

Devoir maison n°2

À rendre le 2 décembre

Soient $m, n \in \mathbf{N}_{>0}$. Le but du problème est de préciser les résultats du cours concernant $\mathbf{M}_{n \times m}(\mathbf{Z})$, en s'intéressant notamment aux aspects *effectifs* : pour chaque question, il faut justifier que les constructions sont calculables algorithmiquement à partir de la division euclidienne. Il n'est pas demandé de calculer la complexité des algorithmes¹.

Si $M_1, M_2 \in \mathbf{M}_{n \times m}(\mathbf{Z})$, on écrit $M_1 \equiv M_2$ (resp. $M_1 \sim M_2$) s'il existe $P \in \mathbf{GL}_n(\mathbf{Z})$ (resp. $(P, Q) \in \mathbf{GL}_n(\mathbf{Z}) \times \mathbf{GL}_m(\mathbf{Z})$) tel que $M_2 = PM_1$ (resp. $M_2 = PM_1Q^{-1}$). Cela définit deux relations d'équivalence² sur $\mathbf{M}_{n \times m}(\mathbf{Z})$.

(1) Soient $a, b \in \mathbf{Z}$ non tous les deux nuls et d leur pgcd. Rappeler l'algorithme d'Euclide étendu, qui fournit des éléments $u, v \in \mathbf{Z}$ tels que $au + bv = d$. En déduire un élément $P \in \mathbf{SL}_2(\mathbf{Z})$ tel que $P \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} d \\ 0 \end{pmatrix}$.

(2) Plus généralement, si $a_1, \dots, a_n \in \mathbf{Z}$ sont non tous nuls et $d = \text{pgcd}(a_1, \dots, a_n)$, construire algorithmiquement $P \in \mathbf{GL}_n(\mathbf{Z})$ telle que $P \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} d \\ 0 \\ \vdots \\ 0 \end{pmatrix}$. Appliquer cet algorithme pour construire $P \in \mathbf{GL}_3(\mathbf{Z})$ telle que $P \begin{pmatrix} 6 \\ 10 \\ 15 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$.

Soit $M = (a_{i,j})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} \in \mathbf{M}_{n \times m}(\mathbf{Z})$. Pour $i \in \{1, \dots, n\}$, notons $p_M(i)$ le plus petit indice $j \in \{1, \dots, m\}$ tel que $a_{i,j} \neq 0$ (avec la convention $p_M(i) = \infty$ si la i -ème ligne de M est nulle). On dit que M est *échelonnée* suivant les lignes lorsque $p_M(i) = \infty$ ou $p_M(i-1) < p_M(i)$ pour tout $i \in \{2, \dots, n\}$. Elle est dite *échelonnée réduite* si en outre pour tout $i \in \{1, \dots, r\}$, on a $a_{i,p_M(i)} > 0$ et $k \in \{1, \dots, i-1\} \Rightarrow 0 \leq a_{k,p_M(i)} < a_{i,p_M(i)}$, où r est le nombre de lignes non nulles de M .

(3) (a) Montrer qu'on peut construire algorithmiquement $P \in \mathbf{GL}_n(\mathbf{Z})$ telle que PM soit échelonnée.

(b) Montrer qu'on peut construire algorithmiquement $P \in \mathbf{GL}_n(\mathbf{Z})$ telle que PM soit échelonnée réduite. Appliquer l'algorithme à la matrice $M = \begin{pmatrix} 4 & 6 & 11 & 22 \\ 8 & 12 & 10 & 31 \\ 18 & 27 & 27 & 74 \end{pmatrix}$.

(4) (Plus difficile) Soient $M_1, M_2 \in \mathbf{M}_{n \times m}(\mathbf{Z})$ échelonnées réduites telles que $M_2 \equiv M_1$. Montrer que $M_1 = M_2$ (procéder par récurrence sur n).

Ce qui précède montre que si $M \in \mathbf{M}_{n \times m}(\mathbf{Z})$, il existe $\widetilde{M} \in \mathbf{M}_{n \times m}(\mathbf{Z})$ échelonnée réduite *unique* telle que $\widetilde{M} \equiv M$. Cette dernière s'appelle la *forme normale de Hermite* de M . On s'en doute, ce qui précède est utile pour résoudre les systèmes linéaires à coefficients entiers (du type $MX = Y$ avec $X \in \mathbf{Z}^m$ et $Y \in \mathbf{Z}^n$), en particulier pour déterminer le noyau et l'image d'un morphisme de groupes $\mathbf{Z}^m \rightarrow \mathbf{Z}^n$, chercher une base adaptées à des sous-modules dans un \mathbf{Z} -module libre de rang fini, *etc.*

1. Encore moins que ces derniers soient performants

2. Associées aux actions de $\mathbf{GL}_n(\mathbf{Z})$ (resp. $\mathbf{GL}_n(\mathbf{Z}) \times \mathbf{GL}_m(\mathbf{Z})$) sur $\mathbf{M}_{n \times m}(\mathbf{Z})$ données par $(P, M) \mapsto PM$ (resp. $((P, Q), M) \mapsto PMQ^{-1}$) pour $P \in \mathbf{GL}_n(\mathbf{Z})$, $Q \in \mathbf{GL}_m(\mathbf{Z})$ et $M \in \mathbf{M}_{n \times m}(\mathbf{Z})$.

(5) Soit $M = (a_{i,j})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} \in \mathbf{M}_{n \times m}(\mathbf{Z})$. On pose $\delta(M) = \max \left\{ \max_{1 \leq i \leq n} |a_{i,1}|, \max_{1 \leq j \leq m} |a_{1,j}| \right\}$ (la plus grande valeur absolue des coefficients de la première ligne et de la première colonne de M).

(a) Montrer qu'on peut calculer algorithmiquement $P \in \mathbf{GL}_n(\mathbf{Z})$ et $Q \in \mathbf{GL}_m(\mathbf{Z})$ telles que $PMQ^{-1} = (b_{i,j})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}}$ vérifie $i > 1 \Rightarrow b_{i,1} = 0$ et $j > 1 \Rightarrow b_{1,j} = 0$ [indication : effectuer des opérations sur les lignes et les colonnes de M de façon à réduire la quantité $\delta(M)$ au maximum].

(b) Montrer qu'on peut calculer algorithmiquement $P \in \mathbf{GL}_n(\mathbf{Z})$ et $Q \in \mathbf{GL}_m(\mathbf{Z})$ telles que PMQ^{-1} soit diagonale.

(6) Soient $a, b \in \mathbf{Z}$ non tous les deux nuls. Posons $d = \text{pgcd}(a, b)$ et $m = \text{ppcm}(a, b)$. Soient $u, v \in \mathbf{Z}$ tel que $au + bv = d$. Écrivons $a = d\alpha$ et $b = d\beta$. Calculer le produit $\begin{pmatrix} u & v \\ -\beta & \alpha \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \begin{pmatrix} 1 & -\beta v \\ & \alpha u \end{pmatrix}$.

(7) En déduire que si $M \in \mathbf{M}_{n \times m}(\mathbf{Z})$, on peut construire algorithmiquement $P \in \mathbf{GL}_n(\mathbf{Z})$ et $Q \in \mathbf{GL}_m(\mathbf{Z})$ telles que $\widehat{M} = PMQ^{-1} = \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_r \end{pmatrix}$ où $d_1, \dots, d_r \in \mathbf{N}_{>0}$ et $d_k \mid d_{k+1}$ pour tout $k \in \{1, \dots, r-1\}$. Appliquer l'algorithme à la matrice $M = \begin{pmatrix} 4 & 6 & 11 & 22 \\ 8 & 12 & 10 & 31 \\ 18 & 27 & 27 & 74 \end{pmatrix}$.

On a vu en cours que les entiers d_1, \dots, d_r sont uniques. La matrice \widehat{M} s'appelle la *forme normale de Smith* de M : elle est unique d'après ce qui précède³.

On s'en doute, hormis celui de la question (3) (b), les algorithmes qui précèdent s'étendent en remplaçant \mathbf{Z} par un anneau euclidien⁴. C'est aussi le cas de celui de la question (3) (b), sous réserve qu'on sache définir convenablement la notion de matrice échelonnée *réduite*.

(8) Définir la notion de matrice échelonnée réduite dans le cas où $A = K[X]$ (où K est un corps).

3. Cela redémontre de façon effective le fait, vu en cours, que les matrices sous forme normale de Smith constituent un système complet de représentants de $\mathbf{M}_{n \times m}(\mathbf{Z})$ pour la relation d'équivalence \sim .

4. Rappelons qu'il s'agit d'un anneau A intègre pour lequel il existe une application $\varphi: A \setminus \{0\} \rightarrow \mathbf{N}$ telle que pour tout $(a, b) \in A \times A \setminus \{0\}$, il existe $q, r \in A$ tels que $a = bq + r$ avec $r = 0$ ou $\varphi(r) < \varphi(b)$ (une telle (on ne requiert pas l'unicité du couple (q, r)). Les exemples à garder à l'esprit sont $A = \mathbf{Z}$ avec $\varphi(a) = |a|$ pour tout $a \in \mathbf{Z} \setminus \{0\}$ et $A = K[X]$ (où K est un corps) avec $\varphi(P) = \deg(P)$ pour tout $P \in K[X] \setminus \{0\}$.