I.F Forme normale de Smith (122) (142) (162)

Soit (A, δ) un anneau euclidien. Soient $m, n \in \mathbb{N}^*$.

Théorème 7: Forme normale de Smith

Pour tout $M \in \mathcal{M}_{m,n}(A)$, il existe $P \in \mathrm{GL}_m(A)$ et $Q \in \mathrm{GL}_n(A)$ telles que :

$$M = P \begin{pmatrix} d_1 & & & & & (0) \\ & \ddots & & & & \\ & & d_s & & & \\ & & & 0 & & \\ & & & & \ddots & \\ (0) & & & & & 0 \end{pmatrix} Q$$

avec $d_1, \cdots, d_s \in A$ tels que $d_1 | \cdots | d_s$, et les d_i sont uniques au sens où si

$$M \sim \begin{pmatrix} d'_1 & & & & & (0) \\ & \ddots & & & & \\ & & d'_t & & & \\ & & & 0 & & \\ & & & & \ddots & \\ (0) & & & & & 0 \end{pmatrix}$$

alors $t = s$ et $d_i \sim_A d'_i$.

Démonstration. Il s'agit d'une preuve algorithmique.

Voici l'algorithme :

1. Si $M = \mathbf{O}$ alors renvoyer M ;
   Sinon passer à l'étape 2
2. Il existe i_0, j_0 tel que $M_{i_0,j_0} \neq 0$.
   Faire $C_1 \longleftrightarrow C_{i_0}$ et $L_1 \longleftrightarrow L_{j_0}$. et passer à l'étape 3 ;

$$M \sim \begin{pmatrix} \overset{\neq 0}{m_{1,1}} & & \\ & * & \\ & & \end{pmatrix}$$

3. On effectue la division euclidienne de $m_{i,1}$ par $m_{1,1}$:

$$m_{i,1} = q_i \times m_{1,1} + r_i \qquad \text{avec} \quad \delta(r_i) < \delta(m_{1,1})$$

   Faire $L_i \longleftarrow L_i - q_i L_1$.
   Si il existe $i > 1$ tel que $m_{i,1} \neq 0$ alors Faire $L_1 \longleftrightarrow L_i$ et retourner à 3 ;
   Sinon passer à 4 ;

$$M \sim \begin{pmatrix} m_{1,1} & & \\ 0 & & \\ 0 & & \\ \vdots & * & \\ 0 & & \\ 0 & & \end{pmatrix}$$

4. On procède de la même manière qu'à l'étape précédente mais sur la première ligne :

$$m_{1,j} = q_j \times m_{1,1} + r_j \qquad \text{avec} \quad \delta(r_j) < \delta(m_{1,1})$$

Faire $C_j \longleftarrow C_j - q_j C_1$.
Si il existe $j > 1$ tel que $m_{1,j} \neq 0$ alors Faire $C_1 \longleftrightarrow C_j$ et retourner à 3 ;
Sinon passer à 5 ;

$$M \sim \begin{pmatrix} m_{1,1} & 0 \\ 0 & M' \end{pmatrix}$$

5. Si il existe (i_1, j_1) tel que $m_{1,1} \nmid m_{i_1,j_1}$ alors Faire $C_1 \longleftarrow C_1 + C_{j_1}$ et retourner à 3 ;
Sinon retourner à 1 avec la matrice M'.

Justifions la terminaison de cet algorithme. Il y a seulement les étapes 3,4 et 5 où l'on peut effectuer un retour en arrière, sinon on passe toujours à l'étape suivante.

* En 3, lors d'un retour en 3 $\delta(m_{1,1})$ décroît strictement, or c'est un entier naturel, donc on ne peut faire qu'un nombre fini de retour en 3 et on passe à l'étape 4.
* En 4 soit en avance en 5 soit on retourne en 3. Si on retourne en 3 alors on le fait en faisant décroître $\delta(m_{1,1})$. Donc on fait qu'un nombre fini de retour en 3 pour la même raison et on passe à l'étape 5.
* En 5, si on retourne à 3 (après être retourné en 3) alors d'après la condition de retour il existe i tel que $\delta(m_{i,1}) < \delta(m_{1,1})$ donc on fait un autre retour en 3 et donc $\delta(m_{1,1})$ décroît encore strictement. On ne fait toujours qu'un nombre fini de retour en 3. On fini donc par obtenir une matrice

$$\begin{pmatrix} m_{1,1} & 0 \\ 0 & M' \end{pmatrix}$$

avec $m_{1,1} | M'$.
On applique alors l'algorithme à M' (si elle existe) qui est de taille $(m-1, n-1)$. On fait donc décroître strictement la taille de la matrice (le produit des deux dimensions) qui est un entier naturel donc il y a un nombre fini de matrice sur lesquelles on travaille.

Finalement on sort de l'algorithme.

Il nous reste à démontrer l'unicité.
On note $\Delta_j(M)$ le pgcd des mineurs de taille j de M.

Supposons

$$M \sim D = \begin{pmatrix} d_1 & & & & & (0) \\ & \ddots & & & & \\ & & d_s & & & \\ & & & 0 & & \\ & & & & \ddots & \\ (0) & & & & & 0 \end{pmatrix} \qquad \text{et} \qquad M \sim D' = \begin{pmatrix} d'_1 & & & & & (0) \\ & \ddots & & & & \\ & & d'_t & & & \\ & & & 0 & & \\ & & & & \ddots & \\ (0) & & & & & 0 \end{pmatrix}.$$

On démontre le résultat intermédiaire suivant :

Lemme 8:

Si $U \sim U'$ alors $\Delta_j(U) \sim_A \Delta_j(U')$ pour tout j.

Démonstration. Si $U = PU'$ alors les lignes de U sont des combinaisons linéaires de celles de U'. Donc par multilinéarité du déterminant un mineur de taille j de U est combinaison linéaire de mineurs de tailles j de U'. Donc :

$$\Delta_j(U) \in \langle \Delta_j(U') \rangle \qquad \text{i.e.} \qquad \Delta_j(U') | \Delta_j(U).$$

Comme on a $U' = P^{-1}U$, on a aussi de la même manière $\Delta_j(U) | \Delta_j(U')$.

Au total si $U = PU'$ alors $\Delta_j(U) \sim_A \Delta_j(U')$.

Si $U = U'Q$, alors on obtient $\Delta_j(U) \sim_A \Delta_j(U')$ directement du premier point simplement en transposant ($\det(U) = \det({}^tU)$).

Le cas général se déduit alors facilement. ■

Finalement $M \sim D \sim D'$ entraîne $\Delta_j(D) \sim_A \Delta_j(D')$ pour tout j donc t et s sont égaux et $d_s \sim_A d'_s$ (regarder Δ_1) puis par induction comme $d_1 \dots d_j \sim_A d'_1 \dots d'_j$, on a $\forall i \quad d_i \sim_A d'_i$ et ceci conclut l'unicité. ■