

DM 15 - 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 $\mathcal{M}_n(\mathbb{Z})$ 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 $n, N \in \mathbb{N}^*$:

- $\mathcal{M}_n(\mathbb{Z})$ 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 $\mathcal{M}_n(\mathbb{Z})$;
- $N\mathcal{M}_n(\mathbb{Z}) = \{N \times A, A \in \mathcal{M}_n(\mathbb{Z})\}$; c'est l'ensemble des matrices de $\mathcal{M}_n(\mathbb{Z})$ dont tous les coefficients sont divisibles par N .

1 Généralités et exemples

On fixe un entier $n \geq 2$.

1. Montrer que $\mathcal{M}_n(\mathbb{Z})$ est un sous-anneau de $\mathcal{M}_n(\mathbb{Q})$.
2. Montrer que $\mathrm{GL}_2(\mathbb{Z})$ est infini, puis que $\mathrm{GL}_n(\mathbb{Z})$ est infini.
3. Soient $M \in \mathcal{M}_n(\mathbb{Z})$ et $m \geq 1$ tel que $M^m = I_n$. Montrer que $M \in \mathrm{GL}_n(\mathbb{Z})$.
4. Montrer que $\mathrm{GL}_n(\mathbb{Z}) \subset \mathrm{GL}_n(\mathbb{Q}) \cap \mathcal{M}_n(\mathbb{Z})$ et montrer que cette inclusion est stricte.
5. Soit M une matrice de $\mathcal{M}_2(\mathbb{Z})$. Montrer que $M \in \mathrm{GL}_2(\mathbb{Z})$ ssi $\det M = \pm 1$.
6. **Matrices de permutation.**
 - (a) Soit σ une permutation de $\llbracket 1, n \rrbracket$. On note P_σ la matrice $(\delta_{i, \sigma(j)})_{1 \leq i, j \leq n}$. Montrer que $P_\sigma \in \mathrm{GL}_n(\mathbb{Z})$.
 - (b) On note $\mathcal{S}_n$ le groupe des permutations de $\llbracket 1, n \rrbracket$. Montrer que l'application

$$\Psi : \begin{cases} \mathcal{S}_n & \rightarrow \mathrm{GL}_n(\mathbb{Z}) \\ \sigma & \mapsto P_\sigma \end{cases}$$

est un morphisme de groupes injectif.

7. Groupe diédral D_{12} .

On note $\alpha = e^{\frac{i\pi}{3}}$ et H l'hexagone régulier $H = \{\alpha^k, k \in \llbracket 0, 5 \rrbracket\}$. On munit¹ $\mathbb{C}$ de sa structure de $\mathbb{R}$ -espace vectoriel et on note D_{12} l'ensemble des $f \in \text{GL}_{\mathbb{R}}(\mathbb{C})$ vérifiant

$$f(H) = H \text{ et } \forall z, w \in \mathbb{C}, |f(z) - f(w)| = |z - w|.$$

- Montrer que D_{12} est un sous-groupe de $\text{GL}_{\mathbb{R}}(\mathbb{C})$.
- Montrer que, si $f \in D_{12}$, alors $f(1)$ et $f(\alpha)$ sont des sommets consécutifs de H .
- Montrer que l'application $f \mapsto (f(1), f(\alpha))$ est une bijection de D_{12} vers l'ensemble des couples de sommets consécutifs de H .
- En déduire le cardinal de D_{12} . Donner une description géométrique de ses éléments.
- On note $\mathbf{e}$ la base du $\mathbb{R}$ -espace vectoriel $\mathbb{C}$ donnée par $\mathbf{e} = (1, \alpha)$. Montrer que l'application $f \mapsto \text{Mat}_{\mathbf{e}}(f)$ définit un morphisme de groupes injectif de D_{12} dans $\text{GL}_2(\mathbb{Z})$.

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

Si $P = \sum_{k=0}^d a_k X^k$ est un polynôme à coefficients réels et si $A \in \mathcal{M}_2(\mathbb{R})$, 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, $(PQ)(A) = P(A)Q(A)$.

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

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

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

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

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

10. En déduire que $\text{Tr } A \in \llbracket -2, 2 \rrbracket$.

11. On définit les polynômes

$$\begin{array}{lll} \bullet P_1 = (X - 1)^2; & \bullet P_3 = X^2 - 1; & \bullet P_5 = X^2 - X + 1; \\ \bullet P_2 = (X + 1)^2; & \bullet P_4 = X^2 + 1; & \bullet P_6 = X^2 + X + 1. \end{array}$$

Montrer que $\chi_A = P_i$, pour un certain $i \in \llbracket 1, 6 \rrbracket$.

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

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

¹Pour éviter les ambiguïtés, on note $\text{GL}_{\mathbb{R}}(\mathbb{C})$ l'ensemble des automorphismes linéaires du $\mathbb{R}$ -espace vectoriel $\mathbb{C}$.

²Par définition, m est le plus petit entier $k \geq 1$ tel que $A^k = I_2$.

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

14. Soit $M \in \text{GL}_n(\mathbb{Z})$, 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 $m' = \frac{m}{p}$.

- (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 .

15. Montrer que

$$\phi_p : \begin{cases} \mathcal{M}_n(\mathbb{Z}) & \rightarrow \mathcal{M}_n(\mathbb{Z}/p\mathbb{Z}) \\ M & \mapsto \overline{M} \end{cases}$$

est un morphisme d'anneaux et qu'il induit un morphisme de groupes – encore noté ϕ_p – de $\text{GL}_n(\mathbb{Z})$ dans $\text{GL}_n(\mathbb{Z}/p\mathbb{Z})$.

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

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

17. Montrer que $\text{GL}_2(\mathbb{Z}/3\mathbb{Z})$ est de cardinal 48. En admettant le théorème de Lagrange⁴, en déduire que $|G|$ est un diviseur de 48.

18. Montrer que la matrice $A = \begin{pmatrix} \overline{0} & \overline{1} \\ \overline{1} & \overline{1} \end{pmatrix} \in \text{GL}_2(\mathbb{Z}/3\mathbb{Z})$ est d'ordre 8. En utilisant la partie précédente, en déduire que $|G|$ est un diviseur strict de 48.⁵

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

⁴Qui affirme que si H est un sous-groupe d'un groupe fini G , alors le cardinal de H divise celui de G

⁵Avec un peu plus d'outils, on peut montrer que les sous-groupes finis de $\text{GL}_2(\mathbb{Z})$ sont les groupes isomorphes à des sous-groupes des groupes diédraux D_8 et D_{12} . En particulier, leur cardinal divise 8 ou 12.