$ les implications* (1) $\Rightarrow$ (2) $\Rightarrow$ (3).

(1) *Tout idéal principal est intégralement clos (i.e., $\mathbf{A}$ est normal).*

(2) $\forall x, y \in \mathbf{A}\ \ (x^2 \in \langle xy, y^2\rangle \ \Rightarrow\ \ x \in \langle y\rangle)$.

(3) *Tout idéal principal est plat.*

Preuve Notons que l'idéal 0 est intégralement clos si et seulement si l'anneau est réduit. On a évidemment (1) $\Rightarrow$ (2) et (2) implique que l'anneau est réduit. Supposons (2) et soient $x, y \in \mathbf{A}$ tels que $xy = 0$. Soit $z = x + y$. On a $x^2 = xz$ donc $x^2 \in \langle xz, z^2\rangle$ et $x = az$. Donc $x = a(x + y)$, $(1 - a)x = ay$, $ay^2 = (1 - a)xy = 0$ et puisque l'anneau est réduit $ay = 0$. Et $(1 - a)x = 0$. □

Le principe de recollement concret suivant résulte du principe de recollement concret des solutions de systèmes linéaires (éventuellement sous conditions homogènes).

Principe local-global concret 5 (recollement concret des idéaux intégralement clos)
Soient $\mathbf{A}$ *un sous anneau d'un anneau* $\mathbf{B}$, $S_1, \ldots S_n$ *des monoïdes comaximaux d'un anneau* $\mathbf{A}$, I *un idéal de* $\mathbf{A}$, $x \in \mathbf{A}$ *et* $y \in \mathbf{B}$.
On a les équivalences suivantes :

(1) x *est entier sur* $I \iff \forall i \in \{1, \ldots, n\}$ $x/1$ *est entier sur* I_{S_i}

(2) y *est entier* $\mathbf{A} \iff \forall i \in \{1, \ldots, n\}$ $y/1 \in \mathbf{B}_{S_i}$ *est entier sur* $\mathbf{A}_{S_i}$

(3) I *est intégralement clos dans* $\mathbf{A} \iff \forall i \in \{1, \ldots, n\}$ I_{S_i} *est intégralement clos dans* $\mathbf{A}_{S_i}$

(4) $\mathbf{A}$ *est intégralement clos dans* $\mathbf{B} \iff \forall i \in \{1, \ldots, n\}$ $\mathbf{A}_{S_i}$ *est intégralement clos dans* $\mathbf{B}_{S_i}$

(5) $\mathbf{A}$ *est un anneau normal* $\iff \forall i \in \{1, \ldots, n\}$ $\mathbf{A}_{S_i}$ *est un anneau normal.*

En particulier un produit fini d'anneaux normaux est un anneau normal.

Proposition 4.6.5 *Tout idéal d'un anneau de Prüfer est intégralement clos. En particulier un anneau de Prüfer est normal, donc intégralement clos dans son anneau total des fractions.*

Preuve Il suffit de montrer que tout idéal de type fini est intégralement clos.

Première preuve. On montre d'abord que tout idéal principal $\langle y \rangle$ est intégralement clos. On considère donc une relation de dépendance intégrale $x^{n+1} + a_1 x^n y + a_2 x^{n-1} y^2 + \cdots + a_n x y^n + a_{n+1} y^{n+1} = 0$ avec les a_i dans $\mathbf{A}$. On veut montrer qu'il existe $b \in \mathbf{A}$ tel que $x = by$. Prenons le cas $n = 4$ pour simplifier les écritures. On considère le système linéaire

$$(B|C) = \left(\begin{array}{cccc|c} x & 0 & 0 & 0 & a_5 y \\ -y & x & 0 & 0 & a_4 y \\ 0 & -y & x & 0 & a_3 y \\ 0 & 0 & -y & x & a_2 y \\ 0 & 0 & 0 & -y & x + a_1 y \end{array}\right)$$

et on vérifie que les idéaux déterminantiels de $(B|C)$ sont égaux à ceux de B :

$$\mathcal{D}_1 = \langle x, y \rangle,\ \mathcal{D}_2 = {\mathcal{D}_1}^2,\ \mathcal{D}_3 = {\mathcal{D}_1}^3,\ \mathcal{D}_4 = {\mathcal{D}_1}^4,\ \mathcal{D}_5 = 0.$$

Pour un idéal de type fini arbitraire, on localise en des monoïdes comaximaux qui rendent l'idéal principal (cf. proposition 3.3.3), puis on utilise le recollement concret de solutions de systèmes linéaires sous conditions homogènes.

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

Troisième preuve. Soit $x_0 \in \mathbf{A}$ entier sur un idéal de type fini $I = \langle x_1, \ldots, x_r \rangle$. On a pour un certain $n \geq 0$ $I(I + \langle x_0 \rangle)^n = (I + \langle x_0 \rangle)^{n+1}$. Puisque l'idéal $J = (I + \langle x_0 \rangle) = \langle x_0, \ldots, x_r \rangle$ est plat on a des éléments comaximaux $s_0, \ldots, s_r$ tels que $J_{s_i} = x_i \mathbf{A}_{s_i}$. Pour $i = 1, \ldots, r$ cela donne $x_0 \in I_{s_i}$. Pour $i = 0$ on obtient $x_0^{n+1} \in x_0^n I_{s_0}$ qui s'écrit $x_0^n(x_0 - y) = 0$ (dans $\mathbf{A}_{s_0}$) avec $y \in I_{s_0}$. Comme $\mathbf{A}_{s_0}$ est localement sans diviseur de zéro on a deux localisations comaximales telles que : dans la première $x_0 = 0$, dans la seconde $x_0 = y \in I$. Il reste à recoller toutes les égalités obtenues. □

Théorème 9 *Les propriétés suivantes sont équivalentes pour un anneau* $\mathbf{A}$.

(1) $\mathbf{A}$ *est un anneau de Prüfer.*

(2) *Tout idéal est intégralement clos.*

(3) *Tout idéal de type fini est intégralement clos.*

(4) *Tout idéal à deux générateurs est intégralement clos.*

(5) **A** *vérifie les deux propriétés,*

$$\forall x, y \in \mathbf{A}\ \ xy \in \langle x^2, y^2\rangle \quad \text{et} \quad \forall x, y \in \mathbf{A}\ \ (x^2 \in \langle xy, y^2\rangle \ \Rightarrow\ \ x \in \langle y\rangle)$$

c'est-à-dire encore

$$\forall x, y \in \mathbf{A}\ \ \langle x, y\rangle^2 = \langle x^2, y^2\rangle \quad \text{et} \quad \forall x, y \in \mathbf{A}\ \ (\langle x, y\rangle^2 = \langle y\rangle\langle x, y\rangle \ \Rightarrow\ \ \langle x, y\rangle = \langle y\rangle)$$

(6) **A** *est normal et vérifie la propriété suivante :* $\forall x, y \in \mathbf{A}\ \exists h, k \in \mathbb{N}\ h + k > 0$ *et* $x^h y^k$ *est dans l'idéal engendré par les* $x^i y^j$ *tels que* $i + j = h + k$ *et* $i \neq h$.

(7) **A** *est normal et* $\forall x, y \in \mathbf{A}\ \ \forall h, k > 0\ \ \exists a, b \in \mathbf{A}\ \ x^h y^k = ax^{h+k} + by^{h+k}$, *c'est-à-dire encore* $\forall x, y \in \mathbf{A}\ \ \forall m > 1\ \ \langle x^m, y^m\rangle = \langle x, y\rangle^m$

(8) **A** *est normal et* $\forall x, y \in \mathbf{A}\ \ xy \in \langle x^2, y^2\rangle$, *c'est-à-dire encore* $\forall x, y \in \mathbf{A}\ \ \langle x^2, y^2\rangle = \langle x, y\rangle^2$

(9) *Si* I, J_1, J_2 *sont trois idéaux de type fini de* **A** *avec* $J_1 \subseteq I$, $J_2 \subseteq I$ *et* $IJ_1 = IJ_2$ *alors* $J_1 = J_2$.

(10) *Si* I, J_1, J_2 *sont trois idéaux de type fini de* **A** *avec* $\mathrm{Ann}(I) \subseteq \mathrm{Ann}(J_1)$, $\mathrm{Ann}(I) \subseteq \mathrm{Ann}(J_2)$ *et* $IJ_1 = IJ_2$ *alors* $J_1 = J_2$.

(11) *Si* I, J_1, J_2 *sont trois idéaux de type fini de* **A** *avec* $\mathrm{Ann}(I) \subseteq \mathrm{Ann}(J_1)$, $\mathrm{Ann}(I) \subseteq \mathrm{Ann}(J_2)$ *et* $IJ_1 \subseteq IJ_2$, *alors* $J_1 \subseteq J_2$.

Preuve

L'implication (1) $\Rightarrow$ (3) a été démontrée à la proposition 4.6.5.

On a évidemment (3) $\Leftrightarrow$ (2), (3) $\Rightarrow$ (4) $\Rightarrow$ (5) $\Rightarrow$ (6) et (7) $\Rightarrow$ (8) $\Rightarrow$ (5)

Montrons (1) $\Rightarrow$ (7). D'après la propriété (*pu*) des monoïdes distributifs, on a $\langle x, y\rangle^{h+k} = \langle x\rangle^{h+k} + \langle y\rangle^{h+k}$ (ici $+$ vaut pour $\vee$) donc $x^h y^k = ax^{h+k} + by^{h+k}$.

Montrons (5) $\Rightarrow$ (1). Il suffit de montrer qu'un idéal non nul $I = \langle x, y\rangle$ est principal après localisation en des éléments comaximaux convenables. On a $xy = ax^2 + by^2$, et $z = ax$ vérifie $z^2 = zy - aby^2$ donc $ax = a'y$ pour un certain a'. De même, $by = b'x$ pour un certain b'. Donc $IJ = \langle xy\rangle$ où $J = \langle xa, yb\rangle$. En outre $xy(1 - a' - b') = 0$. Les trois éléments $(1 - a' - b'), a', b'$ sont comaximaux. Lorsqu'on localise en $(1 - a' - b')$ on a $xy = 0$, et puisque l'anneau est localement sans diviseur de zéro (lemme 4.6.4 : (2) $\Rightarrow$ (3)), après deux nouvelles localisations, $x = 0$ ou $y = 0$ donc I est principal. Lorsqu'on localise en a', on a $I = \langle x\rangle$ puisque $a'y = ax$. Et lorsqu'on localise en b', $I = \langle y\rangle$ puisque $b'x = by$.

Montrons (6) $\Rightarrow$ (5). Tout d'abord, si h ou $k = 0$, on a une relation de dépendance intégrale qui donne $x = by$ ou $y = ax$ puisque l'anneau est normal, donc $xy = by^2$ ou $xy = ax^2$. Sinon, on suppose $h + k \geq 3$ et

$$x^h y^k = a_{h+k}x^{h+k} + a_{h+k-1}x^{h+k-1}y + \cdots + a_0 y^{h+k}$$

avec $h \geq 1$, $k \geq 2$ (et pas de terme en $x^h y^k$ dans le second membre) et on va descendre d'un cran, en remplaccant k par $k - 1$. On considère $z = a_{h+k}x$, en multpliant l'égalité par a_{h+k}^{h+k-1} on voit que z vérifie une relation de dépendance intégrale qui fait que $z = a'y$ (puisque l'idéal $\langle y\rangle$ est intégralement clos). On obtient donc

$$x^h y^k = (a' + a_{h+k-1})x^{h+k-1}y + \cdots + a_0 y^{h+k}$$

Comme y est en facteur et que l'anneau est localement sans diviseur de zéro (lemme 4.6.4), on peut, après localisation supposer que $y = 0$ (auquel cas $xy \in \langle x^2, y^2\rangle$) ou que

$$x^h y^{k-1} = (a' + a_{h+k-1})x^{h+k-1} + \cdots + a_0 y^{h+k-1}$$

(sans terme en $x^h y^{k-1}$ dans le second membre).

On a évidemment (11) $\Rightarrow$ (10) $\Rightarrow$ (9). On a aussi (9) $\Rightarrow$ (3) en lisant la définition 4.6.3 (1).

Montrons (1) $\Rightarrow$ (11). Supposons que **A** est un anneau de Prüfer. Soient I, J_1, J_2 trois idéaux de type fini de **A** comme dans (11). Soit x un élément de J_1 et X un vecteur colonne formé par un système générateur de I. Puisque $xI \subseteq J_2 I$ il existe une matrice G carrée à coefficients dans J_2 telle que $xX = GX$. Donc $(x\mathrm{I} - G)X = 0$. Soit P le polynome caractéristique de G. On a donc $P(x)X = 0$. Donc $P(x) \in \mathrm{Ann}(I) \subseteq \mathrm{Ann}(J_1 + J_2)$. Or $P(x) \in J_1 + J_2$ donc $P(x)^2 = 0$. Donc $P(x) = 0$. Ceci est une relation de dépendance intégrale de x sur J_2. Donc $x \in J_2$. □

Théorème 10 *Soit* **A** *un sous anneau de* **B**. *Supposons que* **A** *soit un anneau de Prüfer, que* **B** *soit normal et que* **B** *soit entier sur* **A**. *Alors* **B** *est un anneau de Prüfer.*

Preuve Supposons tout d'abord que **A** est local, c'est-à-dire est un anneau de valuation. On va montrer que **B** vérifie le propriété (6) du théorème 9 page précédente. Soient $x, y \in \mathbf{B}$, le **A**-module $\mathbf{A}[x,y]$ est de type fini : si x et y vérifient des relations de dépendance intégrale de degrés m et n, $\mathbf{A}[x,y]$ est un **A**-module engendré par mn éléments. Considérons les $mn+1$ éléments $x^h y^k$ avec $h+k=mn$. D'après le lemme 4.2.4 l'un de ces éléments est combinaison linéaire des autres.
Dans le cas général on applique la machinerie de preuve par localisation en des éléments comaximaux convenables. On montre que **B** vérifie aprés localisations la propriété (6) du théorème 9 : on répète la preuve ci-dessus et au lieu d'utiliser le lemme 4.2.4 on se ramène aux hypothèses du lemme 1.4.8 (qui est la vraie raison du lemme 4.2.4). Donc après localisations en des éléments comaximaux convenables, **B** est un anneau de Prüfer. On termine en appliquant le principe de recollement concret des anneaux de Prüfer page 32. □

La proposition classique suivante nous sera utile dans la suite.

Proposition 4.6.6 *Soit* **A** *un anneau normal,* **K** *son anneau total des fractions, et* $f(X) \in \mathbf{A}[X]$ *unitaire. On suppose que* $f(X) = g(X)h(X)$ *dans* $\mathbf{K}[X]$, *avec* g *unitaire. Alors* $g(X) \in \mathbf{A}[X]$.

Preuve La proposition est une conséquence immédiate du lemme plus général suivant.

Lemme 4.6.7 *Soit* **B** *un anneau. On suppose que* $f(X) = g(X)h(X)$ *dans* $\mathbf{B}[X]$, *avec* f *et* g *unitaires. Alors chaque coefficient de* g *est entier sur l'anneau engendré par les coefficients de* f.

Considérons le cas générique où g et h ont pour coefficients des indéterminées (au dessus de l'anneau $\mathbb{Z}$). On introduit formellement les zéros de g et h, qui tous ensemble donnent les zéros de f. Il en résulte que chaque g_i et chaque h_j est un polynome en des zéros de f donc est entier sur l'anneau des coefficients de f. □

Remarque 4.6.8 Le lemme 4.6.7 admet plusieurs généralisations remarquables lorsque les polynomes ne sont plus supposés unitaires. Citons :
– le lemme d'Artin[10] $\forall g, h\ \exists p \in \mathbb{N}\ \mathrm{c}(g)^{p+1}\mathrm{c}(h) = \mathrm{c}(g)^p\mathrm{c}(gh)$. (cf. [32] ou [5] exercice 21 du § 2),
– le théorème de Kronecker : chaque coefficient du produit gh est entier sur l'idéal $\mathrm{c}(gh)$ (cf. [10, 11, 23]), et
– le lemme de Gauss-Joyal : $\sqrt{\mathrm{c}(gh)} = \sqrt{\mathrm{c}(g)\mathrm{c}(h)}$ (cf. [2])

4.7 Domaines de Prüfer

Définition 4.7.1 *Un anneau* **A** *est appelé un* domaine de Prüfer *si c'est un anneau de Prüfer intègre (i.e., sans diviseur de zéro et discret).*

Notez que l'anneau trivial est un domaine de Prüfer.
Un domaine de Prüfer est cohérent (proposition 4.4.9).

Théorème 11 *Pour un anneau* **A** *non trivial, les propriétés suivantes sont équivalentes:*

(1) **A** *est un domaine de Prüfer.*

(2) **A** *est intègre et arithmétique.*

(3) **A** *est intègre et tout module sans torsion est plat.*

(4) **A** *est intègre et tout noyau d'un homomorphisme entre modules projectifs de type fini est facteur direct.*

(5) **A** *est intègre et tout idéal de type fini est projectif.*

(6) **A** *est intègre et tout idéal de type fini non nul est inversible.*

(7) *Tout idéal à deux générateurs est un module de rang constant.*

[10] Ce lemme est souvent appelé lemme de Dedekind-Mertens, mais l'énoncé général tel que nous le donnons semble bien dû à Artin. Voir à ce sujet [32]. Voir également [1]

(8) **A** *est intègre et les idéaux de type fini non nuls forment un monoïde multiplicatif simplifiable.*

(9) **A** *est intègre et les idéaux fractionnaires de type fini non nuls de* **A** *forment un groupe réticulé.*

(10) **A** *est intègre et si* I, J *sont deux idéaux principaux, on a* $(I+J)(I\cap J)=IJ$.

(11) **A** *est intègre, et tout sous anneau* $\mathbf{A}[a/b]$ *du corps des fractions de* **A** *(*$a\in\mathbf{A}$ *et* $b\neq 0\in\mathbf{A}$*) est normal.*

(12) **A** *est intègre, et tout anneau compris entre* **A** *et son corps de fractions est un domaine de Prüfer.*

Preuve Les équivalences de (1) à (10) sont claires d'après les résultats déjà obtenus. Pour les points (11) et (12) voir plus loin la proposition 4.8.3. □

Remarque 4.7.2 La propriété (10) : pour tous idéaux de type fini I et J on a $(I+J)(I\cap J)=IJ$. n'est pas en général une condition suffisante pour qu'un anneau soit arithmétique. On trouve des contre exemples en considérant des anneaux locaux zéros dimensionnels, c'est-à-dire des anneaux dans lesquels tout élément est inversible ou nilpotent (les non diviseurs de zéro sont donc inversibles). Par exemple si **K** est un corps-discret et M un espace vectoriel de dimension finie, on peut munir $\mathbf{A}=\mathbf{K}\oplus M$ d'une structure de **K**-algèbre en posant $xy=0$ si $x,y\in M$. On obtient un anneau local zéro dimensionnel. Si I et J sont deux idéaux de type fini, ou bien $I=\langle 1\rangle$, ou bien $I\neq\langle 1\rangle$, $J=\langle 1\rangle$, ou bien I et J sont deux sous espaces vectoriels de M. Dans les deux premiers cas, l'égalité $(I+J)(I\cap J)=IJ$ est immédiate, dans le dernier cas $(I+J)(I\cap J)=0=IJ$. Cependant, si x et y sont linéairement indépendants l'idéal $\langle x,y\rangle$ n'est pas localement principal. Cet exemple est aussi celui d'un anneau dans lequel tout idéal contenant un non diviseur de zéro est inversible (et même égal à $\langle 1\rangle$) mais qui n'est pas un anneau arithmétique. Enfin cet anneau **A** vérifie la propriété que $\mathrm{c}(f)\mathrm{c}(g)=\mathrm{c}(fg)$ pour tous polynomes f,g mais il n'est pas arithmétique (cf. théorème 14 (7)).

On a aussi le théorème de structure suivant (cf. [6] exercice 12 du §2).

Proposition 4.7.3 *Sur un domaine de Prüfer tout module de présentation finie est somme directe de son sous-module de torsion et d'un sous module projectif (tous deux de type fini).*

Preuve Soit M un **A**-module de présentation finie et T son sous module de torsion. Si $s\neq 0$ dans **A**, et $x\in M$ alors $x\in T$ si et seulement si il est un élément de torsion dans M_s. Il suffit donc de montrer, pour des éléments comaximaux $s_1,\ldots,s_n$, que le sous module de torsion de M_{s_i} est de type fini et facteur direct. Cela montrera que T est de type fini et facteur direct (voir les principes de recollement concret de la section 2.2). Alors le module complémentaire qui est isomorphe à M/T sera sans torsion, donc plat, et de présentation finie, donc projectif de type fini. Or dans le cas local le résultat est donné par la proposition 4.2.9(2). Notez que $\mathbf{A}_s$ est discret puisque **A** est intègre. On peut donc appliquer la machinerie de preuve par localisation. □

Commentaire 4.7.4 La preuve que nous donnons de ce théorème de structure pour un domaine de Prüfer est plus subtile que la preuve classique, dans laquelle on suppose seulement M de type fini et où on se contente de remarquer que le quotient de M par son sous-module de torsion est sans torsion, donc plat, dont projectif (voir proposition 3.2.8). Voici une version constructive de cet énoncé classique. *Si* **A** *est un domaine de Prüfer, si* M *est un* **A***-module de type fini, et si l'espace vectoriel obtenu par extension des scalaires au corps des fractions de* **A** *est fortement discret, alors* M *est somme directe de son sous-module de torsion et d'un sous module projectif (tous deux de type fini).*

Cohérence des domaines de Prüfer

On a facilement le résultat suivant sans équivalent classique.

Lemme 4.7.5 *Un anneau de Prüfer* **A** *non trivial et sans diviseur de zéro est discret si et seulement si il est cohérent.*

Rappelons que la proposition 3.3.9 donne une preuve directe qu'un idéal de type fini localement principal est projectif de type fini, et a fortiori de présentation finie, dans un anneau intègre. Cela implique également le point (5) dans le théorème 11 page ci-contre.

Extensions algébriques des domaines de Prüfer

On sait (proposition 4.4.6) qu'un domaine de Prüfer **A** est fortement discret si et seulement si la relation de divisibilité est explicite. Cela revient encore à dire que **A** est une partie détachable de son corps des fractions.

Théorème 12 *Soit* **A** *un domaine de Prüfer,* **K** *son corps de fraction,* **L** *une extension algébrique de* **K** *et* **B** *la cloture intégrale de* **A** *dans* **L**. *Alors* **B** *est un domaine de Prüfer.*
En outre si **A** *est fortement discret et si on sait calculer le polynome minimal dans* $\mathbf{K}[X]$ *d'un élément de* **L** *alors* **B** *est fortement discret.*

Preuve Vu le théorème 10 seul le dernier point reste à montrer. Soit $x = y/a$ un élément arbitraire de **L**, avec $y \in \mathbf{B}$ et $a \in \mathbf{A}$. Nous devons tester si $x \in \mathbf{B}$. Soit $P \in \mathbf{A}[X]$ un polynome unitaire qui annule y. Nous considérons par ailleurs le polynome minimal unitaire $Q \in \mathbf{K}[X]$ de y, de degré n. D'après la proposition 4.6.6 ce polynome est dans $\mathbf{A}[X]$. Alors $R(X) = Q(aX)/a^n \in \mathbf{A}[X]$ est le polynome minimal unitaire de x dans $\mathbf{K}[X]$ et d'après la proposition 4.6.6, $x \in \mathbf{B}$ si et seulement si les coefficients de R sont dans **A**. □

Commentaire 4.7.6 La première affirmation du théorème précédent revient à dire que l'anneau **B** est arithmétique. La mise en évidence constructive de ce fait résulte ici du théorème 10 dont la preuve est assez subtile. Elle met en oeuvre un algorithme qui est manifestement "exponentiel en nombre d'opérations (par rapport aux degrés[11])", si on prend la peine de suivre l'enchaînement des preuves. Dans le cas d'un anneau intègre, on peut mettre en évidence la distributivité de manière apparemment plus efficace comme suit. Nous nous basons sur [6] exercice 16 du §2. Nous notons $\mathrm{c}(f)_{\mathbf{A}}$ (resp. $\mathrm{c}(f)_{\mathbf{B}}$) l'idéal fractionnaire de **A** (resp. l'idéal fractionnaire de **B**) engendré par les coefficients d'un polynome f à coefficients dans **K** (resp. dans **L**). Soit $I = \langle x, y\rangle_{\mathbf{B}} = \mathrm{c}(xY - yX)_{\mathbf{B}}$, avec x et y non nuls dans **B**. Nous calculons un polynome homogène non nul $Q(X,Y) \in \mathbf{A}[X,Y]$ tel que $Q(x,y) = 0$([12]). Ce polynome Q est donc divisible par $xY - yX$ dans $\mathbf{K}[X,Y]$: $Q(X,Y) = (xY - yX)R(X,Y)$. D'après le théorème de Kronecker (cf. remarque 4.6.8), les générateurs de $x\mathrm{c}(R)_{\mathbf{B}}$ et $y\mathrm{c}(R)_{\mathbf{B}}$ sont entiers sur l'idéal $\mathrm{c}(Q)_{\mathbf{A}}$ de **A**. En particulier ils sont de manière explicite dans **B**. Si z est l'un de ces générateurs, et s'il vérifie une relation de dépendance intégrale de degré p sur $\mathrm{c}(Q)_{\mathbf{A}}$ on obtient $z^p \in (\mathrm{c}(Q)_{\mathbf{B}})^p$ de manière explicite. Ceci implique que pour q assez grand $(I\mathrm{c}(R))^q \subseteq (\mathrm{c}(Q)_{\mathbf{B}})^q$. On obtient donc $(I\mathrm{c}(R))^q = (\mathrm{c}(Q)_{\mathbf{B}})^q$. Finalement si J est l'inverse de $\mathrm{c}(Q)_{\mathbf{A}}$ et $J' = J^q\mathbf{B}$, on a $II^{q-1}(\mathrm{c}(R)_{\mathbf{B}})^q J' = \langle 1\rangle_{\mathbf{B}}$. On a donc calculé l'inverse de I (en tant qu'idéal fractionnaire) et on est capable d'expliciter deux éléments x_1, y_1 de **B** tels que $\langle x, y\rangle_{\mathbf{B}} \langle x_1, y_1\rangle_{\mathbf{B}}$ soit principal et non nul.

HUM *On devrait pouvoir trouver plus simple.*

Dans le corollaire qui suit, nous examinons la question de la noethériannité. Un domaine de Prüfer noethérien et fortement discret est appelé un *domaine de Dedekind.*

Théorème 13 *Soit* **A** *un domaine de Prüfer et* **K** *son corps de fractions. Soit* $f(X) \in \mathbf{A}[X]$ *un polynome unitaire irréductible dans* $\mathbf{K}[X]$ *de discriminant non nul.*
Soit $\mathbf{A}' = \mathbf{A}[X]/f(X)$ *et* **B** *la cloture intégrale de* $\mathbf{A}'$ *dans son corps de fractions. Alors* **B** *est un domaine de Prüfer.*
En outre si **A** *est fortement discret ou noethérien, alors il en va de même pour* **B**.

Preuve Il reste à montrer que si **A** est noethérien, alors **B** l'est également. On a $\mathbf{A}' \subseteq \mathbf{B} \subseteq (1/\Delta)\mathbf{A}'$ où Δ est le discriminant de f. Et $(1/\Delta)\mathbf{A}'$ est isomorphe à $\mathbf{A}^{\deg(f)}$ en tant que **A**-module. Une suite croissante d'idéaux de type fini de **B** est aussi une suite croissante de sous-**A**-modules (de type fini ?) de

[11] On veut calculer l'inverse de $\langle x, y\rangle_{\mathbf{B}}$, où x et y sont deux éléments de **B** vérifiant des relations de dépendance intégrale de degrés m et n sur **A**.

[12] Voici par exemple un calcul de Q où on ne suppose pas **A** intègre. Si x et y sont entiers sur **A** on considère l'algèbre $\mathbf{A}[u,v] = \mathbf{A}[U,V]/\langle P_1(U), P_2(V)\rangle$ où P_1 et P_2 sont deux polynomes unitaires qui annulent x et y. L'algèbre $\mathbf{A}[x,y]$ est un quotient de $\mathbf{A}[u,v]$ et il suffit de calculer $Q(X,Y)$ qui annule (u,v). L'algèbre $\mathbf{A}[u,v]$ est un **A**-module libre de dimension finie. Si M_u et M_v sont les matrices des multiplications par u et v on prend $Q(X,Y) = \det(YM_u - XM_v)$ et on applique le théorème de Cayley-Hamilton homogène pour des matrices carrées qui commutent, on obtient : $Q(M_u, M_v) = 0 = M_{Q(u,v)}$.

$(1/\Delta)\mathbf{A}'$. Il nous suffirait de montrer que $\mathbf{B}$ est un $\mathbf{A}$-module de type fini. Ceci n'est malheureusement pas démontrable constructivement. On peut contourner l'obstacle somme suit. Si $J_1 \subseteq J_2 \subseteq \cdots \subseteq J_n \subseteq \cdots$ est la suite d'idéaux de type fini de $\mathbf{B}$ que l'on considère, on peut supposer sans perte de généralité que $J_n = \langle b_1, \ldots, b_n \rangle_{\mathbf{B}}$. On définit alors une suite croissante $L_1 \subseteq L_2 \subseteq \cdots \subseteq L_n \subseteq \cdots$ de sous-$\mathbf{A}$-modules de type fini de $(1/\Delta)\mathbf{A}'$ comme suit. On définit l'anneau $\mathbf{B}_n = \mathbf{A}[x, b_1, \ldots, b_n]$. C'est un $\mathbf{A}$-module de type fini parce que les b_i sont entiers sur $\mathbf{A}$. Nous considérons alors le sous-$\mathbf{A}$-module de type fini $L_n = \langle b_1 \ldots, b_n \rangle_{\mathbf{B}_n}$ de $(1/\Delta)\mathbf{A}'$. Il est clair que si $L_m = L_{m+1}$ alors $J_m = J_{m+1}$. □

4.8 Anneaux de Prüfer cohérents

Le théorème suivant résume des résultats déjà obtenus (théorème 4 page 35, propositions 4.4.9 et 4.4.14).

Théorème 14 *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 arithmétique quasi intègre.*

(3) *Tout idéal à deux générateurs est projectif.*

(4) $\mathbf{A}$ *est quasi intègre et tout idéal de type fini contenant un non diviseur de zéro est inversible.*

(5) $\mathbf{A}$ *est quasi intègre et tout idéal* $I = \langle x_1, x_2 \rangle$ *avec* x_1 *et* x_2 *non diviseurs de zéro est inversible.*

(6) $\mathbf{A}$ *est quasi intègre et pour tous* $a, b \in \mathbf{A}$*, on a :* $\langle a, b \rangle^2 = \langle a^2, b^2 \rangle = \langle a^2 + b^2, ab \rangle$.

(7) $\mathbf{A}$ *est quasi intègre et pour tous* $f, g \in \mathbf{A}[X]$*, on a :* $\mathrm{c}(f)\mathrm{c}(g) = \mathrm{c}(fg)$.

Rappelons que le nom le plus usuel (mais pas très beau) pour un anneau de Prüfer cohérent est *anneau semi-héréditaire.*

Exemple 4.8.1 Voici un exemple d'anneau de Prüfer non cohérent, qui nous a été donné par Sarah Glaz. Soit $Q = \mathbb{Q}[x]$ l'anneau des polynomes en une variable sur les rationnels. Soit $R = Q^{\mathbb{N}}$, soit B le sous anneau de R formé par les suites qui deviennent constantes à partir d'un certain rang et $A = B[\alpha]$ avec $\alpha = (x, 0, x^2, 0, x^3, 0, \ldots)$. L'anneau A est un anneau de Prüfer mais l'annulateur de α n'est pas de type fini.

Lemme 4.8.2 *Soit* $\mathbf{A}$ *un anneau intégralement clos dans son anneau total des fractions. Si* $\mathbf{A}$ *est quasi intègre, alors* $\mathbf{A}$ *est normal.*

Preuve Tout d'abord remarquons que $\mathbf{A}$ est localement sans diviseur de zéro donc réduit. Soient $x, y \in \mathbf{A}$ et $y^n = a_1 y^{n-1} x + \cdots + a_{n-1} y x^{n-1} + a_n x^n$ une relation de dépendance intégrale de y sur $\langle x \rangle$. Soit r l'idempotent annulateur de x, $s = 1 - r$ et $a'_i = sa_i$. On a $ry^n = 0$, donc puisque $\mathbf{A}$ est réduit $ry = 0$ et $sy = y$. L'annulateur de $x' = r + x$ est 0. Et on a $y^n = a'_1 y^{n-1} x' + \cdots + a'_{n-1} y x'^{n-1} + a'_n x'^n$. Donc $y = cx'$ avec $c \in \mathbf{A}$ et $y = sy = scx' = scx$. Donc $\mathbf{A}$ est normal. □

Proposition 4.8.3 *Soit* $\mathbf{A}$ *un anneau quasi intègre. Les propriétés suivantes sont équivalentes:*

(1) $\mathbf{A}$ *est un anneau de Prüfer.*

(2) *Tout sous anneau* $\mathbf{A}[a/b]$ *de l'anneau total des fractions de* $\mathbf{A}$ *(*$a \in \mathbf{A}$ *et* b *non diviseur de zéro dans* $\mathbf{A}$*) est normal.*

(3) *Tout anneau compris entre* $\mathbf{A}$ *et son anneau total des fractions est un anneau de Prüfer cohérent.*

Preuve Supposons (2) et montrons (1). Nous savons que $\mathbf{A}$ est un anneau normal cohérent. Soient $x, y \in \mathbf{A}$, on va montrer qu'ils vérifient le point (6) dans le théorème 9 page 44. Soit r l'idempotent annulateur de y, et $y_1 = r + y$. On voit facilement que y_1 est non diviseur de zéro. On considère l'anneau normal $\mathbf{A}[c]$ où $c = a/b$ avec $a = x^2$ et $b = y_1^2$. On a $c^2 y_1^2 = x^2$, donc x est entier sur $y_1 \mathbf{A}[c]$ donc on a une égalité $x = P(c) y_1$ avec $P(X) \in \mathbf{A}[X]$ de degré d, on chasse le dénominateur y_1^{2d} et on multiplie par $1 - r$, et on obtient une égalité du type voulu :

$$y^{2d} x = p_0 y^{2d+1} + p_1 y^{2d-1} x^2 + \cdots + p_{d-1} y^3 x^{2d-2} + p_d y x^{2d}$$

Supposons (1) et montrons (3). Soit $\mathbf{B}$ un anneau compris entre $\mathbf{A}$ et son anneau total des fractions. Il est clair que l'annulateur d'un élément a/b dans $\mathbf{B}$ est engendré par le même idempotent r que l'annulateur de a dans $\mathbf{A}$. Il nous suffit de montrer que tout idéal $I = x_1\mathbf{B} + x_2\mathbf{B}$ de $\mathbf{B}$ est localement principal. Mais si $x_1 = a_1/b_1$, $x_2 = a_2/b_2$, alors $I = a_1\mathbf{B} + a_2\mathbf{B}$ et comme $a_1\mathbf{A} + a_2\mathbf{A}$ est localement principal dans $\mathbf{A}$ tout est OK. □

On sait (proposition 4.4.6) qu'un anneau arithmétique $\mathbf{A}$ est fortement discret si et seulement si la relation de divisibilité est explicite. Dans le cas d'un anneau de Prüfer cohérent si $\mathrm{Ann}(a) = \langle r\rangle$, alors $a_1 = a + r$ est non diviseur de zéro et on a a divise b si et seulement si $rb = 0$ et a_1 divise b. Dans le cas d'un anneau de Prüfer cohérent on obtient donc.

Proposition 4.8.4 *Un anneau de Prüfer cohérent et discret $\mathbf{A}$ est fortement discret si et seulement si $\mathbf{A}$ est une partie détachable de son anneau total des fractions.*

Notez enfin qu'un anneau de Prüfer cohérent est discret si et seulement si l'ensemble de ses idempotents est discret.

Théorèmes de structure pour les modules de présentation finie

La proposition suivante généralise la proposition 4.3.1.

Proposition 4.8.5 *Si $\mathbf{A}$ un anneau de Prüfer cohérent, et P un $\mathbf{A}$-module projectif de type fini de rang ℓ, alors P est somme directe de ℓ modules de rang* 1.

Preuve On reprend la preuve de la proposition 4.3.1 en prenant soin de scinder l'anneau $\mathbf{A}$ en composantes chaque fois que le calcul fait découvrir un nouvel idempotent (chaque fois qu'on avait à tester dans le cas intègre si un élément était nul ou non). A la fin on obtient $\mathbf{A} \simeq \mathbf{A}_1 \times \mathbf{A}_2 \times \cdots \times \mathbf{A}_n$, ($\mathbf{A}_i = \mathbf{A}_{r_i}$, avec un sfio $(r_1, \ldots, r_n)$) et chaque $P_{r_i} = P_i$ est somme de ℓ $\mathbf{A}_i$-modules de rang 1 : $P_{r_i} = P_{i,1} \oplus \cdots \oplus P_{i,\ell}$. D'où ensuite $P = P_1 \oplus \cdots \oplus P_\ell$ avec chaque P_k qui est la somme directe des $P_{i,k}$. □

La preuve de la proposition suivante fonctionne de manière similaire, en transformant la preuve donnée pour le cas intègre (proposition 4.7.3). Il faut noter que si $\mathbf{A} \simeq \mathbf{A}_1 \times \mathbf{A}_2 \times \cdots \times \mathbf{A}_n$ et si M est un $\mathbf{A}$-module de type fini, alors M est un module de torsion (resp. un module projectif de type fini) si et seulement si chacune de ses composantes M_i est un module de torsion (resp. un module projectif de type fini).

Proposition 4.8.6 *Si $\mathbf{A}$ un anneau de Prüfer cohérent, et P un $\mathbf{A}$-module de présentation finie, alors P est somme directe de son sous-module de torsion et d'un sous-module projectif (tous deux de type fini).*

Extensions algébriques des anneaux de Prüfer cohérents

Théorème 15 *Soit $\mathbf{A}$ un anneau de Prüfer cohérent. Soit $f(X) \in \mathbf{A}[X]$ un polynome unitaire dont le discriminant est non diviseur de zéro.*
Soit $\mathbf{A}' = \mathbf{A}[X]/f(X)$ et $\mathbf{B}$ la cloture intégrale de $\mathbf{A}'$ dans son anneau total des fractions. Alors $\mathbf{B}$ est un anneau de Prüfer cohérent.
En outre si $\mathbf{A}$ est fortement discret (resp. noethérien), alors il en va de même pour $\mathbf{B}$.

On pourra noter que les résultats restent vrais si r est un idempotent, si $f(X) = rf(X) = rX^n + \cdots + a_1X + a_0$, si $1-r$ est l'annulateur du discriminant de f et si on considère $\mathbf{A}' = \mathbf{A}[X]/(f(X), (1-r)X)$.

Preuve Rappelons pour commencer ce qui se passe lorsque $\mathbf{A}$ est un corps-discret (en un seul mot) $\mathbf{K}$. On a $\mathbf{A}' = \mathbf{K}[X]/f(X)$ avec $c(X)f(X) + d(X)f'(X) = \mathrm{disc}(f)$ inversible dans $\mathbf{K}$. On note x la classe de X dans $\mathbf{A}'$. Montrons que l'annulateur d'un élément arbitraire $g(x)$ de $\mathbf{A}'$ ($g(X) \in \mathbf{K}[X]$, $\deg(g) < \deg(f)$) est engendré par un idempotent de $\mathbf{A}'$. On considère le pgcd h de f et g qui se calcule par l'algorithme d'Euclide. On obtient

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

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

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

avec

$$a(X)f_1(X) + b(X)g_1(X) = 1 \qquad (1)$$

Le résultant de h et f_1 divise le discriminant de f donc est inversible. Cela donne une identité de Bezout

$$u(X)h(X) + v(X)f_1(X) = \mathrm{Res}(h, f_1) \qquad (2)$$

Si on pose $e_1 = e_1(x) = u(x)h(x)/\mathrm{Res}(h, f_1)$ et $e_2 = e_2(x) = v(x)f_1(x)/\mathrm{Res}(h, f_1)$ on a $e_1e_2 = 0$ et $e_1 + e_2 = 1$, donc e_1 et e_2 sont deux idempotents orthogonaux avec $e_1f_1(x) = e_2h(x) = 0$, $e_2f_1(x) = f_1(x)$, $e_1h(x) = h(x)$, et on a des isomorphismes explicites $e_2\mathbf{A}' \simeq \mathbf{K}[X]/h(X)$ et $e_1\mathbf{A}' \simeq \mathbf{K}[X]/f_1(X)$. En multipliant (1) et (2) on obtient $m(x)f_1(x)+n(x)g(x) = 1$ donc $e_1gn(x) = e_1$, i.e., e_1g est inversible dans $\mathbf{K}[X]/f_1(X) \simeq e_1\mathbf{A}'$. Et e_2g, multiple de $e_2h(x)$, est nul. Ceci montre que l'annulateur de g dans $\mathbf{A}'$ est l'idempotent e_2. Et que $\mathbf{B}$, l'anneau total des fractions de $\mathbf{A}'$ est égal à $\mathbf{A}'$. L'important ici est de bien se convaincre que tout ceci fonctionne avec un corps-discret "en un seul mot", c'est-à-dire uniquement sur la base de l'axiome : tout élément est nul ou inversible.

Venons en à la preuve du théorème. Nous supposons tout d'abord $\mathbf{A}$ intègre, ou (ce qui est à peine plus faible) que l'anneau total des fractions est un corps-discret (en un seul mot) $\mathbf{K}$. Notons x la classe de X dans $\mathbf{A}'$. On va montrer que $\mathbf{B}$ est quasi intègre, c'est-à-dire que l'annulateur d'un élément arbitraire $g(x)$ de $\mathbf{A}'$ ($g(X) \in \mathbf{A}[X]$, $\deg(g) < \deg(f)$) est engendré par un idempotent de $\mathbf{B}$. On conclura alors par le lemme 4.8.2 que $\mathbf{B}$ est normal, puis par le théorème 10 page 45 que $\mathbf{B}$ est un anneau de Prüfer. Et il s'ensuit que $\mathbf{B}$ est cohérent (cf. théorème 14 (2)).
L'anneau $\mathbf{A}'$ est un $\mathbf{A}$-module libre de rang égal à $\deg(f)$. L'algèbre $\mathbf{L} = \mathbf{K}[x] = \mathbf{A}' \otimes_{\mathbf{A}} \mathbf{K} \simeq \mathbf{K}[X]/f(X)$ est un $\mathbf{K}$-espace vectoriel de dimension $\deg(f)$.
On a dans $\mathbf{A}[X]$ une égalité $af + bg = \mathrm{Res}(f, g)$, ce qui donne $b(x)g(x) = \mathrm{Res}(f, g)$ dans $\mathbf{A}'$.
Premier cas, $\mathrm{Res}(f, g)$ est non diviseur de zéro, alors $g(x)$ est non diviseur de zéro dans $\mathbf{A}'$ (son annulateur est 0) et $1/g(x) = b(x)/\mathrm{Res}(f, g)$ dans l'anneau total des fractions de $\mathbf{A}'$.
Deuxième cas, $\mathrm{Res}(f, g) = 0$, soit $h(X)$ le pgcd unitaire de $f(X)$ et $g(X)$ dans $\mathbf{K}[X]$ ($\deg(h) > 0$). On écrit $hf_1 = f$ et $hg_1 = g$ dans $\mathbf{K}[X]$. La proposition 4.6.6 donne que h et f_1 sont dans $\mathbf{A}[X]$. On en déduit que g_1, obtenu par division euclidienne de g par h, est aussi dans $\mathbf{A}[X]$. On a $\deg(f_1) < \deg(f)$ et f_1 unitaire, donc $f_1(x)$ est non nul dans $\mathbf{A}'$, et $f_1(x)g(x) = f(x)g_1(x) = 0$. Ainsi $g(x)$ divise zéro.
Comme première conclusion, l'anneau total des fractions de $\mathbf{A}'$ est égal à $\mathbf{L} = \mathbf{K}[x]$ et $\mathbf{A}' \subseteq \mathbf{B} \subseteq \mathbf{K}[x]$.
Continuons l'analyse du deuxième cas. On écrit maintenant $uh + vf_1 = \mathrm{Res}(h, f_1)$ dans $\mathbf{A}[X]$. Le scalaire $\mathrm{Res}(h, f_1) \in \mathbf{A}$ divise le discriminant de f donc il est non diviseur de zéro. On sait que l'annulateur de $g(x)$ dans $\mathbf{B} \otimes_{\mathbf{A}} \mathbf{K} = \mathbf{K}[x]$ est l'idempotent $e_2 = v(x)f_1(x)/\mathrm{Res}(h, f_1)$. La relation de dépendance intégrale $e_2^2 = e_2$ montre que e_2 est bien dans $\mathbf{B}$, et $e_2\mathbf{B}$ est l'annulateur de $g(x)$ dans $\mathbf{B}$. Ceci termine la preuve dans le cas où $\mathbf{A}$ est intègre.

Dans le cas général, l'anneau $\mathbf{A}$ est seulement quasi intègre. On reprend la preuve précédente en prenant soin de scinder l'anneau $\mathbf{A}$ en composantes chaque fois que le calcul fait découvrir un nouvel idempotent. Cela fonctionne comme suit.
Le corps des fractions $\mathbf{K}$ de $\mathbf{A}$ est remplacé par l'anneau total des fractions, que l'on note encore $\mathbf{K}$. On remarque par ailleurs que lorsqu'on a un élément $x \in \mathbf{A}$ qui a pour annulateur un idempotent r, on peut considérer $\mathbf{A}$ comme étant le produit de $\mathbf{A}_r \simeq r\mathbf{A}$ et $\mathbf{A}_{1-r} \simeq (1-r)\mathbf{A}$. Dans la première composante on a $x = 0$, dans la deuxième x est non diviseur de zéro, et il peut être pris comme dénominateur dans l'anneau total des fractions. Au fur et à mesure qu'on suit les calculs dans la preuve initiale, à chaque fois qu'on utilisait le test " $z = 0$ ou z non diviseur de zéro " pour un élément z de $\mathbf{A}$, on casse l'anneau en deux morceaux. On note que chaque morceau reste un anneau de Prüfer cohérent.
Si on a $\mathbf{A} \simeq \mathbf{A}_1 \times \mathbf{A}_2 \times \cdots \times \mathbf{A}_j$, alors $\mathbf{K} \simeq \mathbf{K}_1 \times \mathbf{K}_2 \times \cdots \times \mathbf{K}_j$, $\mathbf{A}' \simeq \mathbf{A}'_1 \times \mathbf{A}'_2 \times \cdots \times \mathbf{A}'_j$ et $\mathbf{B} \simeq \mathbf{B}_1 \times \mathbf{B}_2 \times \cdots \times \mathbf{B}_j$. Dans chacun des morceaux $\mathbf{A}_i$ obtenus, tous les éléments pertinents pour les

calculs sont nuls ou non diviseurs de zéro, et ceci permet d'obtenir le résultat souhaité dans chaque morceau. Il reste à la fin à recoller tous les résultats locaux en un seul résultat global.
Précisément on doit montrer que l'annulateur d'un élément $g(x)$ de $\mathbf{A}'$ est engendré par un idempotent de $\mathbf{B}$. On considère l'annulateur idempotent r de $\mathrm{Res}(f,g)$. Dans $\mathbf{A}_{1-r}$, l'annulateur de $g(x)$ est nul. Dans $\mathbf{A}_r$ on a $\mathrm{Res}(f,g)=0$. On doit considérer le pgcd de f et g. Ceci réclame par exemple son calcul par l'algorithme d'Euclide. Le déroulement de cet algorithme dépend des degrés des restes successifs. Pour chaque reste calculé, l'anneau se scinde éventuellement en morceaux. Dans chaque morceau le reste considéré a un coefficient dominant non diviseur de zéro, ou bien est identiquement nul lorsque le pgcd est atteint. Considérons un morceau $\mathbf{A}_i$ de $\mathbf{A}$ dans lequel l'algorithme produit un pgcd h de degré ≥ 1. On peut écrire $hf_1 = f$ et $hg_1 = g$ dans $\mathbf{K}_i[X]$: en effet, comme le coefficient dominant de h est non diviseur de zéro, on peut faire la division euclidienne de f par h dans $\mathbf{K}_i[X]$ et elle donne un reste nul car la preuve usuelle que l'algorithme d'Euclide fournit un élément h qui engendre le même idéal de $\mathbf{K}_i[X]$ que f et g, fonctionne sans changement. Etc....

Pour ce qui concerne le caractère fortement discret de $\mathbf{B}$ (si $\mathbf{A}$ l'est), on reprend la preuve du fait analogue dans le théorème 12 page 47 en prenant soin de scinder l'anneau $\mathbf{A}$ en composantes chaque fois que le calcul fait découvrir un nouvel idempotent. On sait que l'anneau total des fractions de $\mathbf{B}$ est $\mathbf{L} = \mathbf{K}[x] = \mathbf{K}[X]/f(X)$. En cherchant, comme dans la preuve du théorème 12, à calculer le polynome minimal unitaire d'un élément de $\mathbf{L}$ dans $\mathbf{K}[X]$ on est simplement éventuellement amené à scinder $\mathbf{A}$ en morceaux.

Enfin si $\mathbf{A}$ est noethérien, alors $\mathbf{B}$ l'est également : la même preuve que celle du théorème 13 fonctionne sans changement. □

On peut remarquer que si le nombre d'éléments d'un sfio de $\mathbf{A}$ est borné a priori, il en va de même pour $\mathbf{B}$. Même chose lorsque le nombre de facteurs non triviaux de tout idéal de type fini de $\mathbf{A}$ est borné a priori.

Annexes

Dans les annexes I, II, III et IV, nous rappelons quelques résultats d'algèbre constructive concernant la localisation, les principes local-global, les modules de présentation finie et les modules projectifs de type fini. Ils sont en général faciles et peuvent être trouvés par ailleurs ([9, 17, 20, 21, 22, 26, 30, 31]). Nous avons néanmoins donné quelques preuves. Dans l'annexe V nous donnons quelques lemmes qui peuvent faciliter les calculs dans les domaines de Prüfer et les anneaux de Prüfer.

I Généralités sur la localisation

Dans la suite, lorsque ce n'est pas précisé, S désigne un monoïde (multiplicatif) dans l'anneau commutatif considéré.

Fait I.1 *Si I et J sont deux idéaux de type fini alors $(I : J)_S = I_S : J_S$.*

Fait I.2 *Soit r un idempotent d'un anneau $\mathbf{A}$. Le localisé $\mathbf{A}[1/r]$ est isomorphe à l'anneau $\mathbf{A}/\langle 1-r\rangle$, lui-même isomorphe à $r\mathbf{A}$ vu comme un anneau avec l'élément neutre r.*

Fait I.3 *Si M est un $\mathbf{A}$-module plat alors M_S est un $\mathbf{A}_S$-module plat.*

Fait I.4 *Si M est un sous module de N, on a l'identification canonique de M_S avec un sous module de N_S et de $(N/M)_S$ avec N_S/M_S.*
Si $f : M \to N$ est une application $\mathbf{A}$-linéaire, $\mathrm{Im}(f_S)$ s'identifie canoniquement à $(\mathrm{Im}(f))_S$, $\mathrm{Ker}(f_S)$ s'identifie canoniquement à $(\mathrm{Ker}(f))_S$ et $\mathrm{Coker}(f_S)$ s'identifie canoniquement à $(\mathrm{Coker}(f))_S$.
Si

$$M \xrightarrow{f} N \xrightarrow{g} P$$

est une suite exacte de $\mathbf{A}$-modules et $S \subseteq \mathbf{A}$ un monoïde, alors

$$M_S \xrightarrow{f_S} N_S \xrightarrow{g_S} P_S$$

est une suite exacte de $\mathbf{A}_S$-modules.
Par suite, si M est de type fini, de présentation finie ou projectif de type fini, il en va de même pour M_S.

Soit $\varphi : M \to M$ un endomorphisme d'un $\mathbf{A}$-module projectif de type fini. Supposons que $M \oplus N$ soit isomorphe à un module libre $\mathbf{A}^n$ et prolongeons φ à $M \oplus N$ par l'identité sur N. Alors le déterminant de cette application linéaire $\varphi \oplus \mathrm{Id}_N$ ne dépend que de φ. Le déterminant ainsi défini est appelé le *déterminant de l'endomorphisme φ*.

Fait I.5 *Si $\varphi : M \to M$ est un endomorphisme d'un module projectif de type fini, alors* $\det(\varphi)_S = \det(\varphi_S)$ *(ou si on préfère* $\det(\varphi)/1 =_{\mathbf{A}_S} \det(\varphi_S)$*).*

Fait I.6 *Si M est un $\mathbf{A}$-module cohérent alors M_S est un $\mathbf{A}_S$-module cohérent. Si M est $\mathbf{A}$-module noethérien alors M_S est un $\mathbf{A}_S$-module noethérien.*

Fait I.7 *Soient M et N deux $\mathbf{A}$-modules et S un monoïde de $\mathbf{A}$. Alors l'homomorphisme canonique de $(M \otimes_{\mathbf{A}} N)_S$ dans $M_S \otimes_{\mathbf{A}_S} N_S$ est un isomorphisme de $\mathbf{A}_S$-modules.*

Fait I.8 *Soit M un $\mathbf{A}$-module, k un entier naturel et S un monoïde de $\mathbf{A}$. Alors l'homomorphisme canonique de $(\wedge^k_{\mathbf{A}} M)_S$ dans $\wedge^k_{\mathbf{A}_S}(M_S)$ est un isomorphisme de $\mathbf{A}_S$-modules.*

Pour le foncteur Hom les choses ne se passent pas toujours aussi bien.

Fait I.9 *Soit $f : M \to N$, $g : M \to N$ deux applications linéaires entre $\mathbf{A}$-modules,* avec M de type fini. *Soit S un monoïde de $\mathbf{A}$. Alors $f_S = g_S$ si et seulement si il existe $s \in S$ tel que $sf = sg$. En d'autres termes, l'application canonique $(\mathrm{Hom}_{\mathbf{A}}(M, N))_S \to \mathrm{Hom}_{\mathbf{A}_S}(M_S, N_S)$ est injective.*

Fait I.10 *Soit M et N deux $\mathbf{A}$-modules, S un monoïde de $\mathbf{A}$ et $\varphi : M_S \to N_S$ une application $\mathbf{A}_S$-linéaire. Supposons que M soit de présentation finie ou que $\mathbf{A}$ soit intègre et M de type fini. Alors il existe une application $\mathbf{A}$-linéaire $\phi : M \to N$ et $s \in S$ tels que*

$$\forall x \in M \quad \varphi\left(\frac{x}{1}\right) = \frac{\phi(x)}{s}$$

En d'autres termes, l'application canonique $(\mathrm{Hom}_{\mathbf{A}}(M,N))_S \to \mathrm{Hom}_{\mathbf{A}_S}(M_S, N_S)$ *est bijective.*

II Modules de présentation finie

Un module *de présentation finie* est un $\mathbf{A}$-module M donné par un nombre fini de générateurs et de relations. De manière équivalente, c'est un module M isomorphe au conoyau d'un homomorphisme

$$\gamma : \mathbf{A}^m \longrightarrow \mathbf{A}^q$$

La matrice $G \in \mathbf{A}^{q\times m}$ de γ a pour colonnes les relations entre les générateurs $g_1, \ldots, g_q$ (les g_i sont les images de la base canonique de $\mathbf{A}^q$ par la surjection canonique $\pi : \mathbf{A}^q \to M$). Une telle matrice s'appelle une *matrice de présentation du module M*. Cela se traduit par :

- $(g_1, \ldots, g_q)G = 0$, et
- toute relation entre les g_i est une combinaison linéaire des colonnes de G, c'est-à-dire encore : si $(g_1, \ldots, g_q)C = 0$ avec $C \in \mathbf{A}^{q\times 1}$ il existe $C' \in \mathbf{A}^{m\times 1}$ tel que $C = GC'$.

Un module libre de rang k est présenté par une matrice colonne formée de k zéros[13].

Rappelons qu'il existe un cas facile où une matrice présente un module libre, donné par le lemme de la liberté page 12.

Changement de système générateur

Supposons maintenant qu'un autre système générateur du $\mathbf{A}$-module M soit $h_1, \ldots, h_r$. On a donc des matrices $H_1 \in \mathbf{A}^{q\times r}$ et $H_2 \in \mathbf{A}^{r\times q}$ telles que $(g_1, \ldots, g_q)H_1 = (h_1, \ldots, h_r)$ et $(h_1, \ldots, h_r)H_2 = (g_1, \ldots, g_q)$. Puisque $(g_1, \ldots, g_q)(\mathrm{I}_q - H_1H_2) = 0$, on a aussi une matrice $K \in \mathbf{A}^{m\times q}$ telle que $\mathrm{I}_q - H_1H_2 = GK$.

Alors le module des relations entre les h_j est engendré par les colonnes de H_2G d'une part et de $\mathrm{I}_r - H_2H_1$ d'autre part. En effet d'une part $(h_1, \ldots, h_r)H_2G$ et $(h_1, \ldots, h_r)(\mathrm{I}_r - H_2H_1)$ sont clairement nuls. D'autre part si on a une relation de dépendance linéaire $(h_1, \ldots, h_r)C = 0$, on en déduit $(g_1, \ldots, g_q)H_1C = 0$, donc $H_1C = GC'$ pour un certain vecteur colonne C' donc

$$C = ((\mathrm{I}_r - H_2H_1) + H_2H_1)C = (\mathrm{I}_r - H_2H_1)C + H_2GC' = HC''$$

où $H = ((\mathrm{I}_r - H_2H_1)|H_2G)$ et C'' s'obtient en superposant C et C'([14]).

Cette possibilité de remplacer un système générateur par un autre tout en gardant un nombre fini de relations marche en fait chaque fois qu'on peut parler de structures définies par générateurs et relations, donc au moins avec ce qui relève de l'algèbre universelle. On remplace les anciens

[13] Si on considère qu'une matrice est donnée par deux entiers $q, m \geq 0$ et une famille d'éléments de l'anneau indexée par les couples (i,j) avec $1 \leq i \leq q$, $1 \leq j \leq m$, on peut accepter une matrice vide de type $q \times 0$, qui serait la matrice canonique pour présenter un module libre de dimension q.

[14] On pourra comparer cette preuve purement évidente avec les preuves (du même théorème formulé de manière plus abstraite) qui utilisent le lemme du serpent, comme on les trouve dans la plupart des livres d'algèbre commutative. Ces preuves sont nettement plus difficiles à comprendre, et elles ne disent pas clairement comment on peut écrire la matrice H à partir des matrices G, H_1 et H_2. On peut d'ailleurs douter que les auteurs aient clairement conscience que l'hypothèse dans l'énoncé correspond à la donnée des quatre matrices G, H_1, H_2 et K. Sans doute on peut acquitter Bourbaki (Algèbre, chapitre 10) au bénéfice du doute, et de la grande science de ses auteurs. Mais les épigones ? Ces preuves évoquent immanquablement pour le lecteur averti le fameux aphorisme : pourquoi faire simple quand on peut faire compliqué ? Comment épater les étudiants ou les collègues si les choses sont si simples qu'elles peuvent être comprises avec seulement un petit peu de bon sens ? La complication au lieu de la simplicité, telle semble être la règle universelle du pédantisme qui triomphe à l'Université.

générateurs par les nouveaux et on prend comme nouvelles relations, d'une part, les anciennes dans lesquelles on a remplacé les anciens générateurs par leur expression en fonction des nouveaux, et d'autre part, les relations qui expriment que les nouveaux générateurs se réexpriment en fonction d'eux mêmes en passant par les anciens. Plus précisément, supposons on ait des générateurs $g_1, ..., g_n$ avec des relations $R_1(g_1, ..., g_n), \ldots, R_s(g_1, ..., g_n)$ qui présentent une structure M. Si on a d'autres générateurs $h_1, \ldots, h_m$, on les exprime en fonction des g_j : $h_i = H_i(g)$. On note $S_i(h_i, g_1, \ldots, g_n)$ la relation correspondante. On exprime les g_j en fonction des h_i : $g_j = G_j(h)$. On note $T_j(g_j, h_1, \ldots, h_m)$ la relation correspondante. La structure ne change pas si on remplace la présentation $(g_1, \ldots, g_n; R_1, \ldots, R_s)$ par $(g_1, \ldots, g_n, h_1, \ldots, h_m; R_1, \ldots, R_s, S_1, \ldots, S_m)$. Comme les relations T_j sont vraies elles sont conséquences de $R_1, \ldots, R_s, S_1, \ldots, S_m$. Donc la structure est toujours la même avec la présentation suivante $(g_1, \ldots, g_n, h_1, \ldots, h_m; R_1, \ldots, R_s, S_1, \ldots, S_m, T_1, \ldots, T_n)$. Maintenant, dans chacune des relations R_k et S_j, on peut remplacer chaque g_i par son expression en fonction des h_j (qui est donnée dans T_j) et cela ne change toujours pas la structure présentée. On obtient $(g_1, \ldots, g_n, h_1, \ldots, h_m; R'_1, \ldots, R'_s, S'_1, \ldots, S'_m, T_1, \ldots, T_n)$. Si on enlève un à un les couples $(g_j; T_j)$ il est clair que la structure ne change pas non plus. Donc on a la présentation finie $(h_1, \ldots, h_m; R'_1, \ldots, R'_s, S'_1, \ldots, S'_m)$ ([15]).

Catégorie des modules de présentation finie

La catégorie des modules de présentation finie peut être construite à partir de la catégorie des modules libres de rang fini par un procédé purement catégorique.

Un module de présentation finie M est décrit par une application linéaire entre modules libres $\mathrm{P}_M : \mathrm{R}_M \to \mathrm{G}_M$. On a $M \simeq \mathrm{Coker}\,\mathrm{P}_M$ et $\pi_M : \mathrm{G}_M \to M$ est l'application linéaire surjective de noyau $\mathrm{Im}\,\mathrm{P}_M$. La matrice de P_M est une matrice de présentation de M.

Une application linéaire φ du module M (décrit par $(\mathrm{R}_M, \mathrm{G}_M, \mathrm{P}_M)$) vers le module N (décrit par $(\mathrm{R}_N, \mathrm{G}_N, \mathrm{P}_N)$) est décrite par deux applications linéaires $\mathrm{R}_\varphi : \mathrm{R}_M \to \mathrm{R}_N$ et $\mathrm{G}_\varphi : \mathrm{G}_M \to \mathrm{G}_N$ soumises à la relation de commutation $\mathrm{G}_\varphi \circ \mathrm{P}_M = \mathrm{P}_N \circ \mathrm{R}_\varphi$.

La somme de deux applications linéaires φ et ψ de M vers N représentées par $(\mathrm{R}_\varphi, \mathrm{G}_\varphi)$ et $(\mathrm{R}_\psi, \mathrm{G}_\psi)$ est représentée par $(\mathrm{R}_\varphi + \mathrm{R}_\psi, \mathrm{G}_\varphi + \mathrm{G}_\psi)$.

Pour représenter la composée de deux applications linéaires, on compose leurs représentations.

Enfin une application linéaire φ de M vers N représentée par $(\mathrm{R}_\varphi, \mathrm{G}_\varphi)$ est nulle si et seulement si il existe $Z_\varphi : \mathrm{G}_M \to \mathrm{R}_N$ vérifiant $\mathrm{P}_N \circ Z_\varphi = \mathrm{G}_\varphi$.

Ceci montre que les problèmes concernant les modules de présentation finie se ramènent en général à des problèmes de résolution de systèmes linéaires sur $\mathbf{A}$. Par exemple si on donne M, N et φ et si on cherche une application linéaire $\sigma : N \to M$ vérifiant $\varphi \circ \sigma = \mathrm{I}_N$, on doit trouver $\mathrm{R}_\sigma : \mathrm{R}_N \to \mathrm{R}_M$, $\mathrm{G}_\sigma : \mathrm{G}_N \to \mathrm{G}_M$ et $Z : \mathrm{G}_N \to \mathrm{R}_N$ qui doivent vérifier

$$G_\sigma \circ \mathrm{P}_N = \mathrm{P}_M \circ \mathrm{R}_\sigma \quad \text{et} \quad \mathrm{P}_N \circ Z = \mathrm{G}_\varphi \circ \mathrm{G}_\sigma - \mathrm{I}_{\mathrm{G}_N}$$

Manipulations légitimes des matrices de présentation

On ne change pas la structure d'un module de présentation finie M lorsqu'on fait subir à sa matrice de présentation G une des transformations suivantes :

- ajout d'une colonne nulle, (ceci ne change pas le module des relations entre des générateurs fixés)
- suppression d'une colonne nulle, sauf à aboutir à une matrice vide,
- remplacement de G, de type $q \times m$, par G' de type $(q+1) \times (m+1)$ obtenue à partir de G en rajoutant une ligne nulle en dessous puis une colonne à droite avec 1 en position $(q+1, m+1)$, (ceci revient à rajouter un vecteur parmi les générateurs, en indiquant sa dépendance par rapport aux générateurs précédents) :

$$G \longmapsto G' = \begin{pmatrix} G & C \\ 0_{1,m} & 1 \end{pmatrix}$$

[15] Le lemme du serpent n'a donc vraiment rien à voir dans l'affaire.

- opération inverse de la précédente, sauf à aboutir à une matrice vide,
- ajout à une colonne d'une combinaison linéaire des autres colonnes, (ceci ne change pas le module des relations entre des générateurs fixés)
- ajout à une ligne d'une combinaison linéaire des autres lignes, (ceci revient à changer le système générateur en remplaccant un générateur g_k par un élément de la forme $g_k - \Sigma_{i\neq k}\ \lambda_i g_i$ sans changer les autres générateurs)
- permutation de colonnes ou de lignes,
- multiplication d'une colonne ou d'une ligne par un élément inversible (facultatif).

La preuve que nous avons faites précédemment pour le changement de système générateur correspond aux matrices de présentation successives que voici.

	m
q	G

	m	r
q	G	$-H_1$
r	0	I_r

Rajout de colonnes nulles.

	m	r	q
q	G	$-H_1$	0
r	0	I_r	0

Puisque $\mathrm{I}_q = H_1H_2 + GK$ on obtient la matrice suivante en rajoutant des combinaisons linéaires des premières colonnes au dernières.

	m	r	q
q	G	$-H_1$	I_q
r	0	I_r	$-H_2$

Puis avec $H_3 = \mathrm{I}_r - H_1H_2$ en utilisant le "pivot" I_q pour des manipulations élémentaires de colonnes

	m	r	q
q	0	0	I_q
r	GH_2	H_3	$-H_2$

$$H = \begin{array}{|c|c|} \multicolumn{1}{c}{m} & \multicolumn{1}{c}{r} \\ \hline GH_2 & H_3 \\ \hline \end{array} \; r$$

Plus généralement, on voit aisément que si G et H sont deux matrices de présentation d'un même module M, on peut passer de l'une à l'autre au moyen des transformations décrites ci-dessus. Notez aussi qu'un changement de base de $\mathbf{A}^q$ ou $\mathbf{A}^m$ correspond à la multiplication de G (à gauche ou à droite) par une matrice inversible, et peut être réalisé par les opérations décrites précédemment.

Le lemme classique suivant (cf. [18] chap. IV corollaire 1.6) résulte des considérations précédentes.

Lemme II.1 *Soient deux matrices $G \in \mathbf{A}^{q\times m}$ et $H \in \mathbf{A}^{r\times n}$. Alors les propriétés suivantes sont équivalentes:*

- *G et H présentent le même module (c'est-à-dire leurs conoyaux sont isomorphes)*
- *les deux matrices suivantes (cf. figure 1) sont élémentairement équivalentes : on passe de l'une à l'autre par des manipulations de lignes (ou colonnes) du type ajout à une ligne d'une combinaison linéaire des autres lignes.*
- *les deux matrices suivantes sont équivalentes*

	m	r	q	n
q	G	0	0	0
r	0	I_r	0	0

	m	r	q	n
q	0	0	I_q	0
r	0	0	0	H

FIG. 1: Les deux matrices.

III Modules projectifs de type fini, décomposition canonique

Les modules projectifs de type fini sont caractérisés de la manière suivante.

Proposition et définition III.1 (modules projectifs de type fini) *Les propriétés suivantes pour un $\mathbf{A}$-module M sont équivalentes.*

(*a*) *M est isomorphe à un facteur direct dans un $\mathbf{A}$-module $\mathbf{A}^n$, i.e. il existe un entier n, un $\mathbf{A}$-module N et un isomorphisme $M \oplus N \to \mathbf{A}^n$.*

(*b*) *Il existe un entier* n, *des générateurs* $(g_i)_{i=1,\dots,n}$ *de* M *et des formes linéaires* $(\alpha_i)_{i=1,\dots,n}$ *sur* M *telles que :* $\forall x \in M \quad x = \Sigma\, \alpha_i(x) g_i$.

(*b'*) M *est de type fini et pour tout système fini de générateurs* $(h_i)_{i=1,\dots,m}$ *de* M *il existe des formes linéaires* $(\beta_i)_{i=1,\dots,m}$ *sur* M *telles que :* $\forall x \in M \quad x = \Sigma\, \beta_i(x) h_i$.

(*b''*) *L'image de* $M^\star \otimes_{\mathbf{A}} M$ *dans* $\mathrm{Hom}_{\mathbf{A}}(M, M)$ *par l'homomorphisme canonique* θ_M *contient* Id_M *(*$M^\star$ *désigne le dual de* M *et* θ_M *est défini par* $\theta_M(\alpha \otimes a) = (x \mapsto \alpha(x)a)$.

(*c*) *Il existe un entier* n *et deux applications linéaires* $\varphi : M \to \mathbf{A}^n$ *et* $\psi : \mathbf{A}^n \to M$ *telles que* $\psi \circ \varphi = \mathrm{Id}_M$. *On a alors* $\mathbf{A}^n = \mathrm{Im}(\varphi) \oplus \mathrm{Ker}(\psi)$ *et* $M \simeq \mathrm{Im}(\varphi)$.

(*c'*) M *est de type fini et pour toute application linéaire surjective* $\psi : \mathbf{A}^m \to M$ *il existe une application linéaire* $\varphi : M \to \mathbf{A}^m$ *telle que* $\psi \circ \varphi = \mathrm{Id}_M$. *On a alors* $\mathbf{A}^m = \mathrm{Im}(\varphi) \oplus \mathrm{Ker}(\psi)$ *et* $M \simeq \mathrm{Im}(\varphi)$.

(*d*) M *est de présentation finie et si* M *est isomorphe au conoyau d'une matrice* $F \in \mathbf{A}^{q \times m}$ *il existe une matrice* $G \in \mathbf{A}^{m \times q}$ *telle que* $FGF = F$.

Lorsque ces conditions sont réalisées on dit que le module M *est* projectif de type fini.

Une matrice de projection est une matrice carrée F vérifiant $F^2 = F$. En pratique, conformément au (a) ci-dessus, nous considérerons un module projectif de type fini comme (copie par isomorphisme de l') image d'une matrice de projection F.

Lorsqu'on voit un module projectif de type fini selon la définition (c), la matrice de projection est celle de l'application linéaire $\varphi \circ \psi$. De même, si on utilise la définition (b) la matrice de projection est celle ayant pour entrées les $\alpha_j(g_i)$ en position (i, j).

Rappelons que si r est un idempotent dans un anneau $\mathbf{A}$, alors on a l'isomorphisme canonique $\mathbf{A} \simeq \mathbf{A}/(1-r) \times \mathbf{A}/(r)$ et $\mathbf{A}/(1-r)$ est une $\mathbf{A}$-algèbre canoniquement isomorphe à $r\mathbf{A}$: l'isomorphisme est donné par

$$\text{classe de } x \longmapsto rx$$

(r est élément neutre pour la multiplication à l'intérieur de $r\mathbf{A}$).
Si M est un $\mathbf{A}$-module, $M/(1-r)M$ est un $\mathbf{A}/(1-r)$-module canoniquement isomorphe à rM : l'isomorphisme est donné par

$$\text{classe de } x \longmapsto rx$$

Rappelons aussi que dans un anneau $\mathbf{A}$ un *système fondamental d'idempotents orthogonaux* (sfio) est une liste $(r_1, \dots, r_n)$ d'éléments de $\mathbf{A}$ qui vérifie :

$$r_i r_j = 0 \text{ si } i \neq j, \quad \text{et} \quad \Sigma\, r_i = 1$$

(nous ne réclamons pas qu'ils soient tous non nuls). Ceci implique que $r_h = r_h^2$ pour chaque h.

On obtient alors pour tout $\mathbf{A}$-module M :

Fait III.2 *Si* $(r_1, \dots, r_n)$ *est un sfio d'un anneau* $\mathbf{A}$, *et si* M *est un* $\mathbf{A}$*-module, on a :*

$$\mathbf{A} \simeq \mathbf{A}/(1-r_1) \times \cdots \times \mathbf{A}/(1-r_n)$$
$$M = r_1 M \oplus \cdots \oplus r_n M$$

Notez que $r_1 M$ est un $\mathbf{A}$-module et un $\mathbf{A}/(1-r_1)$-module, mais que ce n'est pas (sauf exception) un $\mathbf{A}/(1-r_2)$-module : $r_1 M \otimes_{\mathbf{A}} \mathbf{A}/(1-r_2) = \{0\}$.

Théorème III.3 (forme matricielle explicite du théorème 1 section 2.3)
Soit $\mathbf{A}$ *un anneau,* $F \in \mathrm{Mat}_n(\mathbf{A})$ *avec* $F^2 = F$ *et* M *le module projectif de type fini image de* F *dans* $\mathbf{A}^n$. *On définit les éléments* r_h *de* $\mathbf{A}$ *pour* $h = 0, \dots, n$ *par les égalités :*

$$\mathrm{R}_M(1+X) := \det(\mathrm{I}_n + XF), \qquad \mathrm{R}_M(X) =: r_0 + r_1 X + \cdots + r_n X^n$$

Alors :

— *a) La famille* $(r_h)_{h=0,\dots,n}$ *est un système fondamental d'idempotents orthogonaux de* $\mathbf{A}$. *L'idempotent* $r_0 = \det(\mathrm{I}_n - F)$ *engendre l'annulateur de* M.

— *b) Pour $h = 0, \ldots, n-1$, si u est un mineur d'ordre $h+1$ de F, on a $r_h u = 0$ dans* $\mathbf{A}$.

— *c) Si les $t_{h,i}$ sont les mineurs diagonaux d'ordre h de F, et si on pose $s_{h,i} = r_h t_{h,i}$ on obtient :*
- *la somme (pour h fixé) des $s_{h,i}$ est égale à r_h,*
- *chaque module $M_{s_{h,i}}$ est libre de rang h sur $\mathbf{A}_{s_{h,i}}$*
- *la matrice F est semblable sur $\mathbf{A}_{s_{h,i}}$ à la matrice $\mathrm{I}_{h,n,n}$*
- *la famille de tous les $s_{h,i}$ a pour somme 1 et convient pour le théorème 1.*

Proposition III.4 *Soit k un entier naturel et M un module projectif de type fini sur un anneau $\mathbf{A}$. Notons $\mathcal{N}$ le nilradical de $\mathbf{A}$. Supposons que F soit une matrice de projection de type $n \times n$ ayant pour image (un module isomorphe à) M. Alors les conditions suivantes sont équivalentes :*

(1) *M est de rang k, i.e., $\det(\mathrm{I}_n + XF) = (1+X)^k$*

(2) *La somme des mineurs diagonaux d'ordre k de F est égale à 1 et $\mathcal{D}_{k+1}(F) = 0$.*

(3) *Lorsqu'on évalue dynamiquement l'anneau $\mathbf{A}$ comme un corps, ou comme un anneau local, le module M devient libre de dimension k.*

(4) *Pour tout $s \in \mathbf{A}$, si M_s est libre sur $\mathbf{A}_s$, il est libre de rang k.*

(5) *Il existe $m \leq \binom{n}{k}$ éléments comaximaux s_i de $\mathbf{A}$ tels que chaque M_{s_i} est libre de dimension k sur $\mathbf{A}_{s_i}$.*

Nous renvoyons à [9, 20, 21] pour une explicitation précise du point (3) cette proposition.

Théorème III.5 *Un $\mathbf{A}$-module M est un module de rang constant égal à 1 si et seulement si l'homomorphisme canonique $M^\star \otimes_{\mathbf{A}} M \to \mathbf{A}$ est un isomorphisme.*

IV Compléments sur les principes local-global concrets

Nous traiterons ici des versions concrètes de principes du type local-global. Pour ces versions concrètes, la localisation est réclamée en un nombre fini de monoïdes de $\mathbf{A}$ qui sont comaximaux. Nous commenccons par des preuves de résultats donnés dans le corps du texte.

Preuve du principe local-global concret 3 page 18 Nous prouvons que les conditions locales sont suffisantes. Le point (3) a été prouvé page 22 avec le principe local-global dynamique 1. Nous montrons ici (1), 2 et (4).

(1) Supposons que M_{S_i} soit un $\mathbf{A}_{S_i}$-module de type fini pour chaque i. Montrons que M est de type fini. Soit $g_{i,1}, \ldots, g_{i,q_i}$ des éléments de M qui engendrent M_{S_i}. Soit $x \in M$ arbitraire. Pour chaque i on a un $s_i \in S_i$ et des $a_{i,j} \in \mathbf{A}$ convenables tels que :

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

on écrit $\sum_{i=1}^n b_i s_i = 1$. On voit que x est combinaison linéaire des $g_{i,j}$.

(2) Supposons que M_{S_i} soit un $\mathbf{A}_{S_i}$- module de présentation finie pour chaque i. Montrons que M est de présentation finie.
Soit $g_1, \ldots, g_q$ un système générateur de M.
Soit $(a_{i,h,1}, \ldots, a_{i,h,q}) \in \mathbf{A}_{S_i}^q$ des relations entre les $g_i/1 \in M_{S_i}$ (i.e., $\Sigma_j\ a_{i,h,j} g_j = 0$ dans M_{S_i}) pour $h = 1, \ldots, k_i$, qui engendrent le $\mathbf{A}_{S_i}$-module (contenu dans $\mathbf{A}_{S_i}^q$) des relations entre les $g_j/1$. On peut supposer sans perte de généralité que chaque $a_{i,h,j}$ est en fait un élément $a'_{i,h,j}/1$ avec $a'_{i,h,j} \in \mathbf{A}$. Il existe alors un $s_i \in S_i$ convenable tel que les vecteurs $s_i(a'_{i,h,1}, \ldots, a'_{i,h,q}) = (a''_{i,h,1}, \ldots, a''_{i,h,q}) \in \mathbf{A}^q$ soient des $\mathbf{A}$-relations entre les $g_j \in M$.
Montrons que les systèmes de relations ainsi construits entre les g_j engendrent toutes les relations. Soit en effet une relation arbitraire $(c_1, \ldots, c_q)$ entre les g_j. Considérons là comme une relation entre les $g_j/1 \in M_{S_i}$ et écrivons là en conséquence comme combinaison $\mathbf{A}_{S_i}$-linéaire des vecteurs $(a''_{i,h,1}, \ldots, a''_{i,h,q}) \in \mathbf{A}_{S_i}^q$. Après multiplication par un $s'_i \in S_i$ convenable on obtient une égalité dans $\mathbf{A}^q$:

$$s'_i(c_1, \ldots, c_q) = e_{i,1}(a''_{i,1,1}, \ldots, a''_{i,1,q}) + \cdots + e_{i,k_i}(a''_{i,k_i,1}, \ldots, a''_{i,k_i,q})$$

on écrit $\sum_{i=1}^{n} u_i s'_i = 1$. On voit que $(c_1, \ldots, c_q)$ est combinaison $\mathbf{A}$-linéaire des $(a''_{i,h,1}, \ldots, a''_{i,h,q})$.

(4) Supposons que M_{S_i} soit un $\mathbf{A}_{S_i}$-module projectif de type fini pour chaque i. Montrons que M est projectif de type fini. Nous savons déjà qu'il est de présentation finie. Soit F une matrice qui présente M. Pour que M soit projectif de type fini, il faut et suffit que l'on puisse trouver une matrice G (de dimensions convenables) telle que $FGF = F$. Si les coefficients de G sont considérées comme des inconnues, on doit donc résoudre un système linéaire. Ce système linéaire admet une solution localement puisque chaque M_{S_i} est projectif de type fini. On conclut donc par le principe de recollement concret des solutions de systèmes linéaires. □

Principe local-global concret 6 (recollement concret des suites exactes)
Supposons que $S_1, \ldots S_n$ soient des monoïdes comaximaux de $\mathbf{A}$, et soit $f : M \to N$ et $g : N \to P$ des applications $\mathbf{A}$-linéaires entre $\mathbf{A}$-modules. Alors la suite

$$M \xrightarrow{f} N \xrightarrow{g} P$$

est exacte si et seulement si les suites

$$M_{S_i} \xrightarrow{f_{S_i}} N_{S_i} \xrightarrow{g_{S_i}} P_{S_i}$$

sont exactes pour $i \in \{1, \ldots, n\}$. En particulier :
Un $x \in M$ est dans $\mathrm{Ker} f$ si et seulement si $x/1$ est dans $\mathrm{Ker} f_{S_i}$ pour $i \in \{1, \ldots, n\}$.
Un $y \in N$ est dans $\mathrm{Im} f$ si et seulement si $y/1$ est dans $\mathrm{Im} f_{S_i}$ pour $i \in \{1, \ldots, n\}$.

Principe local-global concret 7 (recollement concret d'éléments dans un module, ou d'homomorphismes entre modules)

(1) *Soit $\mathbf{A}$ un anneau commutatif, $(S_i)_{1 \le i \le m}$ des monoïdes comaximaux de $\mathbf{A}$ et M un $\mathbf{A}$-module. Notons $M_i := M_{S_i}$ et $M_{i,j} := M_{S_i S_j}$ $(i < j)$.*
Soit un élément $(x_i)_{1 \le i \le m}$ du produit des M_i.
Pour qu'il existe un $x \in M$ vérifiant $x/1 = x_i$ dans chaque M_i il faut et suffit que pour chaque $i < j$ on ait $x_i/1 = x_j/1$ dans $M_{i,j}$. En outre cet x est alors déterminé de manière unique.

(2) *Supposons maintenant que M soit de présentation finie ou que $\mathbf{A}$ soit intègre et M de type fini. Soit un autre module N, et, pour $1 \le i \le m$ un homomorphisme $\psi_i : M_i \to N_i := N_{s_i}$. Pour qu'il existe un $\psi : M \to N$ vérifiant $\psi_{S_i} = \psi_i$ pour chaque i il faut et suffit que pour chaque $i < j$ on ait $(\psi_i)_{S_j} = (\psi_j)_{S_i}$ comme homomorphisme de $M_{i,j}$ vers $N_{i,j}$. En outre cet homomorphisme ψ est alors déterminé de manière unique.*

On notera que le principe s'applique en particulier pour le $\mathbf{A}$-module $\mathbf{A}$.

Preuve
1) La condition est clairement nécessaire. Voyons qu'elle est suffisante.
Montrons l'existence de x. Il existe des $s_i \in S_i$ et des y_i dans M tels qu'on ait $x_i = y_i/s_i$ dans chaque M_i. Le fait que $x_i/1 = x_j/1$ dans $M_{i,j}$ signifie que pour certains $s'_i \in S_i$ et $s'_j \in S_j$ on a $s_j s'_i s'_j y_i = s_i s'_i s'_j y_j$. Soient (a_i) des éléments de $\mathbf{A}$ tels que $\sum a_i s_i s'_i = 1$. Posons $x = \sum a_i s'_i y_i$. Nous devons montrer que $x/1 = x_i$ dans M_i pour chaque i. Par exemple pour $i = 1$. On écrit les égalités suivantes dans M

$$s_1 s'_1 x = s_1 s'_1 \sum a_i s'_i y_i = \sum a_i s_1 s'_1 s'_i y_i = \sum a_i s_i s'_1 s'_i y_1 = \left(\sum a_i s_i s'_i\right) s'_1 y_1 = s'_1 y_1$$

Donc $s_1 s'_1 x = s'_1 y_1$ dans M et $x = y_1/s_1$ dans M_{S_1}.
Enfin, l'unicité de x résulte du principe de recollement concret des égalités.
2) Cela résulte du point (1), vu le fait I.10. □

Vu le fait I.5 concernant la localisation des déterminants, et vu le théorème 1, on obtient la caractérisation suivante du déterminant d'un endomorphisme, qui permet de ramener toute propriété concernant les déterminants au cas des modules libres (par exemple le théorème de Cayley-Hamilton).

Proposition IV.1 *Étant donné un endomorphisme φ d'un module projectif de type fini M, l'élément* $\det(\varphi)$ *est caractérisé par la propriété suivante. Si $s \in \mathbf{A}$ est tel que M_s soit libre, alors* $\det(\varphi)_s = \det(\varphi_s)$.

Notez que le principe de recollement 7 peut servir à donner une définition du déterminant d'un endomorphisme d'un module projectif de type fini en se ramenant au cas des modules libres, si on a démontré auparavant le théorème 1.

Nous donnons maintenant le principe local-global abstrait correspondant au principe local-global concret 2 page 17 pour bien mettre en évidence que ce dernier en est la version constructive.

Principe local-global abstrait 3 *Soit $a, b \in \mathbf{A}$. Alors on a les équivalences suivantes :*

(1) *Recollement abstrait des égalités :*

$$a = b \text{ dans } \mathbf{A} \iff \forall \mathcal{P} \in \mathrm{Spec}(\mathbf{A})\ a/1 = b/1 \text{ dans } \mathbf{A}_{\mathcal{P}}$$

(2) *Recollement abstrait des non diviseurs de zéro :*

$$a \text{ est non diviseur de zéro dans } \mathbf{A} \iff$$
$$\forall \mathcal{P} \in \mathrm{Spec}(\mathbf{A})\ a/1 \text{ est non diviseur de zéro dans } \mathbf{A}_{\mathcal{P}}$$

(3) *Recollement abstrait des inversibles :*

$$a \text{ est inversible dans } \mathbf{A} \iff$$
$$\forall \mathcal{P} \in \mathrm{Spec}(\mathbf{A})\ a/1 \text{ est inversible dans } \mathbf{A}_{\mathcal{P}}$$

(4) *Recollement abstrait des solutions de systèmes linéaires : soit B une matrice $\in \mathbf{A}^{m\times n}$ et C un vecteur colonne $\in \mathbf{A}^{m\times 1}$.*

$$\text{Le système linéaire } BX = C \text{ admet une solution dans } \mathbf{A}^{n\times 1}$$
$$\iff$$
$$\forall \mathcal{P} \in \mathrm{Spec}(\mathbf{A}) \text{ le système linéaire } BX = C \text{ admet une solution dans } \mathbf{A}_{\mathcal{P}}{}^{n\times 1}$$

(5) *Recollement abstrait des solutions de systèmes linéaires sous conditions homogènes : soit B une matrice et C un vecteur colonne dont les entrées sont des indéterminées, soit enfin (φ_ℓ) une famille de polynomes homogènes (à coefficients dans $\mathbf{A}$) en les entrées de B et C. Dans chacune des deux implications ci-dessous, les entrées de B et C sont spécialisées dans l'anneau $\mathbf{A}$, et un $\forall$ est implicite devant l'implication.*

$$(\wedge_\ell\, \varphi_\ell(B,C) =_{\mathbf{A}} 0) \Rightarrow \text{le système } BX = C \text{ admet une solution dans } \mathbf{A}^{n\times 1}$$
$$\iff$$
$$\forall \mathcal{P} \in \mathrm{Spec}(\mathbf{A}) : ((\wedge_\ell\, \varphi_\ell(B,C) =_{\mathbf{A}_{\mathcal{P}}} 0) \Rightarrow \text{le système } BX = C \text{ admet une solution dans } \mathbf{A}_{\mathcal{P}}{}^{n\times 1}$$

(6) *Recollement abstrait de facteurs directs : soit M un sous module de type fini d'un module de présentation finie N.*

$$M \text{ est facteur direct dans } N$$
$$\iff$$
$$\forall \mathcal{P} \in \mathrm{Spec}(\mathbf{A})\ M_{\mathcal{P}} \text{ est facteur direct dans } N_{\mathcal{P}}$$

Montrons qu'en mathématiques classiques le principe abstrait et le principe concret sont équivalents. Il suffit de traiter le point (4) et de montrer que la condition locale est suffisante.

Supposons tout d'abord vrai le principe concret et montrons le principe abstrait. Pour chaque idéal premier $\mathcal{P}$ on peut trouver $s \notin \mathcal{P}$ tel que le système linéaire $BX = C$ admet une solution dans $\mathbf{A}_s^{p\times 1}$. Les ouverts correspondants $U_s = \{\mathcal{P} \in \mathrm{Spec}(\mathbf{A});\ s \notin \mathcal{P}\}$ recouvrent $\mathrm{Spec}(\mathbf{A})$, donc les s correspondants engendrent $\mathbf{A}$ comme idéal, donc un nombre fini d'entre eux, $s_1, \ldots, s_m$ engendrent $\mathbf{A}$ comme idéal. On peut donc faire appel au principe local-global concret correspondant en considérant les monoïdes comaximaux engendrés par les s_i.

Supposons maintenant vrai le principe abstrait et montrons le principe concret. On a des monoïdes comaximaux $(S_i)_{i=1,\ldots,n}$ et pour chaque i le système linéaire $BX = C$ admet une solution dans $\mathbf{A}_{S_i}^{p\times 1}$. Si $\mathcal{P} \in \mathrm{Spec}(\mathbf{A})$ alors l'un des S_i ne coupe pas $\mathcal{P}$ et donc le système linéaire $BX = C$ admet une solution dans $\mathbf{A}_{\mathcal{P}}{}^{n\times 1}$. On peut donc faire appel au principe local-global abstrait correspondant.

Commentaire IV.1 Dans l'article [3], Hyman Bass fait le commentaire suivant concernant une version affaiblie du principe local-global abstrait 3(6) : *aussi élémentaire que ce résultat puisse paraître, il ne semble pas qu'aucune preuve puisse en être donnée sans utiliser, ou reconstruire pour l'essentiel, le foncteur* Tor^1. Ce commentaire est étonnant, au vu du caractère tout à fait anodin de notre preuve

du principe concret correspondant, laquelle ne calcule rien qui ressemble à un Tor^1. En fait, il semble que la machinerie calculatoire des Tor est souvent inutile, et qu'elle peut être court-circuitée par un argument plus élémentaire lorsque le but est de montrer la nullité d'un Tor^1.

V Quelques remarques sur les calculs dans les anneaux de Prüfer cohérents

Nous terminons par quelques lemmes qui peuvent faciliter les calculs dans les anneaux de Prüfer. La preuve du premier est directe.

Lemme V.1 (annulateurs) *Soit dans un anneau* **A** *des éléments* $x_1, \ldots, x_n$ *dont les annulateurs sont engendrés par des idempotents* $r_1, \ldots, r_n$. *Soit* $I = \langle x_1, \ldots, x_n \rangle$, $r = r_1 \cdots r_n$ *et* $x = x_1 + r_1 x_2 + \cdots + r_1 \cdots r_{n-1} x_n$. *Alors* $\mathrm{Ann}(I) = \mathrm{Ann}(x) = \langle r \rangle$.

Lemme V.2 *Un anneau cohérent est fortement discret si et seulement si il y a un test d'égalité à* $\langle 1 \rangle$ *pour les idéaux de type fini.*

Preuve Pour savoir si $a \in \langle x_1, \ldots, x_n \rangle$ on considère le module des relations pour $(a, x_1, \ldots, x_n)$. En projetant sur la première coordonnée on obtient un idéal de type fini J pour lequel il s'agit de savoir si $1 \in J$. □

HUM *Dans le cas d'un anneau de Prüfer cohérent, cela semble a priori moins simple que le critère du test de divisibilité donné à la proposition 4.4.6 pour les anneaux arithmétiques.*

Le quotient exact de deux éléments d'un anneau quasi intègre (voir page 10) se généralise aux idéaux de type fini dans le cas d'un anneau de Prüfer.

Lemme V.3 (quotient exact d'idéaux de type fini) *Soit dans un anneau de Prüfer cohérent* **A** *deux idéaux de type fini* $J = \langle y_1, \ldots, y_m \rangle \subseteq I = \langle x_1, \ldots, x_n \rangle$ *et* $x \in I$ *tel que* $\mathrm{Ann}(I) = \mathrm{Ann}(x) = \langle r \rangle$ *avec* r *idempotent.*

- *Il existe un unique idéal de type fini* I_1 *tel que* $I_1 I = \langle x \rangle$ *et* $r I_1 = 0$.
- *Il existe un unique idéal de type fini* L *tel que* $LI = J$ *et* $rL = 0$.
- *On a* $xL = I_1 J$.
- *Si* **A** *est fortement discret on peut calculer un système de* $n + m - 1$ *générateurs pour* L.

L'idéal L *ci-dessus sera appelé le* quotient exact *de* J *par* I.

Preuve La première affirmation est un cas particulier de la seconde. Dans la seconde, l'existence d'un idéal de type fini L' tel que $L'I = J$ tient à ce que **A** est arithmétique. Ensuite on pose $L = sL'$ avec $s = 1 - r$ et on a $LI = L'sI = L'I = J$. L'unicité de L résulte alors du théorème 9 (10).
L'égalité $xL = I_1 J$ résulte de $I_1 I = \langle x \rangle$ et $LI = J$. Pour calculer L, on calcule d'abord I_1 (avec n générateurs $z_j = sz_j$) puis $I_1 J$ avec $n + m - 1$ générateurs (cf. lemme 4.4.7). En présence du test de divisibilité, chaque générateur de $I_1 J = xL$ s'écrit sous forme xu, et les su correspondants donnent les générateurs de L. □

Lemme V.4 *Soit un anneau de Prüfer cohérent* **A**. *Le module des relations entre* n *éléments* $c_1, \ldots, c_n$ *de* **A** *est engendré par* n *éléments.*

Preuve On sait en effet que le noyau de la forme linéaire $\varphi : (y_i) \mapsto \sum_i c_i y_i$ est facteur direct dans $\mathbf{A}^n$ (théorème 4 section 4.3).
En fait le calcul du module des relations peut être fait à la manière de celui de la proposition 3.3.9. Notons en effet e_i l'idempotent qui définit "l'anneau où vit c_i" c'est-à-dire $e_i = 1 - r_i$ et $\langle r_i \rangle = \mathrm{Ann}(c_i)$. Dans cette proposition le résultat reste vrai, sans l'hypothèse que les c_i sont non diviseurs de zéro, si l'anneau est quasi intègre, si $1 - \sum_i s_i = \prod_i r_i$ (l'idempotent annulateur de I) et si les $a_{i,j}$ vérifient $r_i a_{i,j} = 0$.
En développant $\prod_i (e_i + r_i) = 1$ et en ne gardant que les termes non nuls on obtient un sfio qui casse l'anneau en plusieurs morceaux. Dans chaque morceau les c_i sont nuls ou non diviseurs de zéro. La projection qui définit le noyau de φ comme facteur direct se calcule alors facilement dans chaque morceau. □

On en déduit immédiatement.

Lemme V.5 *Dans un anneau de Prüfer cohérent* **A** *soient deux idéaux de type fini* $J = \langle y_1, \ldots, y_m \rangle$, $I = \langle x_1, \ldots, x_n \rangle$. *On peut calculer un système de* $n + m$ *générateurs de* $I \cap J$.

Références

[1] Arnold J., Gilmer R. *On the contents of polynomials.* Proc. Amer. Math. Soc. **24** , (1970), 556–562.

[2] Banaschewski B., Vermeulen J. *Polynomials and radical ideals.* J. Pure Appl. Algebra **113** (3), (1996), 219–227.

[3] Bass H. *Torsion free and projective modules.* Trans. Amer. Math. Soc. **102**, (1962) 319–327..

[4] Bourbaki. *Algèbre. Chap. 6. Groupes et corps ordonnés.* Hermann, (19..).

[5] Bourbaki. *Algèbre. Chap. 10. Algèbre homologique.* Hermann, (1961).

[6] Bourbaki. *Algèbre Commutative. Chap. 7. Diviseurs.* Hermann, (19..).

[7] Bridges D., Richman F. *Varieties of Constructive Mathematics.* London Math. Soc. LNS 97. Cambridge University Press (1987).

[8] Coquand T., Lombardi H. *Hidden constructions in abstract algebra (3) Krull dimension of distributive lattices and commutative rings.* A paraître chez M. Dekker. Proceedings for the Fourth International Conference on Commutative Ring Theory and Applications held June 7 - 11 , 2001 in Fez, Morocco.

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

[10] Coquand T., Persson H. *Valuations and Dedekind's Prague Theorem* Journal of Pure and Applied Algebra **155** (2001) 121–129

[11] Edwards H. M. *Divisor theory.* Birkhaüser. Boston MA. 1990.

[12] Gilmer R. *Multiplicative Ideal Theory.* Queens papers in pure and applied Math, vol. 90, 1992.

[13] Glaz S. Vasconcelos, W. *The content of Gaussian polynomials.* J. Algebra **202** no. 1, (1998), 1–9.

[14] Hermida J., Sánchez-Giralda T. *Linear Equations over Commutative Rings and Determinantal Ideals.* Journal of Algebra **99**, (1986) 72–79.

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

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

[17] Knight J. *Commutative Algebra.* London Mathematical Society LNS n°5. Cambridge University Press, (1971).

[18] Kunz E. *Introduction to Commutative Algebra and Algebraic Geometry.* Birkhäuser, (1991).

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

[20] Lombardi H. *Relecture constructive de la théorie d'Artin-Schreier.* Annals of Pure and Applied Logic **91**, (1998), 59–92.

[21] Lombardi H. *Le contenu constructif d'un principe local-global avec une application à la structure d'un module projectif de type fini.* Publications Mathématiques de Besanccon. Théorie des nombres. Fascicule 94–95 & 95–96, (1997).

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

[23] Lombardi H. *Hidden constructions in abstract algebra (1) Integral dependance.* Journal of Pure and Applied Algebra **167**, (2002) 259–267.

[24] Lombardi H. *Constructions cachées en algèbre abstraite (4) La solution du 17ème problème de Hilbert par la théorie d'Artin-Schreier.* Publications Mathématiques de Besanccon. Théorie des nombres (2002).

[25] Lombardi H., Quitté C. *Constructions cachées en algèbre abstraite (2) Le principe local global.* A paraître chez M. Dekker. Proceedings for the Fourth International Conference on Commutative Ring Theory and Applications held June 7 - 11 , 2001 in Fez, Morocco.

[26] Lombardi H., Quitté C. *Théorie constructive élémentaire des modules projectifs de type fini.* en préparation.

[27] Matsumura H. *Commutative ring theory.* Cambridge studies in advanced mathematics n°8. Cambridge University Press. 1989.

[28] Mishra B. *Algorithmic Algebra.* Springer. 1993.

[29] Mines R., Julian W., Richman F. *Algebraic numbers, a constructive development.* Pac. J. Math., **74**, (1978), 91–102.

[30] Mines R., Richman F., Ruitenburg W. *A Course in Constructive Algebra.* Universitext. Springer-Verlag, (1988).

[31] Northcott D. *Finite free resolutions.* Cambridge tracts in mathematics n°71. Cambridge University Press, (1976).

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

[33] Richman F. *Non trivial uses of trivial rings.* Proc. Amer. Math. Soc., **103** (1988), 1012–1014.