Forme normale de Smith

Chen Thomas
t.chen.thomas1[at]gmail.com

16 mai 2024

Attention

1. Ce document contient certainement des coquilles. N'hésitez pas à me le signaler. De même si vous avez une question.
2. Pour les recasages, ce sont les miens mais ce développement se case peut-être ailleurs et je n'y ai pas réfléchi.
3. Il se peut que ce développement dure plus de 15 minutes. J'ai essayé de le découper pour faire des recollements personnalisés.

Leçons

- 122 : Anneaux principaux. Exemples et applications.
- 142 : pgcd et ppcm, algorithmes de calcul. Applications.

Références

[1] V. Beck, J. Malick, G. Peyré. *Objectif Agreg.* H& K, 2005.

Tout est dans [1].

Théorème 1. *Soit A un anneau euclidien muni d'un stathme φ. Soit $U \in \mathcal{M}_{p,q}(A)$. Il existe $s \in \mathbb{N}^*, (d_1, \cdots, d_s) \in (A\backslash\{0\})^s$ tels que*

1. $d_s | \cdots | d_1$
2. *U est équivalente à* $\begin{pmatrix} d_s & & & \\ & \ddots & & 0_{s,q-s} \\ & & d_1 & \\ & 0_{p-s,s} & & 0_{p-s,q-s} \end{pmatrix}$.

Il y a unicité au sens où la famille $(d_1, \cdots, d_s)$ est unique à inversible près.

Preuve de l'existence

On donne l'algorithme suivant. Par convention, chaque action sur U renomme la nouvelle matrice U elle-même.

Algorithme de construction

1. Si $U = 0$, c'est fini.
2. Sinon, il existe (i_0, j_0) tel que $\phi(u_{i_0,j_0})$ soit de stathme minimal. On réalise alors $C_1 \leftrightarrow C_{j_0}, L_1 \leftrightarrow L_{i_0}$.
3. *Traitement de la colonne* 1. Soit $i = 2$.

(a) Travail sur i : on réalise la division euclidienne de $u_{i,1}$ par $u_{1,1}$

$$u_{i,1} = q_i u_{1,1} + r_i \text{ avec } \left| \begin{array}{l} \phi(r_i) < \phi(u_{1,1}) \\ \text{ou } r_i = 0 \end{array} \right. .$$

On réalise $L_i \leftarrow L_i - q_i L_1$.

(b) Si $r_i \neq 0$, $L_i \leftrightarrow L_1$ et retourner en 3a.

(c) Si $r_i = 0$ et $i < p$, $i+ = 1$ et retourner en 3a.

(d) Si $r_i = 0$ et $i = p$, aller en 4.

4. *Traitement de la ligne* 1. Soit $j = 2$.

(a) Travail sur j : on réalise la division euclidienne de $u_{1,j}$ par $u_{1,1}$

$$u_{1,j} = q_j u_{1,1} + r_j \text{ avec } \left| \begin{array}{l} \phi(r_j) < \phi(u_{1,1}) \\ \text{ou } r_j = 0 \end{array} \right. .$$

On réalise $C_j \leftarrow C_j - q_j C_1$.

(b) Si $r_j \neq 0$, réaliser $C_1 \leftrightarrow C_j$ et retourner à 3.

(c) Si $r_j = 0$ et $j < q$, réaliser $j+ = 1$ et retourner en 4a.

(d) Si $r_j = 0$ et $j = q$, aller à 5.

5. On obtient une matrice dont la première ligne/colonne est nulle sauf en $(1,1)$ et on travaille la matrice sous-jacente.

(a) Si $u_{1,1}$ ne divise pas un certain u_{i_1,j_1}, $C_1 \leftarrow C_1 + C_{j_1}$ et retourner en 3.

(b) Sinon, retourner en 1 avec la matrice U ôtée de L_1 et C_1.

Preuve de terminaison

- Il suffit de montrer la terminaison de chaque boucle conditionnelle, les conditions 3c et 4c étant triviales. Remarquons que si $u_{1,1} = 1$, on peut passer en $5b$ sans problème de terminaison.
- Dans les autres boucles – $\boxed{3a \to 3b}$, $\boxed{4a \to 4b \to 3}$ et $\boxed{5a \to 3 \to 4}$ –, le variant de boucle est $\varphi(u_{1,1})$.
  * Dans la boucle $\boxed{3a \to 3b}$, si $r_i \neq 0$, alors $u_{1,1} \leftarrow r_i$ et $\varphi(r_i) < \varphi_{u_{1,1}}$ donc le variant de boucle induit une suite strictement décroissante d'entiers.
  * Dans la boucle $\boxed{4a \to 4b \to 3}$, si $r_j \neq 0$ à 4b, alors $u_{1,1} \leftarrow r_j$ et $\phi(r_j) < \phi(u_{1,1})$. En réalisant 3 qui se termine, on a $\phi(u_{1,1}) \leq \phi(r_j)$ donc en revenant à 4b, on a bien $\varphi_{u_{1,1}}$ diminué d'au moins 1 : le variant de boucle induit une suite strictement décroissante d'entiers.
  * Dans la boucle $\boxed{5a \to 3 \to 4}$, après avoir réalisé 5a, au début de 3, on a, en colonne 1, un coefficient non divisible par $u_{1,1}$ ($[C_{j_1}]_1 = 0$) donc 3a donnera un nouveau $u_{1,1}$ de stathme strictement inférieur au précédent puisque
  $$u_{1,1} = q_{i_1} u_{i_1,j_1} + r_{i_1}$$
  avec $\phi(r_{i_1}) < \phi(u_{1,1}), u_{1,1} \leftarrow r_{i_1}$.
- Ainsi, toutes les boucles conditionnelles se terminent.

□

Preuve de correction Ce qui précède montre qu'en début de 5b, il existe $P \in \mathrm{GL}_p(A), Q \in \mathrm{GL}_q(A)$ tel que

$$U = PDQ \text{ avec } D = \begin{pmatrix} d_s & 0_{1,q-1} \\ 0_{p-1,1} & U_1 \end{pmatrix}$$

avec $d_s | [U_1]_{i,j}$ pour tout i, j.

Si U_1 induit $P_1 \in \mathrm{GL}_p(A), Q_1 \in \mathrm{GL}_q(A)$ tel que $U_1 = P_1 D_1 Q_1$ avec D_1 comme l'énoncé, alors en posant

$$\widetilde{P} = \begin{pmatrix} 1 & 0_{1,q-1} \\ 0_{p-1,1} & P_1 \end{pmatrix} , \ \widetilde{Q} = \begin{pmatrix} 1 & 0_{1,q-1} \\ 0_{p-1,1} & Q_1 \end{pmatrix},$$

on a

$$\widetilde{P}\begin{pmatrix} d_s & 0_{1,q-1} \\ 0_{p-1,1} & D_1 \end{pmatrix}\widetilde{Q} = D.$$

Ainsi, $U = (P\widetilde{P})\Delta(Q\widetilde{Q})$ avec Δ comme dans l'énoncé. Par principe de récurrence, le cas $n = 1$ étant immédiat, on a le résultat. □

Preuve de l'unicité

On note $D_j = \prod_{k=0}^{j-1} d_{s-k}$, $D_j = 0$ si $j > s$. On note

$$\Lambda_j(U) = \text{pgcd des mineurs de taille } j \text{ avec } \Lambda_0(U) = 1.$$

Théorème 2. *Soit $j \in [\![1, \min(p,q)]\!]$. Alors*

1. $\langle D_j \rangle = \langle \Lambda_j(U) \rangle$
2. $s = \max\{j : \Lambda_j(U) \neq 0\}$
3. $\forall j \leq s-1, \langle d_{s-j} \rangle = \langle \Lambda_{j+1}(U)/\Lambda_j(U) \rangle$.

Démonstration. 2 et 3 découle de 1. Pour obtenir 1, puisque $D_j = \Lambda_j(D)$, il suffit de savoir que $\Lambda_j(U) = \Lambda_j(U')$ lorsque U et U' sont équivalentes.

- Si $U = PU'$ avec P inversible, alors les colonnes de U sont des combinaisons linéaires entières en les colonnes de U'. Par multilinéarité du déterminant, les mineurs de U sont des combinaisons linéaires entières des mineurs de U' donc en prenant leurs pgcd, on a

$$\langle \Lambda_j(U) \rangle \subset \langle \Lambda_j(U') \rangle.$$

  Puisque $U' = P^{-1}U$, par le même raisonnement, on a l'autre inclusion d'où l'égalité.
- Si $U = U'Q$ avec Q inversible, alors $U^T = Q^T(U')^T$. Ainsi,

$$\langle \Lambda_j(U^T) \rangle = \langle \Lambda_j((U')^T) \rangle.$$

  Or, {mineurs de A} = {mineurs de A^T} donc $\langle \Lambda_j(U) \rangle = \langle \Lambda_j(U') \rangle$.

Ainsi, si $U = PU'Q$,

$$\langle \Lambda_j(U) \rangle = \langle \Lambda_j(P[U'Q]) \rangle = \langle \Lambda_j(U'Q) \rangle \langle \Lambda_j(U') \rangle.$$

□

Ainsi, on a les inclusions d'idéaux suivantes : $\langle d_1 \rangle \subset \langle d_2 \rangle \subset \cdots \subset \langle d_s \rangle$ d'où l'unicité à inverse près. □