CONCOURS CENTRALE•SUPÉLEC

Mathématiques 1

MP MPI

4 heures — Calculatrice autorisée

2026

Sur quelques sous-groupes de $\mathrm{GL}_n(\mathbb{R})$

Dans tout le sujet, n désigne un entier supérieur ou égal à 2. On note :

- $\mathcal{M}_n(\mathbb{R})$ l'ensemble des matrices de taille $n \times n$ à coefficients dans $\mathbb{R}$, I_n sa matrice identité.
- $\mathrm{GL}_n(\mathbb{R})$ le groupe des matrices inversibles de $\mathcal{M}_n(\mathbb{R})$.
- $\mathcal{S}_n^+(\mathbb{R})$ (resp. $\mathcal{S}_n^{++}(\mathbb{R})$) l'ensemble des matrices symétriques positives de $\mathcal{M}_n(\mathbb{R})$ (resp. définies positives).
- $\mathrm{O}_n(\mathbb{R})$ le groupe des matrices orthogonales de $\mathcal{M}_n(\mathbb{R})$, et $\mathrm{SO}_n(\mathbb{R})$ celui des matrices orthogonales de déterminant 1.
- La transposée d'une matrice $M \in \mathcal{M}_n(\mathbb{R})$ sera notée $M^\top$ et sa trace $\operatorname{tr} M$.
- On note $|X|$ le cardinal d'un ensemble X, en convenant que $|X| = +\infty$ si X est un ensemble infini.
- Si $\mathcal{A}$ est une partie finie d'un groupe G, on note $\langle \mathcal{A} \rangle$ le sous-groupe de G engendré par $\mathcal{A}$.

Le problème comporte trois parties indépendantes.

Partie A – Sous-groupes finis de $\mathrm{O}_n(\mathbb{R})$

Soit G un groupe de neutre e. On dit que G est *d'exposant fini* si et seulement si :

$$\exists m \in \mathbb{N}^* \quad \forall x \in G \quad x^m = e$$

De plus, si G est un sous-groupe de $\mathrm{GL}_n(\mathbb{R})$, on note $\operatorname{tr} G$ la *trace du groupe* G, qui est l'ensemble :

$$\operatorname{tr} G = \{\operatorname{tr} A \ ; \ A \in G\}$$

I – Généralités

Soit G un sous-groupe de $\mathrm{GL}_n(\mathbb{R})$.

Q1. Montrer que si G est fini, alors G est d'exposant fini et $\operatorname{tr} G$ est fini.

Q2. Donner un exemple de sous-groupe infini de $\mathrm{GL}_n(\mathbb{R})$ dont la trace soit finie.

Q3. Donner un exemple (pas nécessairement matriciel) de groupe infini qui soit d'exposant fini.

II – Cas particulier : les sous-groupes finis de $\mathrm{O}_2(\mathbb{R})$

Pour tout $\theta \in \mathbb{R}$, on note R_θ et S_θ les matrices :

$$R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \qquad S_\theta = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}$$

On pourra utiliser sans démonstration les relations suivantes, valables pour tout $(\theta, \varphi) \in \mathbb{R}^2$:

$$R_\theta R_\varphi = R_{\theta+\varphi} \qquad R_\theta S_\varphi = S_{\theta+\varphi} \qquad S_\varphi R_\theta = S_{\varphi-\theta} \qquad S_\theta S_\varphi = R_{\theta-\varphi}$$

Q4. Soit $A \in \mathrm{SO}_2(\mathbb{R})$. Montrer qu'il existe un unique réel $\theta \in [0, 2\pi[$ tel que $A = R_\theta$.

Q5. Soit $\theta \in \mathbb{R}$. Dans cette question, $G = \langle R_\theta \rangle$.

a) Vérifier que $G = \{R_{k\theta} \ ; \ k \in \mathbb{Z}\}$.

b) Dans le cas où $\theta = \dfrac{2\pi}{m}$ avec $m \in \mathbb{N}^*$, déterminer $|G|$.

c) Montrer que G est fini si et seulement si $\dfrac{\theta}{\pi} \in \mathbb{Q}$.

d) Montrer que si G est d'exposant fini, alors G est fini.

e) Montrer que si $\operatorname{tr} G$ est fini, alors G est fini.

Q6. Soient θ et θ' deux réels. Dans cette question $G = \langle R_\theta, R_{\theta'} \rangle$.

a) Montrer que $|G| = |(\theta\mathbb{Z} + \theta'\mathbb{Z}) \cap [0, 2\pi[|$.

b) En déduire, pour p et q deux entiers non nuls premiers entre eux, que $\left|\langle R_{\frac{\pi}{p}}, R_{\frac{\pi}{q}} \rangle\right| = 2pq$.

c) Déterminer $\left|\langle R_{\frac{\pi}{p}}, R_{\frac{\pi}{q}} \rangle\right|$ dans le cas général (où p et q ne sont pas forcément premiers entre eux).

Q7. Soit G un sous-groupe fini de $\mathrm{SO}_2(\mathbb{R})$. Montrer que G est monogène.

Q8. Pour $m \in \mathbb{N}^*$, on note $\mathcal{D}_m$ le sous-groupe de $\mathrm{O}_2(\mathbb{R})$ engendré par $R_{\frac{2\pi}{m}}$ et $S_{\frac{\pi}{2}}$.

a) Déterminer le cardinal de $\mathcal{D}_m$.
On pourra montrer que $\mathcal{D}_m \cap \mathrm{SO}_2(\mathbb{R}) = \langle R_{\frac{2\pi}{m}} \rangle$, puis chercher une bijection entre $\mathcal{D}_m \cap \mathrm{SO}_2(\mathbb{R})$ et $\mathcal{D}_m \backslash \mathrm{SO}_2(\mathbb{R})$.

b) Soit G un sous-groupe fini de $\mathrm{O}_2(\mathbb{R})$ qui n'est pas inclus dans $\mathrm{SO}_2(\mathbb{R})$. Montrer qu'il existe $m \in \mathbb{N}^*$ tel que G soit isomorphe à $\mathcal{D}_m$.

III – Une caractérisation des sous-groupes finis de $\mathrm{O}_n(\mathbb{R})$

Dans cette partie, G est un sous-groupe de $\mathrm{O}_n(\mathbb{R})$. On désire montrer que :

$$G \text{ fini} \iff G \text{ d'exposant fini} \iff \operatorname{tr} G \text{ fini}$$

Q9. Rappeler le théorème de réduction des matrices orthogonales.

Q10. On suppose dans cette question que G est d'exposant fini. Montrer, en utilisant le théorème de réduction précédent, que $\operatorname{tr} G$ est fini.

Jusqu'à la fin de cette partie, on suppose maintenant que $\operatorname{tr} G$ est fini. On munit $\mathcal{M}_n(\mathbb{R})$ de son produit scalaire usuel :

$$(A|B) = \operatorname{tr} A^\top B$$

On note $\mathcal{F}$ le sous-espace vectoriel de $\mathcal{M}_n(\mathbb{R})$ engendré par G et $d = \dim \mathcal{F}$.

Q11. Montrer qu'il existe une famille $\mathcal{B} = (A_i)_{i \in [\![1,d]\!]}$ de matrices de G qui forme une base de $\mathcal{F}$.

Q12. Soit $B = ((A_i|A_j))_{(i,j) \in [\![1,d]\!]^2}$. On considère la matrice C des coordonnées des matrices A_i dans la base canonique de $\mathcal{M}_n(\mathbb{R})$.

a) Quelle est la taille de la matrice C ?

b) Montrer que $B = C^\top C$.

c) Montrer que B et C sont de même rang. En déduire que B est inversible.

Q13. Soit $M \in G$. On peut décomposer M dans la base $\mathcal{B}$:

$$M = \sum_{j=1}^{d} x_j A_j$$

On note alors $X_M = \begin{pmatrix} x_1 \\ \vdots \\ x_d \end{pmatrix}$ et $Y_M = \begin{pmatrix} (A_1|M) \\ \vdots \\ (A_d|M) \end{pmatrix}$. Montrer que $X_M = B^{-1} Y_M$.

Q14. Montrer que $\{Y_M \mid M \in G\}$ est un ensemble fini. En déduire que G est fini.

Partie B – Sous-groupes compacts de $\mathrm{GL}_n(\mathbb{R})$

On note $\mathcal{M}_{n,1}(\mathbb{R})$ l'espace vectoriel des matrices colonnes de taille $n \times 1$ à coefficients dans $\mathbb{R}$.

Dans cette partie, on se place dans $\mathcal{M}_{n,1}(\mathbb{R})$, muni de son produit scalaire canonique noté $(.|.)$ et de sa norme associée $\|.\|$. Pour $r \geqslant 0$, on note $\mathcal{B}(0,r)$ la boule fermée de centre 0 et de rayon r de $\mathcal{M}_{n,1}(\mathbb{R})$ pour cette norme, et $\mathcal{B} = \mathcal{B}(0,1)$ la boule unité fermée.

I – Quelques propriétés utiles

Soient $A \in \mathcal{S}_n^{++}(\mathbb{R})$ et $B \in \mathcal{S}_n(\mathbb{R})$.

Q15. On pose, pour X et Y dans $\mathcal{M}_{n,1}(\mathbb{R})$:

$$\langle X, Y \rangle_A = (AX|Y)$$

Montrer que $\langle ., . \rangle_A$ est un produit scalaire sur $\mathcal{M}_{n,1}(\mathbb{R})$.

On note alors $\|.\|_A$ la norme associée à ce produit scalaire et $\mathcal{B}_A$ la boule unité fermée pour cette norme. Existe-t-il une matrice A telle que $\mathcal{B}(0,r) = \mathcal{B}_A$?

Q16. Vérifier que $X \mapsto A^{-1}BX$ est autoadjoint pour le produit scalaire $\langle ., . \rangle_A$. Que peut-on en déduire pour la matrice $A^{-1}B$?

Soient A et B dans $\mathcal{S}_n(\mathbb{R})$. On note $B \preccurlyeq A$ si et seulement si pour tout $X \in \mathcal{M}_{n,1}(\mathbb{R})$, $(BX|X) \leqslant (AX|X)$.

Q17. Montrer que $B \preccurlyeq A$ si et seulement si $A - B \in \mathcal{S}_n^+(\mathbb{R})$.

Q18. Soient A et B dans $\mathcal{S}_n^{++}(\mathbb{R})$. Montrer que $B \preccurlyeq A$ si et seulement si le spectre de $A^{-1}B$ est inclus dans $]0,1]$.
Pour la réciproque, on pourra utiliser une base orthonormée pour le produit scalaire $\langle ., . \rangle_A$ bien choisie.

Q19. On suppose toujours que A et B sont deux matrices de $\mathcal{S}_n^{++}(\mathbb{R})$, et que $B \preccurlyeq A$. Montrer que $\det B \leqslant \det A$, avec égalité si et seulement si $A = B$.

Q20. Montrer que $B \preccurlyeq A$ si et seulement si $\mathcal{B}_A \subset \mathcal{B}_B$.

Q21. Soit $\mathcal{K}$ une partie de $\mathcal{S}_n^+(\mathbb{R})$. Montrer que $\mathcal{K}$ est une partie bornée de $\mathcal{S}_n^+(\mathbb{R})$ si et seulement s'il existe $\alpha \in \mathbb{R}_+^*$ telle que pour tout $A \in \mathcal{K}$, $A \preccurlyeq \alpha I_n$.

II – Stricte log-concavité de l'application det

Soit $\mathcal{C}$ une partie convexe de $\mathcal{M}_n(\mathbb{R})$ et $\varphi : \mathcal{C} \to \mathbb{R}$ une fonction. On dit que φ est *strictement concave* si et seulement si :

$$\forall (A,B) \in \mathcal{C}^2 \quad \forall t \in [0,1] \qquad \varphi(tA + (1-t)B) \geqslant t\varphi(A) + (1-t)\varphi(B)$$

avec égalité si et seulement si $A = B$ ou $t = 0$ ou $t = 1$.

Q22. Montrer que $\mathcal{S}_n^{++}(\mathbb{R})$ est une partie convexe de $\mathcal{M}_n(\mathbb{R})$.

Q23. Montrer que $\varphi : A \mapsto \ln(\det A)$ est une fonction strictement concave sur $\mathcal{S}_n^{++}(\mathbb{R})$.
*On pourra utiliser le résultat de la question **Q16**.*

III – Groupe orthogonal associé à une matrice symétrique définie positive

À toute matrice $A \in \mathcal{S}_n^{++}(\mathbb{R})$ on associe son *groupe orthogonal* :

$$\mathrm{O}(A) = \{M \in \mathcal{M}_n(\mathbb{R}) \ ; \ M^\top A M = A\}$$

Q24. Montrer que $\mathrm{O}(A)$ est un sous-groupe de $\mathrm{GL}_n(\mathbb{R})$, isomorphe à $\mathrm{O}_n(\mathbb{R})$.
On pourra montrer qu'il existe une matrice B telle que $A = B^\top B$, et chercher un isomorphisme sous la forme $M \mapsto B^{-1}MB$.

Q25. Montrer que $\mathrm{O}(A)$ est une partie compacte de $\mathcal{M}_n(\mathbb{R})$.

IV – Sous-groupes compacts de $\mathrm{GL}_n(\mathbb{R})$

Dans cette partie, G désigne un sous-groupe compact de $\mathrm{GL}_n(\mathbb{R})$. On désire montrer que G est alors isomorphe à un sous-groupe de $\mathrm{O}_n(\mathbb{R})$.

Q26. Montrer que pour tout $M \in G$, $|\det M| = 1$.

Q27. On pose :

$$\mathcal{C} = \{MX \ ; \ (M, X) \in G \times \mathcal{B}\}$$

Montrer que $\mathcal{C}$ est compact, et que 0 est un point intérieur à $\mathcal{C}$.

Q28. Montrer qu'il existe une unique matrice $A \in \mathcal{S}_n^{++}(\mathbb{R})$ telle que $\mathcal{C} \subset \mathcal{B}_A$ et qui soit de déterminant maximal.
*On pourra commencer par montrer que $\mathcal{E} = \{A \in \mathcal{S}_n^{+}(\mathbb{R}) \ ; \ \mathcal{C} \subset \mathcal{B}_A\}$ est non vide, compact et convexe, puis utiliser la question **Q23** pour démontrer l'unicité.*

Q29. Montrer que G est un sous-groupe de $\mathrm{O}(A)$.

Partie C – Croissance du groupe de Heisenberg discret

I – Croissance d'un groupe

Soit G un groupe de neutre e, engendré par une partie finie $\mathcal{S} = \{s_i\}_{i \in [\![1,N]\!]}$. À tout élément $g \in G - \{e\}$ on associe sa *longueur relativement à $\mathcal{S}$* par :

$$\ell_{\mathcal{S}}(g) = \min \left\{ \sum_{i=1}^{k} |a_i| \ \middle| \ g = s_1^{a_1} \dots s_k^{a_k} \ ; \ s_i \in \mathcal{S} \ , \ a_i \in \mathbb{Z} \right\}$$

$\ell_{\mathcal{S}}(g)$ est le nombre minimal d'éléments de $\mathcal{S}$ permettant d'obtenir g. Par convention, on pose $\ell_{\mathcal{S}}(e) = 0$. On note alors, pour $p \in \mathbb{N}$:

$$\mathcal{V}_{\mathcal{S}}(p) = \{g \in G \ ; \ \ell_{\mathcal{S}}(g) \leqslant p\}$$

$\mathcal{V}_{\mathcal{S}}(p)$ est l'ensemble des éléments de G s'obtenant à partir d'au maximum p éléments de $\mathcal{S}$.

Nous dirons que G est un groupe à *croissance polynomiale de degré $d \in \mathbb{N}$* si et seulement si il existe deux réels strictement positifs α et β tels que, pour tout $p \geqslant 1$:

$$\alpha p^d \leqslant |\mathcal{V}_{\mathcal{S}}(p)| \leqslant \beta p^d$$

Q30. Montrer que pour tous g et h dans G, $\ell_{\mathcal{S}}(g^{-1}) = \ell_{\mathcal{S}}(g)$ et $\ell_{\mathcal{S}}(gh) \leqslant \ell_{\mathcal{S}}(g) + \ell_{\mathcal{S}}(h)$.

Q31. Soit Σ une autre partie finie génératrice de G. Montrer qu'il existe deux constantes C et C' strictement positives telle que, pour tout $g \in G$:

$$C\ell_{\mathcal{S}}(g) \leqslant \ell_{\Sigma}(g) \leqslant C'\ell_{\mathcal{S}}(g)$$

En déduire que le fait que G soit un groupe à croissance polynomiale de degré d ne dépend pas du système S de générateurs choisis.

Q32. Soit $p \in \mathbb{N}$. Dénombrer le nombre de triplets $(x, y, z) \in \mathbb{N}^3$ tels que $x + y + z \leqslant p$. En déduire que $(\mathbb{Z}^3, +)$ est un groupe à croissance polynomiale et déterminer son degré.

II – Le groupe de Heisenberg discret

Dans cette partie, $n = 3$. On considère les trois matrices suivantes :

$$S = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \qquad T = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad U = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

On note $\mathcal{A} = \{S, T, U\}$. $\mathbb{H}$ désigne alors le sous-groupe de $\mathrm{GL}_3(\mathbb{R})$ engendré par $\mathcal{A}$.

Q33. Pour tout $(i, j, k) \in \mathbb{Z}^3$, calculer $S^i T^j U^k$.

Q34. Pour $(i,j,k,i',j',k') \in \mathbb{Z}^6$, déterminer un triplet $(i'',j'',k'') \in \mathbb{Z}^3$ tel que :

$$S^i T^j U^k S^{i'} T^{j'} U^{k'} = S^{i''} T^{j''} U^{k''}$$

Q35. Vérifier que U commute avec tous les éléments de $\mathbb{H}$, et que pour tout $(i,j) \in \mathbb{Z}^2$:

$$S^i T^j U^{ij} = T^j S^i$$

Q36. Le groupe $\mathbb{H}$ est-il commutatif ? Quel est le groupe engendré par (S,T) ?

Q37. Montrer que l'application f définie par :

$$\begin{array}{rccc} f & : & \mathbb{Z}^3 & \to & \mathbb{H} \\ & & (i,j,k) & \mapsto & S^i T^j U^k \end{array}$$

est bien définie et bijective. Est-ce un isomorphisme de groupe (en munissant $\mathbb{Z}^3$ de sa structure usuelle) ? Peut-on munir $\mathbb{Z}^3$ d'une structure de groupe telle que f soit un isomorphisme ?

Q38. Soit $M \in \mathbb{H}$ et $p \in \mathbb{N}^*$. Montrer que si $\ell_{\mathcal{A}}(M) \leqslant p$, alors il existe $(i,j,k,z) \in \mathbb{Z}^4$ tels que $M = S^i T^j U^{k+z}$ avec $|i|+|j|+|k| \leqslant p$ et $|z| \leqslant |ij|$. En déduire que $|\mathcal{V}_{\mathcal{A}}(p)| = O(p^4)$ quand p tend vers $+\infty$.
On pourra utiliser les résultats de la question ***Q35****.*

Q39. Montrer que, pour tout $(i,j,k) \in \mathbb{Z}^3$, si $|i|+|j| \leqslant p$ et $|k| \leqslant |ij|$, alors $\ell_{\mathcal{A}}(S^i T^j U^k) \leqslant p$.

Q40. Montrer que :

$$\mathrm{card}\{(i,j,k) \in \mathbb{N}^3 \ ,\ i+j \leqslant p \text{ et } k \leqslant ij\} \geqslant \frac{p^3}{2} \sum_{i=0}^{p} \frac{i}{p} \left(1 - \frac{i}{p}\right)^2$$

et déterminer un équivalent de cette dernière quantité quand p tend vers $+\infty$.

Q41. En déduire que $\mathbb{H}$ est un groupe à croissance polynomiale de degré 4.

◇ Fin ◇