Sandrine CARUSO

Facteurs invariants

Références : Objectif Agrégation, page 285 pour l'unicité
Les Matrices, Denis Serre pour l'existence

Théorème. *Soit $\mathbb{A}$ un anneau principal, et soit $U \in \mathcal{M}_{m\times n}(\mathbb{A})$. Il existe $r \geqslant 0$ et $d_1, \dots, d_r \in \mathbb{A}$, non nuls, tels que $d_1|d_2|\cdots|d_r$ et tels que U soit équivalente à*

$$D = \begin{pmatrix} d_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & d_2 & \ddots & \vdots & \vdots & & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots & & \vdots \\ 0 & \cdots & 0 & d_r & 0 & \cdots & 0 \\ 0 & \cdots & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & & & \vdots & \vdots & & \vdots \\ 0 & \cdots & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix}$$

De plus, il y a unicité au sens suivant : si U est aussi équivalente à

$$D' = \begin{pmatrix} d'_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & d'_2 & \ddots & \vdots & \vdots & & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots & & \vdots \\ 0 & \cdots & 0 & d'_s & 0 & \cdots & 0 \\ 0 & \cdots & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & & & \vdots & \vdots & & \vdots \\ 0 & \cdots & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix}$$

*avec $d'_1|d'_2|\cdots|d'_s$, alors $r = s$ et pour tout $i \in \{1, \dots, r\}$, d'_i et d_i sont associés (*ie *il existe un inversible u_i de $\mathbb{A}$ tel que $d_i = u_i d'_i$).*

Unicité. Soit $U \in \mathcal{M}_{m\times n}(\mathbb{A})$, et soit D une matrice vérifiant les hypothèses de l'énoncé. Commençons par introduire quelques notations :

$$D_k = d_1 \cdots d_k \text{ pour } k \in \{1, \dots, r\} \text{ et } D_k = 0 \text{ pour } k > r,$$

et pour $M \in \mathcal{M}_{m\times n}(\mathbb{A})$, on note $\Lambda_k(M)$ un PGCD des mineurs de taille k de M. On pose également $\Lambda_0(M) = 1$.

Proposition. *Pour tout $k \in \{1, \dots, \min(m, n)\}$, on a $(D_k) = (\Lambda_k(U))$.*

Lemme. *Soient U et U' deux matrices équivalentes de $\mathcal{M}_{m\times n}(\mathbb{A})$. Alors $(\Lambda_k(U)) = (\Lambda_k(U'))$ pour tout $k \in \{1,\dots,\min(m,n)\}$.*

Démonstration du lemme. 1) Supposons dans un premier temps qu'il existe $P \in \mathrm{GL}_m(\mathbb{A})$ telle que $U = PU'$. Les lignes de U sont donc des combinaisons linéaires des lignes de U'. Notons L_i (resp. L'_i) la i-ème ligne de U (resp. de U') ainsi que le vecteur correspondant dans la base canonique $(e_1,\dots,e_n)$ de $\mathbb{A}^n$. Le mineur de taille k de U restreint aux lignes d'indice $i_1,\dots,i_k$ et colonnes d'indice $j_1,\dots,j_k$ peut être vu comme le déterminant dans l'espace $\mathrm{Vect}(e_{j_1},\dots,e_{j_k})$ des projetés sur cet espace de $L_{i_1},\dots,L_{i_k}$. Ainsi, par linéarité de la projection et par multilinéarité du déterminant, les mineurs de taille k de U sont combinaison linéaire des mineurs de taille k de U'. Par conséquent, $\Lambda_k(U')|\Lambda_k(U)$, autrement dit, $(\Lambda_k(U)) \subset (\Lambda_k(U'))$. On a également $U' = P^{-1}U$, donc en appliquant ce que l'on vient de démontrer en échangeant les rôles de U et U' et P par P^{-1}, on a $(\Lambda_k(U')) \subset (\Lambda_k(U))$, d'où l'égalité.

2) Supposons à présent qu'il existe $Q \in \mathrm{GL}_n(\mathbb{A})$ telle que $U = U'Q$. En transposant cette égalité, on obtient ${}^tU = {}^tQ\,{}^tU'$, et comme l'ensemble des mineurs de taille k d'une matrice est égal à l'ensemble des mineurs de taille k de sa transposée, le cas 1) donne $(\Lambda_k(U')) = (\Lambda_k(U))$.

3) Dans le cas général, il existe $P \in \mathrm{GL}_m(\mathbb{A})$ et $Q \in \mathrm{GL}_n(\mathbb{A})$ telles que $U = PU'Q$. On applique alors le cas 1) à PU' et U' et le cas 2) à U et PU', ce qui donne le résultat. □

Démonstration de la proposition. Pour établir notre proposition, il suffit de remarquer que pour tout $k \in \{1,\dots,\min(m,n)\}$, on a $(D_k) = (\Lambda_k(D))$. En effet, les hypothèses de divisibilité des d_i montrent que le mineur de taille k en haut à gauche, égal à D_k, divise tous les autres mineurs de taille k. C'est donc bien un PGCD. Comme U et D sont équivalentes, on a bien $(D_k) = (\Lambda_k(U))$. □

Établissons maintenant l'unicité grâce à cette proposition. Soit D' une deuxième matrice telle que décrite dans l'énoncé et en conservant les mêmes notations. On a $r = \max\{k, D_k \neq 0\}$ et donc $r = \max\{k, \Lambda_k(U) \neq 0\}$, et de même, $s = \max\{k, \Lambda_k(U) \neq 0\}$, donc $r = s$. De plus, pour tout $k \in \{1,\dots,r\}$, $\Lambda_{k-1}(U)$ divise $\Lambda_k(U)$ et on a $(d_k) = (\Lambda_k(U)/\Lambda_{k-1}(U))$ et $(d'_k) = (\Lambda_k(U)/\Lambda_{k-1}(U))$. Par conséquent, les idéaux (d_k) et (d'_k) sont égaux, ce qui équivaut à l'égalité de d_k et d'_k à association près.

Existence. Soit $B = (b_{ij}) \in \mathcal{M}_{m\times n}(\mathbb{A})$. Le but est de se ramener, étape par étape, à une matrice de la forme de D, en multipliant à gauche où à droite par des matrices inversibles.

L'étape fondamentale est de faire en sorte que le coefficient en haut à gauche divise tous les coefficients de la matrice (idée qui nous est inspirée par la partie unicité). Pour cela, nous allons construire une suite de matrices $(B^{(p)})_{p\in\mathbb{N}}$, toutes équivalentes à B, et l'on passera de $B^{(p)}$ à $B^{(p+1)}$ à l'aide de l'algorithme suivant :

1) Si p est tel que $b_{11}^{(p)}$ divise tous les coefficients de la première colonne, on passe à l'étape 2. Sinon, soit i tel que $b_{11}^{(p)}$ ne divise pas $b_{i1}^{(p)}$. On procède comme suit. Notons d le PGCD de b_{11} et b_{i1}. Comme $\mathbb{A}$ est principal, d'après le théorème de Bézout, il existe u et v tels que $d = ub_{11} + vb_{i1}$. Soit P la matrice suivante :

$$
\begin{array}{c}
\\
\\
\\
\\
i \rightarrow \\
\\
\\
\\
\end{array}
\begin{pmatrix}
u & & & & v & & & \\
& 1 & & & & & & \\
& & \ddots & & & & & \\
& & & 1 & & & & \\
-\frac{b_{i1}^{(p)}}{d} & & & & \frac{b_{11}^{(p)}}{d} & & & \\
& & & & & 1 & & \\
& & & & & & \ddots & \\
& & & & & & & 1
\end{pmatrix}
$$

On vérifie aisément que cette matrice est de déterminant 1, donc est inversible. On pose alors

$$
B^{(p+1)} = PB^{(p)} = \begin{pmatrix}
d & * & * & * \\
b_{21}^{(p)} & \cdots & \cdots & b_{2n}^{(p)} \\
\vdots & & & \vdots \\
b_{i-1,1}^{(p)} & \cdots & \cdots & b_{i-1,n}^{(p)} \\
0 & * & * & * \\
b_{i+1,1}^{(p)} & \cdots & \cdots & b_{i+1,n}^{(p)} \\
\vdots & & & \vdots \\
b_{m1}^{(p)} & \cdots & \cdots & b_{mn}^{(p)}
\end{pmatrix}
$$

Notons que par cette étape, $b_{11}^{(p+1)}$ divise strictement $b_{11}^{(p)}$ (*ie* ne lui est pas associé).

2) On suppose maintenant que $b_{11}^{(p)}$ divise tous les coefficients de la première colonne. S'il divise également tous les coefficients de la première ligne, on passe à l'étape 3. Sinon, on fait des opérations similaires à l'étape précédente, en multipliant cette fois à droite par la transposée Q d'une matrice du même type que la matrice P définie ci-dessus. Par cette étape, on a également que $b_{11}^{(p+1)}$ divise strictement $b_{11}^{(p)}$. (Il est possible de devoir repasser par l'étape 1 à l'issue de celle-ci.)

3) On suppose qu'on est dans le cas où $b_{11}^{(p)}$ divise tous les coefficients de la première ligne et de la première colonne. Si $b_{11}^{(p)}$ divise tous les coefficients de la matrice, on passe à l'étape suivante. Sinon, soit $b_{ij}^{(p)}$ non multiple de $b_{11}^{(p)}$. Soit a tel que $ab_{i1}^{(p)} = b_{11}^{(p)}$. Soit

alors R la matrice

$$\begin{array}{c} \\ \\ \\ \\ \\ i \rightarrow \\ \\ \\ \\ \\ \end{array} \begin{pmatrix} a+1 & & & & -1 & & & \\ & 1 & & & & & & \\ & & \ddots & & & & & \\ & & & 1 & & & & \\ 1 & & & & 0 & & & \\ & & & & & 1 & & \\ & & & & & & \ddots & \\ & & & & & & & 1 \end{pmatrix}$$

Cette matrice est de déterminant 1, donc inversible. La matrice $RB^{(p)}$ a, d'une part, son coefficient $(1,1)$ égal à $b_{11}^{(p)}$, d'autre part, son coefficient $(1,j)$ égal à $(a+1)b_{1j}^{(p)} - b_{ij}^{(p)}$ qui n'est pas un multiple de $b_{11}^{(p)}$, car $(a+1)b_{1j}^{(p)}$ l'est et $b_{ij}^{(p)}$ ne l'est pas. On applique alors à $RB^{(p)}$ le même traitement qu'en 2, obtenant ainsi la matrice $B^{(p+1)}$ de la forme $RB^{(p)}Q$. Par cette étape 3, une fois encore, $b_{11}^{(p+1)}$ divise strictement $b_{11}^{(p)}$. (Il est possible de devoir repasser par les étapes 1 et 2 à l'issue de celle-ci.)

4) Enfin, si on est dans la situation où $b_{11}^{(p)}$ divise tous les coefficients de la matrice $B^{(p)}$, on interrompt l'algorithme (en fait, on pose $B^{(p+1)} = B^{(p)}$, et en particulier, $b_{11}^{(p+1)} = b_{11}^{(p)}$).

Terminaison de l'algorithme. Pour montrer que l'algorithme se termine, c'est-à-dire que l'on arrive à l'étape 4, nous allons nous intéresser à la suite d'idéaux $(b_{11}^{(p)})$. Remarquons que cette suite d'idéaux est croissante, puisque pour tout p, $b_{11}^{(p+1)} | b_{11}^{(p)}$. De plus, tant que n'est pas arrivé à l'étape 4, c'est-à-dire que l'on passe par les étapes 1, 2 et 3, l'inclusion $(b_{11}^{(p)}) \subset (b_{11}^{(p+1)})$ est stricte. Or, un anneau principal est en particulier noethérien, c'est-à-dire que toute suite croissante d'idéaux est stationnaire. Elle n'est donc pas strictement croissante, et donc on arrive à l'étape 4.

Enfin, il nous reste à terminer la démonstration du résultat. Nous avons obtenu une matrice $\tilde{B}$ équivalente à B telle que $\tilde{b}_{11}$ divise tous les coefficients de $\tilde{B}$. En ajoutant aux lignes 2 à m (puis, resp., aux colonnes 2 à n) un multiple convenable de la première ligne (resp. la première colonne), on obtient ainsi une matrice équivalente à $\tilde{B}$, donc à B, de la forme

$$\begin{pmatrix} d_1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & B' & \\ 0 & & & \end{pmatrix}$$

où d_1 divise tous les coefficients de B'. Une simple récurrence sur $\min(m,n)$ nous permet alors de conclure. Si $\min(m,n) = 1$, alors B' est vide, il n'y a plus rien à faire.

Sinon, on applique l'hypothèse de récurrence à B' : $B' = P'D'Q'$ avec D' de taille $(m-1) \times (n-1)$, de coefficients « diagonaux » non nuls $d_2 | \cdots | d_r$. Le fait que b divise tous les coefficients de B' assure qu'elle divise aussi les coefficients de D' qui sont combinaison linéaire de ceux de B'. Donc $d_1 | d_2 | \cdots | d_r$, et B est équivalente à

$$\begin{pmatrix} d_1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & D' & \\ 0 & & & \end{pmatrix}$$

ce qui conclut.