Invariants de Smith

Notations : Soit $1 \leq k \leq n$, on note $P_k(n)$ les parties de cardinal k de $\{1..n\}$, et si $M \in M_{n,p}(A)$, $I \in P_k(n)$, $J \in P_k(p)$, alors on note

$$\Delta_{I,J}(M) = \det\left((M_{i,j})_{i,j \in I \times J}\right)$$

On note aussi :

$$\partial_k(M) = \bigwedge_{I,J \in P_k(n), P_k(p)} \Delta_{I,J}(M)$$

Théorème. *Soit A un anneau principal, $n, p \geq 1$ et $M \in M_{n,p}(A)$ une matrice. Alors il existe une unique suite $(d_1, ..d_r)$, à relation d'association près, avec $d_1|d_2|..|d_r$, tel qu'il existe $P, Q \in SL_n(A) \times SL_p(A)$, tel que*

$$M = P \begin{bmatrix} d_1 & & & & \\ & d_2 & & & \\ & & d_3 & & \\ & & & \ddots & \end{bmatrix} Q$$

Et

$$\partial_k(M) = d_1 d_2 .. d_k$$

On admet la formule de Cauchy-Binet ; si $(M, N) \in M_{l,m}(A) \times M_{m,n}(A)$, $I \in P_k(l)$, $J \in P_k(n)$, alors

$$\Delta_{I,J}(MN) = \sum_{K \in P_k(m)} \Delta_{I,K}(M)\Delta_{K,L}(N)$$

Démonstration. On commence par l'existence. Pour cela, on va décrire un algorithme à appliquer sur M (qui se formule en terme de multiplication à droite et à gauche de matrice du groupe spécial orthogonal) qui ramène M à une matrice de la forme

$$\begin{bmatrix} d & 0 \\ 0 & M' \end{bmatrix}$$

où d divise tous les coefficients de la matrice M'. Il suffit ensuite d'appliquer ce procédé par récurrence. L'algorithme sera décrit comme un processus itératif qui se termine en fait en un nombre fini d'étapes.

Phase I ; simplification de ligne.
Dans le cas où $m_{1,1}$ ne divise pas tous les coefficients de sa ligne, on choisi $i > 1$ minimal tel que $m_{1,1}$ ne divise pas $m_{1,i}$. On note d leur pgcd. Comme A est principal, il existe

u, v tels que $um_{1,1} + vm_{1,i} = d$. On note $x = m_{1,1}/d$, $y = m_{1,i}/d$, la matrice

$$P = \begin{bmatrix} u & & & & -y & & \\ & 1 & & & & & \\ & & \ddots & & & & \\ & & & 1 & & & \\ v & & & & x & & \\ & & & & & 1 & \\ & & & & & & \ddots \end{bmatrix}$$

est dans $SL_p(A)$, et $(MP)_{1,1} = d$.

Phase II ; simplification de colonne.
Dans le cas où $m_{1,1}$ ne divise pas tous les coefficients de sa colonne, on choisi $j > 1$ minimal tel que $m_{1,1}$ ne divise pas $m_{j,1}$. On note d leur ppcm. Par le même procédé qu'en phase I, on trouve $Q \in SL_n(A)$ telle que $(QM)_{1,1} = d$.

Phase III ; simplification de M'.
Dans le cas où $m_{1,1}$ ne divise pas $m_{i,j}$ où $i, j > 1$, on choisi i, j minimal. On fait alors l'opération $L_1 \leftarrow L_1 + L_i$.

Tant que $m_{1,1}$ ne divise pas toute la matrice :
$\hookrightarrow$ Tant que $m_{1,1}$ ne divise pas sa ligne : **Phase I**
$\hookrightarrow$ Tant que $m_{1,1}$ ne divise pas sa colonne : **Phase II**
$\hookrightarrow$ Si $m_{1,1}$ ne divise pas toute la matrice : **Phase III**
Faire les opérations $L_j \leftarrow L_j - \frac{m_{j,1}}{m_{1,1}} L_1$, $j = 2..n$.
Faire les opérations $C_i \leftarrow C_i - \frac{m_{1,i}}{m_{1,1}} C_1$, $i = 2..p$.

Cette procédure se termine bien : en effet, le coefficient $M_{1,1}$ a un nombre fini de diviseurs et ne peut donc pas "décroître" indéfiniment ; les phases I et II ne peuvent s'appliquer qu'un nombre fini de fois.

Montrons maintenant l'unicité : si M et N sont équivalentes (il existe P, Q inversibles telles que $M = PNQ$), alors pour tout k, $\partial_k(M) = \partial_k(N)$. En effet, pour tout $I, J \in P_k(n), P_k(p)$, la formule de Cauchy-Binet donne :

$$\Delta_{I,J}(M) = \sum_{K,L \in P_k(n), P_k(p)} \Delta_{I,K}(P)\Delta_{K,L}(N)\Delta_{L,J}(Q)$$

Donc $\partial_k(M) | \partial_k(N)$ et réciproquement.
Il suffit donc de calculer $\partial_k \begin{bmatrix} d_1 & & & \\ & d_2 & & \\ & & d_3 & \\ & & & \ddots \end{bmatrix}$ (on note N cette matrice). Si $I \neq J$, $\Delta_{I,J}(N) = 0$ et $\Delta_{I,I}(N) = \prod_{i \in I} d_i$, d'où le résultat.

□

Ces d_i sont appelés diviseurs principaux.

Corollaire. *Soit M un sous-module de A^n. Alors il existe $(f_1, .., f_n)$ une base de A^n et une unique (à association près) suite $(d_1, .., d_r)$ non nuls, ne dépendant pas de (f_i), telle que $d_1|..|d_r$ et $(d_1 f_1, .., d_r f_r)$ est une base de M.*

Corollaire. *Un sous-groupe de $\mathbb{Z}^n$ est isomorphe à un $\mathbb{Z}^k$, où $k \leq n$.*
Soit G un groupe abélien de type fini, il existe une unique suite d'entiers positifs $d_1|..|d_k$ telle que G est isomorphe à $\bigoplus_{i=1}^{k} \frac{\mathbb{Z}}{d_i\mathbb{Z}}$.

Corollaire. *Soit $M \in M_n(K)$, les diviseurs principaux de $XI_n - M$ sont les invariants de similitude de M ; ils sont unique et M est semblable à la matrice diagonale par blocs de blocs $\mathcal{C}_{d_i}$.*

Référence : Serre