# DM 10 - Matrices à coefficients entiers

On étudie dans ce problème divers aspects des matrices carrées à coefficients entiers.

Dans la partie 1, on introduit l'anneau $\mathscr{M}_n(\mathbb{Z})$ et son groupe des inversibles $\mathrm{GL}_n(\mathbb{Z})$, et on donne des exemples de sous-groupes finis de $\mathrm{GL}_n(\mathbb{Z})$. Dans la partie 2, on montre que l'ordre des matrices d'ordre fini de $\mathrm{GL}_2(\mathbb{Z})$ ne peut prendre qu'un petit nombre de valeurs. Dans la partie 3, on montre qu'il existe une majoration uniforme du cardinal des sous-groupes finis de $\mathrm{GL}_n(\mathbb{Z})$.

On introduit les notations suivantes, pour tous $n, N \in \mathbb{N}^*$ :

- $\mathscr{M}_n(\mathbb{Z})$ est l'ensemble des matrices carrées de taille $n$, à coefficients entiers ;
- $\mathrm{GL}_n(\mathbb{Z})$ est le groupe des inversibles de l'anneau $\mathscr{M}_n(\mathbb{Z})$ ;
- $N\mathscr{M}_n(\mathbb{Z}) = \left\{N \times A, A \in \mathscr{M}_n(\mathbb{Z})\right\}$ ; c'est l'ensemble des matrices de $\mathscr{M}_n(\mathbb{Z})$ dont tous les coefficients sont divisibles par $N$.

## 1 Généralités et exemples

On fixe un entier $n \geq 2$.

1. Vérifier que $\mathscr{M}_n(\mathbb{Z})$ est un sous-anneau de $\mathscr{M}_n(\mathbb{Q})$.
2. Montrer que $\mathrm{GL}_2(\mathbb{Z})$ est infini, puis que $\mathrm{GL}_n(\mathbb{Z})$ est infini.
3. Soient $M \in \mathscr{M}_n(\mathbb{Z})$ et $m \geq 1$ tel que $M^m = I_n$. Montrer que $M \in \mathrm{GL}_n(\mathbb{Z})$.
4. Montrer que $\mathrm{GL}_n(\mathbb{Z}) \subset \mathrm{GL}_n(\mathbb{Q}) \cap \mathscr{M}_n(\mathbb{Z})$ et montrer que cette inclusion est stricte.
5. Soit $M$ une matrice de $\mathscr{M}_2(\mathbb{Z})$. Montrer que $M \in \mathrm{GL}_2(\mathbb{Z})$ ssi $\det M = \pm 1$.
6. **Matrices de permutation.**
   (a) Soit $\sigma$ une permutation de $[\![1, n]\!]$. On note $P_\sigma$ la matrice $\left(\delta_{i,\sigma(j)}\right)_{1 \leq i,j \leq n}$.
   Montrer que $P_\sigma \in \mathrm{GL}_n(\mathbb{Z})$.
   (b) On note $\mathscr{S}_n$ le groupe des permutations de $[\![1, n]\!]$. Montrer que l'application
   $$\Psi : \left\{\begin{array}{ll} \mathscr{S}_n & \to \mathrm{GL}_n(\mathbb{Z}) \\ \sigma & \mapsto P_\sigma \end{array}\right.$$
   est un morphisme de groupes injectif.
7. **Groupe diédral $D_{12}$.**
   On note $\alpha = e^{\frac{i\pi}{3}}$ et $H$ l'hexagone régulier $H = \left\{\alpha^k, k \in [\![0, 5]\!]\right\}$.
   On note $D_{12}$ le sous-groupe de permutations de $H$, dont les éléments $f$ vérifient :
   $$\forall h, h' \in H, |f(h) - f(h')| = |h - h'|.$$

(a) Montrer qu'un élément $f$ de $D_{12}$ est entièrement déterminé par les images $f(1)$ et $f(\alpha)$, et que $f(1)$ et $f(\alpha)$ doivent être des sommets consécutifs de $H$.

(b) En déduire que $D_{12}$ est de cardinal 12. On décrira rapidement ses éléments.

(c) Soit $h \in H$. Montrer qu'il existe $a_h, b_h \in \mathbb{Z}$ tels que $h = a_h + b_h\alpha$.

(d) Avec les notations précédentes, montrer que[1] pour tous $h \in H, f \in D_{12}$ :

$$f(h) = a_h f(1) + b_h f(\alpha).$$

(e) Montrer que l'application $\Phi : \begin{cases} D_{12} & \to \mathrm{GL}_2(\mathbb{Z}) \\ f & \mapsto \begin{pmatrix} a_{f(1)} & a_{f(\omega)} \\ b_{f(1)} & b_{f(\omega)} \end{pmatrix} \end{cases}$ est bien définie et est un morphisme de groupes injectif.

## 2 Ordre des éléments de $\mathrm{GL}_2(\mathbb{Z})$

Si $P = \sum_{k=0}^{d} a_k X^k$ est un polynôme à coefficients réels et si $A \in \mathscr{M}_2(\mathbb{R})$, on note $P(A) = \sum_{k=0}^{d} a_k A^k$.
On pourra utiliser sans démonstration que, si $P$ et $Q$ sont deux polynômes, $(PQ)(A) = P(A)Q(A)$.

1. Soit $A \in \mathscr{M}_2(\mathbb{Z})$. On note $\operatorname{Tr} A$ la somme des coefficients diagonaux de $A$ et

$$\chi_A = X^2 - (\operatorname{Tr} A)X + \det A$$

son *polynôme caractéristique*. Montrer que $\chi_A(A) = 0$.

Soit $A \in \mathrm{GL}_2(\mathbb{Z})$ d'ordre $m$.[2]

2. Montrer que si $\lambda$ est une racine de $\chi_A$, alors il existe $V \in \mathscr{M}_{2,1}(\mathbb{C}) \setminus \{0\}$ tel que $AV = \lambda V$. En déduire que $\lambda^m = 1$.

3. En déduire que $\operatorname{Tr} A \in [\![-2, 2]\!]$.

4. On définit les polynômes

- $P_1 = (X-1)^2$ ;
- $P_2 = (X+1)^2$ ;
- $P_3 = X^2 - 1$ ;
- $P_4 = X^2 + 1$ ;
- $P_5 = X^2 - X + 1$ ;
- $P_6 = X^2 + X + 1$.

Montrer qu'il existe $i \in [\![1, 6]\!]$ tel que $\chi_A = P_i$.

5. Montrer réciproquement que chacun des $P_i$ est le polynôme caractéristique d'une matrice d'ordre fini dans $\mathrm{GL}_2(\mathbb{Z})$.

6. Montrer que si $A \in \mathrm{GL}_2(\mathbb{Z})$ est d'ordre fini, son ordre appartient à $\{1, 2, 3, 4, 6\}$.

[1] On pourra admettre que $D_{12}$ est engendré par les permutations $r : \alpha^k \mapsto \alpha^{k+1}$ et $s : \alpha^k \mapsto \alpha^{-k}$.
[2] On rappelle que $m$ est le plus petit entier $k \geq 1$ tel que $A^k = I_2$.

## 3 Sous-groupes finis de $\mathrm{GL}_n(\mathbb{Z})$

1. Soit $M \in \mathrm{GL}_n(\mathbb{Z})$, d'ordre fini $m \geq 2$. Soit $p \geq 3$ un nombre premier. On cherche à montrer que $M - I_n \notin p\mathcal{M}_n(\mathbb{Z})$. On raisonne par l'absurde.

   (a) Montrer qu'il existe $r \geq 1$ et $N \in \mathcal{M}_n(\mathbb{Z}) - p\mathcal{M}_n(\mathbb{Z})$ tels que $M = I_n + p^r N$.

   (b) En utilisant la relation $M^m = I_n$, montrer que $mp^r N \in p^{2r}\mathcal{M}_n(\mathbb{Z})$. En déduire que $p$ divise $m$.

   On note $M' = M^p$ et $m' = \dfrac{m}{p}$.

   (c) Montrer que $M'$ est d'ordre fini $m'$ et exprimer $M'$ sous la forme $M' = I_n + p^{r+1}N'$, où $N' \in \mathcal{M}_n(\mathbb{Z}) - p\mathcal{M}_n(\mathbb{Z})$.

   (d) En déduire une contradiction.

Si $M = (m_{i,j})_{1\leq i,j\leq n} \in \mathcal{M}_n(\mathbb{Z})$, on note $\overline{M}$ la matrice $(\overline{m_{i,j}})_{1\leq i,j\leq n} \in \mathcal{M}_n(\mathbb{Z}/p\mathbb{Z})$ où $\overline{k} \in \mathbb{Z}/p\mathbb{Z}$ est la classe de $k$ modulo $p$.

2. Montrer que
$$\phi_p : \begin{cases} \mathcal{M}_n(\mathbb{Z}) & \to \mathcal{M}_n(\mathbb{Z}/p\mathbb{Z}) \\ M & \mapsto \overline{M} \end{cases}$$
est un morphisme d'anneaux et qu'il induit un morphisme de groupes – encore noté $\phi_p$ – de $\mathrm{GL}_n(\mathbb{Z})$ dans $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$.

3. Soit $G$ un sous-groupe fini de $\mathrm{GL}_n(\mathbb{Z})$. Montrer que $\phi_{p|G} : G \to \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ est injectif. En déduire une constante explicite $\alpha(n)$ telle que tout sous-groupe fini de $\mathrm{GL}_n(\mathbb{Z})$ est de cardinal inférieur à $\alpha(n)$.[3]

Soit $G$ un sous-groupe fini de $\mathrm{GL}_2(\mathbb{Z})$.

4. Montrer que $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ est de cardinal 48. En admettant le théorème de Lagrange, en déduire que $|G|$ est un diviseur de 48.

5. Montrer que la matrice $A = \begin{pmatrix} \overline{0} & \overline{1} \\ \overline{1} & \overline{1} \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ est d'ordre 8. En utilisant la partie précédente, en déduire que $|G|$ est un diviseur strict de 48.[4]

[3] On ne cherchera pas à calculer le cardinal de $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$

[4] Avec un peu plus d'outils, on peut montrer que les sous-groupes finis de $\mathrm{GL}_2(\mathbb{Z})$ sont les groupes isomorphes à des sous-groupes des groupes diédraux $D_8$ et $D_{12}$. En particulier, leur cardinal divise 8 ou 12.