Invariants de Smith (Serre page 67)

Pierre Lissy

April 23, 2010

On va en plus donner une manière effective de calculer les invariants de Smith.
Unicité.

Proof. Posons $M = PDQ = P'D'Q'$. Notons $D_k(N)$ le pgcd des déterminants mineurs d'ordre k de la matrice N. Alors comme les déterminants de P, P', Q, Q' et leur mineurs sont inversibles on a $D_k(M) = D_k(P) = D_k(P')$. Mais trivialement, $D_k(P) = d_1 \dots d_k$ et de même avec $D_k(P')$. Une récurrence triviale permet donc de conclure que pour tout i, par intégrité des anneaux principaux, $d(i) = d'(i)$. □

Existence

Proof. L'analyse que l'on vient de faire permet de s'assurer qu'il faut choisir les d_i tels que $d_1 \dots d_i = D_i(M)$. Notamment, le premier facteur est le pgcd des coefficients de M. Il faut donc commencer par rendre semblable M à une matrice dont le premier coefficient est le pgcd, puis on verra comment on fait pour que la première colonne et la première ligne soient nuls outre ce coefficient. Pour ce faire, on construit une suite de matrices équivalentes M^p telle que M_{11}^p divise M_{11}^{p-1}. Distinguons quatre cas pour passer d'une matrice à l'itéré suivante. Posons $N := M^{p-1}$ et chercons à construire M^p.

1. n_11 divise $n_{12}, \dots n_{1,j-1}$ mais pas $n_{i,j}$. Posons d le pgcd de ces deux éléments. $d = aun_{11} + vn_{ij}$. On pose $w = -n_{1j}/d$ et $z = n_{11}/d$; On définit une matrice Q comme une matrice dont tous les coefficients hors diagonal sont nuls, dont les coefficients diagonaux valent 1, puis $q_{11} = u, q_{j1} = v, q_{1j} = w, q_{jj} = z$. La matrice NQ convient alors (faire le calcul)

2. n_{11} divise tous les $n_{i,j}$, puis divise $n_{21}, \dots n_{i-1,1}$ mais pas $n_{i,1}$. On fait la même chose mais de manière symétrique en agissant ce coup-ci sur les lignes et donc en multipliant à gauche par une certaine matrice P.

3. n_11 divise tous les n_{1k}, tous les n_{k1}.

4. n_{11} divise tous les coefficients de la matrice N: on ne fait plus rien.

On remarque que dans les trois premiers cas le nombre m_{11}^p divise strictement m_{11}^{p-1}. Mais un anneau principal étant noetherien, au bout d'un certain moment la suite des m_{11}^p stationne à un inversible près (on a une suite d'idéaux croissante donc elle stationne). Autrement dit, au bout d'un moment on finit par se retrouver dans le quatrième cas, et m_11 divise tous les autres coefficients. Soit q le rang à partir duquel sa stationne. Notamment, $m_{i1}^q = a_i m_{11}^q$ et $m_{1j}^q = b_j m_{11}^q$. On définit alors une matrice P et une matrice Q de la manière suivante:$p_i i = 1$, $p_i 1 = -a_i$, les autres nuls, $q_i i = 1$, $p_1 j = -b_j$, les autres nuls. La matrice PMQ est équivalente à M et sa première ligne et sa première colonne sont nuls sauf le terme m_11, qui en outre divise tous les autres coefficients de la matrice. On voit que l'on peut maintenant amorcer un raisonnement par récurrence.

r=1 ok

vrai au rang n. Alors au rang $n+1$, on applique l'algo qui rend M semblable à M', puis on applique HR à la sous-matrice. $M'_{ij, i \geqslant 2, j \geqslant 2} = P'D'Q'$. A partir de là, comme m_11 va encore diviser les coefficients d'_i puisque grâce à l'unicité déjà faite nécessairement $d'_1 1 = D_1(M')$, il suffit de poser $P = (1, P')$, $Q = (1, Q')$, $D = (m_1 1, D')$ et on a ce qu'on veut.

□