Développement: Forme normale de Smith

Arthur Maritch-Roy

On montre dans ce développement le théorème de Smith, habituellement rencontré dans des anneaux euclidiens, mais qui peut être généralisé sans grand changement de la philosophie dans un cadre principal. Ce théorème est fondamental en théorie des modules, et permet donc de retrouver des résultats sur les groupes abéliens finis et les endomorphismes d'un espace de dimension finie.

Théorème 1. (forme normale de Smith) Soit $M \in \mathcal{M}_{n,p}(A)$ où A est un anneau principal. Il existe $(P, Q) \in \mathrm{GL}_n(A) \times \mathrm{GL}_p(A)$ telles que

$$PMQ = \begin{pmatrix} d_1 & & & & & \\ & \ddots & & & & \\ & & d_r & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix}.$$

Avec $d_1 | \dots | d_r$. De plus, les (d_i) sont uniques à association près. Cette forme diagonale est appelée *forme (normale) de Smith* de la matrice M, et les (d_i) sont appelés *facteurs invariants*.

Démonstration. On va procéder à une preuve algorithmique. On suppose que l'on a une boîte noire qui permet de calculer les relations de Bezout. L'idée est de procéder récursivement. On cherche à obtenir, avec des opérations élémentaires sur les lignes et des colonnes (*i.e.* des multiplications par des matrices inversibles simples à gauche et à droite) une matrice de la forme

$$M' = \begin{pmatrix} d_1 & 0 \\ 0 & N \end{pmatrix},$$

avec $N \in \mathcal{M}_{n-1,p-1}$ dont les coefficients sont tous divisibles par d_1 puis de recommencer cette étape sur la matrice N.

Lançons-nous donc dans l'algorithme qui va nous permettre d'arriver à la forme ci-dessus. On note $M = (a_{i,j})$. Notre but est de remplacer successivement le coefficient $a_{1,1}$ par un diviseur strict, de telle sorte à ensuite pouvoir annuler les coefficients sur les lignes et les colonnes avec de simples transvections, comme on le ferait sur un corps. Pour faire cela, on utilise ce qu'on a dans un anneau principal : la relation de Bezout. À chaque étape, on parcourt les cinq choix suivants et on effectue le premier qu'il est possible de faire.

— S'il existe $j > 1$ tel que $a_{1,1}$ ne divise pas $a_{1,j}$, on calcule la relation de Bezout $ua_{1,1} + va_{1,j} = \delta$ avec δ un pgcd de $a_{1,1}$ et $a_{1,j}$. On cherche alors une matrice élémentaire qui va nous permettre de remplacer $a_{1,1}$ par δ. On multiplie alors à droite par la matrice

$$\widetilde{Q} = \begin{pmatrix} u & \dots & -\frac{a_{1,j}}{\delta} & \dots \\ \vdots & I_{j-2} & \vdots & \\ v & \dots & \frac{a_{1,1}}{\delta} & \dots \\ \vdots & & \vdots & I_{p-j} \end{pmatrix},$$

où les coefficients écrits sont sur les lignes et colonnes d'indices 1 et j, et avec des 1 sur le reste de la diagonale. Cette matrices est bien inversible puisque son déterminant peut être calculé avec la formule de base et vaut

$$\det(\widetilde{Q}) = \frac{1}{\delta}(ua_{1,1} + va_{1,j}) = 1 \in A^\times.$$

La multiplication à droite par cette matrice correspond aux opérations élémentaires suivantes :

$$C_1 \leftarrow uC_1 + vC_j$$
$$C_j \leftarrow -\frac{a_{1,j}}{\delta}C_1 + \frac{a_{1,1}}{\delta}C_j.$$

On a donc bien remplacé $a_{1,1}$ par un diviseur strict. Remarquons que le coefficient sur la colonne j a été remplacé par 0.

— S'il existe $i > 1$ tel que $a_{1,1}$ ne divise pas $a_{i,1}$, on multiplie à gauche par

$$\widetilde{P} = \begin{pmatrix} u & \dots & v & \dots \\ \vdots & I_{i-2} & \vdots & \\ -\frac{a_{i,1}}{\delta} & \dots & -\frac{a_{1,1}}{\delta} & \dots \\ \vdots & & \vdots & I_{n-i} \end{pmatrix},$$

et on remplace de manière similaire $a_{1,1}$ par un diviseur strict et $a_{i,1}$ par zéro.

— S'il existe un coefficient $a_{1,j}$ non nul tel que $a_{1,1}$ divise $a_{1,j}$ on peut l'annuler avec la transvection

$$C_j \leftarrow C_j - \frac{a_{1,j}}{a_{1,1}}C_1.$$

— De même sur les lignes, s'il existe un coefficient $a_{i,1}$ non nul tel que $a_{1,1}$ divise $a_{i,1}$, on l'annule aussi avec une transvection :

$$L_i \leftarrow L_i - \frac{a_{i,1}}{a_{1,1}}L_1.$$

— Enfin s'il existe (i, j) avec $i > 1, j > 1$ tel que $a_{1,1}$ ne divise pas $a_{i,j}$, on fait apparaître $a_{i,j}$ en position $(i, 1)$ par la transvection

$$C_1 \leftarrow C_1 + C_j.$$

Montrons maintenant la terminaison de notre algorithme. Commençons par remarquer que l'on est sûrs d'arriver au cinquième point de la liste précédente, puisque les quatre étapes précédentes remplacent $a_{1,1}$ par un diviseur strict (et il n'en a qu'un nombre fini car on est dans un anneau principal donc factoriel ou ajoutent un zéro en ligne ou colonne 1). Mais lorsque l'on est au cinquième point, on remplace au moins un zéro de C_1 qui n'est pas divisible par $a_{1,1}$, donc $a_{1,1}$ va encore décroître strictement. Somme toute, la suite des valeurs successives de $a_{1,1}$ ne pouvant pas décroître strictement une infinité de fois, elle stationne. Lorsqu'elle stationne, on a bien que des zéros ailleurs sur la ligne et la colonne 1. On peut donc itérer de procédé comme indiqué précédemment et on obtient bien notre forme de Smith.

Réglons maintenant le problème d'unicité de la forme normale de Smith. On note $\mathcal{I}_k(B)$ l'idéal engendré par les mineurs de taille k de la matrice B. Si U est une matrice de taille convenable, alors $\mathcal{I}_k(UB) \subset \mathcal{I}_k(B)$ d'après la formule de Cauchy-Binet, et de même pour la multiplication à droite. Ainsi, si M et $M' = UMV$ sont deux matrices équivalentes, $\mathcal{I}_k(M') \subset \mathcal{I}_k(M)$. Par symétrie on a égalité. Ainsi, si on a deux jeux de facteurs invariants $d_1|\dots|d_r$ et $d'_1|\dots|d'_s$, alors

d'abord $r = s$ car si $s > r$ on aurait $\langle 0 \rangle = \langle d'_1 \cdots d'_{r+1} \rangle$ donc un des d'_j serait nul par intégrité ce qui est exclu. Ensuite, on a donc

$$\begin{aligned} \langle d_1 \rangle &= \langle d'_1 \rangle \\ \langle d_1 d_2 \rangle &= \langle d'_1 d'_2 \rangle \\ &\cdots \\ \langle d_1 \cdots d_r \rangle &= \langle d'_1 \cdots d'_r \rangle. \end{aligned}$$

De proche en proche, on obtient bien l'association des facteurs invariants. □

Proposition 2. (formule de Cauchy-Binet)
Soit R un anneau principal et $A \in \mathcal{M}_{m,n}(R)$ et $B \in \mathcal{M}_{n,q}(R)$. On note $C = AB \in \mathcal{M}_{m,q}(R)$. Alors pour tous $\{i_1, \ldots, i_p\} \subset [\![1, m]\!]$ et $\{j_1, \ldots, j_p\} \subset [\![1, q]\!]$:

$$|C|_{\substack{i_1,\ldots,i_p \\ j_1,\ldots,j_p}} = \sum_{1 \leq k_1 < \ldots < k_p \leq n} |A|_{\substack{i_1,\ldots,i_p \\ k_1,\ldots,k_p}} |B|_{\substack{k_1,\ldots,k_p \\ j_1,\ldots,j_p}}.$$

Démonstration. On remarque que

$$(C)_{\substack{i_1,\ldots,i_p \\ j_1,\ldots,j_p}} = (A)_{\substack{i_1,\ldots,i_p \\ 1,\ldots,n}} (B)_{\substack{1,\ldots,n \\ j_1,\ldots,j_p}}.$$

On se ramène donc à un déterminant carré d'un produit de deux matrices rectangulaires. On change alors les notations, soient

$$\begin{aligned} A &= (a_{i,j}) \in \mathcal{M}_{p,n}(R) \\ B &= (b_{i,j}) \in \mathcal{M}_{n,p}(R) \\ C &= AB \in \mathcal{M}_p(R). \end{aligned}$$

On cherche à calculer $\det(C)$. On note $A = (A_1 | \ldots | A_n)$ les colonnes de A.

$$\begin{aligned} \det(C) &= \det\left(\sum_{k_1=1}^{n} b_{k_1,1} A_{k_1}, \ldots, \sum_{k_p=1}^{n} b_{k_p,p} A_{k_p} \right) \\ &= \sum_{k_1,\ldots,k_p=1}^{n} b_{k_1,1} \cdots b_{k_p,p} |A|_{\substack{1,\ldots,p \\ k_1,\ldots,k_p}} \\ &= \sum_{1 \leq k_1 < \ldots < k_p \leq n} \sum_{\{l_1,\ldots,l_p\} = \{k_1,\ldots,k_p\}} b_{l_1,1} \cdots b_{l_p,p} |A|_{\substack{1,\ldots,p \\ l_1,\ldots,l_p}} \\ &= \sum_{1 \leq k_1 < \ldots < k_p \leq n} \sum_{\sigma \in \mathfrak{S}_{\{k_1,\ldots,k_p\}}} b_{\sigma(k_1),1} \cdots b_{\sigma(k_p),p} |A|_{\substack{1,\ldots,p \\ \sigma(k_1),\ldots\sigma(k_p)}} \\ &= \sum_{1 \leq k_1 < \ldots < k_p \leq n} \sum_{\sigma \in \mathfrak{S}_{\{k_1,\ldots,k_p\}}} b_{\sigma(k_1),1} \cdots b_{\sigma(k_p),p} \varepsilon(\sigma) |A|_{\substack{1,\ldots,p \\ k_1,\ldots,k_p}} \\ &= \sum_{1 \leq k_1 < \ldots < k_p \leq n} |A|_{\substack{1,\ldots,p \\ k_1,\ldots,k_p}} \sum_{\sigma \in \mathfrak{S}_{\{k_1,\ldots,k_p\}}} \varepsilon(\sigma) b_{\sigma(k_1),1} \cdots b_{\sigma(k_p),p} \\ &= \sum_{1 \leq k_1 < \ldots < k_p \leq n} |A|_{\substack{1,\ldots,p \\ k_1,\ldots,k_p}} |B|_{\substack{k_1,\ldots,k_p \\ 1,\ldots,p}}. \end{aligned}$$

On utilise d'abord la multilinéarité du déterminant, avant de regrouper les indices selon les valeurs prises, puis à réindexer selon les permutations et à utiliser le caractère alterné du déterminant. □

Remarque 1. (Quelques mots sur la complexité de l'algorithme)
On note considère linéaire en k le coût d'une opération élémentaire sur une ligne ou une colonne de taille k (disons inférieur à αk). On note b le coût d'une opération de Bezout (ou d'un test de divisibilité). Dans le pire des cas, pour passer la première étape de la récurrence, on fait $(n-1)+(p-1)$ opérations élémentaires et relations de Bezout puis lorsque l'on arrive au cinquième point de l'algorithme $a_{1,1}$ ne divise aucune des éléments de la sous-matrice en bas à droite, et on est alors obligés de faire revenir une à une les colonnes de cette sous-matrice en C_1, ce qui rajoute au plus $(n-1)(p-1)$ calculs de relations de Bezout et opérations élémentaires. Ainsi, on a la borne suivante (si $C(n,p)$ est le nombre d'opérations pour une matrice de taille $n \times p$) :

$$C(n,p) \leq (\alpha \max(n,p)+b)(n+p-2+(n-1)(p-1))+C(n-1,p-1) \leq A(\alpha N+b)N^2+C(n-1,p-1)$$

On a somme toute une complexité en $\mathrm{O}((\alpha N+b)N^3)$.

Remarque 2. Dans un anneau euclidien, la relation de Bezout s'obtient par l'algorithme d'Euclide. D'ailleurs, on peut effectuer directement l'algorithme d'Euclide dans la matrice pour économiser de la mémoire dans l'ordinateur.

Application 1. (Réduction de Frobenius d'un endomorphisme)
Soit $u \in \mathcal{L}(E)$, où E est un K-espace vectoriel de dimension n. En appliquant l'algorithme des facteurs invariants à la matrice $XI_n - M$, où M est la matrice de u dans une base quelconque, on obtient des polynômes $P_1 | \cdots | P_r$ tels que $XI_n - M$ soit équivalente dans $K[X]$ à

$$\begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & P_1(X) & & & \\ & & & & \ddots & & \\ & & & & & P_r(X) \end{pmatrix}.$$

En effet, il ne peut pas y avoir de zéros puisque le déterminant de notre matrice est $\chi_M \neq 0$.

On considère alors une "action" de $K[X]$ par $P \cdot x := P(u)(x)$. Elle est compatible avec la structure d'anneau de $K[X]$. On peut alors définir un morphisme compatible avec cette action de $K[X]^n$ dans E par $(Q_1, \ldots, Q_n) \mapsto \sum_{i=1}^n Q_i \cdot e_i$ où $(e_1, \ldots, e_n)$ est une base de E. Ce morphisme est clairement surjectif. De plus, l'image de $XI_n - M$ est incluse dans son noyau. On peut alors passer au quotient, comme on le ferait sur un espace vectoriel, en préservant la structure définie par $\cdot$. On note $W := \mathrm{Im}(XI_n - M)$, et on pose $\overline{\varphi} : K[X]^n/W \to E$ qui est surjectif. C'est aussi une application K-linéaire. Par récurrence sur le degré de polynômes (U_i) fixés, on montre qu'il existe des vecteurs (x_i) de E tels que $(U_1, \ldots, U_n) = (x_1, \ldots, x_n) \bmod W$, ce qui donne l'injectivité de $\overline{\varphi}$ par égalité des dimensions. On a donc un isomorphisme entre E et $K[X]^n/W$. Remarquons alors que si deux matrices A et A' sont équivalentes sur un anneau R, alors $R^n/\mathrm{Im}(A) \simeq R^n/\mathrm{Im}(A')$. Ainsi avec notre forme normale de Smith on obtient un isomorphisme

$$\psi : E \to K[X]/(P_1) \times \cdots \times K[X]/(P_r).$$

Soit alors $x_i = \psi^{-1}((0, \ldots, \overline{1}, \ldots, 0))$ où le 1 est en position i. Si on note $\deg(P_i) =: d_i$, alors

$$\mathcal{B} := (x_1, u(x_1), \ldots, u^{d_1-1}(x_1), x_2, \ldots, x_r, u(x_r), \ldots, u^{d_r-1}(x_r))$$

est une K-base de E, et la matrice de U dans cette base est diagonale par blocs, les blocs étant les matrices compagnon des polynômes $P_1, \ldots, P_r$. On retrouve donc le théorème de réduction de Frobenius, avec en plus une méthode algorithmique pour calculer les facteurs invariants.

Application 2. (Systèmes linéaires dans $\mathbb{Z}$)
La forme normale de Smith permet de résoudre des systèmes linéaires à coefficients dans $\mathbb{Z}$. En effet, si on veut résoudre $Ax = b$ dans $\mathbb{Z}^n$, on peut écrire $A = PDQ$ sa forme de Smith et alors on réécrit le problème en $D(Qx) = P^{-1}b$ et cela devient alors plus simple. Remarquons que l'on pourrait seulement échelonner selon les colonnes, on parle alors de forme normale de Hermite.

Référence : La preuve de la forme normale de Smith provient de la page Wikipédia *Théorème des facteurs invariants* et d'un cours de Christian Blanchet accessible ici. Le lien avec la réduction de Frobenius provient du cours de Vincent Guirardel.