Forme normale de Smith

Geoffrey Deperle

Leçons associées :
— 122 : Anneaux principaux. Exemples et applications.
— 142 : PGCD et PPCM, algorithmes de calcul. Applications.
— 162 : Systèmes d'équations linéaires, opérations élémentaires, aspects algorithmiques et conséquences théoriques.

Le but de ce développement est de montrer le théorème suivant :

Théorème. *Soit A un anneau euclidien, δ un stathme euclidien de A et $m, n \in \mathbb{N}^*$ et $M \in \mathcal{M}_{m,n}(A)$.*

$$\exists (P,Q) \in \mathrm{GL}_m(A) \times \mathrm{GL}_n(A) / PMQ = \begin{pmatrix} f_1 & & & & (0) \\ & \ddots & & & \\ & & f_r & & \\ & & & 0 & \\ & & & & \ddots \\ (0) & & & & 0 \end{pmatrix}$$

avec $f_1, \dots, f_r \in A$ tels que $f_1 | \dots | f_r$ avec unicité modulo les inversibles de A.

Preuve :

Étape 1 : Montrons qu'il existe $f_1 \in A$ et P, Q tel que $PMQ = \begin{pmatrix} f_1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & V & \\ 0 & & & \end{pmatrix}$ tel que pour tout $(i,j) \in [\![1, m-1]\!] \times [\![1, n-1]\!], f_1 | V_{ij}$

Si $M = 0$, alors $f_1 = 0$ convient.
Sinon, considérons X la classe des matrices équivalentes à M et considérons

$$f_1 = \{\mathrm{pgcd}(M_{ij}), (i,j) \in [\![1,m]\!] \times [\![1,n]\!], M \in X\}$$

On a alors $\delta(f_1) < \delta(u_{ij})$ pour tout $(i,j) \in [\![1,m]\!] \times [\![1,n]\!], M \in X$. Considérons la matrice M tel que f_1 est un coefficient de M. Quitte à permuter les colonnes et les lignes, on peut supposer que f_1 se situe en haut à gauche de M :

$$M = \begin{pmatrix} f_1 & u_{12} & \dots & u_{1n} \\ u_{21} & & & \vdots \\ \vdots & & & \vdots \\ u_{n1} & \dots & \dots & u_{nn} \end{pmatrix}$$

On effectue la division euclidienne pour C_1 :
$\forall i \in [\![2, m]\!], \exists q_i, r_i \in A / u_{i1} = q_i f_1 + r_i$ avec $\delta(r_i) < \delta(f_1)$

$$(L_i \leftarrow L_i - q_i L_1) \quad \begin{pmatrix} f_1 & \\ r_2 & (*) \\ \vdots & \\ r_m & \end{pmatrix}$$

Par minimalité de f_1, on a $r_2 = \cdots = r_m = 0$.

De même pour L_1 :
$\forall j \in [\![2, n]\!], \exists q_j, r_j \in A / u_{1j} = q_j f_1 + r_j$ avec $\delta(r_j) < \delta(f_1)$

$$(C_j \leftarrow C_j - q_j C_1) \quad \begin{pmatrix} f_1 & r_2 & & r_n \\ 0 & & (*) & \\ \vdots & & & \\ 0 & & & \end{pmatrix}$$

Par minimalité de f_1, on a $r_2 = \cdots = r_n = 0$. Donc M est équivalente à $\begin{pmatrix} f_1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & V & \\ 0 & & & \end{pmatrix}$.

Montrons alors que $\forall i, j, f_1 | V_i j$.

Pour $i \in [\![2, m]\!]$, on effectue $L_1 \leftarrow L_1 + L_i \quad \begin{pmatrix} f_1 & V_{i2} & & V_{in} \\ 0 & & (*) & \\ \vdots & & & \\ 0 & & & \end{pmatrix}$.

On réalise la division euclidienne pour L_1,
$\forall j \in [\![2, n]\!], \exists q_j, r_j \in A / V_{ij} = q_j f_1 + r_j$ avec $\delta(r_j) < \delta(f_1)$ et de même par minimalité de f_1 : $r_2 = \cdots = r_k = 0$ donc $\forall j \in [\![2, n]\!], V_{ij} = q_j f_1$ d'où $\forall i, j, f_1 | V_{ij}$.

Étape 2 : Montrons le théorème par récurrence sur $m + n \in \mathbb{N} \setminus \{0, 1\}$

- Initialisation : Pour $m + n = 2, M \in \mathcal{M}_{1,1}(A)$ ok
- Hérédité : Soit $n, m \in \mathbb{N}^*$ tels que $m + n \geq 3$. Supposons le résultat vrai pour tout $p, q \in \mathbb{N}^*$ tel que $p + q = m + n - 1$ pour tout $N \in \mathcal{M}_{p,q}(A)$, N est équivalente à $\begin{pmatrix} h_1 & & & & \\ & \ddots & & & \\ & & h_s & & \\ & & & 0 & \\ & & & & \ddots \\ & & & & & 0 \end{pmatrix}$ avec $h_1 | \dots | h_s$.
  Si $m = n = 1$, le résultat est acquis.
  Sinon, par ce qui précède, M est équivalente à $\begin{pmatrix} f_1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & f_1 M' & \\ 0 & & & \end{pmatrix}$ et par hypothèse de récurrence M' est équivalente à $\begin{pmatrix} f_2' & & & & \\ & \ddots & & & \\ & & f_r' & & \\ & & & 0 & \\ & & & & \ddots \\ & & & & & 0 \end{pmatrix}$ avec $f_2' | \dots | f_r'$.

Soit $f_j = f_1 f'_j$, on a $f_1 | \dots | f_r$ et M est équivalente à

$$\begin{pmatrix} f_1 & & & & & \\ & \ddots & & & & \\ & & f_r & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix}$$

Étape 3 : Montrons l'unicité modulo les inversibles

Soit $k \in [\![1, \min(m,n)]\!]$, $I_k(M)$ l'idéal engendré par le déterminants des mineurs de taille k de taille M.
Montrons que $\forall P, Q \in \mathrm{GL}_m(A) \times \mathrm{GL}_n(A), I_k(M) = I_k(PMQ)$.
Par multilinéarité du déterminant (*) du déterminant, les mineurs de taille k de PM sont des combinaisons linéaires de mineurs de taille k de M d'où $I_k(PM) \subset I_k(M)$ et de même à droite $I_k(M'Q) \subset I_k(M')$ pour toute matrice M'.
D'où en notant S une forme normale de Smith de M, on a

$$\forall k \in [\![1, \min(m,n)]\!], I_k(M) = I_k(S) = \begin{cases} \langle f_1, \dots, f_k \rangle & \text{si } k \in [\![1, r]\!] \\ 0 & \text{sinon} \end{cases}$$

Ainsi, soit S, S' deux formes de Smith de M de facteurs invariantes respectifs $f_1, \dots, f_k$ et $f'_1, \dots, f'_k$.
On a $\forall k \in [\![1, r]\!], \langle f_1, \dots, f_k \rangle = \langle f'_1, \dots, f'_k \rangle$.
D'où $\begin{cases} f'_1 & = u_1 f_1 \\ \vdots & \vdots \\ f'_1 \dots f'_r & = u_r f_1 \dots f_r \end{cases}$ avec $u_1, \dots, u_r$ inversibles car le pgcd est unique à inversible près.
D'où de proche en proche

$$\forall j \in [\![1, r]\!], \exists u_j \in A^\times / f'_j = u_j f_j$$

D'où l'unicité à inversible près. □

Annexe

Lemme 1 (*)**.** *Soit $M \in \mathcal{M}_{m,n}(A)$, $P \in \mathrm{GL}_m(A)$, les mineurs de taille k de PM sont combinaisons linéaires des mineurs de taille k de M à coefficients dans A.*

Preuve : Soit M_{IJ} la matrice extraite de M en gardant $I = \{i_1, \dots, i_k\}$ lignes de M et $J = \{j_1, \dots, j_k\}$ colonnes de M.
Notons (C_i) les colonnes de M, $M = \begin{pmatrix} C_1 & \dots & C_n \end{pmatrix}$ et $M_{IJ} = \begin{pmatrix} C_{I,j_1} & \dots & C_{I,j_s} \end{pmatrix}$.
Si $P = (p_{ij})_{(i,j)\in[\![1,n]\!]^2}$, on a $MP = \begin{pmatrix} \sum_{i=1}^{n} p_{i1}C_i & \dots & \sum_{i=1}^{n} p_{in}C_i \end{pmatrix}$. D'où :

$$(MP)_{IJ} = \begin{pmatrix} \sum_{i=1}^{n} p_{i1}C_{I,j_1} & \dots & \sum_{i=1}^{n} p_{in}C_{I,j_k} \end{pmatrix}$$

Par multilinéarité du déterminant, on a $\det((MP)_{I,J})$ est combinaison linéaire des mineurs $M_{I,J}$ où J est un ensemble de $k-$indice.

□

Références

[1] Pierre Le Barbenchon et al. *131 développements pour l'oral*. Dunod, 2020.