Forme normale de SMITH

[BECK-MALICK-PEYRÉ, p]

ÉNONCÉ :

Théorème : Soit (A, φ) un anneau euclidien. Soient $m, n \in \mathbb{N}$, et $U \in \mathcal{M}_{m,n}(A)$. Alors il existe une unique suite $(d_1, d_2, \ldots, d_s)$ d'éléments non nuls (appelés facteurs invariants de U) de A telle que $d_s \mid d_{s-1} \mid \ldots \mid d_1$ et U est équivalente à $D \in \mathcal{M}_{m,n}(A)$ définie par :

$$D = \begin{pmatrix} d_s & 0 & \ldots & 0 & 0 & \ldots & 0 \\ 0 & \ddots & \ddots & \vdots & \vdots & & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots & & \vdots \\ 0 & \ldots & 0 & d_1 & 0 & \ldots & 0 \\ 0 & \ldots & \ldots & 0 & 0 & \ldots & 0 \\ \vdots & & & \vdots & \vdots & & \vdots \\ 0 & \ldots & \ldots & 0 & 0 & \ldots & 0 \end{pmatrix}$$

Application : $(A, \varphi) = (\mathbb{Z}, |.|)$. Alors :

$$\begin{pmatrix} 4 & 8 & 4 \\ 4 & 13 & 11 \\ 4 & 16 & 8 \end{pmatrix} \text{ est équivalente à } \begin{pmatrix} 1 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 36 \end{pmatrix}$$

DÉVELOPPEMENT : Donnons les étapes de l'algorithme permettant le calcul des facteurs invariants de la matrice $U = (u_{i,j})$. Notons C_j la j-ième colonne et L_i la i-ième ligne de U.

1. Si $U = 0$, l'algorithme est terminé.
2. Sinon, soit (i_0, j_0) tel que $\varphi(u_{i_0,j_0}) = \inf\{\varphi(u_{i,j}, u_{i,j} \neq 0\}$. Permuter les colonnes C_1 et C_{j_0} puis les lignes L_1 et L_{i_0}, afin de placer u_{i_0,j_0} en haut à gauche de U.
3. Traitement de la première colonne. On commence par $u_{2,1}$ $(2 \mapsto i)$.
   (a) Effectuer la division euclidienne de $u_{i,1}$ par $u_{1,1}$:
   $$u_{i,1} = u_{1,1}q + r_i \quad \text{avec} \quad r_i = 0 \quad \text{ou} \quad \varphi(r_i) < \varphi(u_{1,1})$$
   Soustraire q fois la ligne L_1 par L_i (pour obtenir $u_{i,1} = r_i$)
   (b) Si $r_i \neq 0$, échanger les lignes L_1 et L_i et retourner en 3.
   (c) Si $r_i = 0$ et si $i < m$ passer à la ligne suivante $(i \mapsto i+1)$ et aller en 3.
   (d) Si $r_i = 0$ et si $i = m$, aller en 4.
4. Traitement de la première ligne. On commence par $u_{2,1}$ $(2 \mapsto i)$.
   (a) Effectuer la division euclidienne de $u_{1,j}$ par $u_{1,1}$:
   $$u_{1,j} = u_{1,1}q + s_j \quad \text{avec} \quad s_j = 0 \quad \text{ou} \quad \varphi(s_j) < \varphi(u_{1,1})$$
   Soustraire q fois la colonne C_1 par C_j (pour obtenir $u_{1,j} = s_j$)
   (b) Si $s_j \neq 0$, échanger les colonnes C_1 et C_j et retourner en 3.
   (c) Si $s_j = 0$ et si $j < n$ passer à la colonne suivante $(j \mapsto j+1)$ et aller en 4.
   (d) Si $s_j = 0$ et si $j = m$, aller en 5.
5. Divisibilité.
   (a) S'il existe $i_1 \geq 2$ et $j_1 \geq 2$ tels que $u_{1,1}$ ne divise pas u_{i_1,j_1}, ajouter la colonne C_{j_1} à la colonne C_1 et retourner en 3.
   (b) Sinon retourner en 1 avec la matrice extraite $(u_{i,j})_{2 \leq i \leq m,\ 2 \leq j \leq n}$.

Pourquoi l'algorithme se termine en un nombre fini d'étapes ?
Tout repose sur la décroissance de $\varphi(u_{1,1})$ qui est à valeur dans $\mathbb{N}$.

1. Étape 3 : L'algorithme revient en arrière que si $r_i \neq 0$: On remplace $\varphi(u_{1,1})$ par r_i : $\varphi(u_{1,1})$ décroît strictement $\longrightarrow$ passage nécessairement à l'étape 4.
2. Étape 4 : Retour en 3 seulement si $s_j \neq 0$: $\varphi(u_{1,1})$ a diminué strictement au moins une fois : on ne peut revenir en 3 qu'un nombre fini d'étapes avant d'aller à l'étape 5.

Finalement, on ne peut revenir qu'un nombre fini de fois à l'étapes 3 et donc on aboutit à une matrice de la forme :

$$\begin{pmatrix} u'_{1,1} & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & U_1 & \\ 0 & & & \end{pmatrix}$$

avec $u'_{1,1} \mid u'_{i,j}$ pour $i \geq 2$, $j \geq 2$.

D'où vient l'unicité ?
Pour $j \in \{1, \dots, s\}$, notons $D_j = \prod_{i=0}^{j-1} d_{s-i}$, $D_j = 0$ pour $j > s$ et

$$\Lambda_j(U) = pgcd\{\Delta_j, \quad \Delta_j \text{ mineur de taille } j \text{ de } U\}$$

$\Lambda_j(U)$ est aussi un générateur de l'idéal A engendré par les mineurs de taille j de U.
Voyons que si $U, U' \in \mathcal{M}_{m,n}(A)$ sont équivalentes, alors $(\Lambda_j(U)) = (\Lambda_j(U'))$.

1. Cas où $U = PU'$, $P \in GL_m(A)$: Les lignes de U sont des combinaisons linéaires des lignes de U'. Par multilinéarité du déterminant, on a l'inclusion $(\Lambda_j(U)) \subset (\Lambda_j(U'))$. Mais comme $P^{-1}U = U'$, on a égalité.
2. Cas où $U = U'Q$, $Q \in GL_n(A)$: il suffit de considérer la transposée car $(\Lambda_j(U)) = (\Lambda_j({}^tU))$ et d'utiliser le cas 1.
3. Cas général : Résulte immédiatement des deux cas précédents.

Les relations de divisibilité entre les $(d_i)_{1 \leq i \leq s}$ assurent que $\Lambda_j(D) = D_j$, l'égalité $(D_j) = \Delta_j(U)$ traduit simplement l'équivalence de U et D.