1 Facteurs invariants d'une matrice

THÉORÈME. *Soit A un anneau principal et $M \in \mathcal{M}_{m\times n}(A)$ (où m, $n \in \mathbb{N}^*$). Il existe alors une suite $(d_1, ..., d_s)$ d'éléments de A vérifiant $d_1|...|d_s$ tels que M soit équivalente à la matrice diagonale de coefficients diagonaux $(d_1, ..., d_s)$. Les d_i sont uniques à inversibles près, ils sont appelés facteurs invariants de la matrice M.*

Preuve.
Nous allons faire une preuve algorithmique dans le cas où A est un anneau euclidien. Cette preuve se généralise de manière non constructive dans le cas où A est seulement supposé principal. On note φ le stathme de A.

Étape 0. Si M est la matrice nulle, l'algorithme est terminé.

Étape 1. Sinon, ramener le coefficient non nul de stathme minimale en haut à gauche de la matrice par une permutation de ligne et de colonne.

Étape 2 : Traitement de la première colonne. On commence par m_{21} ($i \leftarrow 2$).
a) On effectue la division euclidienne de m_{i1} par m_{11} : $m_{i1} = qm_{11} + r$ avec $r = 0$ ou $\varphi(r) < \varphi(m_{11})$. On soustrait q fois la ligne L_1 à la ligne L_i.
b) Si $r \neq 0$, on échange les lignes L_1 et L_i et on retourne en 2.a).
c) Si $r = 0$ et $i < m$, on passe à la ligne suivante ($i \leftarrow i + 1$) et on recommence en 2.a).
d) Si $r = 0$ et $i = m$, on passe à l'étape 3.

Étape 3 : Traitement de la première ligne. À ce stade de l'algorithme, la première colonne est nulle à l'exception du premier coefficient.

On commence par m_{12} ($j \leftarrow 2$).
a) On effectue la division euclidienne de m_{1j} par m_{11} : $m_{1j} = qm_{11} + r$ avec $r = 0$ ou $\varphi(r) < \varphi(m_{11})$. On soustrait q fois la colonne C_1 à la colonne C_j.
b) Si $r \neq 0$, on échange les colonnes C_1 et C_j et on retourne en 2.
c) Si $r = 0$ et $j < n$, on passe à la colonne suivante ($j \leftarrow j + 1$) et on recommence en 3.a).
d) Si $r = 0$ et $j = n$, on passe à l'étape 4.

Étape 4. À ce stade de l'algorithme, la première colonne et la première ligne sont nulles à l'exception du premier coefficient. S'il existe m_{ij} tel que m_{11} ne divise pas m_{ij} (avec i, $j \geqslant 2$), on ajoute la colonne C_j à la colonne C_1 et on retourne à l'étape 2. Sinon, on retourne à l'étape 0. avec la matrice extraite $(m_{ij})_{2\leqslant i,j}$.

L'algorithme se termine grâce à la décroissance de $\varphi(m_{11})$. Cette décroissance est stricte à chaque « retour en arrière ».

Montrons maintenant l'unicité, à inversibles près, de la suite $(d_1, ..., d_s)$. Pour une matrice $U \in \mathcal{M}_{m\times n}(A)$, on note $\Lambda_j(U) = \text{pgcd}\{\Delta_j, \Delta_j \text{ mineur de taille } j \text{ de U}\}$. Dans le cas où U est diagonale, on a $\Lambda_j(U) = d_1...d_j$, les idéaux (d_j) sont donc uniquement déterminés par les idéaux (Λ_j). Ils nous suffit donc de montrer que deux matrices équivalentes U et U' ont les

mêmes idéaux (Λ_j).

Supposons d'abord que $U = PU'$ avec $P \in \mathrm{GL}_m(A)$. Les lignes de U sont combinaisons linéaires des lignes de U'. Par multilinéarité du déterminant, un mineur de taille j de U est combinaison linéaire de mineurs de taille j de U', si bien que $(\Lambda_j(U)) \subset (\Lambda_j(U'))$. Comme on a aussi $U' = P^{-1}U$, on obtient de même $(\Lambda_j(U')) \subset (\Lambda_j(U))$, si bien que $(\Lambda_j(U)) = (\Lambda_j(U'))$. On montre de la même manière que si $U = U'Q$ avec $Q \in \mathrm{GL}_n(A)$, on a $(\Lambda_j(U')) = (\Lambda_j(U))$. On déduit de ces deux résultats que si $U = PU'Q$, alors $(\Lambda_j(U')) = (\Lambda_j(U))$, ce qu'il fallait.

□

Corollaire (Théorème de la base adaptée)**.** *Soit A un anneau principal et M un A-module libre de rang n. Si N est un sous-module de M, il existe une base $(e_1, ..., e_n)$ de M et des scalaires non nuls d_1, ..., d_s, uniques à inversibles près, vérifiant $d_1|...|d_s$ et tels que la famille $(d_1e_1, ..., d_se_s)$ soit une base de N.*

Preuve.
On admet ici qu'un sous-module d'un module libre de rang fini est également libre de rang fini.

Soit donc $(v_1, ..., v_m)$ une base de N et $(u_1, ..., u_n)$ une base de M. On écrit U la matrice dans les bases (v_i) et (u_i) de l'injection canonique de N dans M.

D'après le théorème précédent, cette matrice est équivalente à une matrice diagonale U', de coefficients diagonaux non nuls d_1, ..., d_s, tels que $d_1|...|d_s$.

Cela signifie précisément qu'il existe une base $(e_1, ..., e_n)$ de M et une base $(f_1, ..., f_m)$ de N telles que $\mathrm{id}(f_i) = d_ie_i$ pour $i \leqslant s$ et $\mathrm{id}(f_i) = 0$ pour $i > s$. On voit tout de suite que l'on a $s = n$, car cette dernière éventualité est exclue.

Le théorème précédent donne également l'unicité des d_i, à inversibles près.

□

Corollaire (Théorème de structure)**.** *Soit M un module de type fini sur un anneau principal A. Il existe un entier $n \in \mathbb{N}$ (appelé rang de M) et une suite de scalaires non nuls $d_1|...|d_s$, uniques à inversibles près (appelés facteurs invariants de M), tels que $M \simeq A^n \oplus A/(d_1) \oplus ... \oplus A/(d_s)$.*

Preuve.
Le module M étant de type fini, on dispose d'un morphisme surjectif $\varphi : A^m \to M$ (où $m \in \mathbb{N}$).

D'après le théorème précédent, il existe une base $(e_1, ..., e_m)$ de A^m et une suite de scalaires non nuls $d_1|...|d_s$ uniques à inversibles près, tels que $(d_1e_1, ..., d_se_s)$ soit une base de $\mathrm{Ker}\varphi$.

On a alors $M \simeq A^m/\mathrm{Ker}\varphi$ soit $M \simeq A^m/\bigoplus d_ie_i$ et par une identification classique $M \simeq A^n \oplus \bigoplus d_ie_i$, où $n = m - s$. L'unicité découle du théorème précédent.

□

Leçons possibles
109 Anneaux Z/nZ. Applications.
111 Exemples d'applications des idéaux d'un anneau commutatif unitaire.
122 Opérations élémentaires sur les lignes et les colonnes d'une matrice. Résolution d'un système d'équations linéaires. Exemples et applications.
146 Anneaux principaux.
121 Matrices équivalentes. Matrices semblables. Applications.

Références
[BMP05] pp. 285 et suivantes.