Prérequis. Aucun.

Théorème 0.0.1. *Soient A un anneau euclidien et M une matrice à coefficients dans A. Alors il existe une famille $(d_1, \ldots, d_s)$ d'éléments non nuls de A avec $d_s | \ldots | d_1$, telle que M soit équivalente à :*

$$\begin{pmatrix} d_s & \ldots & 0 & 0 & \ldots & 0 \\ \vdots & \ddots & \vdots & \vdots & & \vdots \\ 0 & \ldots & d_1 & 0 & \ldots & 0 \\ 0 & \ldots & 0 & 0 & \ldots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \ldots & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Cette famille est unique à association près.

Démonstration. On décrit un algorithme pour passer de M à sa forme normale de Smith. Le résultat reste vrai si A est seulement principal, mais alors on n'a plus d'algorithme.

1. Si $U = 0$ on s'arrête.

2. Permuter des lignes et colonnes pour placer l'élément de stathme minimal tout en haut à gauche.

3. On traite la première colonne.

3a. Effectuer la division euclidienne de $m_{i,1}$ par $m_{1,1}$:

$$m_{i,1} = q m_{1,1} + r_1$$

et soustraire q fois la première ligne à la i-ème.

3b. Si $r_i \neq 0$, échanger les lignes 1 et i, et retourner en 3a.

3c. Si $r_i = 0$ et i n'était pas la dernière ligne, faire $i \leftarrow i + 1$ et retourner en 3a.

3d. Si $r_i = 0$ et i était la dernière ligne, passer à l'étape 4.

4. Ici, tous les coefficients sous le premier sont nuls dans la première colonne. On traite la première ligne.

4a. Effectuer la division euclidienne de $m_{1,j}$ par $m_{1,1}$:

$$m_{1,j} = q m_{1,1} + s_j$$

et soustraire q fois la première colonne à la j-ème.

4b. Si $s_j \neq 0$, échanger les colonnes 1 et j, pleurer un bon coup, et retourner en 3.

4c. Si $s_j = 0$ et j n'était pas la dernière colonne, faire $j \leftarrow j + 1$ et retourner en 4a.

4d. Si $s_j = 0$ et j était la dernière colonne, passer à l'étape 5.

5. Ici, tous les coefficients de la première ligne et tous les coefficients de la première colonne sont nuls, sauf celui en haut à gauche.

5a. Si $m_{1,1}$ ne divise pas tous les coefficients de la sous-matrice en bas à droite, disons qu'un tel coefficient se trouve sur la colonne $j_{\text{putain de bordel de merde}}$. Ajouter la $j_{\text{putain de bordel de merde}}$-ème colonne à la première et retourner à l'étape 3.

5b. Recommencer à l'étape 1 avec la sous-matrice en bas à droite.

Maintenant, il faut montrer que l'algorithme termine, qu'il est correct, et l'unicité des facteurs invariants.

L'algorithme termine. Le stathme de $m_{1,1}$ décroît strictement à chaque retour en arrière dans l'algorithme.

L'algorithme est correct. Chaque étape de l'algorithme est une opération élémentaire sur les lignes ou les colonnes, donc la matrice que l'on obtient à la fin est bien équivalente à M. Ensuite, elle est bien de la forme attendue puisque l'on ne passe, en étape 5b, à la sous-matrice en bas à droite que lorsque le coefficient en haut à gauche est tout seul, et l'on a le droit d'atteindre 5b que si ce coefficient divise tous les coefficients de la sous-matrice en bas à droite. Donc les d_i se divisent les uns les autres.

Unicité des facteurs invariants à association près. Notons $I_k(M)$ l'idéal de A engendré par les mineurs de taille k de M. Un calcul direct montre que $I_k(PM) \subset I_k(M)$, et de même $I_k(MQ) \subset I_k(M)$. Ainsi si M' est équivalente à M alors on a d'une part $I_k(M') \subset I_k(M)$ et d'autre part $I_k(M) \subset I_k(M')$. Finalement, $I_k(M)$ reste constant au cours de l'algorithme. Une fois terminé, l'algorithme donne :

$$I_k(M) = \langle d_s d_{s-1} \cdot \ldots \cdot d_{s-k+1} \rangle.$$

Ainsi si l'on dispose d'autres facteurs invariants $(d'_s, \ldots, d'_1)$, alors :

$$\begin{aligned} \langle d_s \rangle &= \langle d'_s \rangle \\ \langle d_s d_{s-1} \rangle &= \langle d'_s d'_{s-1} \rangle \\ \langle d_s d_{s-1} d_{s-2} \rangle &= \langle d'_s d'_{s-1} d'_{s-2} \rangle \\ \ldots &= \ldots \end{aligned}$$

La première égalité montre que d_s et d'_s sont associés, puis la seconde montre que d_{s-1} et d'_{s-1} sont associés, et ainsi de suite. □

Remarques.

— Il faut absolument présenter ce développement comme un algorithme, et ne pas présenter d'étape qui soit abstraite. Il faut qu'on comprenne que l'on est capable de calculer cette forme normale à la main si l'on veut.

— Dans la même lignée, il faut absolument savoir exécuter cet algorithme sur un exemple simple (disons, une matrice 3×3). Sinon, on présente un truc qu'on ne connaît pas bien.

— C'est mieux, quand on met ce développement dans une leçon, de l'accompagner de quelques unes au moins de ses innombrables et monstrueuses conséquences. Classification des groupes abéliens de type fini et de manière générale, des modules de type fini sur un anneau principal, réduction de Frobenius, théorème de Jordan, théorème de Cayley-Hamilton, ... Faire une sous-partie ou une partie à propos des modules de type fini sur les anneaux principaux (ou euclidiens) montre que l'on a vraiment compris l'essence de ce théorème.

Recasages.

— 122 : Parfait, pour faire une partie sur les modules de type fini sur les anneaux principaux notamment. Il peut convenir tout seul, mais c'est vraiment moins bien.

— 142 : Au final, on fait tellement de divisions euclidiennes qu'on peut se demander si l'on n'a pas calculé plein de pgcds. La réponse est si bien sûr, puisque le coefficient en haut à gauche est le pgcd des coefficients de M. Et de manière générale le produit des k premiers coefficients est le pgcd des mineurs de taille k de M, c'est d'ailleurs ce que l'on démontre quand on montre l'unicité des facteurs invariants. D'ailleurs, ça permet de trouver les facteurs invariants d'une matrice 2×2 sans avoir à réfléchir ni à exécuter l'algorithme.

— 162 : La forme normale de Smith peut être utile pour résoudre des systèmes $\mathbf{Z}$-linéaires. C'est exactement l'analogue du pivot de Gauss sur des anneaux euclidiens au lieu des corps, et donc ça résout le même genre de problèmes. En plus il y a *opérations élémentaires* dans le titre de la leçon.