Forme normale de Smith

Leçon : , 154, 155, 142, 122, 162 → faire une applicat° aux systèmes linéaires.

Réf. G. Berhuy, Algèbre : le grand combat.

On fixe $\mathcal{P}$ un s.c.r.i (= système complet de représentants irréductibles), ie $\mathcal{P} \subset A$ vérifie : - tt élt de $\mathcal{P}$ est irréductible

- tt élt irréductible de A est associé à un élt de $\mathcal{P}$
- deux élt de $\mathcal{P}$ ne sont pas associés.

Un élt $a \in A$ est normalisé si $a \neq 0$ et si $a = \prod_{p \in \mathcal{P}} p^{v_p(a)}$.

Théorème Soit (A, δ) un anneau euclidien. Toute matrice $C \in \mathcal{M}_{m \times m}(A)$ est équivalente à une matrice de la forme

$$\begin{pmatrix} a_1 & & & \\ & \ddots & & 0 \\ & & a_n & \\ 0 & & & 0 \end{pmatrix} (*)$$

où $a_1, \dots, a_n \in A$ sont non nuls et normalisés et vérifiant $a_1 | \dots | a_n$.

De plus, n et $a_1, \dots, a_n$ sont uniques.

Démonstration

- Existence. On note $E(a_1, \dots, a_n)$ une matrice comme $(*)$.

Si $C = 0$, OK. On suppose donc que $C \neq 0$.

But : Prouver avec un algorithme que $C \sim \begin{pmatrix} a & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & C' & \\ 0 & & & \end{pmatrix}$ où a (normalisé) divise tous les coefficients de C'.

▲ Étape 1 Soit b un coeff non nul de C tq $\delta(b)$ soit minimal, on le place en haut à gauche, avec des échanges de ligne et colonne.

▲ Étape 2, Si b divise tous les élt de la 1ère ligne et de la 1ère colonne, c'est bon.

→ Sinon, $\exists a \in$ 1ère ligne ou 1ère colonne tq $b \nmid a$.

On écrit $a = bq + b_1$, avec $b_1 \neq 0$ et $\delta(b_1) < \delta(b)$. Avec des opérat° du type $\begin{cases} L_k \leftarrow L_k + \alpha L_1 \\ C_k \leftarrow C_k + \alpha C_1 \end{cases}$, on remplace b par b_1, car $b_1 = a - bq$ (après chgt de lignes/colonnes avant).

Quitte à multiplier, on peut supposer que b_1 est normalisé.

→ Si tous les élt de la 1ère ligne et la 1ère colonne sont divisibles par b_1, c'est bon

→ Sinon : on recommence avec cet élt b_2.

Ce procédé termine bien car la suite $\delta(b), \delta(b_1), \ldots, \delta(b_k), \ldots$ ↓↓ et est > 0.

Étape 3 Ainsi, comme l'élt en haut à gauche divise tous les élt de la 1ère ligne et de la 1ère colonne, on peut se ramener à :

$$C \sim \begin{pmatrix} d_1 & 0 \cdots 0 \\ 0 & \\ \vdots & C_1 \\ 0 & \end{pmatrix}$$ où d_1 non nul et normalisé.

→ Si d_1 divise tous les éléments de C_1 : c'est bon

→ Sinon, il existe une ligne i de C_1 tq cette ligne contienne un élt non divisible par d_1. On fait l'opérat° $L_1 \leftarrow L_1 + L_i$, et on recommence l'algo.

On se ramène de nouveau à $\begin{pmatrix} d_2 & 0 \cdots 0 \\ 0 & \\ \vdots & C_2 \\ 0 & \end{pmatrix}$, avec $\underbrace{\delta(d_2) < \delta(d_1)}_{(\delta(d_k))_k \downarrow\downarrow}$.

donc l'algo termine.

Si d_2 divise tous les éléments de C_2 : on s'arrête. Sinon on recommence.

Exemple

• $A = \mathbb{Z}$, $C = \begin{pmatrix} 10 & 14 \\ 6 & 7 \end{pmatrix} \in \mathcal{M}_2(\mathbb{Z})$.

$C \overset{L_1 \leftrightarrow L_2}{\sim} \begin{pmatrix} 6 & 7 \\ 10 & 14 \end{pmatrix}$, $7 = 6 \times 1 + 1$, $6 \nmid 7$.

$C \overset{C_2 \leftarrow C_2 - C_1}{\sim} \begin{pmatrix} 6 & 1 \\ 10 & 4 \end{pmatrix} \overset{C_1 \leftrightarrow C_2}{\sim} \begin{pmatrix} 1 & 6 \\ 4 & 10 \end{pmatrix}$, $1 | 6$ et $1 | 4$.

$C \overset{C_2 \leftarrow C_2 - 6C_1}{\sim} \begin{pmatrix} 1 & 0 \\ 4 & -14 \end{pmatrix}$

$C \overset{L_2 \leftarrow L_2 - 4L_1}{\sim} \begin{pmatrix} 1 & 0 \\ 0 & -14 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 0 & 14 \end{pmatrix}$ en normalisant.

Rmq : Si A est principal, on utilise des matrices faisant apparaître les coeff de Bézout

l'algo s'arrête en considérant $\omega : A \setminus \{0\} \to \mathbb{N}$
$a \mapsto \sum_{p \in \mathcal{P}} v_p(a)$

Pb : peu de côté algorithmique

Pour l'instant on complète le théorème :

Théorème (part 2) De plus $n = rg(C)$, où C est vue comme un élément de $M_{m,m}(\mathrm{Frac}(A))$, et $\forall j \in [\![0, n]\!]$:

$$\mu_j(C) = a_1 \dots a_j$$

où $\mu_j(C)$ désigne le pgcd (normalisé des mineurs d'ordre j de C, convent° : $\mu_0(C) = 1$).

En particulier $a_j = \dfrac{\mu_j(C)}{\mu_{j-1}(C)}$ $\forall j \in [\![1, n]\!]$.

Exemple :

$C = \begin{pmatrix} 10 & 14 \\ 6 & 7 \end{pmatrix} \in M_2(\mathbb{Z})$.

$\mu_1(C) = \mathrm{pgcd}(10, 14, 6, 7) = 1 = a_1$.

$\mu_2(C) = \mathrm{pgcd}\left(\begin{vmatrix} 10 & 14 \\ 6 & 7 \end{vmatrix}\right) = \mathrm{pgcd}(-14) = 14 = a_1 a_2$

donc $a_2 = 14$.

Preuve

Il est clair que n est le rang de C.

- Le pgcd (normalisé) de tous les mineurs d'ordre k de C est invariant par opérations élémentaires sur les lignes et les colonnes, $\forall k \in [\![1, \min(m, m)]\!]$.

On étudie les différentes opérations possibles. Soit M une matrice extraite de C d'ordre k.

→ $L_i \leftarrow L_i + aL_j$: i) Si $L_i, L_j \notin M$ ou M contient uniquement L_j, M ne change pas.

ii) Si $L_i, L_j \in M$, $\det M$ est inchangé.

iii) Si M contient uniquement L_i le nouveau déterminant est de la forme $\det(M) + a\det(M')$, où M' matrice de taille k obtenue par permutat° des lignes d'une autre matrice extraite.

$L_i \leftarrow aL_i$

⊕ dilatat°

→ $C_i \leftarrow C_i + aC_j$: idem

→ $L_i \leftrightarrow L_j$: i) Si $L_i, L_j \in M$ ou $L_i, L_j \notin M$: idem au signe près

ii) M contient 1 ligne : M devient une autre matrice de taille k qui est obtenue par obtenue par permutat° des lignes d'une autre matrice extraire M'. → le mineur est envoyé sur un autre mineur de taille k ($\pm$)

CP: le pgcd des mineurs de taille k reste inchangé.

Donc: $\forall j \in [\![0, n]\!]$, $\mu_j(C) = \mu_j(E(a_1, \dots, a_n))$

$$= \text{pgcd}\{a_{i_1} \cdots a_{i_j},\ 1 \leq i_1 < \dots < i_j \leq n\}$$

$$= a_1 \cdots a_j \text{ car } a_1 | \cdots | a_n.$$

En particulier: $a_j = \dfrac{a_1 \cdots a_j}{a_1 \cdots a_{j-1}} = \dfrac{\mu_j(C)}{\mu_{j-1}(C)}$. (unicité)

□

Si on veut résoudre $AX = B$ dans $M_{n,1}(\mathbb{Z})$, $A \in M_{n,m}(\mathbb{Z})$.

On sait $UAV = S$, S la forme de Smith de A.

$AX = B \iff SY = C$, où $VY = X$ et $C = UB$

de la forme $\begin{cases} f_1 y_1 = c_1 \\ \quad \vdots \\ f_r y_m = c_m. \end{cases}$