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* **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* **A***-module plat de type fini. Si* **A** *est un anneau local, M est libre. Si* **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 **A** sont dits *comaximaux* dans **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 **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 **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 **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 $J_1 = \sum_{k=1}^{n} I_k$, $J_2 = \sum_{1\le j<k\le n}(I_j \cap I_k)$, $\ldots$, $J_r = \sum_{1\le j_1<\cdots<j_r\le n}(I_{j_1} \cap \cdots \cap I_{j_r})$, $\ldots$, $J_n = \cap_{k=1}^{n} I_k$. 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 $I \le_T J$, 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* $\min(I, J) = I + J$.
- $\forall I, J \;\; I \cdot J = (I \wedge J) \cdot (I \vee J)$
- $\forall I, J, K \;\; (\, I \cdot (J \wedge K) = (I \cdot J) \wedge (I \cdot K) \quad \text{et} \quad I \cdot (J \vee K) = (I \cdot J) \vee (I \cdot K)\,)$
- $\forall I, J \in T \; \forall n \in \mathbb{N} \;\; (I^n \wedge J^n = (I \wedge J)^n \;\; \text{et} \;\; I^n \vee J^n = (I \vee J)^n)$
- *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 $J_1 \le_T I$, $J_2 \le_T I$ 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

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

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* $\mathbf{A}_P$ *où* P *est l'image réciproque du radical* $\mathcal{R}(\mathbf{B})$ *(*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 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) $\mathrm{Rad}(\mathbf{A}) = \mathcal{R}(\mathbf{A})$ 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... □