Calcul matriciel généralisé sur les domaines de Prüfer

Gema M. Diaz-Toca[*], Henri Lombardi[†]

Résumé

Dans cet article nous présentons un algorithme pour calculer la forme de Hermite d'une pseudo-matrice sur un domaine de Prüfer. Ceci nous donne des preuves constructives des principaux résultats théoriques concernant les modules de présentation finie et projectifs de type fini sur le domaines de Prüfer, et nous permet de discuter la résolution des systèmes linéaires sur les domaines de Prüfer. Nous généralisons ainsi la méthodologie développée par Henri Cohen pour les domaines de Dedekind. Nous présentons également des résultats concernant la réduction de Smith sur les domaines de Prüfer de dimension $\leqslant 1$.

Abstract

In this paper, we first present an algorithm for computing the Hermite normal form of pseudo-matrices over Prüfer domains. This algorithm allows us to provide constructive proofs of the main theoretical results on finitely presented modules over Prüfer domains and to discuss the resolution of linear systems. In some sense, we generalize the methodology developed by Henri Cohen for Dedekind domains. Finally, we present some results over Prüfer domains of dimension one about the Smith normal form.

Keywords : Prüfer Domains ; Hermite normal form ; pseudomatrices.
MSC classes : 13C10, 13P99.

[*]Departamento de Ingeniería y Tecnología de Computadores, Universidad de Murcia, 30100 Murcia, Spain, gemadiaz@um.es, supported by the Spanish Ministerio de Ciencia, Innovación y Universidades and by the European Regional Development Fund (ERDF), under the project MTM2017-88796-P.

[†]Laboratoire de Mathématiques (UMR CNRS 6623), Université de Franche-Comté, 25030 Besançon, France,henri.lombardi@univ-fcomte.fr

1 Introduction

La résolution algorithmique des systèmes linéaires sur les corps ou sur les anneaux principaux est classique, et elle est équivalente au traitement des matrices par des manipulations élémentaires (et des manipulations de Bezout dans le cas des anneaux principaux) de façon à les ramener à une forme réduite convenable.

On vise ici la généralisation de ce type de procédé à des domaines de Prüfer arbitraires.

À cet effet, on adapte pour un domaine de Prüfer arbitraire le calcul matriciel généralisé d'Henri Cohen [Cohen, Chapitre 1], qu'il a introduit dans le cadre du traitement algorithmique des anneaux d'entiers de corps de nombres.

Notre but est de montrer qu'avec un calcul matriciel généralisé on peut obtenir pour un domaine de Prüfer l'analogue des réductions classiques pour un domaine de Bezout. Ceci donne un traitement algorithmique systématique et «agréable», qui permet d'obtenir, comme conséquences du calcul matriciel considéré, les théorèmes généraux sur les domaines de Prüfer.

En particulier cela donne un moyen pratique pour discuter les systèmes linéaires à coefficients et inconnues dans le domaine de Prüfer considéré.

Du point de vue du Calcul Formel, notre approche permet de traiter des situations plus générales que les approches usuelles. Par exemple, pour les anneaux d'entiers de corps de nombres, comme le véritable ingrédient de nos algorithmes se limite à l'inversion des idéaux de type fini, notre approche permet de traiter le cas où la factorisation du discriminant est impossible en pratique, et plus généralement le cas où le calcul d'une base d'entiers sur $\mathbb{Z}$ est trop coûteux.

Notons que pour les domaines de Dedekind, et plus généralement pour les domaines de Prüfer de dimension $\leqslant 1$, on obtient des résultats plus précis, du type de la réduction de Smith des matrices sur les anneaux principaux. Cela sera discuté dans la section 5. Les méthodes ici relèvent des calculs modulaires et sont les seules vraiment efficaces pour éviter l'explosion de la taille des objets dans les calculs intermédiaires.

2 Quelques rappels

Le premier paragraphe de cette section donne des définitions classiques que nous donnons si nécessaire sous forme constructive. Le deuxième est consacré à des rappels concernant les calculs avec les idéaux de type fini sur les domaines de Prüfer. Le troisième rappelle les principaux résultats concernant les calculs matriciels sur les domaines de Bezout.

Notre référence pour les résultats classiques exposés dans cette section est le livre [Modules], dans lequel tous les résultats sont démontrés de manière algorithmique.

2.1 Quelques définitions

Un anneau $\mathbf{A}$ est dit ***zéro-dimensionnel*** si l'axiome suivant est vérifié

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

Un anneau intègre $\mathbf{A}$ est dit ***de dimension*** $\leqslant 1$ lorsque pour tout $b \neq 0$ dans $\mathbf{A}$, l'anneau quotient $\mathbf{A}/\langle b\rangle$ est zéro-dimensionnel.

Sur un anneau $\mathbf{A}$ arbitraire, un idéal de type fini $\mathfrak{a} = \langle a_1, \ldots, a_n\rangle$ est dit ***localement principal*** s'il existe $s_1, \ldots, s_n \in \mathbf{A}$ tels que $\sum_{i\in[\![1..n]\!]} s_i = 1$ et $s_i\mathfrak{a} \subseteq \langle a_i\rangle$ pour chaque s_i.

Un anneau $\mathbf{A}$ arbitraire est dit ***arithmétique*** si tout idéal de type fini est localement principal.

Un idéal de type fini $\mathfrak{a} = \langle a_1, \ldots, a_n\rangle$ est dit ***inversible*** s'il existe un élément régulier c et un idéal de type fini $\mathfrak{b}$ tel que $\mathfrak{ab} = \langle c\rangle$. Il revient au même de dire que $\mathfrak{a}$ est localement principal et contient un élément régulier.

Un ***domaine de Prüfer*** est un anneau arithmétique intègre. De manière équivalente, c'est un anneau intègre dans lequel tout idéal de type fini non nul est inversible. Dans ce cas, pour tout $a \neq 0$ dans l'idéal de type fini $\mathfrak{a}$, le transporteur $(\langle a\rangle : \mathfrak{a})$ est de type fini, et l'on a l'égalité $\mathfrak{a}\,(\langle a\rangle : \mathfrak{a}) = \langle a\rangle$.

Une matrice $A = (a_{ij})$ sur un anneau arbitraire est dite ***en forme de Smith*** lorsque :
— tous les coefficients a_{ij} sont nuls sauf éventuellement des «coefficients diagonnaux» $a_i = a_{ii}$,
— et a_i divise a_{i+1} pour $i \geqslant 1$.

Lorsque la matrice M admet une réduction de Smith, le module $\operatorname{Coker} M$ est isomorphe à la somme directe des $\mathbf{A}/\langle a_i\rangle$ et les idéaux $\langle a_i\rangle$ sont uniquement déterminés en vertu du fait 1.

Pour un anneau intègre, cela signifie que les a_i sont eux-mêmes bien déterminés «à une unité multiplicative près».

On appelle ***anneau de Smith*** un anneau $\mathbf{A}$ sur lequel toute matrice M est équivalente à une matrice en forme de Smith.

L'***idéal déterminantiel d'ordre*** k d'une matrice M est l'idéal de type fini $\mathfrak{D}_k(M)$ engendré par les mineurs d'ordre k de M.

L'***idéal de Fitting d'ordre*** k d'un module de présentation finie P, conoyau d'une matrice $M \in \mathbb{M}_{n,m}(\mathbf{A})$, est défini par l'égalité $\mathfrak{F}_k(P) := \mathfrak{D}_{n-k}(M)$. Il ne dépend pas de la présentation choisie pour P.

On rappelle les résultats suivants.

Fait (1). ([Modules, théorème V-9.1], [MRR, théorème V-2.4])
Soient $\mathfrak{a}_1 \subseteq \cdots \subseteq \mathfrak{a}_n$ *et* $\mathfrak{b}_1 \subseteq \cdots \subseteq \mathfrak{b}_m$ *des idéaux de* $\mathbf{A}$ *avec* $n \leqslant m$. *Si un module* P *est isomorphe à la fois à* $\mathbf{A}/\mathfrak{a}_1 \oplus \cdots \oplus \mathbf{A}/\mathfrak{a}_n$ *et* $\mathbf{A}/\mathfrak{b}_1 \oplus \cdots \oplus \mathbf{A}/\mathfrak{b}_m$, *alors on a*

1. $\mathfrak{b}_k = \mathbf{A}$ *pour* $n < k \leqslant m$;
2. *et* $\mathfrak{b}_k = \mathfrak{a}_k$ *pour* $1 \leqslant k \leqslant n$.

Fait (2). ([ACMC, exercice IV-16])
Soit $P \simeq \mathbf{A}/\mathfrak{a}_1 \oplus \cdots \oplus \mathbf{A}/\mathfrak{a}_n$ *avec des idéaux de type fini* $\mathfrak{a}_1 \supseteq \cdots \supseteq \mathfrak{a}_n$. *Alors pour* $k \in [\![1..n]\!]$, *on a* $\mathfrak{F}_{n-k}(P) = \mathfrak{a}_1 \cdots \mathfrak{a}_k$.

Fait (3). ([Modules, exercice XVI-9])
Sur un anneau arithmétique zéro-dimensionnel, toute matrice se ramène par manipulations élémentaires de lignes et de colonnes à une matrice en forme de Smith.

Idéaux fractionnaires de type fini

Il est souvent confortable de considérer, sur un pied d'égalité avec les idéaux de type fini, les ***idéaux fractionnaires de type fini***.

Pour un anneau intègre $\mathbf{A}$ de corps de fractions $\mathbf{K}$, nous noterons $\mathrm{Iff}(\mathbf{A})$ l'ensemble des idéaux fractionnaires de type fini de $\mathbf{A}$, c'est-à-dire l'ensemble des sous-$\mathbf{A}$-modules de type fini de $\mathbf{K}$.

Un idéal fractionnaire de type fini $\mathfrak{b}$ peut toujours s'écrire

$$\mathfrak{b} = \tfrac{1}{a}\,\mathfrak{a} = \tfrac{1}{a}\,\langle a_1, \ldots, a_n\rangle \text{ avec } a_1, \ldots, a_n \in \mathbf{A}, \text{ et } a \in \mathbf{A}^*.$$

On dit qu'il est localement principal lorsque $\mathfrak{a}$ est localement principal. Il admet alors la même matrice de localisation principale à coefficients dans $\mathbf{A}$ (voir la section 2.2) que $\mathfrak{a}$, avec les mêmes propriétés.

Le produit de deux idéaux fractionnaires est défini de façon naturelle et l'on a $x\mathfrak{a}\, y\mathfrak{b} = xy\,\mathfrak{a}\mathfrak{b}$ pour $x, y \in \mathbf{K}$.

Concernant les ***transporteurs***, il faut distinguer entre l'idéal fractionnaire

$$(\mathfrak{a} : \mathfrak{b})_{\mathbf{K}} = \{\, x \in \mathbf{K} \mid x\mathfrak{b} \subseteq \mathfrak{a} \,\}$$

et l'idéal (au sens usuel) $(\mathfrak{a} : \mathfrak{b})_{\mathbf{A}} = \{\, x \in \mathbf{A} \mid x\mathfrak{b} \subseteq \mathfrak{a} \,\}$.

Un idéal fractionnaire localement principal non nul $\mathfrak{b}$ admet un inverse $\mathfrak{b}^{-1}$ au sens du produit défini dans $\mathrm{Iff}(\mathbf{A})$: c'est l'idéal fractionnaire $(\mathbf{A} : \mathfrak{b})_{\mathbf{K}}$.

Notons que l'application bilinéaire $\theta : \mathfrak{b} \times \mathfrak{b}^{-1} \to \mathbf{A}$, $(x, y) \mapsto xy$ est une dualité, c'est-à-dire qu'elle permet d'identifier $\mathfrak{b}^{-1}$ au $\mathbf{A}$-module dual de $\mathfrak{b}$.

Un idéal fractionnaire de type fini contenu dans $\mathbf{A}$ est un idéal de type fini usuel et il est appelé un ***idéal entier*** si l'on est dans le contexte des idéaux fractionnaires.

2.2 Calculs sur les idéaux de type fini dans les domaines de Prüfer

Matrice de localisation principale

Un anneau intègre $\mathbf{Z}$ est un domaine de Prüfer *d'un point de vue algorithmique* lorsque l'on dispose d'un algorithme général qui permet d'inverser un idéal de type fini arbitraire.

Comme l'a remarqué Dedekind lorsqu'il insiste sur ce qu'il estime être la propriété la plus décisive dans les anneaux d'entiers de corps de nombres, on peut formuler l'inversibilité de l'idéal $\mathfrak{a} = \langle a_1, \ldots, a_n \rangle \subseteq \mathbf{Z}$ (les $a_i \neq 0$) de la manière suivante.

1. Il existe γ_1, …, γ_n dans $\mathbf{K}$ tels que $\sum_i \gamma_i a_i = 1$ et chacun des $\gamma_i a_j$ est dans $\mathbf{Z}$.

Deux formulations équivalentes sont les suivantes.

2. Il existe s_1, …, $s_n \in \mathbf{Z}$ de somme 1 tels que l'on ait $s_i\mathfrak{a} \subseteq \langle a_i \rangle$ pour chaque s_i non nul.

3. Il existe une ***matrice de localisation principale pour*** *$(a_1, \ldots, a_n)$ i.e., une matrice $C = (c_{ij}) \in \mathbb{M}_n(\mathbf{Z})$ satisfaisant*

— $\mathrm{Tr}(C) = 1$,

— *chaque ligne de C est* ***proportionnelle*** *à $[\, a_1 \ \ldots \ a_n \,]$, i.e.*

$$\begin{vmatrix} c_{i,\ell} & c_{i,j} \\ a_\ell & a_j \end{vmatrix} = 0 \text{ pour tous } i, j, \ell.$$

Pour passer de *1* à *2* on pose $s_i = \gamma_i a_i$, et dans l'autre sens $\gamma_i = \frac{s_i}{a_i}$. Pour passer de *2* à *3* on pose $c_{ij} = \frac{s_i a_j}{a_i}$.

La matrice de localisation principale permet de nombreux calculs, comme indiqués dans [Modules, théorème IX-2.3, lemme IX-2.5, et exercice XVI-8]. En particulier pour un anneau intègre, on a $C^2 = C$ (matrice de projection de rang 1) et $\mathrm{I}_n - C$ est une matrice de présentation de l'idéal $\mathfrak{a}$ pour le système générateur $(a_1, \ldots, a_n)$. En tant que $\mathbf{Z}$-module, $\mathfrak{a}$ est isomorphe à l'image de C dans $\mathbf{Z}^n$.

Notons que, lorsque la divisibilité est explicite dans $\mathbf{Z}$, une matrice de localisation principale pour $(a_1, \ldots, a_n)$ est connue à partir de sa diagonale.

Nous ferons cette hypothèse de divisibilité explicite dans la suite.

Le système générateur $(a_1, \ldots, a_n)$ d'un idéal de type fini sera toujours accompagné d'une liste d'éléments s_i de somme 1 qui satisfont les inclusions $s_i\mathfrak{a} \subseteq \langle a_i \rangle$.

Sans l'hypothèse de divisibilité explicite, il faudrait travailler avec les matrices de localisation principale elles-mêmes, qui sont des objets plus lourds à manipuler.

Pour qu'un anneau intègre $\mathbf{Z}$ soit un domaine de Prüfer, il suffit que les idéaux *à deux générateurs* soient inversibles, ce qui s'exprime comme suit. Pour tous a, $b \in \mathbf{Z}$, il existe u, v, s, $t \in \mathbf{Z}$ satisfaisant :

$$s + t = 1,\ sa = vb,\ tb = wa. \tag{1}$$

Autrement dit, on a pour (a, b) la matrice de localisation principale $\begin{bmatrix} t & w \\ v & s \end{bmatrix}$.

Supposons $a \neq 0$. Alors $ts = vw$, $\langle t, w\rangle = \frac{t}{a}\langle a, b\rangle$ et $\langle t, w\rangle \langle t, v\rangle = \langle t\rangle$. Donc, si $t, a \neq 0$, $\langle t, w\rangle^{-1} = \frac{1}{t}\langle t, v\rangle$ et $\langle a, b\rangle^{-1} = \frac{1}{a}\langle t, v\rangle$ (notation des idéaux fractionnaires).

Opérations élémentaires sur les idéaux de type fini

Nous supposons travailler avec un domaine de Prüfer explicite. Autrement dit une boite noire[1] donne pour toute suite finie non nulle $(a_1, \ldots, a_n) = (\underline{a})$ une suite finie $(s_1, \ldots, s_n) = (\underline{s})$ avec $\sum_i s_i = 1$ et $s_i a_j \in \langle a_i\rangle$ pour tous i, j.

Nous supposons aussi que le domaine de Prüfer est à divisibilité explicite.

Tout ce qui est écrit par la suite fonctionne aussi bien avec des idéaux fractionnaires de type fini qu'avec des idéaux de type fini entiers. Nous parlerons donc simplement d'idéaux de type fini.

Signification de $s_k = 0$. Si $s_k = 0$, en additionnant les égalités $s_i a_k = c_{i,k} a_i$ pour $i \neq k$, on obtient l'égalité $a_k = \sum_{i\neq k} c_{i,k} a_i$, autrement dit le générateur a_k de l'idéal $\mathfrak{a}$ est superflu. En supprimant la ligne et la colonne correspondante, on obtient une matrice de localisation principale pour les a_i restants.

Inversement, si l'on rajoute un générateur combinaison linéaire de ceux déjà donnés, on peut obtenir une matrice de localisation principale pour le nouveau système générateur en rajoutant une ligne nulle pour le nouveau générateur, et la colonne correspondant au nouveau générateur qui exprime la combinaison linéaire comme indiqué ci-avant.

Pour $\mathfrak{a}$ et $\mathfrak{b}$ de type fini, on a $\boxed{1 \in (\mathfrak{a} : \mathfrak{b})_{\mathbf{Z}} + (\mathfrak{b} : \mathfrak{a})_{\mathbf{Z}}}$. On écrit $\mathfrak{a} = \langle a_1, \ldots, a_n\rangle$ et $\mathfrak{b} = \langle b_1, \ldots, b_p\rangle$. On a des s_i de somme 1 tels que $s_i\mathfrak{a} \subseteq \langle a_i\rangle$, des t_j de somme 1 tels que $t_j\mathfrak{b} \subseteq \langle b_j\rangle$, et pour chaque couple (i, j) deux éléments u_{ij} et v_{ij} de somme 1 tels que

$$u_{ij}\langle a_i, b_j\rangle \subseteq \langle a_i\rangle \text{ et } v_{ij}\langle a_i, b_j\rangle \subseteq \langle b_j\rangle.$$

On obtient donc

$$u_{ij}s_it_j(\mathfrak{a} + \mathfrak{b}) \subseteq \langle a_i\rangle \subseteq \mathfrak{a} \text{ et } v_{ij}s_it_j(\mathfrak{a} + \mathfrak{b}) \subseteq \langle b_j\rangle \subseteq \mathfrak{b}.$$

On prend $\boxed{s = \sum_{ij} u_{ij}s_it_j}$ et $\boxed{t = \sum_{ij} v_{ij}s_it_j}$. On a alors $s + t = 1$ et

1. Dans les cas que l'on traite sur machine, cette boite noire cache un algorithme.

$$s(\mathfrak{a}+\mathfrak{b}) \subseteq \mathfrak{a} \text{ (i.e. } s\mathfrak{b} \subseteq \mathfrak{a}) \quad \text{et} \quad t(\mathfrak{a}+\mathfrak{b}) \subseteq \mathfrak{b} \text{ (i.e. } t\mathfrak{a} \subseteq \mathfrak{b}).$$

Notons que lorsque $p = 1$ la matrice de localisation principale pour (b_1) est simplement I_1 (voir [Modules, exercice XVI-8]).

Somme (pgcd). Avec les mêmes données qu'au point précédent, on voit que si l'on pose

$$\boxed{u_i = \textstyle\sum_j u_{ij} s_i t_j} \quad \text{et} \quad \boxed{v_j = \textstyle\sum_i v_{ij} s_i t_j},$$

on a $u_i(\mathfrak{a}+\mathfrak{b}) \subseteq \langle a_i \rangle$, $v_j(\mathfrak{a}+\mathfrak{b}) \subseteq \langle b_j \rangle$ et $\sum_i u_i + \sum_j v_j = 1$.
Ainsi la liste $(u_1, \ldots, u_n, v_1, \ldots, v_p)$ convient pour le système générateur $(a_1, \ldots, a_n, b_1, \ldots, b_p)$ de l'idéal $\mathfrak{a}+\mathfrak{b}$.
NB : cette procédure explique pourquoi on peut se ramener au cas où la boite noire fonctionne uniquement pour les idéaux à deux générateurs.

Intersection (ppcm). Avec les mêmes données qu'avant, on a $\boxed{s\mathfrak{b} + t\mathfrak{a} = \mathfrak{a} \cap \mathfrak{b}}$. En effet, on a évidemment $s\mathfrak{b} \subseteq \mathfrak{b} \cap \mathfrak{a}$ et $t\mathfrak{a} \subseteq \mathfrak{b} \cap \mathfrak{a}$. Et pour l'autre inclusion $s\mathfrak{b} + t\mathfrak{a} \supseteq \mathfrak{a} \cap \mathfrak{b}$, si $m \in \mathfrak{a} \cap \mathfrak{b}$, alors $m = (s+t)m = sm + tm \in s\mathfrak{b} + t\mathfrak{a}$.

Inverse. Soit $a = \sum_i a_i x_i = [\, a_1 \ \cdots \ a_n \,] X$, alors on a

$$\langle \underline{a} \rangle \, \langle \underline{b} \rangle = \langle a \rangle \text{ avec } \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix} = C \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = CX$$

(où C est une matrice de localisation principale pour $(\underline{a})$). En effet

$$\textstyle\sum_i a_i b_i = [\, a_1 \ \cdots \ a_n \,] \, C \, X = [\, a_1 \ \cdots \ a_n \,] \, X = a,$$

donc $a \in \mathfrak{b}\mathfrak{a}$. En outre

$$b_i a_j = \textstyle\sum_k c_{ik} \, x_k \, a_j = \sum_k c_{ij} \, x_k \, a_k = c_{ij} \, (\sum_k x_k a_k) = c_{ij} \, a,$$

donc $\mathfrak{b}\mathfrak{a} \subseteq \langle a \rangle$. Ainsi $\mathfrak{b}\mathfrak{a} = \langle a \rangle$ (voir [Modules, lemme IX-2.5]).

Test d'appartenance. Si $\mathfrak{a} = \langle a_1, \ldots, a_n \rangle$ et si $s_1, \ldots, s_n \in \mathbf{Z}$ vérifient $s_i \mathfrak{a} \subseteq \langle a_i \rangle$ et $\sum_i s_i = 1$, alors $x \in \mathfrak{a}$ si, et seulement si, chaque $s_i x \in \langle a_i \rangle$. Comme on suppose que $\mathbf{Z}$ est à divisibilité explicite on a un test d'appartenance aux idéaux fractionnaires, et donc aussi un test pour l'inclusion d'un idéal fractionnaire dans un autre.

Changement de système générateur Si $\langle a_1, \ldots, a_n \rangle = \langle b_1, \ldots, b_m \rangle$ et si l'on a $s_i a_j \in \langle a_i \rangle$ avec $\sum_i s_i = 1$, on peut calculer $(t_1, \ldots, t_m)$ vérifiant $t_i b_j \in \langle b_i \rangle$ avec $\sum_i t_i = 1$.
Pour cela on utilise l'implication *1* $\Rightarrow$ *2* dans les propriétés équivalentes du départ puisque l'on dispose d'un inverse de l'idéal $\mathfrak{a} = \langle b_1, \ldots, b_m \rangle$.

NB : un calcul plus général mais plus compliqué, sans l'hypothèse que $\mathbf{Z}$ est intègre, est donné dans l'implication *1* $\Rightarrow$ *3* du théorème XVI-2.2 de Modules)

2.3 Formes réduites de matrices sur un domaine de Bezout

On considère un domaine de Bezout $\mathbf{B}$ (cas particulier de domaine de Prüfer).

Définition (1). *Une* ***matrice de Bezout*** *de taille n est une matrice carrée, égale à la matrice identité, à l'exception de quatre coefficients en positions (i,i), (j,j), (i,j) et (j,i) avec $1 \leqslant i < j \leqslant n$ et $\begin{vmatrix} a_{ii} & a_{ij} \\ a_{ji} & a_{jj} \end{vmatrix} = 1$. Nous pouvons noter cette matrice $\mathrm{Bz}(n,i,j;a_{ii},a_{ij},a_{ji},a_{jj})$. Par exemple (avec des cases vides en guise de zéros)*

$$B = \mathrm{Bz}(6,2,4;u,v,s,t) = \begin{bmatrix} 1 & & & & & \\ & u & & v & & \\ & & 1 & & & \\ & s & & t & & \\ & & & & 1 & \\ & & & & & 1 \end{bmatrix} \quad \textit{avec} \quad ut - sv = 1.$$

Effectuer une ***manipulation de Bezout*** *sur une matrice M c'est la multiplier à gauche (manipulation de lignes) ou à droite (manipulation de colonnes) par une matrice de Bezout.*

Si l'on a une égalité matricielle $[\,a\;b\,]\begin{bmatrix} u & v \\ s & t \end{bmatrix} = [\,g\;0\,]$, alors pour une matrice $A \in \mathbb{M}_{6,n}(\mathbf{B})$ ayant des coefficients a et b dans la ligne k en positions $(k,2)$ et $(k,4)$, effectuer le produit $A\,B$ revient à faire les manipulations de colonnes simultanées suivantes sur la matrice A :

$$\begin{cases} C_2 \leftarrow uC_2 + sC_4 \\ C_4 \leftarrow vC_2 + tC_4 \end{cases}$$

Le résultat sera (entre autres) que les coefficients en position $(k,2)$ et $(k,4)$ seront remplacés par g et 0. De la même manière, effectuer un produit $B'A$ par une matrice de Bezout du style $B' = {}^{\mathrm{t}}B$ permettra de remplacer un couple de coefficients (a,b) situés sur une même colonne par un couple $(g,0)$.

Réduction de Hermite (manipulations de colonnes, échanges de lignes). Soit une matrice $F \in \mathbb{M}_{m,n}(\mathbf{B})$. Il existe un entier $k \in [\![0..\inf(m,n)]\!]$, une matrice $C \in \mathbb{GL}_n(\mathbf{B})$ et une matrice de permutation $P \in \mathbb{GL}_m(\mathbf{B})$ telles que l'on ait

$$P\,F\,C = \begin{array}{|c|c|}\hline T & 0 \\ \hline G & 0 \\ \hline \end{array}$$

avec $T \in \mathbb{M}_k(\mathbf{B})$ triangulaire inférieure de déterminant $\neq 0$.

Forme réduite triangulaire (manipulations de colonnes et de lignes). Il existe un entier $k \in [\![0..\inf(m,n)]\!]$, une matrice $C' \in \mathbb{GL}_n(\mathbf{B})$ et une matrice $L \in \mathbb{GL}_m(\mathbf{B})$ telles que l'on ait

$$L\,F\,C' = \begin{array}{|c|c|}\hline T' & 0 \\ \hline 0 & 0 \\ \hline \end{array}$$

avec $T' \in \mathbb{M}_k(\mathbf{B})$ triangulaire inférieure de déterminant $\neq 0$.

Réduction de Smith en dimension $\leqslant 1$, (manipulations de lignes et de colonnes).

Théorème (1). *Un domaine de Bezout de dimension $\leqslant 1$ est un anneau de Smith.*

Démonstration. D'après le paragraphe précédent, il suffit de savoir traiter une matrice carrée (triangulaire) M de déterminant $d \neq 0$. Comme l'anneau quotient $\mathbf{B}/\langle d\rangle$ est zéro-dimensionnel et arithmétique, toute matrice sur $\mathbf{B}/\langle d\rangle$ se ramène par manipulations élémentaires de lignes et de colonnes à une matrice en forme de Smith (fait 3).

On peut donc ramener, modulo d, la matrice M à une forme diagonale de Smith, disons $\mathrm{Diag}(\overline{a_1},\dots,\overline{a_n})$. Notons $\mathfrak{d}_k = \mathfrak{D}_k(M)$.

Puisque $\mathbf{B}$ est un domaine de Bezout, on a $\mathfrak{d}_i = \langle d_i\rangle$ pour des éléments d_i de $\mathbf{B}$, et

$$1 = d_0 \mid d_1 \mid d_2 \mid \dots \mid d_n = d.$$

On a donc des éléments c_1, …, c_n tels que $d_k = c_1 \cdots c_k$ pour $k \in [\![1..n]\!]$.

Quand on fait l'extension des scalaires $\mathbf{B} \to \mathbf{B}' = \mathbf{B}/\langle d\rangle$, on obtient $\langle\overline{a_1 \dots a_k}\rangle = \mathfrak{D}_k(\overline{M}) = \overline{\mathfrak{d}_k}$, c'est-à-dire $\langle a_1 \cdots a_k, d\rangle = \langle c_1 \cdots c_k\rangle$.
En fait, on a aussi $\langle a_k, d\rangle = \langle c_k\rangle$. Pour le voir, on considère le $\mathbf{B}$-module conoyau $\mathrm{Coker}(M) = K$. On a $dK = 0$, donc

$$K = K/dK \simeq \mathbf{B}'/\langle\overline{a_1}\rangle \oplus \cdots \oplus \mathbf{B}'/\langle\overline{a_n}\rangle \simeq \mathbf{B}/\langle a_1, d\rangle \oplus \cdots \oplus \mathbf{B}/\langle a_n, d\rangle\,.$$

En notant $a'_i = \mathrm{pgcd}(a_i, d)$, comme $\langle\overline{a_i}\rangle \subseteq \langle\overline{a_{i-1}}\rangle$, on a $a'_{i-1} \mid a'_i$. Cela montre [2] que $\mathfrak{d}_k = \langle a'_1 \cdots a'_k\rangle$. Comme $\mathfrak{d}_k = \langle c_1 \cdots c_k\rangle$, puisque $\mathbf{B}$ est intègre et les c_i non nuls, on obtient de proche en proche $\langle a'_k\rangle = \langle c_k\rangle$.

Les manipulations élémentaires modulo d se relèvent en des manipulations élémentaires sur $\mathbf{B}$, d'où une égalité $LMC = M'$, où $\overline{M'} = \mathrm{Diag}(\overline{a_1},\dots,\overline{a_n})$. On voit que la k-ème ligne de M' est multiple de $c_k = \mathrm{pgcd}(a_k, d)$. On peut donc écrire $M' = \mathrm{Diag}(c_1,\dots,c_n)C_1$ avec $C_1 \in \mathbb{M}_n(\mathbf{B})$. Et comme $\det(M') = d$, on obtient $\det(C_1) = 1$. D'où enfin $LMC_2 = \mathrm{Diag}(c_1,\dots,c_n)$ avec $C_2 = CC_1^{-1}$. □

2. Ici on utilise le fait que deux matrices de même format qui ont des conoyaux isomorphes ont les mêmes idéaux déterminantiels : ce sont les idéaux de Fitting du conoyau.

3 Pseudo-bases et pseudo-matrices

Dans cette section, **A** est un anneau intègre et l'on s'intéresse aux applications linéaires entre modules qui sont sommes directes de modules projectif de rang 1. Nous notons **K** le corps de fractions. On développe un «calcul matriciel généralisé» pour les applications linéaires entre modules projectifs de type fini qui sont isomorphes à des sommes directes d'idéaux inversibles.

Il s'avérera dans la section suivante que, pour les domaines de Prüfer, ce calcul est suffisamment efficace et général pour couvrir tous les aspects de la théorie des modules de présentation finie.

3.1 Pseudo-bases

Soit E un **A**-module projectif de type fini isomorphe à une somme directe finie d'idéaux inversibles, $E = E_1 \oplus \cdots \oplus E_r$ avec $E_i \simeq \mathfrak{e}_i \in \mathrm{Iff}(\mathbf{A})$ (inversibles). On peut regarder E comme un sous-**A**-module du **K**-espace vectoriel E_S obtenu en inversant les éléments du monoïde $S = \mathbf{A}^*$. Comme $(E_i)_S$ est un **K**-module projectif de rang 1, il est isomorphe à **K** et l'on obtient

$$E = \mathfrak{e}_1 e_1 \oplus \cdots \oplus \mathfrak{e}_r e_r,$$

où les $e_i \in E_S$ forment une base du **K**-espace vectoriel E_S.
Notons que si $b\mathfrak{e}_1 = a\mathfrak{h}_1$ pour deux idéaux de type fini $\mathfrak{e}_1$ et $\mathfrak{h}_1$ on a l'égalité $E_1 = \mathfrak{e}_1 e_1 = \mathfrak{h}_1(\frac{a}{b} e_1) = \mathfrak{h}_1 e_1'$ ($\mathfrak{e}_1$ et $\mathfrak{h}_1$ sont deux **A**-modules isomorphes). Ainsi la décomposition $E = E_1 \oplus \cdots \oplus E_r$ ne donne pas une écriture unique sous forme $\mathfrak{e}_i e_i$ pour les E_i.

On appelle ***pseudo-base*** de E, un r-uplet

$$\boxed{((e_1, \mathfrak{e}_1), \ldots, (e_r, \mathfrak{e}_r))} \text{ tel que } E = \mathfrak{e}_1 e_1 \oplus \cdots \oplus \mathfrak{e}_r e_r,$$

où les e_i sont des éléments de E_S et les $\mathfrak{e}_i$ des idéaux fractionnaires inversibles de **A**. Un $x \in E$ s'écrit alors de manière unique sous forme $\sum_i x_i e_i$ où les $x_i \in \mathfrak{e}_i$ (et donc $x_i e_i \in E$).

Fait (4). *Donner une pseudo-base $\mathcal{E} = ((e_1, \mathfrak{e}_1), \ldots, (e_r, \mathfrak{e}_r))$ pour le module E, revient exactement à donner un isomorphisme*

$$\psi_{\mathcal{E}} : \mathfrak{e}_1 \times \cdots \times \mathfrak{e}_r \longrightarrow E,\ (x_1, \ldots, x_r) \longmapsto \sum_{i \in [\![1..r]\!]} x_i e_i,$$

dans lequel les images inverses des e_i (après l'extension de $\psi_{\mathcal{E}}$ à E_S) forment la base canonique de $\mathbf{K}^r$ ($\mathfrak{e}_1 \times \cdots \times \mathfrak{e}_r \subseteq \mathbf{K}^r$).

Remarque. Dans la suite, on pourrait imaginer que tous les modules projectifs qui interviennent sont des sous-$\mathbf{A}$-modules de $\mathbf{K}$-espaces vectoriels $\mathbf{K}^n$, où n est supérieur ou égal au rang r du module.
Dans un tel contexte les e_i sont soumis à la seule contrainte d'être des vecteurs linéairement indépendants du $\mathbf{K}$-espace vectoriel $\mathbf{K}^n$ considéré, et E_S est simplement le sous-$\mathbf{K}$-espace vectoriel de $\mathbf{K}^n$ dont une base est donnée par les vecteurs e_i. Les e_i sont donnés par une matrice $M \in \mathbb{M}_{n,r}(\mathbf{K})$. On pourrait dans ce cadre aussi bien dire que la pseudo-base $\mathcal{E}$ est donnée par une matrice $M \in \mathbb{M}_{n,r}(\mathbf{K})$ et une liste de r idéaux fractionnaires inversibles de $\mathbf{A}$.
Il nous semble cependant préférable de garder pour nos explications un cadre plus général. ∎

3.2 Pseudo-matrices

Matrice d'une application linéaire sur des pseudo-bases

Rappelons que toute cette section s'applique à un anneau intègre arbitraire $\mathbf{A}$ pour des modules qui admettent des pseudo-bases, c'est-à-dire qui sont isomorphes à des sommes directes finies d'idéaux inversibles.

Soit $\varphi : E \to H$ une application linéaire entre modules projectifs de rangs m et n. Si

$$\mathcal{E} = ((e_1, \mathfrak{e}_1), \ldots, (e_m, \mathfrak{e}_m)) \text{ et } \mathcal{H} = ((h_1, \mathfrak{h}_1), \ldots, (h_n, \mathfrak{h}_n))$$

sont des pseudo-bases de E et H, l'application $\varphi_S : E_S \to H_S$ admet une matrice $\underline{A} \in \mathbf{K}^{n\times m}$ sur les $\mathbf{K}$-bases $(e_1, \ldots, e_m)$ et $(h_1, \ldots, h_n)$ de E_S et H_S.

Les coefficients a_{ij} de cette matrice ne sont pas arbitraires dans $\mathbf{K}$. En effet, vue l'égalité $\varphi_S(e_j) = \sum_{i\in[\![1..m]\!]} a_{ij}h_i$, l'inclusion $\varphi_S(E) \subseteq H$ est satisfaite si, et seulement si, pour tout $j \in [\![1..m]\!]$, tout $x_j \in \mathfrak{e}_j$ et tout $i \in [\![1..n]\!]$, on a $a_{ij}x_j \in \mathfrak{h}_i$. Autrement dit, pour tous i, j, on doit avoir

$$a_{ij}\mathfrak{e}_j \subseteq \mathfrak{b}_i,$$

c'est-à-dire encore

$$a_{ij} \in \mathfrak{h}_i\mathfrak{e}_j^{-1}.$$

Définition et notation (2). *(Avec les notations ci-dessus)*

1. *On appelle* ***matrice de*** φ ***sur les pseudo-bases*** $\mathcal{E}$ ***et*** $\mathcal{H}$ *la donnée*

$$A = (\mathfrak{h}_1, \ldots, \mathfrak{h}_n; \mathfrak{e}_1, \ldots, \mathfrak{e}_m; \underline{A}) = (\underline{\mathfrak{h}}; \underline{\mathfrak{e}}; \underline{A}), \text{ où } \underline{A} = (a_{ij})_{ij} \in \mathbb{M}_{n,m}(\mathbf{K}).$$

Cette donnée satisfait les inclusions $a_{ij}\mathfrak{e}_j \subseteq \mathfrak{h}_i$. *On note* $\boxed{A = \mathscr{M}_{\mathcal{E},\mathcal{H}}(\varphi)}$.

2. *On appelle* ***pseudo-matrice*** *toute «matrice»* $(\underline{\mathfrak{h}};\underline{\mathfrak{e}};\underline{A})$ *de ce type, i.e. satisfaisant les inclusions* $a_{ij}\mathfrak{e}_j \subseteq \mathfrak{h}_i$.
3. *Pour des listes* $\underline{\mathfrak{e}}$ *et* $\underline{\mathfrak{h}}$ *fixées, l'ensemble formé par ces pseudo-matrices est noté* $\boxed{\mathbb{M}_{\underline{\mathfrak{h}};\underline{\mathfrak{e}}}(\mathbf{A})}$.
4. *Cet ensemble est muni d'une structure naturelle de* $\mathbf{A}$*-module : pour additionner* A *et* B*, on additionne* $\underline{A}$ *et* $\underline{B}$.
5. *On définit également le produit de deux pseudo-matrices de formats convenables :*
$$\textit{Si } B = (\underline{\mathfrak{c}};\underline{\mathfrak{h}};\underline{B}) \textit{ et } A = (\underline{\mathfrak{h}};\underline{\mathfrak{e}};\underline{A}), \quad \textit{alors} \quad B \cdot A := (\underline{\mathfrak{c}};\underline{\mathfrak{e}};\underline{B}\cdot\underline{A})$$

Dans le cas envisagé au point *1* ci-dessus, les modules $\mathbb{M}_{\underline{\mathfrak{h}};\underline{\mathfrak{e}}}(\mathbf{A})$ et $\mathscr{L}_{\mathbf{A}}(E,H)$ sont isomorphes.

Les pseudo-matrices ont donc pour «indices de colonnes» des couples $(j,\mathfrak{e}_j)$, pour «indices de lignes» des couples $(i,\mathfrak{h}_i)$, et les coefficients a_{ij} satisfont les inclusions $a_{ij}\mathfrak{e}_j \subseteq \mathfrak{h}_i$. On pourra visualiser les choses comme suit, par exemple pour une pseudo-matrice A de format 3×4 :

$$A = \begin{array}{c} \\ \mathfrak{h}_1 \\ \mathfrak{h}_2 \\ \mathfrak{h}_3 \end{array} \begin{array}{c} \begin{array}{cccc} \mathfrak{e}_1 & \mathfrak{e}_2 & \mathfrak{e}_3 & \mathfrak{e}_4 \end{array} \\ \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \end{bmatrix} \end{array} \quad a_{ij}\mathfrak{e}_j \subseteq \mathfrak{h}_i.$$

Notez que le module $\mathbb{M}_{n,m}(\mathbf{A})$ des matrices usuelles correspond au cas particulier où les idéaux $\mathfrak{e}_i$ et $\mathfrak{h}_j$ sont tous égaux à $\langle 1\rangle$.

En l'absence de modules de référence E et H, si $(e_1,\dots,e_m)$ et $(h_1,\dots,h_n)$ désignent les bases canoniques de $\mathbf{K}^m$ et $\mathbf{K}^n$, la pseudo-matrice A est vue comme la matrice d'une application $\mathbf{A}$-linéaire $\varphi : E \to F$, où

$$\begin{array}{rcccccl} E & = & \mathfrak{e}_1\times\cdots\times\mathfrak{e}_m & = & e_1\mathfrak{e}_1+\cdots+e_m\mathfrak{e}_m & \subseteq & \mathbf{K}^m \quad \text{et} \\ F & = & \mathfrak{h}_1\times\cdots\times\mathfrak{h}_n & = & h_1\mathfrak{h}_1+\cdots+h_n\mathfrak{h}_n & \subseteq & \mathbf{K}^n\,. \end{array}$$

Calcul matriciel généralisé, premiers résultats.

Théorème et définition (2) (Déterminant d'une application linéaire sur des pseudo-bases). *Avec les notations précédentes, on suppose que E et H ont même rang n et l'on considère la matrice $A = \mathscr{M}_{\mathcal{E},\mathcal{H}}(\varphi)$ d'une application $\mathbf{A}$-linéaire $\varphi : E \to H$. On a donc $A \in \mathbb{M}_{\underline{\mathfrak{h}};\underline{\mathfrak{e}}}(\mathbf{A})$.*
*Notons $\mathfrak{h} = \prod_{i\in[\![1..n]\!]} \mathfrak{h}_i$ et $\mathfrak{e} = \prod_{i\in[\![1..n]\!]} \mathfrak{e}_i$. Le déterminant de la matrice $\underline{A}$, qui est un élément de $\mathbf{K}$, est noté $\boxed{\det_{\mathcal{E},\mathcal{H}}(\varphi)}$ et on l'appelle **le déterminant de φ sur les pseudo-bases $\mathcal{E}$ et $\mathcal{H}$**. Ci-après $\Delta := \det_{\mathcal{E},\mathcal{H}}(\varphi) = \det(\underline{A})$.*

1. *On a $\Delta\mathfrak{e} \subseteq \mathfrak{h}$, i.e. $\Delta \in \mathfrak{h}\mathfrak{e}^{-1}$. En particulier si $\mathfrak{e} = \mathfrak{h}$ on a $\Delta \in \mathbf{A}$.*
2. *Les propriétés suivantes sont équivalentes.*
   a. *L'application linéaire φ est un isomorphisme.*
   b. *On a l'égalité $\Delta\mathfrak{e} = \mathfrak{h}$.*
   c. *L'application linéaire φ est surjective.*

   *Dans ce cas, la matrice A est une **pseudo-matrice inversible**.*
   Son inverse $A^{-1} = (\underline{\mathfrak{e}}; \underline{\mathfrak{h}}; \underline{A}^{-1})$ est un élément de $\mathbb{M}_{\underline{\mathfrak{e}};\underline{\mathfrak{h}}}(\mathbf{A})$: c'est la matrice de l'isomorphisme φ^{-1} sur les pseudo-bases $\mathcal{H}$ et $\mathcal{E}$.
3. *L'application linéaire φ est injective si, et seulement si, $\Delta \neq 0$.*
4. *Lorsque $E = H$ et $\mathcal{E} = \mathcal{H}$, Δ est un élément de $\mathbf{A}$, il ne dépend que de φ, et c'est le déterminant de φ au sens «usuel», noté* $\det(\varphi)$.

Démonstration. 1. Puisque $a_{ij}\mathfrak{e}_j \subseteq \mathfrak{h}_i$ et $\Delta = \sum_{\sigma\in\mathcal{P}_n} \operatorname{sign}(\sigma)(a_{1j_1}\cdots a_{nj_n})$, on obtient $\Delta\mathfrak{e} \subseteq \mathfrak{h}$.

2a ⇔ 2c. Évidemment si φ est un isomorphisme, alors φ est un surjective. Si φ est surjective, alors φ est scindable ([Modules, théorème XIII-2.1]), donc $H \simeq E \oplus \operatorname{Ker}\varphi$, et puisque les modules E et H ont le même rang, φ est un isomorphisme.

2a ⇒ 2b. Si ψ est l'isomorphisme réciproque, il est représenté par une matrice $B \in \mathbb{M}_{\underline{\mathfrak{e}};\underline{\mathfrak{h}}}(\mathbf{A})$ sur les pseudo-bases $\mathcal{H}$ et $\mathcal{E}$, et l'on a $AB = (\underline{\mathfrak{h}}; \underline{\mathfrak{h}}; \mathrm{I}_n)$. Si on applique le point *1* avec $\det(B) = \frac{1}{\Delta}$, on obtient $\frac{1}{\Delta}\mathfrak{h} \subseteq \mathfrak{e}$ et donc $\mathfrak{h} \subseteq \Delta\mathfrak{e}$.

2b ⇒ 2a. Si $\Delta\mathfrak{e} = \mathfrak{h}$, nous allons montrer que la matrice $\underline{A}^{-1} = \frac{1}{\Delta}\,\underline{\widetilde{A}}$ définit une pseudo-matrice de $\mathbb{M}_{\underline{\mathfrak{e}};\underline{\mathfrak{h}}}(\mathbf{A})$. Ainsi cette pseudo-matrice définit un application linéaire $\psi : H \to E$ sur les pseudo-bases $\mathcal{H}$ et $\mathcal{E}$, et comme $\varphi\circ\psi$ et $\psi\circ\varphi$ sont représentées par la matrice identité (sur les pseudo-bases convenables), ψ et φ sont deux isomorphismes réciproques.

Il faut montrer $\boxed{\frac{1}{\Delta}\ \widetilde{a}_{ij}\ \mathfrak{h}_j \subseteq \mathfrak{e}_i}$. On note que de manière générale

$$\widetilde{a}_{ij}\prod\nolimits_{r\neq i}\mathfrak{e}_r \subseteq \prod\nolimits_{s\neq j}\mathfrak{h}_s, \quad \text{ou encore} \quad \boxed{\widetilde{a}_{ij}\,\mathfrak{h}_j\,\mathfrak{e} \subseteq \mathfrak{e}_i\,\mathfrak{h}}. \tag{2}$$

D'où le résultat puisque $\Delta\mathfrak{e} = \mathfrak{h}$.

3. Les modules E et H sont sans torsion et peuvent être vus comme des sous-$\mathbf{A}$-modules de $\mathbf{K}^n$. Donc φ est injective si, et seulement si, $\varphi_S : \mathbf{K}^n \to \mathbf{K}^n$ est injective. Et φ_S est injective si, et seulement si, $\Delta \neq 0$.

4. Le déterminant d'un endomorphisme se comporte bien par extension des scalaires. En particulier lorsque l'on passe du $\mathbf{A}$-module E au $\mathbf{K}$-espace vectoriel E_S le déterminant ne change pas. Or la matrice de φ sur la pseudo-base $((e_1, \mathfrak{e}_1), \ldots, (e_n, \mathfrak{e}_n))$ n'est autre que la matrice de φ_S sur la base $(e_1, \ldots, e_n)$. □

Commentaire. On notera que les deux choses suivantes sont totalement indépendantes des «vecteurs» e_j et h_i qui interviennent dans les pseudo-bases $\mathcal{E}$ et $\mathcal{H}$.

— Le fait que la matrice est bien celle d'une application linéaire de E dans H : ceci est contrôlé par les inclusions $a_{ij}\mathfrak{e}_j \subseteq \mathfrak{h}_i$.

— Le fait que l'application linéaire est un isomorphisme : ceci est contrôlé par l'égalité $\Delta\mathfrak{e} = \mathfrak{h}$. ∎

Matrice de changement de pseudo-bases

Considérons deux pseudo-bases différentes,

$$\mathcal{E} = ((e_1, \mathfrak{e}_1), \ldots, (e_r, \mathfrak{e}_r)) \text{ et } \mathcal{E}' = ((e'_1, \mathfrak{e}'_1), \ldots, (e'_r, \mathfrak{e}'_r)),$$

pour un même module E, avec les e_i et les e'_i dans le $\mathbf{K}$-espace vectoriel E_S.

La pseudo-matrice $A = \mathscr{M}_{\mathcal{E}',\mathcal{E}}(\mathrm{Id}_E)$ s'appelle la ***matrice de passage de $\mathcal{E}$ à $\mathcal{E}'$*** : la matrice $\underline{A} \in \mathbb{M}_r(\mathbf{K})$ a pour colonnes les e'_i exprimés sur les e_i. C'est la matrice de passage de la base $(e_1, \ldots, e_r)$ à la base $(e'_1, \ldots, e'_r)$ dans E_S. L'important, pour que cela fonctionne au niveau du $\mathbf{A}$-module E, est que les coefficients p_{ij} de la matrice de passage P vérifient $p_{ij}\mathfrak{e}'_j \in \mathfrak{e}_i$ et que le déterminant Δ vérifie $\Delta\mathfrak{e}' = \mathfrak{e}$.

En fait, chaque fois que l'on a une pseudo-matrice inversible P pour deux familles $(\mathfrak{e}_1, \ldots, \mathfrak{e}_n)$ et $(\mathfrak{e}'_1, \ldots, \mathfrak{e}'_n)$, si l'on considère un $\mathbf{A}$-module E qui admet une pseudo-base du type $\mathcal{E} = ((e_1, \mathfrak{e}_1), \ldots, (e_n, \mathfrak{e}_n))$, la matrice P peut être vue comme une matrice de changement de pseudo-base pour E. Il suffit pour cela de considérer les vecteurs e'_j qui sont donnés par les colonnes de la matrice $\underline{P}$ (i.e., $e'_j = \sum_i p_{ij}e_i$).

En effet, considérons le module $E' = \bigoplus_j e'_j\mathfrak{e}'_j$, et $\mathcal{E}' = ((e'_1, \mathfrak{e}'_1), \ldots, (e'_n, \mathfrak{e}'_n))$, la matrice P est celle d'une application linéaire $\varphi : E' \to E$ sur les pseudo-bases $\mathcal{E}'$ et $\mathcal{E}$. Mais, vu que les e'_i sont donnés par les colonnes de $\underline{P}$, on a $\varphi_S = \mathrm{Id}_{E_S}$. Ceci montre que φ est une application linéaire d'inclusion de E' dans E. Enfin, puisque cette inclusion est un isomorphisme, elle est surjective et l'on obtient $E = E'$ et $\varphi = \mathrm{Id}_E$.

3.3 Idéaux déterminantiels

On a défini le déterminant d'une application linéaire sur des pseudo-bases. On généralise les choses comme suit, en application du point *1* du théorème 2.

Définition (3). (Idéaux déterminantiels d'une pseudo-matrice)

1. *Pour une pseudo-matrice carrée $A = (\underline{\mathfrak{h}}; \underline{\mathfrak{e}}; \underline{A})$ on définit son* ***idéal déterminant****, noté $\mathfrak{det}(A)$: c'est l'idéal*

$$\boxed{\mathfrak{det}(A) = \det(\underline{A})\,\mathfrak{e}\,\mathfrak{h}^{-1}}, \text{ où } \mathfrak{e} = \prod_j \mathfrak{e}_j \text{ et } \mathfrak{h} = \prod_i \mathfrak{h}_i.$$

2. *Soient $\beta = [\beta_1, \dots, \beta_r] \subseteq [\![1..n]\!]$ et $\alpha = [\alpha_1, \dots, \alpha_r] \subseteq [\![1..m]\!]$ des listes extraites en ordre croissant. Nous notons $A_{\beta,\alpha}$ la pseudo-matrice extraite sur les lignes (d'indices dans) β et les colonnes α. Précisément*
$$A_{\beta,\alpha} = (\mathfrak{h}_{\beta_1}, \dots, \mathfrak{h}_{\beta_r}; \mathfrak{e}_{\alpha_1}, \dots, \mathfrak{e}_{\alpha_r}, \underline{A}_{\beta,\alpha}).$$
On dit que l'idéal
$$\mathfrak{m}_{\beta,\alpha}(A) := \mathfrak{det}(A_{\beta,\alpha}) = \det(\underline{A}_{\beta,\alpha})(\textstyle\prod_{i=0}^{r} \mathfrak{e}_{\alpha_i})(\prod_{j=0}^{r} \mathfrak{h}_{\beta_j})^{-1}$$
est ***l'idéal mineur d'ordre r de la matrice A extrait sur les lignes β et les colonnes α.***

3. *Pour une pseudo-matrice arbitraire, et $r \leqslant \inf(m,n)$ on définit* ***l'idéal déterminantiel d'ordre r de A****, noté $\mathfrak{D}_r(A)$, comme la somme des idéaux mineurs d'ordre r de A.*
Pour $r > \inf(m,n)$ on définit $\mathfrak{D}_r(A) = 0$.
Pour $r \leqslant 0$ on définit $\mathfrak{D}_r(A) = \langle 1 \rangle$.

Fait (5). *Si A et B sont deux pseudo-matrices carrées telles que le produit AB est défini, on a $\mathfrak{det}(AB) = \mathfrak{det}(A)\,\mathfrak{det}(B)$. Une pseudo-matrice carrée est inversible si, et seulement si, son idéal déterminant est égal à $\langle 1 \rangle$.*

Théorème et définition (3) (Idéaux déterminantiels d'une application linéaire). *On continue avec la notation $A = (\mathfrak{h}_1, \dots, \mathfrak{h}_n; \mathfrak{e}_1, \dots, \mathfrak{e}_m; \underline{A})$.*

1. *Lorsque $m = n$, l'idéal déterminant de la matrice $A = \mathscr{M}_{\mathcal{E},\mathcal{H}}(\varphi)$ ne dépend pas des pseudo-bases choisies pour E et H. On l'appelle* ***l'idéal déterminant de l'application linéaire*** *φ, noté $\mathfrak{det}(\varphi)$. On a les équivalences*
   — *$\mathfrak{det}(\varphi) = \langle 1 \rangle$ si, et seulement si, φ est un isomorphisme,*
   — *$\mathfrak{det}(\varphi) \neq \langle 0 \rangle$ si, et seulement si, φ est injective.*

2. *Les idéaux déterminantiels de la matrice A ne dépendent pas des pseudo-bases choisies pour E et H. On les appelle les* ***idéaux déterminantiels de l'application linéaire*** *φ, on les note $\mathfrak{D}_r(\varphi)$.*
3. *L'application linéaire est surjective si, et seulement si, $\mathfrak{D}_n(\varphi) = \langle 1\rangle$ si, et seulement si, elle admet un inverse à droite. Elle est injective si, et seulement si, $\mathfrak{D}_m(\varphi) \neq 0$. Elle admet un inverse à gauche si, et seulement si, $\mathfrak{D}_m(\varphi) = \langle 1\rangle$.*
4. *Soit $s \in \mathbf{A}^*$ tel que les modules $E[1/s]$ et $H[1/s]$ sont libres sur $\mathbf{A}[1/s]$. Notons $\varphi_s : E[1/s] \to H[1/s]$ l'extension de φ par $\mathbf{A} \to \mathbf{A}[1/s]$.*
   Alors pour chaque r on a $\mathfrak{D}_r(\varphi)\mathbf{A}[1/s] = \mathfrak{D}_r(\varphi_s)$ (idéaux déterminantiels usuels définis pour une application linéaire entre modules libres).
5. *On a les inclusions*

$$\{0\} = \mathfrak{D}_{1+\min(m,n)}(\varphi) \subseteq \cdots \subseteq \mathfrak{D}_1(\varphi) \subseteq \mathfrak{D}_0(\varphi) = \langle 1\rangle = \mathbf{A} \tag{3}$$

Plus précisément pour tous $k, r \in \mathbb{N}$ on a une inclusion

$$\mathfrak{D}_{k+r}(\varphi) \subseteq \mathfrak{D}_k(\varphi)\,\mathfrak{D}_r(\varphi) \tag{4}$$

Démonstration. Le point *1* résulte du fait 5 et du théorème 2. Les autres points (comme d'ailleurs le point *1*) sont conséquences du point *4* (qui est facile) et des résultats analogues concernant les applications linéaires entre modules libres. En effet, un idéal est caractérisé par ses localisations en des éléments comaximaux [3]. Et les propriétés d'injectivité et de surjectivité pour des applications linéaires également. □

Un cas important est celui des idéaux mineurs d'ordre 1,

$$\boxed{\mathfrak{m}_{ij}(A) = a_{ij}\mathfrak{e}_j\mathfrak{h}_i^{-1}},$$

qui interviendront dans les manipulations de matrices conduisant à des formes réduites agréables.

3.4 Pseudo-matrices par blocs

Les calculs par blocs se font pour les pseudo-matrices aussi bien que pour les matrices usuelles. Considérons une pseudo-matrice $M = (\mathfrak{h}_1, \ldots, \mathfrak{h}_n; \mathfrak{e}_1, \ldots, \mathfrak{e}_m; \underline{M})$ et des entiers $p \in [\![2..n-1]\!]$,

3. Puisque l'anneau est intègre, l'idéal est même l'intersection de ses localisés, vus comme sous-$\mathbf{A}$-modules de $\mathbf{K}$.

$q \in [\![2..m-1]\!]$. Décomposons $\underline{M}$ en quatre blocs $\underline{A} \in \mathbf{K}^{p\times q}$, $\underline{B} \in \mathbf{K}^{p\times(m-q)}$, $\underline{C} \in \mathbf{K}^{(n-p)\times q}$ et $\underline{D} \in \mathbf{K}^{(n-p)\times(m-q)}$,

$$M = \begin{array}{|c|c|}\hline \underline{A} & \underline{B} \\ \hline \underline{C} & \underline{D} \\ \hline \end{array}$$

ce qui donne quatre pseudo-matrices $A = (\mathfrak{h}_1, \dots, \mathfrak{h}_p; \mathfrak{e}_1, \dots, \mathfrak{e}_q; \underline{A})$, etc. Alors on note

$$M = \begin{array}{|c|c|}\hline A & B \\ \hline C & D \\ \hline \end{array}.$$

3.5 Pivot de Gauss pour les pseudo-matrices.

Définition et notation (4).

- *Une pseudo-matrice est dite* ***strictement carrée*** *lorsqu'elle est de la forme $A = (\underline{\mathfrak{e}}; \underline{\mathfrak{e}}; \underline{A})$. On note l'algèbre des pseudo-matrices correspondante par*
$$\boxed{\mathbb{M}_{\mathfrak{e}_1,\dots,\mathfrak{e}_n}(\mathbf{A}) = \mathbb{M}_{\underline{\mathfrak{e}}}(\mathbf{A})}.$$
- *On appelle* ***pseudo-matrice élémentaire*** *une pseudo-matrice strictement carrée A telle que $\underline{A}$ est une matrice élémentaire usuelle (sur $\mathbf{K}$).*
Si $a_{ij} \in \mathbf{K}$ est le coefficient non nul en dehors de la diagonale, on doit donc avoir $a_{ij}\,\mathfrak{e}_j \subseteq \mathfrak{e}_i$.
- *On appelle* ***manipulation élémentaire de colonnes (resp. de lignes)*** *sur une pseudo-matrice la postmultiplication (resp. la prémultiplication) par une pseudo-matrice élémentaire.*

Exemples.

Manipulation de colonnes. Considérons une pseudo-matrice $L = \begin{matrix} \\ \mathfrak{c} \end{matrix} \begin{matrix} \begin{matrix} \mathfrak{a} & \mathfrak{b} \end{matrix} \\ \begin{bmatrix} a & b \end{bmatrix} \end{matrix}$.

Si $\mathfrak{m}_{11}(L) \supseteq \mathfrak{m}_{12}(L)$, c'est-à-dire si $a\mathfrak{a} \supseteq b\mathfrak{b}$, on a une pseudo-matrice élémentaire $P = \begin{matrix} \\ \mathfrak{a} \\ \mathfrak{b} \end{matrix} \begin{matrix} \begin{matrix} \mathfrak{a} & \mathfrak{b} \end{matrix} \\ \begin{bmatrix} 1 & -\frac{b}{a} \\ 0 & 1 \end{bmatrix} \end{matrix}$, de sorte que l'on obtient, comme pour le pivot de Gauss classique

$$LP = \begin{matrix} \\ \mathfrak{c} \end{matrix} \begin{matrix} \begin{matrix} \mathfrak{a} & \mathfrak{b} \end{matrix} \\ \begin{bmatrix} a & 0 \end{bmatrix} \end{matrix}$$

Ainsi, dans le processus «pivot de Gauss» ce qui tient lieu, pour une pseudo-matrice, de «a_{11} divise a_{12}» dans le cas des matrices usuelles, c'est maintenant «$\mathfrak{m}_{11} \supseteq \mathfrak{m}_{12}$», ou encore «$\mathfrak{m}_{12}\mathfrak{m}_{11}^{-1} \subseteq \mathbf{A}$», ce qui se dit aussi «$\mathfrak{m}_{11}$ divise $\mathfrak{m}_{12}$».

Manipulation de lignes. Considérons une pseudo-matrice $L = \begin{array}{c} \\ \mathfrak{c}_1 \\ \mathfrak{c}_2 \end{array} \begin{array}{c} \mathfrak{a} \\ \begin{bmatrix} a \\ b \end{bmatrix} \end{array}$.
Si $\mathfrak{m}_{11}(L) \supseteq \mathfrak{m}_{21}(L)$, c'est-à-dire si $a\mathfrak{c}_2 \supseteq b\mathfrak{c}_1$, on a une pseudo-matrice élémentaire $P = \begin{array}{c} \\ \mathfrak{c}_1 \\ \mathfrak{c}_2 \end{array} \begin{array}{c} \mathfrak{c}_1 \quad \mathfrak{c}_2 \\ \begin{bmatrix} 1 & 0 \\ -\frac{b}{a} & 1 \end{bmatrix} \end{array}$, de sorte que l'on obtient $PL = \begin{array}{c} \\ \mathfrak{c}_1 \\ \mathfrak{c}_2 \end{array} \begin{array}{c} \mathfrak{a} \\ \begin{bmatrix} a \\ 0 \end{bmatrix} \end{array}$.

Ainsi, dans le processus «pivot de Gauss» ce qui tient lieu, pour une pseudo-matrice, de «a_{11} divise a_{21}» dans le cas des matrices usuelles, c'est maintenant «$\mathfrak{m}_{11} \supseteq \mathfrak{m}_{21}$», ce qui se dit aussi «$\mathfrak{m}_{11}$ divise $\mathfrak{m}_{21}$». ∎

Voici une autre généralisation naturelle d'un résultat classique pour les matrices usuelles.

Lemme (4) (Lemme du mineur inversible pour les pseudo-matrices). *On considère une pseudo-matrice*

$$A = (\mathfrak{h}_1, \dots, \mathfrak{h}_n; \mathfrak{e}_1, \dots, \mathfrak{e}_m; \underline{A}).$$

On suppose que l'idéal mineur $\mathfrak{m}_{[\![1..k]\!],[\![1..k]\!]}(A)$ *est égal à* $\langle 1 \rangle$.

1. (Pivot sur les colonnes) *Il existe une pseudo-matrice inversible*

$$C = (\mathfrak{e}_1, \dots, \mathfrak{e}_m; \mathfrak{h}_1, \dots, \mathfrak{h}_k, \mathfrak{e}_{k+1}, \dots, \mathfrak{e}_m, \underline{C})$$

décrite par blocs comme $C = \begin{array}{|c|c|} \hline C_1 & C_2 \\ \hline 0 & \mathrm{I}_{m-k} \\ \hline \end{array}$ *avec* $C_1 = {A_{[\![1..k]\!],[\![1..k]\!]}}^{-1}$ *telle que la pseudo-matrice* AC *soit de la forme* $\begin{array}{|c|c|} \hline \mathrm{I}_k & 0 \\ \hline B & D \\ \hline \end{array}$.

2. (Pivots sur les lignes et les colonnes)
La pseudo-matrice A *est équivalente à une pseudo-matrice*

$$A' = (\mathfrak{h}_1, \dots, \mathfrak{h}_n; \mathfrak{h}_1, \dots, \mathfrak{h}_k, \mathfrak{e}_{k+1}, \dots, \mathfrak{e}_m; \underline{A'}) = \begin{array}{|c|c|} \hline \mathrm{I}_k & 0 \\ \hline 0 & A'' \\ \hline \end{array}$$

et l'on a $\mathfrak{D}_r(A'') = \mathfrak{D}_{k+r}(A)$ *pour tout* $r \in \mathbb{Z}$.
En particulier si $\mathfrak{D}_{k+1}(A) = \langle 0 \rangle$, *on a une forme réduite*

$$L\,A\,C = \begin{array}{|c|c|} \hline \mathrm{I}_k & 0 \\ \hline 0 & 0 \\ \hline \end{array}.$$

NB : Si A possède un mineur d'ordre $k > 0$ égal à $\langle 1 \rangle$, on obtient des résultats analogues après permutation de lignes et/ou de colonnes.

Démonstration. On recopie la démonstration usuelle pour les matrices usuelles.

1. Notons $A = \begin{array}{|c|c|}\hline A_1 & A_2 \\ \hline A_3 & A_4 \\ \hline \end{array}$ où $\underline{A_1} \in \mathbb{M}_k(\mathbf{K})$.

La matrice C est la matrice par blocs $C = \begin{array}{|c|c|}\hline C_1 & C_2 \\ \hline 0 & \mathrm{I}_{m-k} \\ \hline \end{array}$ où $C_1 = {A_1}^{-1}$ et $C_2 = -C_1 A_2$. On obtient la matrice $A\,C$ donnée dans l'énoncé.

2. On continue en multipliant à gauche par la matrice strictement carrée définie par blocs $L = \begin{array}{|c|c|}\hline \mathrm{I}_k & 0 \\ \hline -B & \mathrm{I}_\ell \\ \hline \end{array} \in \mathbb{M}_{\mathfrak{h}_1,\dots,\mathfrak{h}_n}(\mathbf{Z})$ avec $\ell = n - k$. On obtient pour $L\,A\,C$ la pseudo-matrice donnée dans l'énoncé. Enfin $\mathfrak{D}_r(A'') = \mathfrak{D}_{k+r}(A') = \mathfrak{D}_{k+r}(A)$ pour tout $r \in \mathbb{Z}$. □

Remarque. On a obtenu $A' = L\,A\,C$ avec C inversible et L strictement carrée inversible. Si en outre on a $\mathfrak{e}_i = \mathfrak{h}_i$ pour $i \in [\![1..k]\!]$, la matrice C est également strictement carrée. ∎

4 Domaines de Prüfer, systèmes linéaires, réduction de Hermite

Dans cette section $\mathbf{Z}$ est un domaine de Prüfer à divisibilité explicite et $\mathbf{K}$ son corps de fractions.

4.1 Systèmes linéaires, généralités

On considère un système linéaire $AX = B$ de n équations à m inconnues sur $\mathbf{Z}$. Dans la situation usuelle, tous les idéaux indexant les lignes et les colonnes des matrices A, B (données) et X (inconnue) sont égaux à $\langle 1 \rangle$, les inconnues (coordonnées de X) sont dans $\mathbf{Z}$ et $\underline{A} \in \mathbb{M}_{n,m}(\mathbf{Z})$. Plus généralement, on considère des pseudo-matrices $A = (\mathfrak{h}_1, \dots, \mathfrak{h}_n; \mathfrak{e}_1, \dots, \mathfrak{e}_m; \underline{A})$ et $B = (\underline{\mathfrak{h}}; \mathfrak{b}; \underline{B})$, et la matrice inconnue X est dans $\mathbb{M}_{\underline{\mathfrak{e}};\mathfrak{b}}(\mathbf{Z})$.

Comme on le voit sur la démonstration, le premier résultat vaut sur un anneau intègre arbitraire.

Proposition (5) (Principe local-global). *Soient s_1, …, s_ℓ comaximaux dans $\mathbf{Z}$. Le système linéaire $AX = B$ admet une solution $X \in \mathbb{M}_{\underline{\mathfrak{e}};\mathfrak{b}}(\mathbf{Z})$ si, et seulement si, il admet une solution dans chaque $\mathbb{M}_{\underline{\mathfrak{e}};\mathfrak{b}}(\mathbf{Z}_{s_i})$.*

Démonstration. La condition est évidemment nécessaire. Soit $X_i = \frac{1}{s_i^k} Y_i$ une solution dans $\mathbb{M}_{\underline{\mathfrak{e}};\mathfrak{b}}(\mathbf{Z}_{s_i})$ avec $Y_i \in \mathbb{M}_{\underline{\mathfrak{e}};\mathfrak{b}}(\mathbf{Z})$, de sorte que $AY_i = s_i^k B$. On écrit $\sum_{i=1}^{\ell} u_i s_i^k = 1$ avec les $u_i \in \mathbf{Z}$. Alors $X = \sum_{i=1}^{\ell} u_i Y_i$ est une solution dans $\mathbb{M}_{\underline{\mathfrak{e}};\mathfrak{b}}(\mathbf{Z})$. □

Le point *1* du théorème suivant, bien que cas très particulier, est intéressant car le calcul de la solution se fait dans **K**. Le point *2* reprend dans le langage des pseudo-matrices le point *3* du théorème XII-3.2 dans [ACMC].

Théorème (6) (Systèmes linéaires sur un domaine de Prüfer, I).

1. *Cas particulier : on donne une pseudo-matrice carrée avec* $\mathfrak{Det}(A) \neq \langle 0 \rangle$ *et l'on suppose que les idéaux mineurs d'ordre* 1 *du vecteur colonne* B *sont tous contenus dans* $\mathfrak{Det}(A)$*. Alors la solution* $\underline{X}$ *calculée dans* **K** *fournit une pseudomatrice* $X \in \mathbb{M}_{\underline{\mathfrak{e}},\mathfrak{b}}(\mathbf{Z})$*, autrement dit* $x_j \mathfrak{b} \subseteq \mathfrak{e}_j$ *pour* $j \in [\![1..n]\!]$*.*
2. *Cas général : le système linéaire admet une solution si, et seulement si, les idéaux déterminantiels de* $[\, A \mid B \,]$ *sont égaux à ceux de* A*.*

Démonstration. Le point *1* peut se démontrer par calcul direct en utilisant la comatrice de $\underline{A}$. Il est clair aussi qu'il résulte du point *2*.

2. Considérons des éléments comaximaux s_i de **Z** tels que, après localisation en chacun des s_i, chacun des idéaux $\mathfrak{h}_j$, $\mathfrak{e}_i$ et $\mathfrak{b}$ est principal, c'est-à-dire libre de rang 1. Ceci nous ramène au cas des matrices usuelles, pour lesquelles l'équivalence est établie dans [ACMC, XII-3.2]. □

4.2 Manipulations du type Bezout

Les manipulations de colonnes (resp. de lignes) de type Bezout que nous examinons correspondent à des changements de pseudo-base pour le module de départ (resp. d'arrivée). On désire faire apparaître un coefficient nul de la même façon que ce que l'on fait dans le cas des domaines de Bezout avec des matrices usuelles.

On commence par un cas particulier.
On traite la pseudo-matrice particulière suivante de format 1×2

$$L = \begin{array}{c} \\ \mathfrak{c} \end{array} \begin{array}{c} \begin{array}{cc} \mathfrak{a} & \mathfrak{b} \end{array} \\ \begin{bmatrix} a & a \end{bmatrix} \end{array}.$$

Plutôt que de donner tout de suite la solution, expliquons d'où elle vient. Cela nous prend une quinzaine de lignes, mais cela éclaire la chose. On a une suite exacte scindable

$$0 \to \mathfrak{a} \cap \mathfrak{b} \xrightarrow{{}^t[-1\ 1]} \mathfrak{a} \oplus \mathfrak{b} \xrightarrow{[1\ 1]} \mathfrak{a} + \mathfrak{b} \to 0$$

qui donne un isomorphisme $(\mathfrak{a}+\mathfrak{b})\oplus(\mathfrak{a}\cap\mathfrak{b}) \xrightarrow{\psi} \mathfrak{a}\oplus\mathfrak{b}$.
Plus précisément, regardons $\mathfrak{a}\oplus\mathfrak{b}$ comme le sous-$\mathbf{Z}$-module E de $\mathbf{K}^2$ muni de la pseudo-base $\mathcal{E}=((e_1,\mathfrak{a}),(e_2,\mathfrak{b}))$ ((e_1,e_2), base canonique de $\mathbf{K}^2$), i.e.

$$E = e_1\mathfrak{a}\oplus e_2\mathfrak{b} = E_1\oplus E_2.$$

Il nous faut maintenant trouver une pseudo-base $\mathcal{H}=((f_1,\mathfrak{a}+\mathfrak{b}),(f_2,\mathfrak{a}\cap\mathfrak{b}))$ de E, c'est-à-dire une matrice $B\in\mathbb{M}_2(\mathbf{K})$ convenable, dont les colonnes exprimeront f_1 et f_2 sur la base (e_1,e_2).

Pour cela, on utilise l'égalité $(\mathfrak{a}:\mathfrak{b})_{\mathbf{Z}}+(\mathfrak{b}:\mathfrak{a})_{\mathbf{Z}}=\langle 1\rangle$. On a donc

$$s\in(\mathfrak{b}:\mathfrak{a})_{\mathbf{Z}} \text{ et } t\in(\mathfrak{a}:\mathfrak{b})_{\mathbf{Z}} \text{ avec } s+t=1,$$

d'où $s(\mathfrak{a}+\mathfrak{b})\subseteq\mathfrak{b}$, $t(\mathfrak{a}+\mathfrak{b})\subseteq\mathfrak{a}$ et $s\mathfrak{a}+t\mathfrak{b}=\mathfrak{a}\cap\mathfrak{b}$. D'où la matrice de passage de $\mathcal{E}$ à $\mathcal{H}$ avec $f_1=te_1+se_2$ et $f_2=-e_1+e_2$.

$$B=\mathscr{M}_{\mathcal{H},\mathcal{E}}(\mathrm{Id}_M)=\begin{array}{c} \\ \mathfrak{a} \\ \mathfrak{b}\end{array}\begin{array}{c}\begin{array}{cc}\mathfrak{a}+\mathfrak{b} & \mathfrak{a}\cap\mathfrak{b}\end{array}\\ \begin{bmatrix} t & -1 \\ s & 1\end{bmatrix}\end{array},$$

avec pour inverse

$$\mathscr{M}_{\mathcal{E},\mathcal{H}}(\mathrm{Id}_M)=\begin{array}{c} \\ \mathfrak{a}+\mathfrak{b} \\ \mathfrak{a}\cap\mathfrak{b}\end{array}\begin{array}{c}\begin{array}{cc}\mathfrak{a} & \mathfrak{b}\end{array}\\ \begin{bmatrix} 1 & 1 \\ -s & t\end{bmatrix}\end{array}.$$

Notons que l'égalité $\mathfrak{a}\,\mathfrak{b}=(\mathfrak{a}+\mathfrak{b})(\mathfrak{a}\cap\mathfrak{b})$ nous assurait que la première matrice était celle d'un isomorphisme, donc il n'y a aucune surprise à voir que la matrice inverse est bien celle d'une application $\mathbf{Z}$-linéaire.
En résumé B est une pseudo-matrice inversible et l'on obtient le résultat souhaité :

$$LB=\begin{array}{c} \\ \mathfrak{c}\end{array}\begin{array}{c}\begin{array}{cc}\mathfrak{a}+\mathfrak{b} & \mathfrak{a}\cap\mathfrak{b}\end{array}\\ \begin{bmatrix} a & 0\end{bmatrix}\end{array}$$

Le cas général.
On veut maintenant traiter la pseudo-matrice générale de format 1×2

$$L=\begin{array}{c} \\ \mathfrak{c}\end{array}\begin{array}{c}\begin{array}{cc}\mathfrak{a} & \mathfrak{b}\end{array}\\ \begin{bmatrix} a & b\end{bmatrix}\end{array}.$$

On se demande d'abord si le pivot de Gauss fonctionne (c'est-à-dire est-ce que $a\mathfrak{a}\supseteq b\mathfrak{b}$ ou $a\mathfrak{a}\subseteq b\mathfrak{b}$?), auquel cas on fait appel au pivot de Gauss.
Si ce n'est pas le cas, il suffit de se ramener au cas particulier précédent, en considérant les

idéaux $\mathfrak{a}' = b^{-1}\,\mathfrak{a}$ et $\mathfrak{b}' = a^{-1}\,\mathfrak{b}$.[4] On a alors une pseudo-matrice inversible

$$P = \begin{array}{c} \\ \mathfrak{a} \\ \mathfrak{b} \end{array} \begin{array}{c} \begin{array}{cc} \mathfrak{a}' & \mathfrak{b}' \end{array} \\ \begin{bmatrix} b & 0 \\ 0 & a \end{bmatrix} \end{array} \quad \text{avec} \quad LP = \begin{array}{c} \\ \mathfrak{c} \end{array} \begin{array}{c} \begin{array}{cc} \mathfrak{a}' & \mathfrak{b}' \end{array} \\ \begin{bmatrix} ab & ab \end{bmatrix} \end{array}.$$

En fin de compte ce sont donc les idéaux $\mathfrak{a}'$ et $\mathfrak{b}'$ qui seront traités selon la méthode donnée dans le cas particulier étudié en premier. En particulier, on prendra s et $t \in \mathbf{A}$ tels que $s + t = 1$, $s\mathfrak{a}' \subseteq \mathfrak{b}'$ et $t\mathfrak{b}' \subseteq \mathfrak{a}'$ (i.e. $sa\mathfrak{a} \subseteq b\mathfrak{b}$ et $tb\mathfrak{b} \subseteq a\mathfrak{a}$).

4.3 Réduction de Hermite : images et noyaux d'applications linéaires

Dans cette sous-section, on montre comment la réduction de Hermite des pseudo-matrices permet de démontrer sous forme très concrète les théorèmes de structure généraux concernant aussi bien les systèmes linéaires que les modules de présentation finie sur les domaines de Prüfer.

Théorème (7) (Réduction de Hermite). *Soit* $\mathbf{Z}$ *un domaine de Prüfer de corps de fractions* $\mathbf{K}$ *pour lequel on a un test de divisibilité et un algorithme d'inversion des idéaux de type fini. Soit*

$$A = ((\mathfrak{h}_i)_{i\in[\![1..n]\!]}, (\mathfrak{e}_j)_{j\in[\![1..m]\!]}, \underline{A}) \text{ avec } \underline{A} = (a_{ij}) \in \mathbb{M}_{n,m}(\mathbf{K})$$

une pseudo-matrice sur $\mathbf{Z}$ *(i.e.,* $a_{ij}\mathfrak{e}_j \subseteq \mathfrak{h}_i$ *pour tous* i, j*). On peut calculer une pseudo-matrice inversible*

$$C = ((\mathfrak{e}_j)_{j\in[\![1..m]\!]}, (\mathfrak{e}'_j)_{j\in[\![1..m]\!]}, \underline{C}) \text{ avec } \underline{C} = (c_{j,k}) \in \mathbb{M}_m(\mathbf{K})$$

(on regarde C *comme opérant un changement de pseudo-base au départ), et une matrice de permutation* $\underline{L} \in \mathbb{M}_n(\mathbf{Z})$ *(la pseudo-matrice* L *correspondante opère un changement de pseudo-base à l'arrivée), telles que la matrice* $L\,A\,C$ *soit en forme réduite de Hermite :* $H = \begin{array}{|c|c|}\hline T & 0 \\ \hline G & 0 \\ \hline \end{array}$, T *carrée triangulaire inférieure de déterminant non nul.*

Démonstration. Cela résulte des manipulations de colonnes de type pivot de Gauss et de type Bezout décrites précédemment. Tout se passe comme pour une matrice sur un anneau de Bezout intègre, à ceci près que l'on doit remplacer les matrices usuelles par des pseudo-matrices. □

Notons que le test de divisibilité est utilisé uniquement pour vérifier que dans certains cas, des manipulations élémentaires du type pivot de Gauss sont admissibles. On pourrait donc se passer

4. Dans le cas où l'on mène tous les calculs avec des idéaux entiers, on considère un élément $x \in \mathbf{K}$ tels que les idéaux fractionnaires $\mathfrak{a}' = xb^{-1}\,\mathfrak{a}$ et $\mathfrak{b}' = xa^{-1}\,\mathfrak{b}$ soient entiers, i.e. $x \in b\mathfrak{a}^{-1} \cap a\mathfrak{b}^{-1}$. Simplement, on peut prendre pour x un multiple commun des numérateurs de a et b, ce qui donne xb^{-1} et $xa^{-1} \in \mathbf{A}$, et a fortiori $\mathfrak{a}'$ et $\mathfrak{b}'$ entiers.

de cette hypothèse en faisant fonctionner l'algorithme de réduction de Hermite uniquement avec des manipulations de type Bezout. Cependant, comme déjà indiqué, nous faisons toujours l'hypothèse que l'anneau $\mathbf{Z}$ est un domaine de Prüfer à divisibilité explicite (au sens constructif).

Les théorèmes qui suivent sont tous des corollaires faciles du théorème 7 concernant les pseudo-matrices.

Théorème (8) (Image d'une pseudo-matrice). *L'image de toute pseudo-matrice est isomorphe à une somme directe d'idéaux inversibles.*

Démonstration. On effectue une réduction de Hermite de la matrice. La multiplication à droite par une pseudo-matrice inversible ne change pas le module image. Il suffit de traiter l'image d'une pseudo-matrice $(\underline{\mathfrak{h}}; \underline{\mathfrak{e}'}; H)$ où $H = \begin{array}{|c|c|}\hline T & 0 \\ \hline G & 0 \\ \hline \end{array}$ est en forme réduite de Hermite.

C'est aussi l'image de la pseudo-matrice $(\underline{\mathfrak{h}}; \mathfrak{e}'_1, \ldots, \mathfrak{e}'_r; H_1)$ où $H_1 = \begin{array}{|c|}\hline T \\ \hline G \\ \hline \end{array}$. Comme $\det(T) \neq 0$, l'application linéaire

$$\mathfrak{e}'_1 \times \cdots \times \mathfrak{e}'_r \longrightarrow \mathfrak{h}_1 \times \cdots \times \mathfrak{h}_n$$

définie par H_1 est injective. Donc $\operatorname{Im} A = \operatorname{Im} H = \operatorname{Im} H_1 \simeq \mathfrak{e}'_1 \times \cdots \times \mathfrak{e}'_r$.
Précisément, supposons que l'on traite la pseudo-matrice A d'une application $\mathbf{Z}$-linéaire $\varphi : E \to H$ sur des pseudo-bases $\mathcal{E} = ((e_1, \mathfrak{e}_1), \ldots, (e_m, \mathfrak{e}_m))$ et $\mathcal{H} = ((h_1, \mathfrak{h}_1), \ldots, (h_n, \mathfrak{h}_n))$ de E et H. Alors l'image de φ est le module somme directe $\mathfrak{e}'_1 h'_1 \oplus \cdots \oplus \mathfrak{e}'_r h'_r$, où les h'_i sont les vecteurs exprimés par les colonnes de la matrice H_1 sur les h_i (qui sont des éléments de $\mathbf{K} \otimes_{\mathbf{Z}} H$). □

Théorème (9) (Images).

1. *Tout $\mathbf{Z}$-module projectif de type fini est isomorphe à une somme directe d'idéaux inversibles, autrement dit, il possède une pseudo-base.*
2. *L'image d'une application linéaire entre $\mathbf{Z}$-modules projectifs de type fini est un module projectif de type fini dont on peut calculer une pseudo-base.*
3. — *Tout sous-$\mathbf{Z}$-module de type fini de $\mathbf{K}^n$ est projectif de type fini.*
   — *Si $g_1, \ldots, g_m \in \mathbf{K}^n$ et si $\mathfrak{e}_1, \ldots, \mathfrak{e}_m$ sont des idéaux de type fini non nuls, on peut calculer une pseudo-base du $\mathbf{Z}$-module $E = \sum_j g_j \mathfrak{e}_j$.*

Démonstration. 1. Puisqu'un module projectif de type fini est isomorphe à l'image d'une matrice de projection usuelle, cela résulte du théorème 8.

2. Il s'agit pour l'essentiel d'une reformulation du théorème 8. En effet, vu le point *1*, tout module projectif de type fini possède une pseudo-base. Alors une application linéaire entre modules projectifs de type fini est représentée par une pseudo-matrice sur les pseudo-bases des modules.

3. Les deux points sont équivalents. Le second résulte du théorème 8 car E est l'image d'une pseudo-matrice $(\langle d\rangle, \dots, \langle d\rangle ; \mathfrak{e}_1, \dots, \mathfrak{e}_m; \underline{G})$, où $\underline{G}$ a pour colonnes les g_j exprimés sur la base canonique de $\mathbf{K}^n$, et où l'élément $d \in \mathbf{K}$ est choisi de façon que $g_{ij}\mathfrak{e}_j \subseteq d\mathbf{Z}$ pour tous les (i,j).□

Théorème (10) (Noyaux). *Soit $\varphi : E \to H$ une application linéaire entre modules projectifs de type fini sur un domaine de Prüfer. Le noyau* $\operatorname{Ker}\varphi$ *est facteur direct dans E (a fortiori projectif de type fini). Plus précisément, on peut calculer une pseudo-base de E dont les derniers termes forment une pseudo-base de* $\operatorname{Ker}\varphi$*.*

Démonstration. Comme dans le théorème précédent, il suffit de faire la démonstration pour le noyau d'une pseudo-matrice, et l'on prend les notations du théorème 7. Le changement de pseudo-base donné par la matrice C fournit une nouvelle pseudo-base $((u_1, \mathfrak{e}'_1), \dots, (u_m, \mathfrak{e}'_m))$ (les u_j sont exprimés par les colonnes de la matrice C), pour laquelle l'application linéaire est exprimée par la nouvelle pseudo-matrice H. Pour cette matrice il est clair que le noyau est fourni par la somme directe des sous-modules $u_j\mathfrak{e}'_j$ pour les numéros j des colonnes nulles de H. □

4.4 Pseudo-matrices surjectives

La proposition suivante reprend le point *3* du théorème 3, qui généralise un théorème bien connu pour les matrices usuelles.

Dans le point *3* du théorème 3, l'application linéaire φ, ici représentée par A, admet un inverse à droite ψ du fait qu'elle est surjective et que l'image est un module projectif. Le module source de φ est égal à $\operatorname{Im}\psi \oplus \operatorname{Ker}\varphi$. Lorsque $\operatorname{Ker}\varphi$ est une somme directe de modules projectifs de rang 1, la matrice A peut être complétée en la pseudo-matrice inversible B qui représente l'application linéaire $\varphi|_{\operatorname{Im}\psi} \oplus \operatorname{Id}_{\operatorname{Ker}\varphi}$, laquelle a pour source $\operatorname{Im}\psi \oplus \operatorname{Ker}\varphi$ et pour image $\operatorname{Im}\varphi \oplus \operatorname{Ker}\varphi$.

Une fois que l'existence de la pseudo-matrice B est assurée par un argument général, il reste le problème algorithmique d'un calcul aussi simple que possible de cette pseudo-matrice.

Nous sommes intéressés ici par une démonstration matricielle algorithmique du résultat dans le contexte des domaines de Prüfer, pour lesquels les calculs sur les pseudo-matrices sont simplifiés.

Proposition (11) (Pseudo-matrices surjectives). *Soit $\mathbf{Z}$ un domaine de Prüfer et soit $n \in [\![1..m]\!]$. Soit $A = (\mathfrak{h}_1, \dots, \mathfrak{h}_n; \mathfrak{e}_1, \dots, \mathfrak{e}_m; \underline{A}) \in \mathbb{M}_{\mathfrak{h},\mathfrak{e}}(\mathbf{Z})$. Cette pseudo-matrice représente une application linéaire surjective si, et seulement si, $\mathfrak{D}_n(A) = \langle 1\rangle$. Dans ce cas, A peut être complétée en une pseudo-matrice inversible*

$$B = (\mathfrak{h}_1, \dots, \mathfrak{h}_m; \mathfrak{e}_1, \dots, \mathfrak{e}_m; \underline{B}).$$

La matrice AB^{-1} est alors en forme de Smith :

$$AB^{-1} = \begin{array}{c} \\ \mathfrak{h}_1 \\ \mathfrak{h}_2 \\ \vdots \\ \mathfrak{h}_n \end{array} \begin{array}{c} \begin{array}{ccccccc} \mathfrak{h}_1 & \mathfrak{h}_2 & \cdots & \mathfrak{h}_n & \mathfrak{h}_{n+1} & \cdots & \mathfrak{h}_m \end{array} \\ \begin{bmatrix} 1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & 1 & \ddots & \vdots & \vdots & & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots & & \vdots \\ 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \end{bmatrix} \end{array}.$$

Et la pseudo-matrice extraite sur les n premières colonnes de B^{-1} est un inverse à droite de A.

Démonstration. On démontre l'implication difficile.
D'après le théorème 7, on peut calculer une pseudo-matrice inversible

$$C = ((\mathfrak{e}_j)_{j\in[\![1..m]\!]}; \mathfrak{e}'_1, \ldots, \mathfrak{e}'_n, \mathfrak{h}_{n+1}, \ldots, \mathfrak{h}_m; \underline{C}) \text{ avec } \underline{C} = (c_{j,k}) \in \mathbb{M}_m(\mathbf{K})$$

telle que la matrice $A\,C$ soit en forme réduite de Hermite : $H = \boxed{\begin{array}{c|c} T & 0 \end{array}}$, où T est carrée triangulaire inférieure. On a $\mathfrak{D}_n(T) = \mathfrak{D}_n(A) = \langle 1\rangle$, donc T est inversible. En fait les idéaux mineurs d'ordre 1 diagonaux $\mathfrak{m}_{ii}(T)$ ont leur produit égal à $\langle 1\rangle$, donc sont tous égaux à $\langle 1\rangle$, ce qui autorise la méthode du pivot par manipulations élémentaires de colonnes. On termine en inversant la matrice diagonale obtenue. On a ainsi ramené T à la forme $(\mathfrak{h}_1, \ldots, \mathfrak{h}_n; \mathfrak{h}_1, \ldots, \mathfrak{h}_n; \mathrm{I}_n)$. Ceci donne une pseudo-matrice inversible C' telle que $A\,C\,C' = \boxed{\begin{array}{c|c} \mathrm{I}_n & 0 \end{array}}$ et l'on pose $B := (C\,C')^{-1}$.
En regardant B comme une pseudo-matrice par blocs $B = \boxed{\begin{array}{c} B_1 \\ \hline B_2 \end{array}}$, on obtient $\boxed{\begin{array}{c|c} \mathrm{I}_n & 0 \end{array}} \boxed{\begin{array}{c} B_1 \\ \hline B_2 \end{array}} = A$ et $B_1 = A$. □

4.5 Double réduction de Hermite, conoyaux

Théorème (12) (Double réduction de Hermite). *Mêmes hypothèses qu'au théorème 7. On peut calculer une pseudo-matrice inversible C opérant un changement de pseudo-base au départ, et une pseudo-matrice inversible L opérant un changement de pseudo-base à l'arrivée, telles que $L\,A\,C = \boxed{\begin{array}{c|c} T & 0 \\ \hline 0 & 0 \end{array}}$, où T est triangulaire inférieure de déterminant non nul.*

Démonstration. On fait une réduction de Hermite sur les colonnes, suivie d'une réduction de Hermite sur les lignes. □

Le théorème suivant est une forme précise, «pseudo-matricielle», du théorème XIV-2.5 de [Modules].

Théorème (13) (Conoyaux). *Soit $\varphi : E \to H$ une application linéaire entre modules projectifs de type fini sur un domaine de Prüfer.*

1. *Le saturé de* $\operatorname{Im}\varphi$ *dans H est en facteur direct dans H. Plus précisément, on peut calculer une pseudo-base de H dont les premiers termes forment une pseudo-base du saturé de* $\operatorname{Im}\varphi$.
2. *Le module conoyau* $\operatorname{Coker}\varphi$ *est un module de présentation finie, somme directe de son sous-module de torsion et d'un module projectif de type fini.*
3. *Le sous-module de torsion de* $\operatorname{Coker}\varphi$ *est le quotient d'un module projectif par un sous-module projectif de même rang. Il est isomorphe au conoyau d'une pseudo-matrice carrée injective.*

En particulier tout module de présentation finie sans torsion est projectif.

Démonstration. Le point *1* résulte du théorème 12 et du fait que lorsque l'on sature l'image d'une pseudo-matrice carrée injective, on obtient le module d'arrivée en entier. Le reste suit facilement. □

Remarque. Dans le théorème 13, la structure du sous-module de torsion et celle du sous-module projectif de type fini ne sont pas décryptées de manière complètement satisfaisante. En particulier, ce théorème, bien que constructif, ne donne pas de solution algorithmique générale aux deux problèmes suivants :

— déterminer si deux modules de présentation finie de torsion sont ou ne sont pas isomorphes ;
— déterminer si deux modules projectifs de type fini sont ou ne sont pas isomorphes.

On verra dans la section 5 que lorsque le domaine de Prüfer $\mathbf{Z}$ est de dimension 1, on sait répondre à la première question, mais pas nécessairement à la seconde, qui se ramènera à la question de savoir si un idéal de type fini $\mathfrak{e}$ est principal. Ce problème n'admet pas de solution algorithmique générale, même pour les domaines de Dedekind. ∎

4.6 Systèmes linéaires, via la réduction de Hermite

Le théorème 7 donne le corollaire suivant pour le traitement des systèmes linéaires. On notera que les tests proposés ici sont explicites parce que le divisibilité dans $\mathbf{Z}$ est explicite.

Théorème (14) (Systèmes linéaires sur un domaine de Prüfer, II). *On considère un système linéaire $AX = B$ de n équations à m inconnues sur $\mathbf{Z}$. Dans la situation usuelle, tous les idéaux indexant les lignes et les colonnes des matrices A, B (données) et X (inconnue) sont égaux à $\langle 1\rangle$, les inconnues (coordonnées de X) sont dans $\mathbf{Z}$ et $\underline{A} \in \mathbb{M}_{n,m}(\mathbf{Z})$.*
Les résultats s'appliquent aussi bien avec des pseudo-matrices $A = (\underline{\mathfrak{h}}; \underline{\mathfrak{e}}; \underline{A})$ et $B = (\underline{\mathfrak{h}}; \mathfrak{b}; \underline{B})$,

en adaptant le format de la colonne X aux données : les inconnues sont des éléments $x_j \in \mathbf{K}$ soumis aux conditions $x_j\mathfrak{b} \in \mathfrak{e}_j$.

On considère une double réduction de Hermite $L\,A\,C = \begin{array}{|c|c|}\hline T & 0 \\ \hline 0 & 0 \\ \hline \end{array}$, avec la matrice $\underline{T} \in \mathbb{M}_r(\mathbf{K})$ triangulaire inférieure injective. Les pseudo-matrices $C = (\underline{\mathfrak{e}}, \underline{\mathfrak{e}'}, \underline{C})$ et $L = (\underline{\mathfrak{h}'}, \underline{\mathfrak{h}}, \underline{L})$ sont inversibles, et l'on introduit les nouvelles inconnues $Y = C^{-1}X$.

1. *La solution générale du système homogène sans second membre $AX = 0$ est donnée par $y_1 = \cdots = y_r = 0$. Ceci donne pour Y le sous-$\mathbf{Z}$-module*
$$K = \{0\} \times \cdots \times \{0\} \times \mathfrak{e}'_{r+1} \times \cdots \times \mathfrak{e}'_m$$
et pour X, le $\mathbf{Z}$-module $C(K)$ paramétré par
$$(y_{r+1}, \ldots, y_m) \in \mathfrak{e}'_{r+1} \times \cdots \times \mathfrak{e}'_m,$$
c'est aussi l'image de la pseudo-matrice extraite de C sur les $m - r$ dernières colonnes.
2. *Le système linéaire avec second membre $AX = B$ admet une solution si, et seulement si, le sous-$\mathbf{Z}$-module de $\mathbf{K}^n$ codé par LB est contenu dans l'image de la pseudo-matrice*
$$\Big(\mathfrak{h}'_1, \ldots, \mathfrak{h}'_n; \mathfrak{e}'_1, \ldots, \mathfrak{e}'_r; \begin{bmatrix} T \\ 0 \end{bmatrix}\Big).$$
   - *Les contraintes données par l'annulation des $n - r$ dernières coordonnées de $\underline{L}\,\underline{B}$ signifient exactement que le système $\underline{A}\,\underline{X} = \underline{B}$ a une solution dans $\mathbf{K}^m$.*
   - *Les contraintes sur les r premières coordonnées de $\underline{L}\,\underline{B}$ peuvent être testées de proche en proche, vue la forme triangulaire de $\underline{T}$.*
   - *On peut donc tester l'existence d'une solution et calculer une solution particulière lorsqu'il en existe une.*

Démonstration. Il faut juste préciser la question du test pour une solution particulière : toute solution donne par soustraction une solution avec les «inconnues auxiliaires» nulles, donc le test peut porter uniquement sur l'équation $TZ = B'$ avec Z et B' donnés par troncatures de Y et LB aux r premières coordonnées. Comme T est injective, la solution, si elle existe, est unique.□

Commentaire. L'énoncé du corollaire sur les systèmes linéaires est un peu plus simple dans le cas d'un système linéaire usuel, mais il n'est pas «nettement plus simple», car les idéaux $\mathfrak{e}'_j$ et $\mathfrak{h}'_i$ introduits par la double réduction de Hermite, ainsi que les coefficients de $\underline{T}$ dans $\mathbf{K}$ et non dans $\mathbf{Z}$, semblent des ingrédients inévitables. ∎

5 Calculs modulaires et réduction de Smith en dimension 1

Dans cette section, $\mathbf{Z}$ est un domaine de Prüfer à divisibilité explicite, de dimension $\leqslant 1$.

Définition (5). *Soit $A = (\mathfrak{h}_1, \dots, \mathfrak{h}_n; \mathfrak{e}_1, \dots, \mathfrak{e}_m; \underline{A}) \in \mathbb{M}_{\underline{\mathfrak{h}},\underline{\mathfrak{e}}}(\mathbf{Z})$ et $p = \inf(m, n)$. La pseudo-matrice A est dite **en forme de Smith** si la matrice $\underline{A} = (a_{ij})$ a tous ses coefficients nuls hormis éventuellement des coefficients a_{ii} et si les idéaux mineurs d'ordre 1 $\mathfrak{c}_i := \mathfrak{m}_{ii}(A) = a_{ii}\mathfrak{e}_i\mathfrak{h}_i^{-1}$ satisfont les relations attendues :*

$$\mathfrak{c}_1 \supseteq \mathfrak{c}_2 \supseteq \cdots \supseteq \mathfrak{c}_p.$$

Théorème (15). *Soit $\mathbf{Z}$ un domaine de Dedekind explicite, i.e., un domaine de Prüfer noethérien à divisibilité explicite. Toute pseudo-matrice sur $\mathbf{Z}$ est équivalente à une pseudo-matrice en forme de Smith.*

Démonstration. L'algorithme est le même que pour la réduction de Smith d'une matrice sur un anneau principal, en remplaçant les matrices usuelles par des pseudo-matrices. On peut se reporter à [Modules, Algorithme IV-2.2]. □

5.1 Sur l'unicité d'une réduite de Smith usuelle

Lorsqu'une matrice $M \in \mathbb{M}_{n,m}(\mathbf{A})$ admet une réduction de Smith dont la partie carrée est égale à $\mathrm{Diag}(a_1, \dots, a_n)$, le module $\mathrm{Coker}\, M$ est isomorphe à la somme directe des $\mathbf{A}/\langle a_i\rangle$:

$$\mathrm{Coker}\, M \;\simeq\; \mathbf{A}/\langle a_1\rangle \oplus \cdots \oplus \mathbf{A}/\langle a_n\rangle \quad \text{avec des idéaux} \quad \langle a_1\rangle \supseteq \cdots \supseteq \langle a_n\rangle\,.$$

Les idéaux $\mathfrak{e}_i = \langle a_i\rangle$ sont uniquement déterminés (fait 1).

Plus précisément, si aucun des a_i n'est inversible, la liste $(\mathfrak{e}_1, \dots, \mathfrak{e}_n)$ ne dépend que du module $\mathrm{Coker}\, M$.

Cela ne signifie pas nécessairement que pour deux matrices équivalentes en forme de Smith $A = (a_{ij})$ et $A' = (a'_{ij})$ les a'_{ii} soient associés aux a_{ii}.

Néanmoins, c'est vrai lorsque $\mathbf{A}$ est intègre, et le lemme suivant montre que c'est aussi le cas pour un anneau zéro-dimensionnel.

Lemme (16). *Soient a et $b \in \mathbf{A}$ zéro-dimensionnel. Si $\langle a\rangle = \langle b\rangle$, alors a et b sont **associés** : $a = wb$ pour un élément $w \in \mathbf{A}^\times$.*

Démonstration. On a $a = ub$ et $b = va$, donc $a(uv-1) = 0$. Comme $\mathbf{A}$ est zéro-dimensionnel on a un idempotent e tel que $uv-1$ est nilpotent modulo e et inversible modulo $1-e$. Dans la composante $\mathbf{A}/\langle e\rangle$, on a $uv = 1+x$ avec x nilpotent, donc u est inversible. Dans la composante $\mathbf{A}/\langle 1-e\rangle$, $a = 0$ donc $b = 0$ et l'on a $a = 1.b$. En bref $a = wb$ avec $w = u.(1-e) + 1.e$ inversible. □

On montre maintenant un lemme qui complète en quelque sorte le lemme précédent.

Lemme (17). *Soit* $\mathrm{Diag}(a_1, \ldots, a_n)$ *une matrice en forme de Smith sur un anneau* $\mathbf{A}$*, et des* $u_i \in \mathbf{A}^\times$ *tels que* $\prod_i u_i = 1$*. Définissons* $a'_i = a_i u_i$*, alors les deux matrices* $\mathrm{Diag}(a_1, \ldots, a_n)$ *et* $\mathrm{Diag}(a'_1, \ldots, a'_n)$ *sont élémentairement équivalentes.*

Démonstration. Il suffit de traiter le cas suivant, avec $b = ca$, $a' = au$, $uv = 1$, $b' = bv$, $A = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$ et $B = \begin{bmatrix} a' & 0 \\ 0 & b' \end{bmatrix}$.

$$\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \xrightarrow{1} \begin{bmatrix} a & a'-a \\ 0 & b \end{bmatrix} \xrightarrow{2} \begin{bmatrix} a' & a'-a \\ b & b \end{bmatrix} \xrightarrow{3} \begin{bmatrix} a' & a'-a \\ 0 & b' \end{bmatrix} \xrightarrow{4} \begin{bmatrix} a' & 0 \\ 0 & b' \end{bmatrix}$$

$1 : C_2 \leftarrow C_2 + (u-1)C_1$.
$2 : C_1 \leftarrow C_1 + C_2$.
$3 : L_2 \leftarrow L_2 - cvL_1$, avec $b - cv(a'-a) = b - ca + cva = cva = vb = b'$.
$4 : C_2 \leftarrow C_2 + (v-1)C_1$.

En bref

$$\begin{bmatrix} 1 & 0 \\ -cv & 1 \end{bmatrix} A \begin{bmatrix} 1 & u-1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & v-1 \\ 0 & 1 \end{bmatrix} = B.$$

□

5.2 La structure des modules de présentation finie de torsion, et quelques calculs matriciels

Rappelons la démonstration de la proposition suivante [Modules, XVI-4.6].

Proposition (18). *Un module de présentation finie de torsion* P *sur un domaine de Prüfer* $\mathbf{Z}$ *de dimension* 1 *est isomorphe à une somme directe*

$$\mathbf{Z}/\mathfrak{a}_1 \oplus \cdots \oplus \mathbf{Z}/\mathfrak{a}_n, \quad \textit{avec des idéaux inversibles } \mathfrak{a}_1 \supseteq \cdots \supseteq \mathfrak{a}_n.$$

Si les $\mathfrak{a}_i$ sont $\neq \langle 1\rangle$ cette écriture est unique [5]. Plus généralement, deux écritures de ce type de même longueur sont identiques (fait 1).

Démonstration. Le module P est annulé par un élément $\delta \neq 0$, parce qu'il est de torsion et de type fini (il suffit que δ annule chacun des générateurs).

L'anneau quotient $\mathbf{Z}' = \mathbf{Z}/\langle\delta\rangle$ est zéro-dimensionnel et arithmétique, donc est un anneau de Smith ([Modules, XVI-4.2]).

Ainsi, on a un isomorphisme de $\mathbf{Z}$-modules (ce sont aussi des $\mathbf{Z}'$-modules) du type suivant

$$P = P/\delta P \simeq \mathbf{Z}'/\langle\overline{a_1}\rangle \oplus \cdots \oplus \mathbf{Z}'/\langle\overline{a_n}\rangle \simeq \mathbf{Z}/\langle\delta, a_1\rangle \oplus \cdots \oplus \mathbf{Z}/\langle\delta, a_n\rangle\,,$$

avec les inclusions $\langle\delta, a_1\rangle \supseteq \cdots \supseteq \langle\delta, a_n\rangle$.

En pratique, cela se passe précisément comme suit. Le module P est présenté par une matrice $M \in \mathbb{M}_{n,m}(\mathbf{Z})$ avec $\mathfrak{d}_n := \mathfrak{D}_n(M) = \mathfrak{F}_0(P) \neq \langle 0\rangle$.
Pour un $\delta \neq 0$ dans $\mathfrak{d}_n$, on calcule sur $\mathbf{Z}'$ une réduite de Smith par manipulations élémentaires $\overline{L}\,\overline{M}\,\overline{C} = \begin{array}{|c|c|}\hline D & 0 \\ \hline \end{array}$ avec $D = \mathrm{Diag}(\overline{a_1}, \ldots, \overline{a_n})$ et $\langle\overline{a_1}\rangle \supseteq \cdots \supseteq \langle\overline{a_n}\rangle$. On en déduit la structure de P comme ci-dessus, de sorte que $\mathfrak{D}_k(M) = \mathfrak{F}_{n-k}(P) = \langle a_1 \cdots a_k, \delta\rangle = \mathfrak{a}_1 \cdots \mathfrak{a}_k$ et $\mathfrak{a}_k = \langle a_k, \delta\rangle$ pour chaque $k \in [\![0..n]\!]$. □

On en déduit le corollaire suivant.

Corollaire (19). *Sur un domaine de Prüfer de dimension $\leqslant 1$, la structure d'un module de présentation finie de torsion P est caractérisée par ses idéaux de Fitting $\mathfrak{F}_k(P)$.*

Démonstration. En effet, dans la proposition 18, notons $\mathfrak{d}_i = \mathfrak{F}_{n-i}(P)$. On a alors $\mathfrak{d}_1 = \mathfrak{a}_1$, et plus généralement $\mathfrak{d}_k = \mathfrak{a}_1 \cdots \mathfrak{a}_k$ pour $k \in [\![2..n]\!]$ (fait 2) ; donc $\mathfrak{a}_k = (\mathfrak{d}_k : \mathfrak{d}_{k-1})$ car $\mathfrak{a}_k \neq \langle 0\rangle$. □

Le corollaire suivant est plus surprenant.

Corollaire (20). *Soit $M \in \mathbb{M}_{n,m}(\mathbf{Z})$ avec $\mathfrak{D}_n(M) \neq 0$. Soit $\delta \neq 0$ dans $\mathfrak{D}_n(M)$. On considère l'anneau arithmétique zéro-dimensionnel $\mathbf{Z}' = \mathbf{Z}/\langle\delta\rangle$. On note $\overline{x}$ pour $x \bmod \delta$. On calcule par manipulations élémentaires une réduite de Smith de $\overline{M}$, disons*

$$\overline{M'} \equiv \begin{array}{|c|c|}\hline D & 0 \\ \hline \end{array} \bmod \delta \text{ avec } D = \mathrm{Diag}(\overline{a_1}, \ldots, \overline{a_n}) \text{ et } \langle\overline{a_1}\rangle \supseteq \cdots \supseteq \langle\overline{a_n}\rangle\,.$$

Alors :

1. $\langle a_1 \cdots a_i, \delta\rangle = \langle a_1, \delta\rangle \cdots \langle a_i, \delta\rangle$ *pour* $i \in [\![2..n]\!]$.

5. Dans la mesure où nous supposons que $\mathbf{Z}$ est à divisibilité explicite, on pourra se débarrasser des idéaux égaux à $\langle 1\rangle$.

2. $\mathfrak{D}_n(M) = \langle a_1, \delta\rangle \cdots \langle a_n, \delta\rangle$.

3. $(\langle \prod_{i\in I\cup J} a_i, \delta\rangle : \langle \prod_{i\in I} a_i, \delta\rangle) = \langle \prod_{i\in J} a_i, \delta\rangle$ *dans les cas suivants :*
$I = [\![1..k]\!]$ *et* $J = [\![k+1..\ell]\!] \subseteq [\![1..n]\!]$, *ou vice versa.*

4. $(\prod_{i\in I\cup J} \overline{a_i} : \prod_{i\in I} \overline{a_i}) = \prod_{i\in J} \overline{a_i}$ *dans les cas suivants :*
$I = [\![1..k]\!]$ *et* $J = [\![k+1..\ell]\!] \subseteq [\![1..n]\!]$, *ou vice versa.*

Démonstration. Les points *1* et *2*. Cas particulier de ce qui a été expliqué dans la démonstration de la proposition 18.
Le point *3* résulte des égalités $\mathfrak{d}_i = \mathfrak{a}_1 \cdots \mathfrak{a}_i$, car $\mathbf{Z}$ est un domaine de Prüfer.
Le point *4* en résulte parce que lorsqu'on a trois idéaux $I \subseteq J \subseteq K$ dans un anneau $\mathbf{A}$, on a l'égalité

$$(J : K)_{\mathbf{A}} \bmod I = (J/I : K/I)_{\mathbf{A}/I}.$$

□

Et maintenant on obtient la «réduction de Smith avec pseudo-bases» d'une matrice carrée de déterminant non nul sans effort.

Proposition (21). *Soit* $M \in \mathbb{M}_n(\mathbf{Z})$ *une matrice avec* $d = \det(M) \neq 0$ *(*$\mathbf{Z}$ *domaine de Prüfer de dimension* 1*). Cette matrice est équivalente à une pseudo-matrice de la forme*

$$M_1 = \begin{array}{c} \\ \langle 1\rangle \\ \langle 1\rangle \\ \vdots \\ \langle 1\rangle \end{array} \begin{array}{c} \begin{array}{cccc} \mathfrak{a}_1 & \mathfrak{a}_2 & \cdots & \mathfrak{a}_n \end{array} \\ \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{bmatrix} \end{array}$$

avec $\mathfrak{a}_1 \supseteq \mathfrak{a}_2 \supseteq \cdots \supseteq \mathfrak{a}_n$, $\prod_i \mathfrak{a}_i = \langle d\rangle$ *et chaque* $\mathfrak{a}_i$ *de la forme* $\langle a_i, d\rangle$.

Démonstration. On reprend ce qui a été expliqué dans la démonstration de la proposition 18 (éventuellement avec $\delta = d$). En examinant ce qui se passe dans le calcul de la réduction de Smith modulaire par manipulations élémentaires, on obtient sur $\mathbf{Z}$ une égalité et une congruence

$$LMC = M' \equiv \mathrm{Diag}(a_1, \ldots, a_n) \bmod \delta\ .$$

Considérons la pseudo-matrice [6]

$$E := \begin{array}{c} \\ \mathfrak{a}_1 \\ \vdots \\ \mathfrak{a}_n \end{array} \begin{array}{c} \begin{array}{ccc} \langle 1\rangle & \cdots & \langle 1\rangle \end{array} \\ \begin{bmatrix} & & \\ & M' & \\ & & \end{bmatrix} \end{array}.$$

Puisque $M' = \mathrm{Diag}(a_1, \ldots, a_n) \bmod \delta$, elle est de la forme

$$E = \begin{array}{c} \\ \mathfrak{a}_1 \\ \mathfrak{a}_2 \\ \vdots \\ \mathfrak{a}_n \end{array} \begin{array}{c} \begin{array}{cccc} \langle 1\rangle & \langle 1\rangle & \cdots & \langle 1\rangle \end{array} \\ \begin{bmatrix} a_1 + \delta x_{11} & \delta x_{12} & \cdots & \delta x_{1n} \\ \delta x_{21} & a_2 + \delta x_{22} & & \vdots \\ \vdots & & \ddots & \vdots \\ \delta x_{n1} & \cdots & & a_n + \delta x_{nn} \end{bmatrix} \end{array}.$$

Alors c'est une pseudo-matrice de changement de pseudo-base. En effet, $\prod_{i=1}^{n} \mathfrak{a}_i = \langle d\rangle$ avec $d = \det(M) = \det(LMC) = \det(M') = \det(\underline{E})$, donc $\mathfrak{Det}(E) = \langle 1\rangle$. Son inverse est la pseudo-matrice

$$E^{-1} = \begin{array}{c} \\ \langle 1\rangle \\ \vdots \\ \langle 1\rangle \end{array} \begin{array}{c} \begin{array}{ccc} \mathfrak{a}_1 & \cdots & \mathfrak{a}_n \end{array} \\ \begin{bmatrix} & & \\ & M'^{-1} & \\ & & \end{bmatrix} \end{array}$$

Posons $C_1 = CE^{-1}$. On obtient $LMC_1 = M_1$ de la forme annoncée, où L et C_1 sont des pseudo-matrices de changements de base (L et M sont des matrices usuelles vues comme des pseudo-matrices ayant les idéaux $\langle 1\rangle$ en indices de lignes et en colonnes). □

Voici maintenant le résultat analogue pour une matrice « usuelle » plus large que haute. Il nous faut faire ici appel à la proposition 11 concernant les pseudo-matrices surjectives en espérant qu'elle soit efficace sur un domaine de Prüfer de dimension 1.

Théorème (22). *Soit $M \in \mathbb{M}_{n,m}(\mathbf{Z})$ une matrice avec $\mathfrak{D}_n(M) \neq 0$. Soit un élément δ non nul de $\mathfrak{D}_n(M)$. Cette matrice est équivalente à une pseudo-matrice de la forme*

$$M_1 = \begin{array}{c} \\ \langle 1\rangle \\ \langle 1\rangle \\ \vdots \\ \langle 1\rangle \end{array} \begin{array}{c} \begin{array}{cccccc} \mathfrak{a}_1 & \mathfrak{a}_2 & \cdots & \mathfrak{a}_n & \cdots & \mathfrak{a}_m \end{array} \\ \begin{bmatrix} 1 & 0 & \cdots & 0 & \cdots & 0 \\ 0 & 1 & \ddots & \vdots & & \vdots \\ \vdots & \ddots & \ddots & 0 & \cdots & \vdots \\ 0 & \cdots & 0 & 1 & \cdots & 0 \end{bmatrix} \end{array}$$

6. On vérifie immédiatement que c'est bien une pseudo-matrice.

avec $\mathfrak{a}_1 \supseteq \mathfrak{a}_2 \supseteq \cdots \supseteq \mathfrak{a}_n$, $\prod_{i=1}^n \mathfrak{a}_i = \mathfrak{D}_n(M)$, *chaque* $\mathfrak{a}_i$ *de la forme* $\langle a_i, \delta\rangle$ *et* $\bigoplus_{k=1}^m \mathfrak{a}_k \simeq \mathbf{Z}^m$.

Démonstration. On reprend ce qui a été expliqué dans la démonstration de la proposition 18. En examinant ce qui se passe dans le calcul de la réduction de Smith modulaire par manipulations élémentaires, on obtient sur $\mathbf{Z}$ une égalité et une congruence

$$LMC = M' \equiv \left[\begin{array}{c|c} D & 0 \end{array}\right] \bmod \delta$$

avec $D = \mathrm{Diag}(\overline{a_1}, \ldots, \overline{a_n})$ et $\langle\overline{a_1}\rangle \supseteq \cdots \supseteq \langle\overline{a_n}\rangle$. Considérons la pseudo-matrice [7]

$$E := \begin{array}{c} \\ \mathfrak{a}_1 \\ \vdots \\ \mathfrak{a}_n \end{array} \begin{array}{c} \begin{array}{ccccc} \langle 1\rangle & \cdots & \cdots & \cdots & \langle 1\rangle \end{array} \\ \left[\begin{array}{ccccc} & & & & \\ & & M' & & \\ & & & & \end{array}\right] \end{array}.$$

Elle est de la forme

$$E = \begin{array}{c} \\ \mathfrak{a}_1 \\ \mathfrak{a}_2 \\ \vdots \\ \mathfrak{a}_n \end{array} \begin{array}{c} \begin{array}{cccccc} \langle 1\rangle & \langle 1\rangle & \cdots & \langle 1\rangle & \cdots & \langle 1\rangle \end{array} \\ \left[\begin{array}{cccccc} a_1 + \delta x_{11} & \delta x_{12} & \cdots & \delta x_{1n} & \cdots & \delta x_{1m} \\ \delta x_{21} & a_2 + \delta x_{22} & & & & \vdots \\ \vdots & & \ddots & & & \vdots \\ \delta x_{n1} & \cdots & & a_n + \delta x_{nn} & \cdots & \delta x_{nm} \end{array}\right] \end{array}.$$

Alors c'est une pseudo-matrice surjective. En effet,

$$\prod_{i=1}^n \mathfrak{a}_i = \mathfrak{D}_n(M) \text{ avec } \mathfrak{D}_n(M) = \mathfrak{D}_n(LMC) = \mathfrak{D}_n(M') = \mathfrak{D}_n(\underline{E}),$$

donc $\mathfrak{D}_n(E) = \langle 1\rangle$. D'après la proposition 11, on peut la compléter en une pseudo-matrice inversible $B = (\mathfrak{a}_1, \ldots, \mathfrak{a}_m; \langle 1\rangle, \ldots, \langle 1\rangle\,; \underline{B})$ telle que la pseudo-matrice $M'B^{-1}$ soit la matrice M_1 de l'énoncé. Avec $C_1 = CB^{-1}$, on obtient $LMC_1 = M_1$, où L et C_1 sont des pseudo-matrices de changements de base (L et M sont des matrices usuelles vues comme des pseudo-matrices ayant les idéaux $\langle 1\rangle$ en indices de lignes et en colonnes). □

Références

[ACMC] Lombardi H. & Quitté C. *Algèbre Commutative. Méthodes constructives.* Calvage&Mounet (2011).

7. On vérifie immédiatement que c'est bien une pseudo-matrice.

[CACM] English version of [ACMC]. Springer (2015).

[Cohen] Cohen H. *Advanced topics in computational number theory*. Graduate texts in mathematics 193. Springer-Verlag (1999).

[Modules] Díaz-Toca G.-M., Lombardi H. & Quitté C. *Modules sur les anneaux commutatifs*. Calvage&Mounet (2014).

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

Table des matières