ANNALES CORRIGÉES · CONCOURS D'ENTRÉE AUX ÉCOLES D'INGÉNIEURS

Centrale-Supélec 2026 · MP

Mathématiques 1 · 4 heures

Énoncé officiel ressaisi + corrigé détaillé + remarques de méthode

Corrigé par **Pr. Abdelfattah ELAKILI**, agrégé de mathématiques



Au programme : groupes, sous-groupes finis de $\mathrm{O}_n(\mathbb{R})$, groupes diédraux, réduction des matrices orthogonales, matrice de Gram · matrices symétriques positives, ordre de Loewner, log-concavité du déterminant, compacité, ellipsoïde de John-Loewner · croissance d'un groupe, groupe de Heisenberg discret.

Source : sujet officiel © Concours Centrale-Supélec (session 2026, licence CC BY-NC-SA), ressaisi à l'identique ; original sur concours-centrale-supelec.fr.

Toutes les annales corrigées, en accès libre, sur prepasmaths360.com

DÉBUT DU SUJET

CONCOURS CENTRALE-SUPÉLEC · SESSION 2026 MP, MPI

Mathématiques 1

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

4 heures · Calculatrice autorisée

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 A est une partie finie d'un groupe G, on note $\langle A \rangle$ le sous-groupe de G engendré par 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 $\theta = \frac{2\pi}{m}$ avec $m \in \mathbb{N}^*$, déterminer $|G|$.
c) Montrer que G est fini si et seulement si $\frac{\theta}{\pi} \in \mathbb{Q}$.
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 $\langle R_{\frac{\pi}{p}}, R_{\frac{\pi}{q}} \rangle = 2pq$.
c) Déterminer $\langle R_{\frac{\pi}{p}}, R_{\frac{\pi}{q}} \rangle$ 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 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 D_m.
On pourra montrer que $D_m \cap \mathrm{SO}_2(\mathbb{R}) = \langle R_{\frac{2\pi}{m}} \rangle$, puis chercher une bijection entre $D_m \cap \mathrm{SO}_2(\mathbb{R})$ et $D_m \setminus \mathrm{SO}_2(\mathbb{R})$.
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 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 F le sous-espace vectoriel de $\mathcal{M}_n(\mathbb{R})$ engendré par G et $d = \dim F$.

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

Q12. Soit $B = \big((A_i \,|\, A_j)\big)_{(i,j) \in [\![1,d]\!]^2}$. 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 $B(0,r)$ la boule fermée de centre 0 et de rayon r de $\mathcal{M}_{n,1}(\mathbb{R})$ pour cette norme, et $\mathbb{B} = B(0,1)$ 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 $\mathbb{B}_A$ la boule unité fermée pour cette norme. Existe-t-il une matrice A telle que $B(0,r) = \mathbb{B}_A$?

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 $\mathbb{B}_A \subset \mathbb{B}_B$.

Q21. Soit K une partie de $\mathcal{S}_n^+(\mathbb{R})$. Montrer que 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 $A \in K$, $A \preccurlyeq \alpha I_n$.

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 :

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

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 : $C = \{MX \ ; \ (M, X) \in G \times \mathbb{B}\}$.
Montrer que C est compact, et que 0 est un point intérieur à C.

Q28. Montrer qu'il existe une unique matrice $A \in \mathcal{S}_n^{++}(\mathbb{R})$ telle que $C \subset \mathbb{B}_A$ et qui soit de déterminant maximal.
On pourra commencer par montrer que $E = \{A \in \mathcal{S}_n^{+}(\mathbb{R}) \ ; \ C \subset \mathbb{B}_A\}$ 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 $S = \{s_i\}_{i \in [\![1,N]\!]}$. À tout élément $g \in G - \{e\}$ on associe sa longueur relativement à S par :

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

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

$$V_S(p) = \{g \in G \ ; \ \ell_S(g) \leqslant p\}$$

$V_S(p)$ est l'ensemble des éléments de G s'obtenant à partir d'au maximum p éléments de 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 $p \geqslant 1$:

$$\alpha p^d \leqslant |V_S(p)| \leqslant \beta p^d$$

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

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 $g \in G$:

$$C\ell_S(g) \leqslant \ell_\Sigma(g) \leqslant C'\ell_S(g)$$

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 $\mathcal{A} = \{S, T, U\}$. 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 H, et que pour tout $(i, j) \in \mathbb{Z}^2$:

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

Q36. Le groupe H est-il commutatif ? Quel est le groupe engendré par (S, T) ?

Q37. Montrer que l'application f définie par :

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

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 $M \in H$ 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 $|V_{\mathcal{A}}(p)| = O(p^4)$ 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 :

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

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

Q41. En déduire que H est un groupe à croissance polynomiale de degré 4.

◇ **Fin** ◇

prepasmaths360.com

Corrigé détaillé

par Pr. Abdelfattah Elakili, agrégé de mathématiques · prepasmaths360.com

Avant de commencer

Partie	Chapitres à maîtriser	Temps	Difficulté
Partie A	Groupes, ordre d'un élément, rotations et réflexions du plan, réduction des matrices orthogonales, matrices de Gram	1 h 20	standard, Q6 et Q8(b) délicates
Partie B	Matrices symétriques, endomorphismes autoadjoints, ordre de Loewner, convexité, compacité	1 h 30	standard à sélective (Q28)
Partie C	Groupe engendré par une partie, dénombrement, équivalents, sommes de Riemann	1 h 10	standard, Q38–Q41 sélectives

Stratégie conseillée : les trois parties sont indépendantes. La partie B, I (Q15 à Q21) et la partie C, II (Q33 à Q37) sont des calculs sans piège qui rapportent vite. Attention : les questions Q6(a), Q38 et Q39 sont incorrectes telles qu'elles sont posées (voir le corrigé) ; sur une copie, il fallait le signaler et démontrer l'énoncé rectifié. Les temps et niveaux sont indicatifs.

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

Q1

Si G est fini, de cardinal N, le théorème de Lagrange donne $x^N = e$ pour tout $x \in G$ (l'ordre de x divise N) : G est d'exposant fini (avec $m = N$). Et $\operatorname{tr} G$ est l'image de l'ensemble fini G par l'application tr : il est fini.

Q2

$G = \left\{ \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \oplus I_{n-2} \ ; \ k \in \mathbb{Z} \right\}$ (bloc 2×2 en haut à gauche, I_{n-2} ensuite ; possible car $n \geqslant 2$).
En notant N_k ces matrices, $N_k N_{k'} = N_{k+k'}$ et $N_k^{-1} = N_{-k}$: c'est un sous-groupe de $\mathrm{GL}_n(\mathbb{R})$, infini (les N_k sont distinctes), et $\operatorname{tr} G = \{n\}$ est fini.

Q3

Le groupe $\left((\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}, +\right)$ des suites à valeurs dans $\mathbb{Z}/2\mathbb{Z}$, muni de l'addition terme à terme, est infini, et $x + x = 0$ pour tout x : il est d'exposant 2.

Q4

Soit $A = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \mathrm{SO}_2(\mathbb{R})$. Ses colonnes forment une base orthonormée : $a^2 + b^2 = 1$, donc il existe un unique $\theta \in [0, 2\pi[$ tel que $(a, b) = (\cos\theta, \sin\theta)$. La seconde colonne est unitaire et orthogonale à la première, donc $(c, d) = \pm(-\sin\theta, \cos\theta)$. Enfin $\det A = 1$ impose le signe + : $A = R_\theta$.
Unicité : si $R_\theta = R_{\theta'}$ avec $\theta, \theta' \in [0, 2\pi[$, alors $\cos\theta = \cos\theta'$ et $\sin\theta = \sin\theta'$, donc $\theta = \theta'$.

Q5

a) Le sous-groupe engendré par un élément est l'ensemble de ses puissances entières. Or $R_\theta^k = R_{k\theta}$ pour $k \in \mathbb{N}$ (récurrence, avec $R_\theta R_\varphi = R_{\theta+\varphi}$) et $R_\theta^{-1} = R_{-\theta}$. Donc $G = \{R_{k\theta} \ ; \ k \in \mathbb{Z}\}$.
b) $R_{2k\pi/m} = I_2 \iff \frac{2k\pi}{m} \in 2\pi\mathbb{Z} \iff m \mid k$: $R_{2\pi/m}$ est d'ordre m, et $|G| = m$ (les $R_{2k\pi/m}$, $0 \leqslant k < m$, sont distincts par Q4).
c) Si $\frac{\theta}{\pi} = \frac{r}{s}$ ($r \in \mathbb{Z}$, $s \in \mathbb{N}^*$), alors $R_\theta^{2s} = R_{2r\pi} = I_2$: R_θ est d'ordre fini et G est fini. Réciproquement, si G est fini, il existe $k \neq k'$ tels que $R_{k\theta} = R_{k'\theta}$, donc $(k-k')\theta \in 2\pi\mathbb{Z}$, et $\frac{\theta}{\pi} \in \mathbb{Q}$.
d) Si G est d'exposant m, alors $R_\theta^m = R_{m\theta} = I_2$, donc $m\theta \in 2\pi\mathbb{Z}$, $\frac{\theta}{\pi} \in \mathbb{Q}$, et G est fini par c).
e) Supposons $\frac{\theta}{\pi} \notin \mathbb{Q}$. Alors les réels $k\theta$ ($k \in \mathbb{Z}$) sont deux à deux non congrus modulo 2π (sinon on conclut comme en c)). Pour c fixé, l'égalité $2\cos(k\theta) = c$ impose $k\theta \equiv \pm\arccos(c/2) \pmod{2\pi}$, ce qui laisse au plus deux valeurs de k. Si $\operatorname{tr} G = \{2\cos k\theta \ ; \ k \in \mathbb{Z}\}$ était fini, $\mathbb{Z}$ serait fini. Donc $\operatorname{tr} G$ fini implique $\frac{\theta}{\pi} \in \mathbb{Q}$, puis G fini.

Q6

Comme R_θ et $R_{\theta'}$ commutent, $G = \{R_{a\theta+b\theta'} \ ; \ (a,b) \in \mathbb{Z}^2\}$.
a) Attention, l'énoncé est inexact en général. Avec $\theta = \theta' = 1$, $G = \langle R_1 \rangle$ est infini (Q5(c)), alors que $(\mathbb{Z}+\mathbb{Z}) \cap [0, 2\pi[= \{0, 1, \ldots, 6\}$ a 7 éléments. Le résultat correct est

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

qui coïncide avec la formule de l'énoncé dès que $2\pi \in \theta\mathbb{Z} + \theta'\mathbb{Z}$. C'est le cas dans les questions b) et c).
Preuve. Notons $\Lambda = \theta\mathbb{Z} + \theta'\mathbb{Z} + 2\pi\mathbb{Z}$, et $\Phi : t \in \Lambda \cap [0, 2\pi[\mapsto R_t$. Comme $R_{2\pi} = I_2$, Φ est à valeurs dans G. Elle est surjective : $R_{a\theta+b\theta'} = R_t$ où t est le reste de $a\theta + b\theta'$ modulo 2π, et $t \in \Lambda \cap [0, 2\pi[$. Elle est injective par l'unicité de Q4.
b) On peut supposer $p, q > 0$ (changer p en $-p$ ne change pas le groupe). Par Bézout, $q\mathbb{Z}+p\mathbb{Z} = \mathbb{Z}$, donc $\frac{\pi}{p}\mathbb{Z} + \frac{\pi}{q}\mathbb{Z} = \frac{\pi}{pq}(q\mathbb{Z} + p\mathbb{Z}) = \frac{\pi}{pq}\mathbb{Z}$, qui contient 2π. L'ensemble $\frac{\pi}{pq}\mathbb{Z} \cap [0, 2\pi[= \left\{\frac{k\pi}{pq} \ ; \ 0 \leqslant k < 2pq\right\}$ a $2pq$ éléments : $|\langle R_{\pi/p}, R_{\pi/q}\rangle| = 2pq$ (l'énoncé a omis les barres de cardinal ; dans le cas de signes quelconques, on trouve $2|pq|$).
c) Soit $\delta = p \wedge q$, $p = \delta p'$, $q = \delta q'$, et $\mu = \delta p' q' = \operatorname{ppcm}(p, q)$. Alors $\frac{\pi}{p}\mathbb{Z} + \frac{\pi}{q}\mathbb{Z} = \frac{\pi}{\mu}(q'\mathbb{Z} + p'\mathbb{Z}) = \frac{\pi}{\mu}\mathbb{Z}$, qui contient 2π. Le même dénombrement donne

$$|\langle R_{\pi/p}, R_{\pi/q}\rangle| = 2\operatorname{ppcm}(|p|, |q|),$$

et le groupe est $\langle R_{\pi/\mu}\rangle$.

Q7

Si $G = \{I_2\}$, $G = \langle I_2 \rangle$. Sinon, par Q4, $\Theta = \{\theta \in]0, 2\pi[\ ; \ R_\theta \in G\}$ est fini et non vide ; soit θ_0 son minimum. Pour $R_\theta \in G$ ($\theta \in [0, 2\pi[$), écrivons $\theta = k\theta_0 + r$ avec $k \in \mathbb{N}$ et $0 \leqslant r < \theta_0$. Alors $R_r = R_\theta R_{\theta_0}^{-k} \in G$ et $r \in [0, \theta_0[$: par minimalité, $r = 0$, donc $R_\theta = R_{\theta_0}^k$. Ainsi $G = \langle R_{\theta_0} \rangle$ est monogène.

Q8

a) Notons $\rho = R_{2\pi/m}$ et $\sigma = S_{\pi/2}$. Les relations données donnent $\sigma^2 = R_0 = I_2$, $\rho^k\sigma = S_{\frac{\pi}{2}+\frac{2k\pi}{m}}$, et les produits de deux éléments de

$$D' = \{R_{2k\pi/m}\ ;\ 0 \leqslant k < m\} \cup \{S_{\frac{\pi}{2}+\frac{2k\pi}{m}}\ ;\ 0 \leqslant k < m\}$$

restent dans D' : pour $\alpha, \beta \in \frac{2\pi}{m}\mathbb{Z}$, on a $R_\alpha R_\beta = R_{\alpha+\beta}$, $R_\alpha S_{\frac{\pi}{2}+\beta} = S_{\frac{\pi}{2}+\alpha+\beta}$, $S_{\frac{\pi}{2}+\beta}R_\alpha = S_{\frac{\pi}{2}+\beta-\alpha}$ et $S_{\frac{\pi}{2}+\alpha}S_{\frac{\pi}{2}+\beta} = R_{\alpha-\beta}$ (les angles étant pris modulo 2π). D' est donc une partie finie de $\mathrm{O}_2(\mathbb{R})$, stable par produit et contenant I_2 : c'est un sous-groupe, car l'inverse d'un élément x d'ordre r est $x^{r-1} \in D'$. Il contient ρ et σ, et il est contenu dans D_m : donc $D_m = D'$.
Les S_φ sont de déterminant -1 : $D_m \cap \mathrm{SO}_2(\mathbb{R}) = \{R_{2k\pi/m}\} = \langle\rho\rangle$. L'application $M \mapsto M\sigma$ est une bijection de $D_m \cap \mathrm{SO}_2(\mathbb{R})$ sur $D_m \setminus \mathrm{SO}_2(\mathbb{R})$ (elle est sa propre réciproque, car $\sigma^2 = I_2$). D'où $|D_m| = 2m$.
b) $G^+ = G \cap \mathrm{SO}_2(\mathbb{R})$ est un sous-groupe fini de $\mathrm{SO}_2(\mathbb{R})$, monogène par Q7. Si $m = |G^+|$, tout élément de G^+ vérifie $x^m = I_2$, donc $G^+ \subset \{R_{2k\pi/m}\}$, et par cardinal $G^+ = \langle R_{2\pi/m}\rangle$.
$\det : G \to \{\pm 1\}$ est un morphisme surjectif (car $G \not\subset \mathrm{SO}_2(\mathbb{R})$), de noyau G^+. Fixons $S_\varphi \in G$: alors $G \setminus G^+ = G^+S_\varphi = \{S_{\varphi+2k\pi/m}\}$. Posons $\gamma = \frac{1}{2}\left(\varphi - \frac{\pi}{2}\right)$ et $P = R_\gamma$. On a $PR_\alpha P^{-1} = R_\alpha$ et $PS_\beta P^{-1} = S_{\beta+\gamma}R_{-\gamma} = S_{\beta+2\gamma}$. Donc $PS_{\frac{\pi}{2}+\frac{2k\pi}{m}}P^{-1} = S_{\varphi+\frac{2k\pi}{m}}$, et $PD_mP^{-1} = G$. La conjugaison $M \mapsto PMP^{-1}$ est un isomorphisme de groupes : $G \simeq D_m$.

Remarque du professeur

La partie II est le classique « sous-groupes finis de $\mathrm{O}_2(\mathbb{R})$ » : ce sont les groupes cycliques $\langle R_{2\pi/m}\rangle$ (rotations d'un polygone régulier) et les groupes diédraux D_m (isométries d'un polygone régulier à m côtés, d'ordre $2m$). À connaître, de même que la méthode de Q7 : dans un sous-groupe de rotations, on prend le plus petit angle strictement positif et on fait une division euclidienne. C'est la même idée que pour les sous-groupes de $(\mathbb{R}, +)$.

Q9

Pour toute $M \in \mathrm{O}_n(\mathbb{R})$, il existe $P \in \mathrm{O}_n(\mathbb{R})$ et des entiers $p, q, r \geqslant 0$ $(p + q + 2r = n)$ tels que

$$P^\top MP = \mathrm{diag}\left(I_p,\ -I_q,\ R_{\theta_1}, \ldots, R_{\theta_r}\right), \qquad \theta_1, \ldots, \theta_r \in]0, \pi[\cup]\pi, 2\pi[.$$

Q10

Soit m un exposant de G et $M \in G$, réduite comme en Q9. $M^m = I_n$ donne $R_{\theta_i}^m = R_{m\theta_i} = I_2$, donc $\theta_i \in \frac{2\pi}{m}\mathbb{Z}$. Ainsi

$$\mathrm{tr}\, M = p - q + 2\sum_{i=1}^{r} \cos\theta_i,$$

où $p, q, r \leqslant n$ et chaque θ_i appartient à l'ensemble fini $\left\{\frac{2k\pi}{m}\ ;\ 1 \leqslant k \leqslant m-1\right\}$. Il n'y a qu'un nombre fini de valeurs possibles : $\mathrm{tr}\, G$ est fini.

Q11 et Q12

Q11. F est de dimension finie et G en est une famille génératrice. Une sous-famille libre de G de cardinal maximal (cardinal $\leqslant d$) engendre F : sinon, on pourrait la compléter par un élément de G hors de son sous-espace engendré. C'est donc une base $(A_1, \ldots, A_d)$ de F formée d'éléments de G.
Q12. a) La j-ème colonne de C contient les n^2 coordonnées de A_j : $C \in \mathcal{M}_{n^2,d}(\mathbb{R})$.

b) La base canonique (E_{kl}) est orthonormée pour $(A \mid B) = \operatorname{tr}(A^\top B) = \sum_{k,l} a_{kl} b_{kl}$. Donc $(A_i \mid A_j) = \sum_r c_{ri} c_{rj} = (C^\top C)_{ij}$.
c) Si $C^\top C X = 0$, alors $0 = X^\top C^\top C X = \|CX\|^2$, donc $CX = 0$: $\ker(C^\top C) = \ker C$, et par le théorème du rang, $\operatorname{rg} B = \operatorname{rg} C$. Les colonnes de C sont les coordonnées d'une famille libre : $\operatorname{rg} C = d$. Donc $B \in \mathcal{M}_d(\mathbb{R})$ est de rang d : elle est inversible.

Q13 et Q14

Q13. Pour tout i, $(A_i \mid M) = \sum_j x_j (A_i \mid A_j)$, c'est-à-dire $Y_M = B X_M$, d'où $X_M = B^{-1} Y_M$.
Q14. $A_i \in \mathrm{O}_n(\mathbb{R})$, donc $A_i^\top = A_i^{-1} \in G$, et $A_i^\top M \in G$ pour $M \in G$. Ainsi $(A_i \mid M) = \operatorname{tr}(A_i^\top M) \in \operatorname{tr} G$, et $Y_M \in (\operatorname{tr} G)^d$, qui est fini. Comme $M \mapsto X_M = B^{-1} Y_M$ est injective (X_M est la colonne des coordonnées de M dans $\mathcal{B}$), G est fini.
Bilan : G fini $\Rightarrow$ exposant fini (Q1) $\Rightarrow$ $\operatorname{tr} G$ fini (Q10) $\Rightarrow$ G fini (Q11 à Q14).

Remarque du professeur

L'astuce des questions Q11 à Q14 est de **coder chaque élément de G par des traces**. Grâce à la matrice de Gram B, la matrice M est déterminée par les produits scalaires $(A_i \mid M)$, qui sont des traces d'éléments de G. C'est une version élémentaire du théorème de Burnside (1905) : un sous-groupe de $\mathrm{GL}_n(\mathbb{C})$ d'exposant fini est fini. Retenez l'outil : une famille libre a une matrice de Gram inversible ; c'est exactement Q12(c).

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

Q15

$\langle X, Y \rangle_A = Y^\top A X$ est bilinéaire. Elle est symétrique car $(AX \mid Y) = (X \mid AY) = (AY \mid X)$ (A symétrique). Elle est définie positive car $\langle X, X \rangle_A = (AX \mid X) > 0$ pour $X \neq 0$ ($A \in \mathcal{S}_n^{++}(\mathbb{R})$). C'est un produit scalaire.
$\mathbb{B}_A = \{X \ ; \ (AX \mid X) \leqslant 1\}$. Pour $r > 0$, $A = \frac{1}{r^2} I_n$ convient : $(AX \mid X) \leqslant 1 \iff \|X\| \leqslant r$. Pour $r = 0$, c'est impossible : $B(0,0) = \{0\}$, alors qu'une boule unité fermée contient des vecteurs non nuls.

Q16

Pour $X, Y \in \mathcal{M}_{n,1}(\mathbb{R})$, comme B est symétrique :

$$\langle A^{-1}BX, Y \rangle_A = (BX \mid Y) = (X \mid BY) = (X \mid A(A^{-1}BY)) = (AX \mid A^{-1}BY) = \langle X, A^{-1}BY \rangle_A.$$

L'endomorphisme $X \mapsto A^{-1}BX$ est autoadjoint pour $\langle ., . \rangle_A$. Par le théorème spectral (dans l'espace euclidien $(\mathcal{M}_{n,1}(\mathbb{R}), \langle ., . \rangle_A)$), $A^{-1}B$ est **diagonalisable**, à valeurs propres réelles, dans une base orthonormée pour $\langle ., . \rangle_A$.

Q17 et Q18

Q17. $A - B$ est symétrique, et $B \preccurlyeq A \iff \forall X, \ ((A-B)X \mid X) \geqslant 0 \iff A - B \in \mathcal{S}_n^+(\mathbb{R})$.
Q18. Soit $(E_1, \ldots, E_n)$ une base $\langle ., . \rangle_A$-orthonormée de vecteurs propres de $A^{-1}B$: $A^{-1}BE_i = \lambda_i E_i$ (Q16). On a

$$(BE_i \mid E_i) = \langle A^{-1}BE_i, E_i \rangle_A = \lambda_i \quad \text{et} \quad (AE_i \mid E_i) = 1.$$

Comme $B \in \mathcal{S}_n^{++}(\mathbb{R})$, $\lambda_i > 0$: le spectre de $A^{-1}B$ est toujours dans $]0, +\infty[$.

($\Rightarrow$) Si $B \preccurlyeq A$, $\lambda_i = (BE_i \,|\, E_i) \leqslant (AE_i \,|\, E_i) = 1$.
($\Leftarrow$) Si tous les $\lambda_i \leqslant 1$: pour $X = \sum x_i E_i$, $(AX \,|\, X) = \|X\|_A^2 = \sum x_i^2$ et $(BX \,|\, X) = \langle A^{-1}BX, X\rangle_A = \sum \lambda_i x_i^2 \leqslant \sum x_i^2$.

Q19 et Q20

Q19. $\dfrac{\det B}{\det A} = \det(A^{-1}B) = \prod_i \lambda_i \in]0,1]$ par Q18, d'où $\det B \leqslant \det A$. Égalité $\iff \prod \lambda_i = 1 \iff$ tous les λ_i valent 1 (ils sont dans $]0,1]$) $\iff A^{-1}B = I_n$ ($A^{-1}B$ est diagonalisable de seule valeur propre 1) $\iff A = B$.
Q20 (avec $A \in \mathcal{S}_n^{++}(\mathbb{R})$, $B \in \mathcal{S}_n(\mathbb{R})$, $\mathbb{B}_B = \{X \ ; \ (BX \,|\, X) \leqslant 1\}$). Si $B \preccurlyeq A$ et $X \in \mathbb{B}_A$, alors $(BX \,|\, X) \leqslant (AX \,|\, X) \leqslant 1 : \mathbb{B}_A \subset \mathbb{B}_B$.
Réciproquement, supposons $\mathbb{B}_A \subset \mathbb{B}_B$ et soit $X \neq 0$. Alors $Y = X/\sqrt{(AX \,|\, X)} \in \mathbb{B}_A \subset \mathbb{B}_B$, donc $(BY \,|\, Y) \leqslant 1$, soit $(BX \,|\, X) \leqslant (AX \,|\, X)$. C'est aussi vrai pour $X = 0 : B \preccurlyeq A$.

Q21

Munissons $\mathcal{M}_n(\mathbb{R})$ de la norme d'opérateur $\|A\|_{\text{op}} = \sup_{\|X\|=1} \|AX\|$ (toutes les normes sont équivalentes).
Si K est bornée, il existe $M > 0$ tel que $\|A\|_{\text{op}} \leqslant M$ pour $A \in K$. Alors $(AX \,|\, X) \leqslant \|AX\|\,\|X\| \leqslant M\|X\|^2$ (Cauchy-Schwarz) : $A \preccurlyeq MI_n$.
Réciproquement, si $0 \preccurlyeq A \preccurlyeq \alpha I_n$ pour tout $A \in K$, les valeurs propres de A (symétrique) sont dans $[0,\alpha]$: pour un vecteur propre unitaire X, $\lambda = (AX \,|\, X) \leqslant \alpha$. Par le théorème spectral, $\|A\|_{\text{op}} = \max|\lambda| \leqslant \alpha$: K est bornée.

Q22 et Q23

Q22. Si $A, B \in \mathcal{S}_n^{++}(\mathbb{R})$ et $t \in [0,1]$, $tA + (1-t)B$ est symétrique et, pour $X \neq 0$, $((tA + (1-t)B)X \,|\, X) = t(AX \,|\, X) + (1-t)(BX \,|\, X) > 0$ (t et $1-t$ sont positifs et non tous deux nuls).
Q23. Soient $A, B \in \mathcal{S}_n^{++}(\mathbb{R})$, et $\mu_1, \ldots, \mu_n > 0$ les valeurs propres de $A^{-1}B$ (diagonalisable, Q16 et Q18). Alors $tA + (1-t)B = A\big(tI_n + (1-t)A^{-1}B\big)$, et

$$\varphi(tA + (1-t)B) = \ln\det A + \sum_{i=1}^{n} \ln\big(t \cdot 1 + (1-t)\mu_i\big).$$

Par concavité de ln : $\ln(t \cdot 1 + (1-t)\mu_i) \geqslant t \ln 1 + (1-t)\ln\mu_i$. En sommant :

$$\varphi(tA + (1-t)B) \geqslant \ln\det A + (1-t)\ln\det(A^{-1}B) = t\varphi(A) + (1-t)\varphi(B).$$

Pour $t \in]0,1[$, ln étant strictement concave, l'égalité impose $\mu_i = 1$ pour tout i, donc $A^{-1}B = I_n$ et $A = B$. Réciproquement, les cas $A = B$, $t = 0$ et $t = 1$ donnent bien l'égalité.

Q24 et Q25

Q24. $A = PDP^\top$ avec $P \in \mathrm{O}_n(\mathbb{R})$ et $D = \mathrm{diag}(d_i)$, $d_i > 0$. Posons $B = D^{1/2}P^\top$ (inversible) : $B^\top B = PDP^\top = A$. Soit $\psi : N \in \mathrm{O}_n(\mathbb{R}) \mapsto B^{-1}NB$. Pour $N \in \mathrm{O}_n(\mathbb{R})$:

$$(B^{-1}NB)^\top A(B^{-1}NB) = B^\top N^\top (B^{-1})^\top B^\top BB^{-1}NB = B^\top N^\top NB = B^\top B = A,$$

donc $\psi(N) \in \mathrm{O}(A)$. Réciproquement, si $M \in \mathrm{O}(A)$, alors $(BMB^{-1})^\top(BMB^{-1}) = (B^{-1})^\top M^\top AMB^{-1} = (B^{-1})^\top AB^{-1} = I_n$. ψ est donc une bijection de $\mathrm{O}_n(\mathbb{R})$ sur $\mathrm{O}(A)$, de réciproque $M \mapsto BMB^{-1}$, et $\psi(NN') = \psi(N)\psi(N')$. Ainsi $\mathrm{O}(A) = \psi(\mathrm{O}_n(\mathbb{R}))$ est l'image du

groupe $\mathrm{O}_n(\mathbb{R})$ par le morphisme de groupes $N \mapsto B^{-1}NB$ de $\mathrm{GL}_n(\mathbb{R})$ dans lui-même : c'est un sous-groupe de $\mathrm{GL}_n(\mathbb{R})$, isomorphe à $\mathrm{O}_n(\mathbb{R})$.
Q25. ψ est linéaire, donc continue sur $\mathcal{M}_n(\mathbb{R})$, et $\mathrm{O}_n(\mathbb{R})$ est compact : $\mathrm{O}(A) = \psi(\mathrm{O}_n(\mathbb{R}))$ est compact.

Q26 et Q27

Q26. $\det(G)$ est l'image du compact G par l'application continue det : elle est bornée. Si $M \in G$ avait $|\det M| = c \neq 1$, alors $M^k \in G$ pour $k \in \mathbb{Z}$ et $|\det M^k| = c^k$ ne serait pas borné (prendre $k \to +\infty$ si $c > 1$, $k \to -\infty$ si $c < 1$).
Q27. C est l'image du compact $G \times \mathbb{B}$ par l'application continue $(M, X) \mapsto MX$: il est compact. Comme $I_n \in G$, $\mathbb{B} \subset C$, et la boule ouverte $B_o(0,1) \subset C$: 0 est intérieur à C.

Q28

E est non vide. C est borné : $C \subset B(0,R)$ avec $R > 0$. Pour $A_0 = \frac{1}{R^2} I_n$, $(A_0 X \,|\, X) = \frac{\|X\|^2}{R^2} \leqslant 1$ sur C, donc $A_0 \in E$.
E est convexe. Si $A, A' \in E$ et $t \in [0,1]$: $tA + (1-t)A' \in \mathcal{S}_n^+(\mathbb{R})$, et pour $X \in C$, $((tA + (1-t)A')X \,|\, X) \leqslant t + (1-t) = 1$.
E est fermé. $E = \mathcal{S}_n^+(\mathbb{R}) \cap \bigcap_{X \in C} \{A \,;\, (AX \,|\, X) \leqslant 1\}$: intersection de fermés ($\mathcal{S}_n^+(\mathbb{R})$ est fermé et $A \mapsto (AX \,|\, X)$ est linéaire continue).
E est borné. Si $A \in E$, $\mathbb{B}_{I_n} = \mathbb{B} \subset C \subset \mathbb{B}_A$, donc $A \preccurlyeq I_n$ (Q20 avec $I_n \in \mathcal{S}_n^{++}(\mathbb{R})$), et E est bornée (Q21). Ainsi E est compact.
Existence. det est continue sur le compact E : elle y atteint son maximum en A_1. Comme $\det A_1 \geqslant \det A_0 > 0$, $A_1 \in \mathcal{S}_n^{++}(\mathbb{R})$.
Unicité. Si $A_1 \neq A_2$ réalisent le maximum Δ, alors $\frac{A_1+A_2}{2} \in E \cap \mathcal{S}_n^{++}(\mathbb{R})$ (convexité) et, par stricte concavité (Q23), $\ln\det\frac{A_1+A_2}{2} > \frac{1}{2}\ln\Delta + \frac{1}{2}\ln\Delta = \ln\Delta$. Cela contredit la maximalité.

Q29

Soit $M \in G$ et $A' = M^\top A M \in \mathcal{S}_n^{++}(\mathbb{R})$. Pour $X \in C$, $MX \in C$ (C est stable par G : $M(NY) = (MN)Y$), donc $(A'X \,|\, X) = (AMX \,|\, MX) \leqslant 1$: $A' \in E$. De plus, $\det A' = (\det M)^2 \det A = \det A$ par Q26. Par unicité (Q28), $A' = A$, c'est-à-dire $M \in \mathrm{O}(A)$. Donc G est un sous-groupe de $\mathrm{O}(A)$, et par Q24, $M \mapsto BMB^{-1}$ envoie G isomorphiquement sur un sous-groupe de $\mathrm{O}_n(\mathbb{R})$.

prepasmaths360.com

Remarque du professeur

L'ensemble $\mathbb{B}_A$ est un *ellipsoïde*, de volume proportionnel à $(\det A)^{-1/2}$. Maximiser $\det A$ sous la contrainte $C \subset \mathbb{B}_A$, c'est donc chercher **le plus petit ellipsoïde contenant** C : c'est l'ellipsoïde de John-Loewner. Son unicité (Q28) force sa stabilité par G (Q29), et G devient un groupe d'isométries pour la norme $\|.\|_A$. Retenez la conclusion : *tout sous-groupe compact de* $\mathrm{GL}_n(\mathbb{R})$ *est conjugué à un sous-groupe de* $\mathrm{O}_n(\mathbb{R})$. Le schéma « unicité d'un objet extrémal, donc invariance par le groupe » est très fréquent.

Partie C — Croissance du groupe de Heisenberg discret

Q30 et Q31

Q30. Si $g = s_1^{a_1}\cdots s_k^{a_k}$, alors $g^{-1} = s_k^{-a_k}\cdots s_1^{-a_1}$, avec la même somme $\sum|a_i| : \ell_S(g^{-1}) \leqslant \ell_S(g)$, et l'inégalité inverse s'obtient en échangeant g et g^{-1}. En concaténant une écriture minimale de g et une de h, on obtient une écriture de gh de poids $\ell_S(g)+\ell_S(h)$ (les cas $g=e$ ou $h=e$ sont immédiats).

Q31. Posons $c = \max\big(1, \max_{\sigma\in\Sigma}\ell_S(\sigma)\big)$ (fini, car Σ est fini). Si $g = \sigma_1^{b_1}\cdots\sigma_k^{b_k}$ avec $\sum|b_i| = \ell_\Sigma(g)$, Q30 donne $\ell_S(\sigma^b) \leqslant |b|\ell_S(\sigma)$, puis $\ell_S(g) \leqslant \sum|b_i|\ell_S(\sigma_i) \leqslant c\,\ell_\Sigma(g)$. De même, $\ell_\Sigma \leqslant c'\ell_S$ avec $c' = \max\big(1, \max_{s\in S}\ell_\Sigma(s)\big)$. D'où $C = \frac{1}{c}$ et $C' = c'$.

Conséquence. $V_\Sigma(p) \subset V_S(cp)$ et $V_S(q) \subset V_\Sigma(c'q)$. Si $\alpha p^d \leqslant |V_S(p)| \leqslant \beta p^d$ pour $p \geqslant 1$, alors $|V_\Sigma(p)| \leqslant \beta c^d p^d$. Pour la minoration, si $p \geqslant c'$ et $q = \lfloor p/c'\rfloor \geqslant \frac{p}{2c'}$:

$$|V_\Sigma(p)| \geqslant |V_S(q)| \geqslant \alpha\Big(\frac{p}{2c'}\Big)^d,$$

et si $1 \leqslant p < c'$, $|V_\Sigma(p)| \geqslant 1 \geqslant \big(\frac{p}{c'}\big)^d$. La croissance polynomiale de degré d ne dépend donc pas de la partie génératrice.

Q32

En ajoutant une variable d'écart $w = p-x-y-z \geqslant 0$, il s'agit de compter les $(x,y,z,w)\in\mathbb{N}^4$ de somme p : il y en a $\binom{p+3}{3}$.

Dans $\mathbb{Z}^3$ avec $S = \{e_1,e_2,e_3\}$ (notation additive), $\ell_S(a,b,c) = |a|+|b|+|c|$. En effet, cette somme est atteinte, et dans toute écriture la somme des coefficients portant sur e_1 vaut a, donc la somme de leurs valeurs absolues est au moins $|a|$. Donc $V_S(p) = \{(a,b,c)\ ;\ |a|+|b|+|c| \leqslant p\}$. L'application $(a,b,c)\mapsto(|a|,|b|,|c|)$ envoie $V_S(p)$ sur les triplets comptés ci-dessus, chacun ayant au plus 8 antécédents. Pour $p \geqslant 1$:

$$\frac{p^3}{6} \leqslant \binom{p+3}{3} \leqslant |V_S(p)| \leqslant 8\binom{p+3}{3} \leqslant \frac{8(4p)^3}{6}.$$

$(\mathbb{Z}^3,+)$ est à croissance polynomiale de degré 3.

Q33 à Q35

Notons E_{ab} les matrices élémentaires : $S = I+E_{23}$, $T = I+E_{12}$, $U = I+E_{13}$, avec $E_{ab}E_{cd} = \delta_{bc}E_{ad}$.

Q33. $E_{23}^2 = E_{12}^2 = E_{13}^2 = 0$, donc $S^i = I+iE_{23}$, $T^j = I+jE_{12}$, $U^k = I+kE_{13}$ pour tout entier

relatif ($(I+iE)(I-iE)=I$). Comme $E_{23}E_{12}=0$, $E_{12}E_{13}=0$ et $E_{23}E_{13}=0$:

$$S^iT^jU^k=\begin{pmatrix}1&j&k\\0&1&i\\0&0&1\end{pmatrix}.$$

Q34. Le produit de deux telles matrices vaut

$$\begin{pmatrix}1&j&k\\0&1&i\\0&0&1\end{pmatrix}\begin{pmatrix}1&j'&k'\\0&1&i'\\0&0&1\end{pmatrix}=\begin{pmatrix}1&j+j'&k+k'+ji'\\0&1&i+i'\\0&0&1\end{pmatrix},$$

donc $(i'',j'',k'')=(i+i',\ j+j',\ k+k'+ji')$.
Q35. Par Q34, $US=SU=S^1T^0U^1$ et $UT=TU=S^0T^1U^1$. Donc U commute avec S, T, U et leurs inverses, puis avec tout produit de ces matrices, c'est-à-dire avec tout élément de H. Enfin, Q34 avec $(0,j,0)$ et $(i,0,0)$ donne $T^jS^i=S^iT^jU^{ij}$.

Q36 et Q37

Q36. $TS=STU\neq ST$: H n'est pas commutatif. Comme $U=(ST)^{-1}TS\in\langle S,T\rangle$, on a $\langle S,T\rangle=H$.
Q37. f est bien définie, car $S,T,U\in H$. Elle est injective : la matrice de Q33 détermine (i,j,k). L'image de f contient I_3, S, T, U et est stable par produit (Q34) et par inverse. En effet, Q34 donne $(S^iT^jU^k)^{-1}=S^{-i}T^{-j}U^{ij-k}$, car $k+k'+j(-i)=0$ pour $k'=ij-k$. C'est donc un sous-groupe contenant $\mathcal{A}$: il est égal à H, et f est surjective.
f n'est pas un morphisme pour l'addition usuelle : $f(0,1,0)f(1,0,0)=TS=f(1,1,1)\neq f(1,1,0)$. D'ailleurs H n'est pas commutatif. On transporte la structure : la loi

$$(i,j,k)\star(i',j',k')=(i+i',\ j+j',\ k+k'+ji')$$

fait de $\mathbb{Z}^3$ un groupe, et f un isomorphisme (par construction, $x\star y=f^{-1}(f(x)f(y))$).

Q38

L'énoncé est inexact. Par Q35, $T^aS^bT^{-a}S^{-b} = S^bT^aU^{ab}T^{-a}S^{-b} = U^{ab}$. Donc $M = U^{100}$ vérifie $\ell_{\mathcal{A}}(M) \leqslant 40$ (avec $a = b = 10$). Mais, par unicité de l'écriture (Q37), $M = S^iT^jU^{k+z}$ impose $i = j = 0$ et $k + z = 100$: on ne peut avoir à la fois $|k| \leqslant 40$ et $|z| \leqslant |ij| = 0$. L'énoncé correct, qui suffit pour la conclusion, est :

$$\ell_{\mathcal{A}}(M) \leqslant p \implies M = S^iT^jU^{k+z} \text{ avec } |i| + |j| + |k| \leqslant p \text{ et } |z| \leqslant p^2.$$

Preuve. Écrivons $M = s_1^{a_1} \cdots s_m^{a_m}$ avec $\sum |a_l| \leqslant p$. Notons I', J', K' les sommes des $|a_l|$ portant respectivement sur S, T, U (donc $I' + J' + K' \leqslant p$). Montrons par récurrence sur m que $s_1^{a_1} \cdots s_m^{a_m} = S^iT^jU^{k+z}$ avec $|i| \leqslant I'$, $|j| \leqslant J'$, $|k| \leqslant K'$ et $|z| \leqslant I'J'$. On multiplie à droite par le facteur suivant :

- par U^c : k devient $k + c$ (U est central) ;
- par T^b : $S^iT^jU^{k+z}T^b = S^iT^{j+b}U^{k+z}$;
- par S^a : $T^jS^a = S^aT^jU^{ja}$ (Q35), donc z devient $z+ja$, avec $|z+ja| \leqslant I'J'+J'|a| = (I'+|a|)J'$.

D'où $|i| + |j| + |k| \leqslant p$ et $|z| \leqslant I'J' \leqslant \frac{p^2}{4}$.

Conséquence. $V_{\mathcal{A}}(p) \subset \{S^iT^jU^c \ ; \ |i| \leqslant p, \ |j| \leqslant p, \ |c| \leqslant p + p^2\}$. Avec l'injectivité de f, on obtient, pour $p \geqslant 1$:

$$|V_{\mathcal{A}}(p)| \leqslant (2p + 1)^2(2p^2 + 2p + 1) \leqslant (3p)^2 \cdot 5p^2 = 45p^4.$$

Donc $|V_{\mathcal{A}}(p)| = O(p^4)$.

Q39

L'énoncé est inexact pour k du signe opposé à ij. Avec $i = j = 1$, $k = -1$ et $p = 2$: les éléments de longueur $\leqslant 2$ dont les exposants totaux en S et en T valent 1 sont $ST = S\,T\,U^0$ et $TS = S\,T\,U^1$. Donc $\ell_{\mathcal{A}}(STU^{-1}) > 2$. Le résultat est vrai si k est compris entre 0 et ij, ce qui est le seul cas utilisé en Q40–Q41.

Preuve dans ce cas. Supposons d'abord $i, j \geqslant 0$ et $0 \leqslant k \leqslant ij$. Considérons un mot formé de i lettres S et j lettres T, d'exposants $+1$. Par Q35, en ramenant toutes les lettres S à gauche, chaque couple « une lettre T placée avant une lettre S » produit un facteur U : le mot vaut $S^iT^jU^z$, où z est le nombre de tels couples. Or z prend toutes les valeurs de 0 à ij. Par exemple, si $i \geqslant 1$ et $k = qi + r$ ($0 \leqslant r < i$), le mot $T^qS^{i-r}TS^rT^{j-q-1}$ donne $z = qi + r$ si $q < j$, et T^jS^i donne $z = ij$. Ce mot a pour poids $i + j \leqslant p$. Pour des signes quelconques, on utilise des lettres $S^{\pm 1}$, $T^{\pm 1}$ de signes fixés : chaque couple contribue ± 1, du signe de ij. On obtient ainsi tous les k compris entre 0 et ij.

Q40 et Q41

Q40. Le cardinal vaut $\sum_{i+j\leqslant p}(ij+1) \geqslant \sum_{i=0}^{p} i\sum_{j=0}^{p-i} j = \sum_{i=0}^{p} \frac{i(p-i)(p-i+1)}{2} \geqslant \sum_{i=0}^{p} \frac{i(p-i)^2}{2}$. Or $i(p-i)^2 = p^3 \cdot \frac{i}{p}\left(1-\frac{i}{p}\right)^2$, d'où l'inégalité. C'est une somme de Riemann :

$$\frac{p^3}{2}\sum_{i=0}^{p}\frac{i}{p}\left(1-\frac{i}{p}\right)^2 = \frac{p^4}{2}\cdot\frac{1}{p}\sum_{i=0}^{p}\frac{i}{p}\left(1-\frac{i}{p}\right)^2 \underset{p\to+\infty}{\sim} \frac{p^4}{2}\int_0^1 x(1-x)^2\,\mathrm{d}x = \frac{p^4}{24}.$$

Q41. Par Q39 (cas $i,j,k\geqslant 0$) et l'injectivité de f, $|V_{\mathcal{A}}(p)|$ est au moins égal au cardinal de Q40, qui est équivalent à $\frac{p^4}{24}$. Il existe donc p_0 tel que $|V_{\mathcal{A}}(p)| \geqslant \frac{p^4}{48}$ pour $p\geqslant p_0$; pour $1\leqslant p<p_0$, $|V_{\mathcal{A}}(p)|\geqslant 1 \geqslant \frac{p^4}{p_0^4}$. Avec la majoration de Q38, pour tout $p\geqslant 1$:

$$\min\left(\frac{1}{48},\frac{1}{p_0^4}\right)p^4 \leqslant |V_{\mathcal{A}}(p)| \leqslant 45p^4.$$

H est à croissance polynomiale de degré 4 (et ce, pour toute partie génératrice finie, par Q31).

Remarque du professeur

Le groupe de Heisenberg est « presque » $\mathbb{Z}^3$ en tant qu'ensemble (Q37), mais il croît comme p^4 et non comme p^3. Le centre $\langle U\rangle$ est « quadratique » : un commutateur $T^aS^bT^{-a}S^{-b}=U^{ab}$ fabrique U^{ab} avec seulement $2(a+b)$ lettres. C'est précisément ce phénomène qui rend fausses les questions Q38 et Q39 telles qu'elles sont posées : le jury a vraisemblablement voulu écrire $|z|\leqslant p^2$ en Q38, et k entre 0 et ij en Q39. Sur une copie, un contre-exemple court, suivi de la démonstration de l'énoncé rectifié, est exactement ce qu'on attend. Pour aller plus loin : le degré $4=1+1+2\times 1$ est donné par la formule de Bass-Guivarc'h, et un théorème célèbre de Gromov (1981) caractérise les groupes à croissance polynomiale.

Pour aller plus loin : le rapport du jury. Le concours Centrale-Supélec publie chaque année un rapport détaillant, question par question, les réussites et les erreurs les plus fréquentes des candidats. Lisez celui de cette épreuve après avoir composé : **rapports de jury, filière MP, sur concours-centrale-supelec.fr**.



Pr. Abdelfattah ELAKILI

Agrégé de mathématiques depuis 1991, plus de 20 ans d'enseignement en classes préparatoires.

Cours particuliers à Casablanca ou à distance :

WhatsApp +212 648 66 22 39

Annales corrigées, cours et exercices :

prepasmaths360.com

WhatsApp