Devoir facultatif n° 12

Ce problème étudie certaines propriétés des matrices à coefficients entiers. Les parties **II** et **III** sont indépendantes et chacune utilise des résultats de la partie **I**.

Notations.

Dans tout le problème, n et p désignent des entiers supérieurs ou égeux à deux.

- On note $\mathscr{M}_{n,p}(\mathbb{Z})$ l'ensemble des matrices à n lignes et p colonnes, à coefficients dans $\mathbb{Z}$.
- On note $\mathscr{M}_n(\mathbb{Z})$ l'ensemble des matrices carrées d'ordre n à coefficients dans $\mathbb{Z}$.
- On note $\mathscr{GL}_n(\mathbb{Z})$ l'ensemble des matrices inversibles de $\mathscr{M}_n(\mathbb{Z})$, dont l'inverse est dans $\mathscr{M}_n(\mathbb{Z})$.
- On dit que deux matrices A et B de $\mathscr{M}_n(\mathbb{Z})$ sont $\mathbb{Z}$-équivalentes s'il existe $P, Q \in \mathscr{GL}_n(\mathbb{Z})$ telles que $B = PAQ$.
- On considère sur $\mathscr{M}_n(\mathbb{Z})$ trois opérations élémentaires sur les lignes d'une matrice :
  - $L_i \leftarrow -L_i$ qui transforme L_i en son opposé ;
  - $L_i \leftrightarrow L_j$ qui échange les lignes L_i et L_j ;
  - $L_i \leftarrow L_i + \lambda L_j$ qui ajoute λ fois la ligne L_j à la ligne L_i, avec $\lambda \in \mathbb{Z}$.
- On définit de même les mêmes opérations élémentaires sur les colonnes.
- Pour des entiers $a_1, \dots, a_n$, on définit $\operatorname{diag}(a_1, \dots, a_n) = \begin{pmatrix} a_1 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & a_n \end{pmatrix}$.
- On dit qu'une matrice $A \in \mathscr{M}_{n,p}(\mathbb{Z})$ est dite *échelonnée* (par lignes) si, pour toute ligne, le premier coefficient non nul de cette ligne est strictement à droite du premier coefficient non nul de la ligne précédente.
  Plus formellement, en notant $p(i) = \min \{ j \in [\![1, p]\!] \mid a_{i,j} \neq 0 \}$ (avec $p(i) = +\infty$ si cet ensemble est vide), on demande à ce que pour tout $1 \leqslant i < n$, $p(i) < p(i+1)$.

Partie I : Généralités.

1) Une matrice inversible à coefficients entiers est-elle nécessairement dans $\mathscr{GL}_n(\mathbb{Z})$?

2) Montrer que $(\mathscr{GL}_n(\mathbb{Z}), \times)$ est un groupe. Est-il commutatif ?

3) Montrer que « A est $\mathbb{Z}$-équivalente à B » est une relation d'équivalence sur $\mathscr{M}_n(\mathbb{Z})$.

4) Montrer que, si $A \in \mathscr{M}_n(\mathbb{Z})$, alors $\det A \in \mathbb{Z}$.

5) Montrer que, si $A \in \mathscr{GL}_n(\mathbb{Z})$, alors $\det A \in \{-1; +1\}$.

6) Montrer réciproquement que, si $A \in \mathscr{M}_n(\mathbb{Z})$ vérifie $\det A \in \{-1; +1\}$, alors $A \in \mathscr{GL}_n(\mathbb{Z})$.

7) Soit $A \in \mathscr{M}_n(\mathbb{Z})$. Montrer que toute matrice déduite de A par opérations élémentaires sur ses lignes ou ses colonnes est $\mathbb{Z}$-équivalente à A.

Partie II : Échelonnement de matrice à coefficients entiers.

8) Soit $a, b \in \mathbb{Z}$, notons $d = \mathrm{PGCD}(a, b)$ et $a = da'$, $b = db'$. En utilisant des relations de Bézout, montrer qu'il existe $M \in \mathscr{GL}_2(\mathbb{Z})$ telle que

$$M \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} d \\ 0 \end{pmatrix}.$$

9) Soit $a_1, \ldots, a_n \in \mathbb{Z}$, notons $d = \mathrm{PGCD}(a_{n-1}, a_n)$. Montrer qu'il existe $M \in \mathscr{GL}_n(\mathbb{Z})$ telle que

$$M \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} a_1 \\ \vdots \\ a_{n-2} \\ d \\ 0 \end{pmatrix}.$$

10) Soit $a_1, \ldots, a_n \in \mathbb{Z}$, notons $d = \mathrm{PGCD}(a_1, \ldots, a_n)$. Montrer qu'il existe $M \in \mathscr{GL}_n(\mathbb{Z})$ telle que

$$M \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} d \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

11) Soit $A \in \mathscr{M}_{n,p}(\mathbb{Z})$, écrite par blocs $A = \begin{pmatrix} E & B \\ 0 & C \end{pmatrix}$, où E est échelonnée, carrée de taille ℓ, avec $\ell \leqslant \min(n, p)$. Soit $M \in \mathscr{GL}_{n-\ell}(\mathbb{Z})$ et $d = \mathrm{PGCD}(a_{\ell+1,\ell+1}, \ldots, a_{n,\ell+1})$ tels que

$$M \begin{pmatrix} a_{\ell+1,\ell+1} \\ \vdots \\ a_{n,\ell+1} \end{pmatrix} = \begin{pmatrix} d \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Que peut-on dire du produit $\begin{pmatrix} \mathrm{I}_\ell & 0_{\ell,n-\ell} \\ 0_{n-\ell,\ell} & M \end{pmatrix} \times A$?

12) En déduire que, pour tout $A \in \mathscr{M}_{n,p}(\mathbb{Z})$, il existe $P \in \mathscr{GL}_n(\mathbb{Z})$ tel que PA est échelonnée.

13) Application. On cherche à résoudre sur $\mathbb{Z}^3$ l'équation diophantienne

$$2x + 3y + 5z = 0, \qquad (\mathscr{E})$$

que l'on écrit $XA = 0$, avec $X = \begin{pmatrix} x & y & z \end{pmatrix}$ et $A = \begin{pmatrix} 2 \\ 3 \\ 5 \end{pmatrix}$. On note $B = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$.

a) Déterminer une matrice $M \in \mathscr{GL}_3(\mathbb{Z})$ telle que $MA = B$.

b) En déduire que $(\mathscr{E})$ est équivalente à une équation de la forme $YB = 0$, où l'on précisera Y.

c) Donner l'ensemble des solutions $Y \in \mathscr{M}_{1,3}(\mathbb{Z})$ de l'équation précédente et en déduire l'ensemble des solutions de $(\mathscr{E})$.

Partie III : Réduction sous forme normale de Smith.

Soit $A \in \mathscr{M}_n(\mathbb{Z})$ non nulle. On note $\mathscr{A}$ l'ensemble des matrices $\mathbb{Z}$-équivalentes à A dont le coefficient supérieur gauche est strictement positif :

$$\mathscr{A} = \{\, B \in \mathscr{M}_n(\mathbb{Z}) \mid b_{1,1} > 0 \text{ et } \exists P, Q \in \mathscr{GL}_n(\mathbb{Z}),\ B = PAQ \,\}.$$

Soit $B \in \mathscr{A}$ tel que $b_{1,1}$ soit minimal : pour tout $B' \in \mathscr{A}$, $b'_{1,1} \geqslant b_{1,1}$. On pose $d = b_{1,1}$.

14) Justifier l'existence d'un tel B.

15) Montrer que, pour tout $2 \leqslant i \leqslant n$, d divise $b_{i,1}$.

16) Montrer qu'il existe $C \in \mathscr{M}_n(\mathbb{K})$ telle que :

— $C = \begin{pmatrix} d & 0 & \dots & 0 \\ 0 & c_{2,2} & \dots & c_{2,n} \\ \vdots & \vdots & & \vdots \\ 0 & c_{n,2} & \dots & c_{n,n} \end{pmatrix}$;

— C est $\mathbb{Z}$-équivalente à A.

17) Montrer que d divise tous les coefficients de la matrice C précédente.

18) En déduire qu'il existe des entiers naturels $d_1, \dots, d_p$ non nuls tels que $D = \mathrm{diag}(d_1, \dots, d_p, 0, \dots, 0)$ est $\mathbb{Z}$-équivalente à A et $d_1 | d_2 | \dots | d_p$.

— FIN —