Anaël Marit ENS Rennes

FORME NORMALE DE SMITH

- 122, 142, 149, 162 –

—

Quoi qu'on en dise, l'algorithme du pivot de Gauss est un outil d'algèbre fondamental, tant du point de vue de la pratique que pour l'immense variété de ses conséquences théoriques. Hélas, celui-ci repose fortement sur la possibilité de diviser par des scalaires, c'est-à-dire sur le fait qu'on travaille sur un corps. *Pourtant, de nombreux champs d'algèbre exploitent de façon cruciale les modules, qui sont l'équivalent des espaces vectoriels où l'on a substitué un anneau au corps de base, et dans ce contexte, le pivot de Gauss échoue à produire quelque résultat que ce soit...*

On va, dans ce développement, étudier un algorithme d'élimination des coefficients pour les systèmes linéaires à coefficients dans des anneaux principaux, et appliquer cet algorithme à l'élaboration d'une forme normale réduite pour les matrices à coefficients dans notre anneau. Cette forme, dite de Smith, est l'analogue dans les anneaux principaux du représentant canonique des orbites d'équivalence des matrices à coefficients dans un corps.

D'une façon surprenante peut-être (en tout cas qui moi me surprend) la forme réduite de Smith a des conséquences théoriques absolument dantesques, parmi lesquelles on peut citer le théorème de structure des modules de type fini sur un anneau principal, dont le théorème de structure des groupes abéliens de type fini et le théorème de Frobenius sont deux corollaires célèbres.

La présentation qu'on va en faire ici est très tournée algorithmique (on va même réaliser des preuves formelles de terminaison d'algorithmes !) et se place dans le cas principal, que je trouve plus intéressant que le cas euclidien, même si celui-ci est certainement plus intuitif.

Dans toute la suite, on fixe $\mathbb{A}$ un anneau principal. Etant donnée une matrice $M \in \mathbb{M}_{n,p}(\mathbb{A})$, $i \in [\![1,n]\!]$ et $j \in [\![1,p]\!]$, on notera $M(i,j)$ le coefficient de M situé en i-ème ligne et j-ième colonne [(i)]. Etant donné $S \subset \mathbb{A}$, on notera $\langle S \rangle$ l'idéal de $\mathbb{A}$ engendré par S. Notre objectif est de démontrer :

Théorème 1 (Smith). *Soit $M \in \mathbb{M}_{n,p}(\mathbb{A})$. Il existe un unique entier r et une suite $(a_1, \dots, a_r)$ d'éléments de $\mathbb{A}$, uniques modulo l'association, tels que $d_r | \dots | d_1$ et M soit équivalente à la matrice :*

$$\left(\begin{array}{ccc|c} d_1 & & & \\ & \ddots & & 0 \\ & & d_r & \\ \hline & 0 & & 0 \end{array}\right) \tag{1}$$

(i). Quitte à parler d'algorithmes, autant le faire dans la tradition des informaticien.ne.s !

Contactez-moi en cas de coquille à prénom.nom@ens-rennes.fr !

Préliminaires : matrices de Bézout et techniques d'élimination ([2], chapitre IV, théorème 1.1)

Cette première partie vise à introduire les outils et techniques de base qui seront ceux qu'on utilisera pour arriver à la forme de Smith.

Considérons a et b deux éléments de $\mathbb{A}$ avec $a \neq 0$. L'objectif est de trouver une matrice inversible B telle que :

$$B \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} g \\ 0 \end{pmatrix} \tag{2}$$

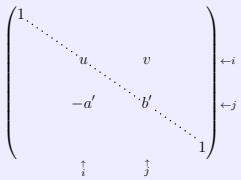
où g est un autre élément de a ayant de bonnes propriétés. On distingue trois cas :

1. *Le cas trivial* où $b = 0$. Dans ce cas, il n'y a rien à faire.
2. *Le cas simple* où $a|b$. Dans ce cas, on écrit $b = da$ et on résout le problème par transvection, en posant :
$$B = \begin{pmatrix} 1 & 0 \\ d & 1 \end{pmatrix} \tag{3}$$
Dans ce cas, $g = a$.
3. *Le cas décisif* où a ne divise pas b. Tout repose alors sur les propriétés des anneaux principaux. D'une part, a et b admettent un pgcd noté g. D'une autre, un anneau principal satisfait le théorème de Bézout : on dispose de u et v tels que $au + bv = g$. Enfin, si on note $a = a'g,\ b = b'g$, on peut écrire :
$$g = g(a'u + b'v) \tag{4}$$
et comme $\mathbb{A}$ est intègre, cela implique que $a'u + b'v = 1$. Enfin, on a :
$$0 = ab - ab = g(ab' - a'b) \tag{5}$$
et donc toujours par intégrité, $ab' - a'b = 0$. Finalement, posons :
$$B = \begin{pmatrix} u & v \\ -a' & b' \end{pmatrix} \tag{6}$$
Cette matrice est de déterminant 1, donc inversible, et on a bien l'égalité matricielle voulue. On a par ailleurs que g est un diviseur strict de a, ce qui en terme d'idéaux se traduit par $\langle a \rangle \subsetneq \langle g \rangle$.

Cette étude contient à elle seule (presque) tous les ingrédients nécessaires pour la mise en place de l'algorithme. Si vous l'avez comprise, vous avez (presque) tout compris au développement !

Formalisons un peu tout ça :

Définition 2 (Matrice de Bézout). *On appelle* matrice de Bézout *tout matrice carrée de* $\mathbb{M}_n(\mathbb{A})$ *de la forme :*



(où les pointillés figurent des 1) avec :

$$ub' + va' = 1 \tag{7}$$

Remarque : La multiplication à droite par une matrice de Bézout correspond à faire simultanément les opérations :

$$\begin{cases} L_i \leftarrow uL_i + vL_J \\ L_j \leftarrow -a'L_i + b'L_j \end{cases} \tag{8}$$

ce qui correspond à notre technique d'élimination dans le cas décisif.

Tout est maintenant en place pour mettre en place l'algorithme.

Existence de la forme de Smith ([2], chapitre IV, 2.2 et 2.3)

Soit $M \in \mathbb{M}_{n,p}(\mathbb{A})$. Si M est nulle, elle est déjà sous forme de Smith. On suppose donc que M admet un coefficient non nul. Quitte à permuter des lignes et / ou des colonnes (ce qui correspond à multiplier à gauche et / ou à droite par des matrices de permutation, inversibles), on peut supposer $M(1,1) \neq 0$. On va dans un premier temps ignorer la condition de divisibilité sur les termes diagonaux et montrer que M est équivalente à une matrice diagonale, dont on s'occupera ensuite d'ordonner les termes. Pour cela, on procède de façon récursive sur la taille de la matrice. On commence par proposer un algorithme, dont on prouvera la terminaison et la correction, qui prenant la matrice M en entrée, renvoie une matrice équivalente à M de la forme :

$$\left(\begin{array}{c|c} a_1 & 0 \\ \hline 0 & M' \end{array}\right) \tag{$\star$}$$

avec M' une matrice de $\mathbb{M}_{n-1,p-1}(\mathbb{A})$ à laquelle on pourra de nouveau appliquer l'algorithme. Donnons dans un premier temps la procédure, qu'on expliquera ensuite :

Algorithme :
Entrée : $M \in \mathbb{M}_{n,p}(\mathbb{A})$.
Sortie : une matrice équivalente à M sous forme $(\star)$.

1. Etape préliminaire :
   (a) Si M est nulle, retourner M

(b) Sinon, multiplier M par des matrices de permutation de sorte à ce que $M(1,1)$ soit non nul.

2. Pour i allant de 2 à n :
   (a) Si $M(i,1) = 0$, ne rien faire. *(Cas trivial)*
   (b) Si $M(1,1)|M(i,1)$, éliminer $M(i,1)$ par transvection. *(Cas simple)*
   (c) Sinon, éliminer $M(i,1)$ par transformation de Bézout. *(Cas décisif)*
3. Pour j allant de 2 à p :
   (a) Si $M(1,j) = 0$, ne rien faire. *(Cas trivial)*
   (b) Si $M(1,1)|M(1,j)$, éliminer $M(1,j)$ par transvection. *(Cas simple)*
   (c) Sinon, éliminer $M(1,j)$ par transformation de Bézout. Stopper l'exécution de l'étape 3 et recommencer l'étape 2. *(Cas décisif)*

   Retourner M.

Des explications s'imposent !

- A chaque tour de boucle de l'étape 2, un coefficient de la première colonne est éliminé. Chacune de ces étapes ne perturbe aucune autre colonne que la première et la colonne cible, aussi, en sortie du i-ème tour de boucle, les coefficients 2 à i de la première colonne sont nuls.
- Idem pour l'étape 3 qui élimine successivement les coefficients de la première ligne.
- Le cas 3c pose un problème majeur : il perturbe la première colonne, en y réintroduisant éventuellement des termes non nuls. De même, l'étape 2c perturbe la première ligne. La terminaison de l'algorithme n'est donc pas assurée.
- Le coefficient $M(1,1)$ ne change que lors des étapes décisives.

L'algorithme mieux compris, attelons-nous à montrer qu'il fonctionne. On notera pour plus de clareté $M^{(n)}$ la matrice obtenue à l'issue de la n-ième étape (avec $M^{(0)} = M$).

Correction de l'algorithme

La correction est assez facile à voir. Premièrement, $M^{(n)}$ est équivalente à M pour tout $n \in \mathbb{N}$ par récurrence immédiate. En effet chacun des cas correspond soit à multiplier (à gauche lors de l'étape 2, à droite lors de l'étape 3) par l'identité dans le cas trivial, par une matrice de transvection dans le cas simple ou par une matrice de Bézout dans le cas décisif, et ces matrices sont toutes inversibles.

De plus, on a la propriété suivante :

Lemme 3. *A l'issue du j-ième tour de boucle de l'étape 3, les coefficients de la première ligne situés en position 2 à j sont nuls. Si de plus ce j-ième tour de boucle ne s'est pas traduit par une étape décisive, tous les coefficients de la première ligne, à l'exception du premier, sont nuls.*

Démonstration. C'est une récurrence assez immédiate. Au commencement de l'étape 3, la première colonne est nulle, à l'exception du premier terme (cf remarques ci-dessus). A chaque tour de boucle, un nouveau coefficient est éliminé, et le reste de la première ligne n'est pas perturbé (à l'exception encore du premier coefficient). Comme seule l'étape décisive peut perturber la première colonne, on obtient le lemme. □

Comme il est évident que l'algorithme ne peut pas terminer par une étape décisive, l'algorithme est nécessairement correct. Reste à montrer qu'il s'arrête effectivement...

Terminaison de l'algorithme

Si vous aimez les anneaux, c'est là que ça devient intéressant ! Pour prouver la terminaison d'un algorithme, il nous faut exhiber un "variant de boucle", c'est-à-dire une quantité qui décroit à chaque tour de boucle. Le plus souvent, on choisit un entier pour variant, et comme $\mathbb{N}$ est bien ordonné, la suite ne peut être strictement décroissante, ce qui est le cœur de l'argument de terminaison. C'est ce qui se passe dans le cas euclidien : le variant de boucle est le stathme du coefficient $M^{(n)}(1,1)$, qui ne décroit strictement que lors des étapes décisives.

Ici, nous n'avons pas de stathme. Toutefois, nous n'avons pas réellement besoin que le variant de boucle soit à valeurs dans $\mathbb{N}$: il suffit qu'il soit à valeurs dans un poset artinien, c'est-à-dire un ensemble partiellement ordonné qui n'admet aucune suite strictement décroissante. De façon duale, on peut plutôt chercher pour variant une suite croissante à valeurs dans un poset noetherien... vous voyez on je veux en venir n'est-ce pas ? C'est là la beauté de l'argument dans le cas principal : nous avons à notre disposition un splendide poset noethérien en la qualité de l'ensemble des idéaux de $\mathbb{A}$ muni de l'inclusion, puisqu'un anneau principal est toujours noetherien. [(ii)]. Voici donc notre variant : on pose :

$$V_n := \langle M^{(n)}(1,1) \rangle \tag{9}$$

Lemme 4. *La suite (V_n) est une suite croissante d'idéaux de $\mathbb{A}$. De plus, on a :*

$$V_n \subsetneq V_{n+1} \iff \textit{la n-ième étape est un cas décisif} \tag{10}$$

Démonstration. Plaçons-nous au début de la $n+1$-ème étape. On a alors $\langle M^{(n)}(1,1) \rangle = V_n$. Si cette étape se solde par un cas trivial ou simple, le coefficient en haut à gauche n'est pas perturbé, c'est-à-dire que $M^n(1,1) = M^{n+1}(1,1)$ et donc $V_n = V_{n+1}$. S'il s'agit par contre d'un cas décisif, $M^{(n)}(1,1)$ est remplacé par le pgcd de lui-même et d'un élément non-nul de $\mathbb{A}$, qui est donc un diviseur non nul strict de $M^{(n)}(1,1)$. Cette divisibilité stricte se traduit exactement par $V_n \subsetneq V_{n+1}$. □

Ainsi, par noetherianité de $\mathbb{A}$, la suite (V_n) est stationnaire à partir d'un certain rang, c'est-à-dire que que l'algorithme n'effectue qu'un nombre fini d'étapes décisives. En d'autres termes, l'algorithme termine.

Travail de la forme diagonale

Une application récursive de l'algorithme fournit donc une matrice équivalente à M dont tous les coefficients hors de la diagonale sont nuls. Notons cette matrice $\bar{M}$ et r le plus grand indice tel que $\bar{M}(r,r) \neq 0$. Il résulte de l'algorithme que pour $i \leqslant r$, $\bar{M}(i,i) \neq 0$. On note ces termes $a_1, \ldots, a_r$. Il nous reste à montrer que l'on peut ordonner ces coefficients pour la divisibilité. Pour cela, il suffit de le constater avec une matrice de taille 2×2. Considérons :

$$A = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \tag{11}$$

(ii). Si tout ceci ne vous parle pas beaucoup, je vous invite à voir l'annexe.

avec a et b non nuls. On veut montrer que A est équivalente à une matrice de la forme :

$$\begin{pmatrix} c & 0 \\ 0 & g \end{pmatrix} \tag{12}$$

où g et c sont non nuls et $g|c$. On propose une suite d'opérations élémentaires :

$$\begin{pmatrix} a & 0 \\ b & b \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \tag{13}$$

Notons $g = a \wedge b$, u et v des coefficients de Bézout tels que $au + bv = g$ et a' et b' tels que $a'g = a$, $b'g = b$. On effectue une transformation de Bézout :

$$\begin{pmatrix} g & vb \\ 0 & a'b \end{pmatrix} = \begin{pmatrix} u & v \\ -b' & a' \end{pmatrix} \begin{pmatrix} a & 0 \\ b & b \end{pmatrix} \tag{14}$$

On a alors que $g|vb$ et $g|a'b$. Par transvection, on élimine le coefficient en haut à droite, puis une multiplication par ue matrice de permutation donne la forme voulue :

$$\begin{pmatrix} a'b & 0 \\ 0 & g \end{pmatrix} = \begin{pmatrix} g & vb \\ 0 & a'b \end{pmatrix} \begin{pmatrix} 1 & -vb' \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{15}$$

Ainsi, on peut utiliser cette technique pour imposer que le coefficient a_r divise tous les autres, puis on impose que le coefficient a_{r-1} divise tous ceux de rang supérieur. Malheureusement, à cette étape, le coefficient a_r pourrait ne plus diviser a_{r-1}, donc il faut recommencer avec a_r, puis avec a_{r-1}, etc. C'est encore un argument de noetherianité qui prouve que la procédure termine, et à la fin, on obtient une jolie forme de Smith de la matrice M !

Unicité des facteurs invariants ([1], proposition 6.78)

Remarquons tout d'abord que l'entier r est unique. En effet, comme $\mathbb{A}$ est intègre, on peut voir M comme une matrice à coefficients dans le corps des fractions de $\mathbb{A}$, équivalente à sa forme de Smith. Or il est alors clair que r est le rang de M, qui est invariant par équivalence matricielle.

Pour montrer l'unicité modulo l'association des facteurs invariants, on va exploiter les *idéaux déterminantiels* :

Définition 5 (Idéaux déterminantiels). *Lorsque M est une matrice de $\mathbb{M}_{n,p}(\mathbb{A})$, on appelle k-ième idéal déterminantiel de M, noté $\Delta_k(M)$ l'idéal de $\mathbb{A}$ engendré par les mineurs de taille k de M.*

Proposition 6. *Si M et N sont deux matrices équivalentes de $\mathbb{M}_{n,p}(\mathbb{A})$, alors on a :*

$$\forall k \in [\![1 \min\{n,p\}]\!],\ \Delta_k(M) = \Delta_k(N) \tag{16}$$

Démonstration. Considérons tout d'abord le cas où il existe $P \in GL_n(\mathbb{A})$ tel que $M = PN$. Alors les colonnes de M, vues comme éléments de $\mathbb{A}^n$, sont combinaisons linéaires à coefficients dans $\mathbb{A}$ des colonnes de N, et par suite, les colonnes de toute matrice extraite de M sont combinaisons linéaires des colonnes de la matrice extraite de N selon les mêmes indices. Or le déterminant

est multilinéaire. On en déduit que tout mineur de taille k de M est combinaison linéaire des mineurs de taille k de N, et donc $\Delta_k(M) \subset \Delta_k(N)$. Or l'inversibilité de P fait que la situation est symétrique en M et N : $N = P^{-1}M$, donc on a l'égalité des idéaux déterminentiels.

Le même raisonnement s'applique dans le cas où $M = NP$ en raisonnant sur les lignes plutôt que sur les colonnes, d'où la proposition. □

Dans notre cas, la condition de divisibilité sur les facteurs invariants trivialise l'expression des idéaux déterminentiels : si $a_r|\dots|a_1$ sont les termes diagonaux d'une forme de Smith de M, alors pour $k \leqslant \min\{n,p\}$, on a :

$$\Delta_k(M) = \langle \prod_{i=0}^{\min\{k,r-1\}} a_{r-i} \rangle \tag{17}$$

Ainsi, si M est équivalente à une autre matrice sous forme de Smith, dont on note $b_r|\dots|b_1$ les coefficients diagonaux, on a :

$$\forall k \in [\![0, r-1]\!],\ \langle \prod_{i=1}^{k} a_{r-i} \rangle = \langle \prod_{i=1}^{k} b_{r-i} \rangle \tag{18}$$

En particulier, pour $k = r-1$, $\langle a_r \rangle = \langle b_r \rangle$, c'est-à-dire que a_r et b_r sont associés. De même pour $a_r a_{r-1}$ et $b_r b_{r-1}$, puis de proche en proche, on en déduit que les (a_i) est les (b_i) sont associés, d'où l'unicité modulo l'association des facteurs invariants.

Annexe - anneaux noetheriens, domaines de Bézout, anneaux principaux...

J'ai trouvé intéressant dans cette annexe de discuter un peu des hypothèses qui sont mises sur l'anneau de base $\mathbb{A}$ vis-à-vis du théorème de réduction de Smith, d'une part pour observer qu'on a atteint les hypothèses optimales pour que notre algorithme fonctionne, d'une autre pour tisser des liens entre différents types d'anneaux qu'on peut être ammené à manipuler.

Notre algorithme repose sur deux résultats fondamentaux qui dépendent de la nature intrinsèque de l'anneau : la noetherianité et le théorème de Bézout. On va voir qu'un anneau dans lequel on dispose de ces outils est nécessairement principal.

Théorème 7 (Bézout). *Soit $\mathbb{A}$ un anneau intègre. Les assertions suivantes sont équivalentes :*

1. *Pour tout couple $(a,b) \in \mathbb{A}^2$, il existe $g \in \mathbb{A}$ un pgcd de a et b et un couple $(u,v) \in \mathbb{A}^2$ tel que :*
$$au + bv = g \tag{19}$$
2. *Tout idéal de type fini de $\mathbb{A}$ est principal.*

Si ces conditions sont remplies, on dit que $\mathbb{A}$ est un domaine de Bézout.

Démonstration.

Dans le sens direct , considérons $I = \langle a_1, \dots, a_n \rangle$ un idéal de type fini de $\mathbb{A}$. Le théorème de Bézout donne, par récurrence immédiate, l'existence de g un pgcd de la famille $(a_1, \dots, a_n)$

et de coefficients de Bézout $u_1, \dots, u_n \in \mathbb{A}^n$ tels que :

$$\sum_{i=1}^{n} u_i a_i = g \tag{20}$$

Donc $I \subset \langle g \rangle$. L'inclusion réciproque est immédiate car g divise chacun des a_i. Donc I est un idéal principal.

Dans le sens réciproque , on se donne a et b des éléments de $\mathbb{A}$. Par hypothèse, il existe $g \in \mathbb{A}$ tel que :

$$\langle a, b \rangle = \langle g \rangle \tag{21}$$

Ceci implique que g est un pgcd de a et de b pour lequel on dispose de coefficients de Bézout.

□

Ainsi, il est clair que notre algorithme ne peut pas fonctionner hors d'un domaine de Bézout. Voyons ce qui se passe si on ajoute la noetherianité :

Proposition 8. *Soit $\mathbb{A}$ un anneau intègre. Les assertions suivantes sont équivalentes :*

1. *$\mathbb{A}$ est principal.*
2. *$\mathbb{A}$ est un domaine de Bézout noetherien.*

Démonstration.

Dans le sens direct , il est évident que si $\mathbb{A}$ est principal, c'est un domaine de Bézout. Considérons une suite croissante (I_n) d'idéaux de $\mathbb{A}$. Pour $n \in \mathbb{N}$, on se donne a_n un générateur de I_n et on pose :

$$\langle I \rangle := \langle a_n \mid n \in \mathbb{N} \rangle \tag{22}$$

Alors il est clair que chacun des (I_n) est contenu dans I. Si de plus g est un générateur de I, il existe une famille finie d'indices $i_1, \dots i_k$ et des coefficients $(u_1, \dots, u_k) \in \mathbb{A}^k$ tels que :

$$g = \sum_{j=1}^{k} u_j a_{i_j} \tag{23}$$

Donc :

$$I \subset \sum_{j=1}^{k} I_{i_k} = I_{\max_{1 \leqslant j \leqslant k} i_j} \tag{24}$$

Ce qui implique que la chaîne (I_n) est ultimement stationnaire.

Dans le sens indirect , on considère I un idéal quelconque de $\mathbb{A}$ et $\mathscr{I}$ l'ensemble des idéaux de type fini de $\mathbb{A}$ contenus dans I qu'on munit de l'inclusion. Alors, par noetherianité de $\mathbb{A}$, et comme $\mathscr{I}$ contient l'idéal nul, $(\mathscr{I}, \subset)$ est un ensemble inductif non vide. Par le lemme de Zorn, il contient un élément maximal M. Il est évident que $M = I$, car sinon, on pourrait prendre un élément $a \in I \setminus M$ et considérer l'idéal de type fini contenu dans I $M + \langle a \rangle$, ce qui contredirait la maximalité de M. Donc I est de type fini, et comme $\mathbb{A}$ est un domaine de Bézout, I est principal.

□

Références

[1] Vincent Beck, Jerôme Malick et Gabriel Peyré. *Objectif agrégation*. H&K, 2005. isbn : 2914010923.

[2] Gema-Maria Diaz-Toca, Henri Lombardi et Claude Quitté. *Modules sur les anneaux commutatifs*. Calvage et Mounet, 2014.