Forme normale de Smith

Leçons : 108, 122, 150, 162.

Énoncés : • Th : A un anneau euclidien, $m, n \geq 1$:

$\rightsquigarrow$ pour toute $M \in M_{m,n}(A)$ il existe $P \in GL_m(A)$, $Q \in GL_n(A)$ tq $M = PDQ$

avec $D = \left[\begin{array}{c|c} d_1 & 0 \\ \ddots & \\ d_r & \\ \hline 0 & 0 \end{array}\right] \in M_{m,n}(A)$ où $d_1 | \cdots | d_r$ sont dans $A \setminus \{0\}$;

$\rightsquigarrow$ $GL_n(A)$ est engendré par l'ensemble des transvections et des dilatations inversibles.

• Appli : cela permet de résoudre les systèmes $MX = B$ en $X \in A^n$, où $M \in M_{m,n}(A)$ et $B \in A^m$.

⊛ Th.

• Une dilatation inversible est $D_i(a) = \left[\begin{array}{ccccc} 1 & & & & \\ & \ddots & & & \\ & & a & & \\ & & & \ddots & \\ & & & & 1 \end{array}\right]$ (pos i) avec $a \in A^\times$, une transvection $T_{i,j}(a) = \left[\begin{array}{ccc} 1 & & \\ & \ddots & a \\ & & \ddots \\ & & 1 \end{array}\right]$ ← pos i, pos j.

On note G_n le sg de $GL_n(A)$ engendré par ces matrices (de $\hat{m}$ pour m). On montre le point 1 pour G_n et G_n et on en déduira le point 2. Pour cela on considère l'action de $G_m \times G_n$ sur $M_{m,n}(A)$ donnée par $(P,Q) \cdot M = PMQ^{-1}$.

D'abord remarquons que pour $i \neq j$ dans $[1;n]$, la matrice de transposition $P_{(i\,j)}$ appartient à G_n.
En effet on peut vérifier que $P_{(i\,j)} = D_i(-1)\, T_{i,j}(-1) T_{j,i}(1)\, T_{i,j}(-1)$.
On rappelle que la multiplication à gauche par les matrices élémentaires agit sur les lignes, et à droite sur les colonnes.

• Pour $M \in M_{m,n}(A)$ non nulle on note $\mu(M) = \min \{ \nu(M_{i,j}) \,;\, M_{i,j} \neq 0 \}$, où ν est le stathme euclidien. On fixe $M \neq 0$. Les matrices de l'orbite de M sont non nulles donc μ est défini dessus ; on peut alors prendre N qui minimise $\mu(N)$ dans l'orbite.
Soit (i,j) tq $\mu(N) = \nu(N_{i,j})$: quitte à effectuer les opérations $L_1 \leftrightarrow L_i$ et $C_1 \leftrightarrow C_j$, on peut sq $(i,j) = (1,1)$.

• Mq $N_{1,1}$ divise tous les coefficients de N. Soit $2 \leq j \leq n$: on fait la DE de $N_{1,j}$ par $N_{1,1}$:
$N_{1,j} = N_{1,1} q_j + r$ avec $q_j, r \in A$ et $r = 0$ ou $\nu(r) < \nu(N_{1,1})$. Effectuer l'opération $C_j \leftarrow C_j - q_j C_1$ donne une matrice de l'orbite dont le coef $(1,j)$ est r : par minimalité on ne peut avoir $\nu(r) < \nu(N_{1,1}) = \mu(N)$ donc $r = 0$. Ainsi $N_{1,1} | N_{1,j}$. De $\hat{m}$ pour $2 \leq i \leq m$ on a que $N_{1,1} | N_{i,1}$.
Notons N' la matrice obtenue en effectuant les transvections issues des DE sur les colonnes, cad $C_j \leftarrow C_j - q_j C_1$ pour chaque $2 \leq j \leq n$. On fixe un $2 \leq j \leq n$ et on effectue encore l'opération $C_1 \leftarrow C_1 + C_j$ pour obtenir une matrice N'' (tjs dans l'orbite). On a alors, pour $2 \leq i \leq m$,
$N''_{i,1} = N'_{i,1} + N'_{i,j} = N_{i,1} + (N_{i,j} - q_j N_{i,1}) \equiv N_{i,j}\ [N_{i,1}]$, et $N''_{i,1} \equiv N_{i,j}\ [N_{1,1}]$

puisque $N_{1,1} \mid N_{i,1}$. Mais N'' vérifie encore $\nu(N''_{1,1}) = \mu(N'') = \mu(N)$, donc comme pour N, $N_{1,1} = N''_{1,1} \mid N''_{i,2}$. On a donc finalement $N_{1,1} \mid N_{i,j}$.

Reprenons à partir de N. On effectue, pour $2 \leq j \leq n$ et $2 \leq i \leq m$, les opérations $C_j \leftarrow C_j - \frac{N_{1,j}}{N_{1,1}} C_1$ et $L_i \leftarrow L_i - \frac{N_{i,1}}{N_{1,1}} L_1$, afin d'obtenir une matrice N^* dans l'orbite dont les coefficients sur la première ligne et la première colonne, hormis en $(1,1)$, sont tous nuls. Tous les coefficients de N^* sont encore multiples de $N_{1,1}$. On peut donc écrire $N^* = \left[\begin{array}{c|c} N_{1,1} & 0 \\ \hline 0 & N_{1,1} \cdot M' \end{array}\right]$ avec $M' \in M_{m-2,n-2}(A)$.

- On montre mtn le point 1 du th par réc sur $m+n$ avec $m, n \geq 1$. L'initialisation à $(m,n) = (1,1)$ est triviale. Soient (m,n) avec $m \geq 2$ ou $n \geq 2$ et $M \in M_{m,n}(A)$. Si $M = 0$ c'est trivial, sinon d'après ce qui précède M a dans son orbite une matrice de la forme $\left[\begin{array}{c|c} d_1 & 0 \\ \hline 0 & d_1 M' \end{array}\right]$ avec $d_1 \in A \setminus \{0\}$ et $M' \in M_{m-1,n-1}(A)$. Si $m = 1$ ou $n = 1$, M' est la matrice vide et on a la forme voulue. Sinon par HR écrivons $M' = P' D' Q'$ avec $P' \in G_{m-1}$, $Q' \in G_{n-1}$, $D' = \left[\begin{array}{c|c} k_2 \ddots k_n & 0 \\ \hline 0 & 0 \end{array}\right] \in M_{m-1,n-1}(A)$ où $k_2 \mid \cdots \mid k_n$ sont dans $A \setminus \{0\}$.

  Posons $P = \left[\begin{array}{c|c} 1 & 0 \\ \hline 0 & P' \end{array}\right]$ et $Q = \left[\begin{array}{c|c} 1 & 0 \\ \hline 0 & Q' \end{array}\right]$. Si S est une transvection ou dilatation inversible de taille $m-1$, $\left[\begin{array}{c|c} 1 & 0 \\ \hline 0 & S \end{array}\right]$ en est une de taille m ; par produit par blocs on obtient $P \in G_m$, de même $Q \in G_n$.

  On note $d_2 = d_1 k_2, \cdots, d_n = d_1 k_n$: finalement M a dans son orbite

  $$\left[\begin{array}{c|c} d_1 & 0 \\ \hline 0 & P'(d_1 D) Q' \end{array}\right] = P \left[\begin{array}{c|c} d_1 & 0 \\ \hline 0 & \begin{array}{c|c} d_2 \ddots d_n & 0 \\ \hline 0 & 0 \end{array} \end{array}\right] Q \text{, donc } \left[\begin{array}{c|c} d_1 \ddots d_n & 0 \\ \hline 0 & 0 \end{array}\right].$$

- Terminons par mq $G_n = GL_n(A)$. Soit $M \in GL_n(A)$: en appliquant ce qui précède avec $m = n$ il existe $P, Q \in G_n$ et $d_1 \mid \cdots \mid d_n$ dans $A \setminus \{0\}$ tq $M = P \left[\begin{array}{c|c} d_1 \ddots d_n & 0 \\ \hline 0 & 0 \end{array}\right] Q$. D'abord $n = n$. Ensuite $M, P, Q \in GL_n(A)$ donc on des déterminants inversibles ; ainsi $d_1 \cdots d_n \in A^\times$. Cela impose $d_1, \cdots, d_n \in A^\times$. On a alors $M = P D_1(d_1) \cdots D_n(d_n) Q \in G_n$.

□

⊛ Appli.

$M \in \mathcal{M}_{m,n}(A)$, $B \in A^m$: on veut résoudre $MX = B$.

On écrit $M = PDQ$ avec $P \in GL_m(A)$, $Q \in GL_n(A)$, $D = \left[\begin{array}{c|c} d_1 \ddots d_r & 0 \\ \hline 0 & 0 \end{array}\right]$ avec $d_1 | \cdots | d_r$ non nuls.

$MX = B \Leftrightarrow DQX = P^{-1}B$ donc les sol sont $Q^{-1}Y$ pour Y sol de $DY = P^{-1}B$. Or si $C \in A^m$, $DY = C$ a des sol ssi $d_i | C_i$ pour $1 \le i \le r$ et $C_i = 0$ pour $r+1 \le i \le m$; lorsque c'est le cas ces sols sont $\left(\frac{C_1}{d_1}, \dots, \frac{C_r}{d_r}, k_{r+1}, \dots, k_m\right)$ pour $k_{r+1}, \dots, k_m \in A$. □

Complément 1 : Vérification de $P_{(i\,j)} = D_i(-1)\, T_{i,j}(-1)\, T_{j,i}(1)\, T_{i,j}(-1)$.

On part de $T_{i,j}(-1) = \begin{bmatrix} 1 & & \\ & \ddots & \\ & & -1 \\ & & & \ddots \\ & & & & 1 \end{bmatrix} \leftarrow i$ (j). Par $L_j \leftarrow L_j + L_i$ on obtient $\begin{bmatrix} 1 & & & & \\ & \ddots & & & \\ & & -1 & & \\ & & 1 & \ddots & \\ & & 1 & & 0 \end{bmatrix} \leftarrow i$ (i), $\leftarrow j$ (j).

L'opération $L_i \leftarrow L_i - L_j$ donne alors $\begin{bmatrix} 1 & & & & \\ & \ddots & & & \\ & & 0 & & -1 \\ & & & \ddots & \\ & & 1 & & -1 \end{bmatrix} \leftarrow i$ (i), $\leftarrow j$ (j). La dernière opération, $L_i \leftarrow -L_i$, donne bien $P_{(i\,j)}$. □

Complément 2 : Algorithme de calcul.

- Ce qui a été fait n'est pas tout à fait constructif car on ne sait pas a priori construire N minimisant $\mu(N)$. Un algorithme formel est le suivant.

(i) Par deux transpositions on amène un M_{ij} tq $\nu(M_{ij}) = \mu(M)$ en $(1,1)$.

(ii) On fait les transvections issues des DE pour chaque C_j, $2 \le j \le n$ et L_i, $2 \le i \le m$.
Si on trouve un reste non nul on retourne en (i).

(iii) On a une matrice $\left[\begin{array}{c|c} d_1 & 0 \\ \hline 0 & M' \end{array}\right]$: si il existe $i \ge 2$, $j \ge 2$ tq $d_1 \nmid M_{ij}$, on effectue $C_1 \leftarrow C_1 + C_j$ et on retourne en (ii).

(iv) On a une matrice de la forme ci-dessus avec $d_1 | M_{ij}$ pour tous $i \ge 2$, $j \ge 2$.
On applique récursivement l'algo à M'.

L'algo termine car $\nu(M_{1,1})$ décroit strictement qd on revient en arrière : ce nb de retours est donc fini.
Il n'est pas tjs optimal : en pratique on peut s'arranger pour faire moins d'allers-retours. Mais il est correct et termine.

- Pour déterminer P et Q en plus de D, on part de la matrice

$\left[\begin{array}{c|c} M & I_m \\ \hline I_n & \end{array}\right]$ (le coin inférieur droit est vide, on n'y touchera pas) et on effectue les opérations sur les lignes et colonnes. On arrive alors à $\left[\begin{array}{c|c} D & P^{-1} \\ \hline Q^{-1} & \end{array}\right]$ où P et Q sont bien tq

$M = PDQ$. En effet $\left[\begin{array}{c|c} M & I_m \\ \hline I_n & 0 \end{array}\right] = \left[\begin{array}{c|c} P & 0 \\ \hline 0 & I_m \end{array}\right] \left[\begin{array}{c|c} D & R_1 \\ \hline R_2 & 0 \end{array}\right] \left[\begin{array}{c|c} Q & 0 \\ \hline 0 & I_m \end{array}\right]$ d'où $PR_1 = I_m$ et $R_2Q = I_m$.

Remarquons que dans l'appli à la résolution de $MX = B$, on a besoin de calculer $P^{-1}B$ et $Q^{-1}Y$: or ici nous obtenons directement P^{-1} et Q^{-1} : il n'y a aucun inverse à calculer !

- Exemple : $A = \mathbb{Z}$, $M = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 6 & 6 \end{bmatrix}$.

$$\left[\begin{array}{ccc|cc} 1 & 2 & 3 & 1 & 0 \\ 4 & 6 & 6 & 0 & 1 \\ \hline 1 & 0 & 0 & & \\ 0 & 1 & 0 & & \\ 0 & 0 & 1 & & \end{array}\right] \xrightarrow{L_2 \leftarrow L_2 - 4L_1} \left[\begin{array}{ccc|cc} 1 & 2 & 3 & 1 & 0 \\ 0 & -2 & -6 & -4 & 1 \\ \hline 1 & 0 & 0 & & \\ 0 & 1 & 0 & & \\ 0 & 0 & 1 & & \end{array}\right] \xrightarrow{\substack{C_2 \leftarrow C_2 - 2C_1 \\ C_3 \leftarrow C_3 - 3C_1}} \left[\begin{array}{ccc|cc} 1 & 0 & 0 & 1 & 0 \\ 0 & -2 & -6 & -4 & 1 \\ \hline 1 & -2 & -3 & & \\ 0 & 1 & 0 & & \\ 0 & 0 & 1 & & \end{array}\right]$$

$$\xrightarrow{C_3 \leftarrow C_3 - 3C_2} \left[\begin{array}{ccc|cc} 1 & 0 & 0 & 1 & 0 \\ 0 & -2 & 0 & -4 & 1 \\ \hline 1 & -2 & 3 & & \\ 0 & 1 & -3 & & \\ 0 & 0 & 1 & & \end{array}\right] \xrightarrow{L_2 \leftarrow -L_2} \left[\begin{array}{ccc|cc} 1 & 0 & 0 & 1 & 0 \\ 0 & 2 & 0 & 4 & -1 \\ \hline 1 & -2 & 3 & & \\ 0 & 1 & -3 & & \\ 0 & 0 & 1 & & \end{array}\right]$$

Donc (en imposant les d_i positifs) $D = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \end{bmatrix}$, $P^{-1} = \begin{bmatrix} 1 & 0 \\ 4 & -1 \end{bmatrix}$, $Q^{-1} = \begin{bmatrix} 1 & -2 & 3 \\ 0 & 1 & -3 \\ 0 & 0 & 1 \end{bmatrix}$. □

<u>Complément 3 :</u> si on note $\Delta_i(M)$ le pgcd des mineurs de taille i de M, pour $1 \leq i \leq r$ on a $d_1 \cdots d_i = \Delta_i(M)$ à association près. En particulier $d_1, \cdots, d_r$ sont uniques à association près dans la décomposition. Une classe d'équivalence correspond à un r-uplet $d_1 | \cdots | d_r$ d'éléments de $A \setminus \{0\}$ à association près pour un $0 \leq r \leq m$.

Preuve.

Si D est de la forme voulue il est clair que ses mineurs de taille $1 \leq i \leq n$ non nuls sont les $\prod_{j \in J} d_j$ pour $J \subset [\![1; n]\!]$ de cardinal i, et donc que $\Delta_i(D) = d_1 \cdots d_i$ à association près. Pour avoir le résultat on montre que si M et M' sont équivalentes sur A, $\Delta_i(M) = \Delta_i(M')$ à association près.

D'abord si $M = PM'$, les lignes de M sont combinaisons linéaires des lignes de M'. Par multilinearité les mineurs de taille i de M sont alors combinaisons linéaires de ceux de M', d'où $\Delta_i(M') \mid \Delta_i(M)$. On a aussi $M' = P^{-1}M$ donc $\Delta_i(M)$ et $\Delta_i(M')$ sont associés.

Ensuite si $M = M'Q$, ${}^tM = {}^tQ\,{}^tM'$ donc $\Delta_i(M) = \Delta_i({}^tM) = \Delta_i({}^tM') = \Delta_i(M')$ à association près d'après ce qui précède. Finalement si $M = PM'Q$, on a bien, à association près, $\Delta_i(M) = \Delta_i(M'Q) = \Delta_i(M')$.

□

Réf: • FGN - Algèbre 1 : ↑ 329 (th, complément 1).
• Artin - Algèbre : ↑ 419 (complément 2).
• Objectif agrégation : ↑ 285 (compléments 2 et 3).
• Berhuy : ↑ 574 (compléments 1, 2 et 3).

↳ Probablement un peu long : ne pas annoncer l'appli. S'il reste du temps : parler de l'appli, ou éventuellement du complément 3 (unicité).

↳ Légère généralisation p/r à FGN : matrices rectangulaires, A euclidien. Même preuve.

↳ La 3e partie de la preuve du th fonctionne pour $n = 1$ ou $n = 1$ (matrice inférieure droite vide, à utiliser dans la réc). Certaines opérations et vérifications sont alors superflues.

↳ L'exemple du complément 2 vient d'Artin. On a déjà $|M_{1,1}| = 1$ minimisant μ sur l'orbite : pas de retour en arrière lié avec DE. Dans ce cas l'algo général d'Artin correspond à l'algo de FGN qui suppose N trouvée. Par ailleurs attention aux notations : P et Q ne désignent pas la même chose dans Artin et ici.

↳ L'unicité dans le complément 3 classifie les orbites de l'action par équivalence. Dans le cas particuliers usuels on peut imposer une condition sur les d_i pour enlever « à association près » ($A = \mathbb{Z}$: $d_i > 0$; $A = K[X]$: d_i unitaire ; $A = K$: $d_i = 1$).

↳ Application : th de structure des A-modules de type fini pour A euclidien (existence), par le th de la base adaptée. Fait dans FGN (pour $\mathbb{Z}$, groupe abélien fini).

↳ Le th ainsi que l'unicité sont encore vrais pour A principal. C'est plus difficile et il n'y a plus l'algorithme présenté (on peut cependant calculer les d_i par la formule du complément 3). L'existence est cas du th de structure des A-modules de type fini pour A euclidien ; la preuve de l'unicité reste la même.

↳ Au fond la preuve donnée et l'algo du complément 2 ont les mêmes idées ; la différence est que dans la preuve on part directement avec une matrice N minimisant $\mu(N)$, alors que dans l'algo on part de la matrice de départ et on revient en arrière si besoin, la terminaison étant assurée par la décroissance stricte de $\nu(M_{1,1}) \in \mathbb{N}$. Notons bien qu'il s'agit du même argument (toute partie de $\mathbb{N}$ admet un minimum ; il n'y a pas de suite strictement décroissante dans $\mathbb{N}$).

↳ Berlucy très bonne réf pour l'approche algorithmique (et m en général).
Artin et Oljagreq bien aussi.