



PULSARS

CORRECTION INDÉPENDANTE

Centrale-Supélec 2026 — Mathématiques 1 (MP, MPI)

SESSION	NIVEAU	DURÉE	FILIÈRES
2026	CPGE	—	MP • MPI

Correction indépendante rédigée par Pulsars. Elle n'est ni officielle ni affiliée à l'organisateur du concours. Les énoncés ne sont pas reproduits : le sujet officiel reste consultable sur le site du concours.

Partie A · I — Généralités (Q1 à Q3)

G désigne un sous-groupe de $GL_n(\mathbb{R})$. Un groupe est dit **d'exposant fini** lorsqu'un même entier m vérifie $x^m = e$ pour tout élément, et on note $\text{tr } G$ l'ensemble des traces de ses éléments.

- **Q1** — un sous-groupe fini est d'exposant fini et sa trace est finie.

Q1. Soit G fini, d'ordre N .

Le théorème de Lagrange donne, pour tout x de G , que l'ordre de x divise N , donc $x^N = e$: l'entier $m = N$ convient et G est d'exposant fini.

Par ailleurs $\text{tr } G$ est l'image de G par l'application trace, donc $|\text{tr } G| \leq |G| = N < +\infty$.

Les deux réciproques sont fausses en général — c'est tout l'objet des parties qui suivent, où elles redeviennent vraies dans $GL_n(\mathbb{R})$.

- **Q2** — un contre-exemple : un sous-groupe infini de trace finie.

Q2. Prenons les matrices de transvection

$T_t = I_n + t E_{\{1,2\}}$, où $E_{\{1,2\}}$ est la matrice élémentaire.

Comme $E_{\{1,2\}}^2 = 0$, on a $T_t T_s = I_n + (t + s) E_{\{1,2\}} = T_{\{t+s\}}$: la famille $G = \{T_t ; t \in \mathbb{R}\}$ est un sous-groupe de $GL_n(\mathbb{R})$, isomorphe à $(\mathbb{R}, +)$, donc infini.

Or $\text{tr } T_t = n$ pour tout t : $\text{tr } G = \{n\}$ est fini.

- **Q3** — un groupe infini d'exposant fini, matriciel ou non.

Q3. Un groupe infini d'exposant fini : l'ensemble des suites (x_k) d'éléments de $\mathbb{Z}/2\mathbb{Z}$ nulles à partir d'un certain rang, muni de l'addition terme à terme.

Il est infini, et tout élément x vérifie $x + x = 0$, donc $m = 2$ convient.

Autrement dit, la somme directe d'une infinité de copies de $\mathbb{Z}/2\mathbb{Z}$ — ou encore le groupe additif d'un espace vectoriel de dimension infinie sur le corps à deux éléments.

Partie A · II — Les sous-groupes finis de $O_2(\mathbb{R})$ (Q4 à Q8)

On note R_θ la rotation d'angle θ et S_θ la réflexion associée, avec les relations rappelées par le sujet.

- **Q4** — toute matrice de $SO_2(\mathbb{R})$ s'écrit R_θ pour un unique θ de $[0, 2\pi[$.

Q4. Soit $A \in SO_2(\mathbb{R})$, de colonnes C_1 et C_2 .

C_1 est unitaire : $a^2 + c^2 = 1$, donc il existe un unique $\theta \in [0, 2\pi[$ tel que $a = \cos \theta$ et $c = \sin \theta$.

C_2 est unitaire et orthogonale à C_1 , donc $C_2 = \pm(-\sin \theta, \cos \theta)$. Le déterminant vaut $\cos^2 \theta + \sin^2 \theta = 1$ avec le signe $+$, et -1 avec le signe $-$. Comme $\det A = 1$, c'est le signe $+$: $A = R_\theta$.

L'unicité vient de celle de θ dans $[0, 2\pi[$ pour un couple $(\cos \theta, \sin \theta)$ donné.

- **Q5** — étude du groupe engendré par une seule rotation : forme des éléments, cardinal pour $\theta = 2\pi/m$, finitude équivalente à θ/π rationnel, et les deux réciproques (exposant fini, trace finie).

Q5. a) De $R_\theta R_\varphi = R_{\theta+\varphi}$ et $R_0 = I_2$ on tire $R_\theta^k = R_{\{k\theta\}}$ pour tout $k \in \mathbb{Z}$ (récurrence, puis passage à l'inverse).

L'ensemble $\{R_{\{k\theta\}} ; k \in \mathbb{Z}\}$ est donc un sous-groupe contenant R_θ , et tout sous-groupe contenant R_θ le contient : c'est bien $\langle R_\theta \rangle$.

b) Pour $\theta = 2\pi/m$, on a $R_{\{k\theta\}} = R_{\{k'\theta\}}$ si et seulement si $(k - k') \cdot 2\pi/m \in 2\pi\mathbb{Z}$, c'est-à-dire $k \equiv k' \pmod{m}$.

Les éléments $R_0, R_\theta, \dots, R_{\{(m-1)\theta\}}$ sont donc deux à deux distincts et épuisent G : $|G| = m$.

c) Si G est fini, deux exposants coïncident : $R_{\{k\theta\}} = R_{\{k'\theta\}}$ avec $k \neq k'$, donc $(k - k')\theta = 2\pi l$ pour un entier l , d'où $\theta/\pi = 2l/(k - k') \in \mathbb{Q}$.

Réciproquement, si $\theta/\pi = p/q$ avec $q \neq 0$, alors $2q\theta = 2p\pi \in 2\pi\mathbb{Z}$, donc $R_\theta^{2q} = I_2$: l'ordre de R_θ est fini et G aussi.

d) Si G est d'exposant fini, $R_\theta^m = I_2$ pour un certain $m \geq 1$, donc $m\theta \in 2\pi\mathbb{Z}$ et $\theta/\pi \in \mathbb{Q}$: G est fini d'après **c**).

e) On a $\text{tr } R_{\{k\theta\}} = 2 \cos(k\theta)$.

Supposons $\theta/\pi \notin \mathbb{Q}$ et posons $H = \theta\mathbb{Z} + 2\pi\mathbb{Z}$, sous-groupe de $(\mathbb{R}, +)$.

H n'est pas de la forme $a\mathbb{Z}$: sinon $\theta = pa$ et $2\pi = qa$, d'où $\theta/2\pi = p/q \in \mathbb{Q}$, exclu. Un sous-groupe de $(\mathbb{R}, +)$ étant **discret ou dense**, H est dense dans $\mathbb{R}$.

Les réels $k\theta$ modulo 2π sont donc denses dans $[0, 2\pi[$, et $\cos y$ prend une infinité de valeurs : $\text{tr } G$ serait infini.

Par contraposée, $\text{tr } G$ fini entraîne $\theta/\pi \in \mathbb{Q}$, donc G fini d'après **c**).

- **Q6** — le groupe engendré par deux rotations, puis le cas $\langle R_{\pi/p}, R_{\pi/q} \rangle$.

Q6. a) Notons $H = \theta Z + \theta' Z + 2\pi Z$ l'ensemble des angles α tels que $R_\alpha \in G$ — l'ajout de $2\pi Z$ est licite puisque $R_{2\pi} = I_2 \in G$.

Comme $R_\alpha = R_\beta$ si et seulement si $\alpha - \beta \in 2\pi Z$, l'application $\alpha \mapsto R_\alpha$ induit une bijection de $H \cap [0, 2\pi[$ sur G :

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

C'est la lecture qu'il faut donner de l'énoncé : sans le terme $2\pi Z$, l'égalité tomberait en défaut, par exemple pour $\theta = 1$ et $\theta' = 2$, où le groupe est infini alors que $Z \cap [0, 2\pi[$ ne compte que sept éléments.

b) Pour $\theta = \pi/p$ et $\theta' = \pi/q$:

$$(\pi/p)Z + (\pi/q)Z = (\pi/pq)(qZ + pZ) = (\pi/pq) \cdot \text{pgcd}(p, q)Z = (\pi/pq)Z$$

puisque p et q sont premiers entre eux — c'est le théorème de Bézout.

Ce groupe contient $2\pi Z$, donc $H = (\pi/pq)Z$ et le nombre de ses éléments dans $[0, 2\pi[$ est $2\pi \div (\pi/pq) = 2pq$.

c) Sans hypothèse de coprimarité, $qZ + pZ = \text{pgcd}(p, q)Z$, donc $H = (\pi \cdot \text{pgcd}(p, q) / pq)Z = (\pi / \text{ppcm}(p, q))Z$ et

$$|\langle R_{\pi/p}, R_{\pi/q} \rangle| = 2 \cdot \text{ppcm}(p, q) = 2pq / \text{pgcd}(p, q).$$

- **Q7** — tout sous-groupe fini de $S_2(\mathbb{R})$ est monogène.

Q7. Soit G un sous-groupe fini de $S_2(\mathbb{R})$, et H l'ensemble des angles correspondants : c'est un sous-groupe de $(\mathbb{R}, +)$ contenant $2\pi Z$.

H n'est pas dense, sans quoi G serait infini : il est donc **discret**, de la forme aZ avec $a > 0$ son plus petit élément strictement positif.

Alors $G = \{R_{ka} \mid k \in \mathbb{Z}\} = \langle R_a \rangle$ est **monogène**, engendré par la rotation d'angle $2\pi/|G|$.

- **Q8** — le groupe diédral D_m : son cardinal, et le fait que tout sous-groupe fini de $O_2(\mathbb{R})$ non inclus dans $S_2(\mathbb{R})$ lui est isomorphe.

Q8. a) Posons $D_m = \langle R_{2\pi/m}, S_{\pi/2} \rangle$.

Les relations $R_\theta S_\varphi = S_{\theta+\varphi}$ et $S_\varphi S_\psi = R_{\varphi-\psi}$ montrent qu'un produit de générateurs est une rotation ou une réflexion, et que

$$D_m \cap S_2(\mathbb{R}) = \langle R_{2\pi/m} \rangle, \text{ de cardinal } m \text{ d'après Q5.b).}$$

L'application $A \mapsto A \cdot S_{\pi/2}$ envoie $D_m \cap S_2(\mathbb{R})$ dans $D_m \setminus S_2(\mathbb{R})$ — une rotation composée d'une réflexion est une réflexion — et l'application $A \mapsto A \cdot S_{\pi/2}$ en sens inverse lui est réciproque, $S_{\pi/2}$ étant involutive.

C'est donc une bijection entre les deux moitiés : $|D_m| = 2m$.

b) Soit G un sous-groupe fini de $O_2(\mathbb{R})$ non inclus dans $S_2(\mathbb{R})$.

$G \cap S_2(\mathbb{R})$ est un sous-groupe fini de $S_2(\mathbb{R})$, donc monogène d'après **Q7** : $G \cap S_2(\mathbb{R}) = \langle R_{2\pi/m} \rangle$ pour un certain m .

Fixons $S \in G \setminus S_2(\mathbb{R})$: c'est une réflexion, et $A \mapsto AS$ est une bijection de $G \cap S_2(\mathbb{R})$ sur $G \setminus S_2(\mathbb{R})$, d'où $|G| = 2m$.

Enfin $G = \langle R_{2\pi/m}, S \rangle$, et les relations satisfaites par ces deux générateurs sont celles de D_m : l'application qui envoie $R_{2\pi/m}$ sur $R_{2\pi/m}$ et $S_{\pi/2}$ sur S induit un isomorphisme $D_m \cong G$.

Partie A · III — Caractérisation des sous-groupes finis de $O_n(\mathbb{R})$ (Q9 à Q14)

G est ici un sous-groupe de $O_n(\mathbb{R})$, et l'on veut établir les équivalences

G fini $\Leftrightarrow G$ d'exposant fini $\Leftrightarrow \text{tr } G$ fini.

- **Q9** — rappeler le théorème de réduction des matrices orthogonales.

Q9. Pour toute $M \in O_n(\mathbb{R})$, il existe $P \in O_n(\mathbb{R})$ telle que $P^{-1} M P$ soit diagonale par blocs, de la forme

$\text{diag}(I_p, -I_q, R_{\{\theta_1\}}, \dots, R_{\{\theta_r\}})$ avec $p + q + 2r = n$ et $\theta_i \in]0, \pi[$,

les $R_{\{\theta_i\}}$ étant les blocs de rotation 2×2 .

- **Q10** — exposant fini entraîne trace finie.
- **Q11 à Q14** — la réciproque, en considérant le sous-espace F engendré par G dans $M_n(\mathbb{R})$, une base extraite de G , la matrice de Gram associée et les coordonnées d'un élément de G dans cette base.

Q10. Soit m un exposant de G et $M \in G$. Réduisons M comme ci-dessus.

De $M^m = I_n$ on tire $R_{\{\theta_i\}}^m = R_{\{m\theta_i\}} = I_2$, donc $m\theta_i \in 2\pi\mathbb{Z}$: chaque θ_i appartient à $(2\pi/m)\mathbb{Z} \cap]0, \pi[$, ensemble d'au plus m éléments.

Or la trace est invariante par conjugaison :

$$\text{tr } M = p - q + 2(\cos \theta_1 + \dots + \cos \theta_r).$$

Le triplet (p, q, r) prend un nombre fini de valeurs — au plus $(n+1)^3$ — et chaque θ_i un nombre fini de valeurs : $\text{tr } G$ est fini.

Q11. $F = \text{Vect}(G)$ est engendré par la famille G . Le théorème de la base extraite fournit une sous-famille de G qui est une base de F : c'est la famille $B = (A_i)_{i \in [1, d]}$, avec $d = \dim F$.

Q12. a) C a pour colonnes les coordonnées des d matrices A_i dans la base canonique de $M_n(\mathbb{R})$, laquelle compte n^2 vecteurs : C est de taille $n^2 \times d$.

b) La base canonique de $M_n(\mathbb{R})$ est **orthonormée** pour le produit scalaire $(A|B) = \text{tr}(A^T B)$. Le coefficient (i, j) de $C^T C$ vaut donc

$$\sum_k C_{\{k, i\}} C_{\{k, j\}} = (A_i | A_j) = B_{\{i, j\}}, \text{ d'où } B = C^T C.$$

c) Pour toute matrice C , $\text{rg}(C^T C) = \text{rg}(C)$ — les noyaux coïncident, car $C^T C X = 0$ entraîne $\|CX\|^2 = X^T C^T C X = 0$ donc $CX = 0$.

Les colonnes de C sont les coordonnées d'une famille libre, donc $\text{rg}(C) = d$, et B est une matrice carrée de taille d et de rang d : elle est **invertible**.

Q13. Par bilinéarité, pour tout i :

$$(A_i | M) = (A_i | \sum_j x_j A_j) = \sum_j x_j (A_i | A_j) = (B X_M)_i.$$

Autrement dit $Y_M = B X_M$, et B étant invertible, $X_M = B^{-1} Y_M$.

Q14. Ici A_i et M appartiennent à $G \subset O_n(\mathbb{R})$, donc $A_i^T = A_i^{-1}$ et $A_i^{-1} M \in G$. Ainsi

$$(A_i | M) = \text{tr}(A_i^T M) = \text{tr}(A_i^{-1} M) \in \text{tr } G.$$

Chaque coordonnée de Y_M vit donc dans l'ensemble fini $\text{tr } G$, et $\{Y_M ; M \in G\}$ compte au plus $|\text{tr } G|^d$ éléments : il est fini.

Or $X_M = B^{-1} Y_M$ détermine $M = \sum_j x_j A_j$. L'application $M \mapsto Y_M$ est donc **injective** sur G , à valeurs dans un ensemble fini : G est fini.

Les trois propriétés sont ainsi équivalentes : **Q1** donne « fini $\Rightarrow$ exposant fini » et « fini $\Rightarrow$ trace finie », **Q10** donne « exposant fini $\Rightarrow$ trace finie », et **Q14** referme la boucle.

Partie B · I — Quelques propriétés utiles (Q15 à Q21)

A et B désignent des matrices symétriques, A définie positive. On pose $\langle X, Y \rangle_A = (AX|Y)$ et l'on note $B \leq A$ lorsque $(BX|X) \leq (AX|X)$ pour tout X .

- **Q15** — $\langle \cdot, \cdot \rangle_A$ est un produit scalaire ; une boule euclidienne est-elle une boule pour une telle norme ?

Q15. La bilinéarité est immédiate. Pour la symétrie, A étant symétrique :

$$\langle X, Y \rangle_A = (AX)^T Y = X^T A^T Y = X^T A Y,$$

expression symétrique en X et Y puisque c'est un scalaire, égal à sa transposée. Enfin $\langle X, X \rangle_A = X^T A X > 0$ pour $X \neq 0$, A étant définie positive : c'est bien un **produit scalaire**.

Quant à la boule $B(0, r)$, elle est de la forme B_A : il suffit de prendre

$$A = (1/r^2) I_n \in S_n^{++}(R),$$

car $\langle X, X \rangle_A = \|X\|^2 / r^2 \leq 1$ équivaut à $\|X\| \leq r$.

- **Q16** — $X \mapsto A^{-1}BX$ est autoadjoint pour ce produit scalaire.
- **Q17 à Q21** — caractérisations de $\leq$: par la positivité de $A - B$, par le spectre de $A^{-1}B$, par les déterminants, par l'inclusion des boules, et enfin le lien entre partie bornée de $S_n^+(R)$ et majoration par αI_n .

Q16. Pour tous X et Y :

$$\langle A^{-1}BX, Y \rangle_A = (A A^{-1} B X | Y) = (BX | Y) = X^T B Y,$$

et de même $\langle X, A^{-1}BY \rangle_A = (BY | X) = Y^T B X$, qui est le transposé du scalaire précédent, donc lui est égal. L'endomorphisme est **autoadjoint**.

Le théorème spectral s'applique alors : $A^{-1}B$ est **diagonalisable dans une base orthonormée pour $\langle \cdot, \cdot \rangle_A$** , et son **spectre est réel**.

Q17. $A - B$ est symétrique, et par définition

$$B \leq A \Leftrightarrow \forall X, (AX|X) - (BX|X) \geq 0 \Leftrightarrow \forall X, ((A-B)X|X) \geq 0 \Leftrightarrow A - B \in S_n^+(R).$$

Q18. Supposons $B \leq A$ et soit λ une valeur propre de $A^{-1}B$, de vecteur propre $X \neq 0$: $BX = \lambda AX$. En prenant le produit scalaire avec X :

$$(BX|X) = \lambda (AX|X), \text{ donc } \lambda = (BX|X)/(AX|X).$$

Le dénominateur est > 0 et le numérateur aussi (B est définie positive), donc $\lambda > 0$; et $\lambda \leq 1$ puisque

$$(BX|X) \leq (AX|X). \text{ D'où } \text{Sp}(A^{-1}B) \subset]0, 1].$$

Réciproquement, prenons une base (e_i) orthonormée pour $(\cdot, \cdot)_A$ qui diagonalise $A^{-1}B$ (**Q16**), de valeurs propres $\lambda_i \in]0, 1]$. Pour $X = \sum x_i e_i$:

$$(BX|X) = (A^{-1}BX, X)_A = \sum \lambda_i x_i^2 \leq \sum x_i^2 = (X, X)_A = (AX|X).$$

Q19. Avec les notations précédentes, $\det(A^{-1}B) = \lambda_1 \cdots \lambda_n \leq 1$, donc

$$\det B \leq \det A.$$

Il y a égalité si et seulement si tous les λ_i valent 1, c'est-à-dire — la matrice étant diagonalisable — si et seulement si $A^{-1}B = I_n$, soit $A = B$.

Q20. Si $B \leq A$ et $X \in B_A$, alors $(BX|X) \leq (AX|X) \leq 1$ donc $X \in B_B$: $B_A \subset B_B$.

Réciproquement, supposons $B_A \subset B_B$ et soit $X \neq 0$. Posons $t = 1/\sqrt{(AX|X)}$, de sorte que $(A(tX)|tX) = 1$ et $tX \in B_A \subset B_B$. Alors

$$t^2(BX|X) \leq 1, \text{ c'est-à-dire } (BX|X) \leq (AX|X).$$

Q21. Si $A \leq \alpha I_n$ pour tout $A \in K$, alors pour $\|X\| = 1$ on a $(AX|X) \leq \alpha$. Or pour une matrice symétrique positive, $\max_{\|X\|=1} (AX|X)$ est sa plus grande valeur propre, qui majore sa norme d'opérateur : K est **bornée**.

Réciproquement, si K est bornée, toutes les normes étant équivalentes en dimension finie, il existe $M > 0$ majorant la norme d'opérateur sur K . Alors

$$(AX|X) \leq |A| \cdot |X|^2 \leq M |X|^2 = (M I_n X | X),$$

donc $A \leq M I_n$: $\alpha = M$ convient.

Partie B · II — Stricte log-concavité du déterminant (Q22, Q23)

- **Q22** — $S_n^{++}(R)$ est une partie convexe de $M_n(R)$.

Q22. Soient A et B dans $S_n^{++}(R)$ et $t \in [0, 1]$.

La matrice $tA + (1-t)B$ est symétrique comme combinaison de matrices symétriques, et pour $X \neq 0$:

$$X^T (tA + (1-t)B) X = t \cdot X^T A X + (1-t) \cdot X^T B X > 0,$$

les deux termes étant positifs et l'un au moins strictement — pour $t \in]0, 1[$ les deux le sont, et pour $t = 0$ ou $t = 1$ on retrouve B ou A .

- **Q23** — $A \mapsto \ln(\det A)$ y est **strictement** concave, au sens défini par le sujet (égalité seulement si $A = B$, $t = 0$ ou $t = 1$).

Q23. Soient A et B dans $S_n^{++}(R)$.

D'après **Q16**, il existe une base orthonormée pour $(\cdot, \cdot)_A$ diagonalisant $A^{-1}B$. En notant P la matrice de passage correspondante, cela se traduit par la **réduction simultanée** :

$$P^T A P = I_n \text{ et } P^T B P = D = \text{diag}(\lambda_1, \dots, \lambda_n), \text{ avec } \lambda_i > 0.$$

Alors, pour tout $t \in [0, 1]$:

$$P^T (tA + (1-t)B) P = t I_n + (1-t) D,$$

d'où, en passant au déterminant et en posant $\kappa = \det(P)^2$:

$$\det(tA + (1-t)B) = (1/\kappa) \cdot \prod_i (t + (1-t)\lambda_i), \quad \det A = 1/\kappa, \quad \det B = (1/\kappa) \cdot \prod_i \lambda_i.$$

L'inégalité à démontrer,

$$\ln \det(tA + (1-t)B) \geq t \cdot \ln \det A + (1-t) \cdot \ln \det B,$$

se réduit donc, après simplification par $-\ln \kappa$, à

$$\sum_i \ln(t \cdot 1 + (1-t)\lambda_i) \geq \sum_i [t \cdot \ln 1 + (1-t) \cdot \ln \lambda_i],$$

c'est-à-dire à la concavité de $\ln$ appliquée terme à terme aux points 1 et λ_i . Elle est vraie, et **stricte** dès que $\lambda_i \neq 1$ et $t \in]0, 1[$.

Il y a donc égalité si et seulement si $t \in \{0, 1\}$, ou bien $\lambda_i = 1$ pour tout i , c'est-à-dire $D = I_n$, soit $A = B$: la fonction φ est **strictement concave**.

Partie B · III — Groupe orthogonal d'une matrice définie positive (Q24, Q25)

À $A \in S_n^{++}(\mathbb{R})$ on associe $O(A) = \{M \in M_n(\mathbb{R}) ; M^T A M = A\}$.

- Q24 — $O(A)$ est un sous-groupe de $GL_n(\mathbb{R})$, isomorphe à $O_n(\mathbb{R})$.

Q24. A étant symétrique définie positive, elle s'écrit $A = B^T B$ avec B inversible — par exemple $B = A^{1/2}$, la racine carrée symétrique définie positive obtenue par le théorème spectral, ou n'importe quelle factorisation de Cholesky.

Pour $M \in M_n(\mathbb{R})$, posons $N = B M B^{-1}$. Alors

$$N^T N = B^{-T} M^T B^T B M B^{-1} = B^{-T} (M^T A M) B^{-1},$$

donc $M^T A M = A$ équivaut à $N^T N = B^{-T} A B^{-1} = I_n$, c'est-à-dire à $N \in O_n(\mathbb{R})$.

L'application $\varphi : M \mapsto B M B^{-1}$ réalise donc une bijection de $O(A)$ sur $O_n(\mathbb{R})$. Elle transforme les produits en produits, et $O_n(\mathbb{R})$ est un groupe : $O(A) = \varphi^{-1}(O_n(\mathbb{R}))$ en est un aussi, et φ est un **isomorphisme de groupes**.

Tout élément de $O(A)$ est bien inversible : de $M^T A M = A$ on tire $(\det M)^2 \cdot \det A = \det A$, donc $\det M = \pm 1$.

- Q25 — $O(A)$ est une partie compacte de $M_n(\mathbb{R})$.

Q25. $O(A) = B^{-1} O_n(\mathbb{R}) B$ est l'image du compact $O_n(\mathbb{R})$ par l'application continue $N \mapsto B^{-1} N B$: c'est une partie **compacte** de $M_n(\mathbb{R})$.

On peut aussi le voir directement : $O(A)$ est fermé comme image réciproque du fermé $\{A\}$ par l'application continue $M \mapsto M^T A M$, et borné puisque $\|M\|_A = 1$ pour la norme associée.

Partie B · IV — Les sous-groupes compacts de $GL_n(\mathbb{R})$ (Q26 à Q29)

G désigne un sous-groupe **compact** de $GL_n(\mathbb{R})$. Le but est de montrer qu'il est isomorphe à un sous-groupe de $O_n(\mathbb{R})$.

- **Q26** — tout élément de G a un déterminant de valeur absolue 1.

Q26. L'application $\det$ est un morphisme continu de G dans $(\mathbb{R}^*, \times)$, donc $\det(G)$ est un sous-groupe **compact** de $\mathbb{R}^*$, en particulier borné.

Si $|\det M| > 1$ pour un $M \in G$, alors $|\det(M^k)| = |\det M|^k \rightarrow +\infty$, ce qui contredit la bornitude. Si $|\det M| < 1$, le même argument appliqué à M^{-1} conclut. Donc $|\det M| = 1$.

- **Q27** — l'ensemble $C = \{MX ; M \in G, X \in B\}$ est compact et 0 lui est intérieur.

Q27. L'application $(M, X) \mapsto MX$ est continue et $G \times B$ est compact comme produit de deux compacts : son image C est **compacte**.

Comme $I_n \in G$, on a $B \subset C$, et B contient la boule ouverte de centre 0 et de rayon 1 : 0 est **intérieur** à C .

- **Q28** — il existe une unique matrice A définie positive de déterminant maximal telle que $C \subset B_A$.

Q28. Posons $E = \{A \in S_n^+(\mathbb{R}) ; C \subset B_A\}$.

Non vide : C est borné, donc contenu dans une boule $B(0, r)$, et $B(0, r) = B_{\{r^{-2}I_n\}}$ d'après **Q15** : $r^{-2}I_n \in E$.

Fermé : E est l'intersection, sur les X de C , des fermés $\{A ; (AX|X) \leq 1\}$, image réciproque d'un fermé par une application continue.

Borné : 0 étant intérieur à C , il existe $\rho > 0$ avec $B(0, \rho) \subset C$. Pour $A \in E$ et $\|X\| \leq \rho$, on a $(AX|X) \leq 1$, d'où $A \leq \rho^{-2}I_n$, et **Q21** donne la bornitude.

E est donc **compact**. Il est de plus **convexe** : si A et A' y sont et $t \in [0, 1]$, alors $((tA + (1-t)A')X|X) = t(AX|X) + (1-t)(A'X|X) \leq 1$.

L'application $\det$, continue sur le compact E , y atteint son maximum. Ce maximum est strictement positif, puisque E contient la matrice définie positive $r^{-2}I_n$: toute matrice qui le réalise est inversible, donc appartient à $S_n^{++}(\mathbb{R})$.

Unicité : soient $A \neq A'$ deux matrices de E réalisant ce maximum d . Leur milieu $(A + A')/2$ appartient à E par convexité, et la **stricte** concavité de $\ln \circ \det$ (**Q23**) donne

$$\ln \det((A + A')/2) > \frac{1}{2} \ln \det A + \frac{1}{2} \ln \det A' = \ln d,$$

donc un déterminant strictement supérieur à d : contradiction. D'où l'unicité.

- **Q29** — G est alors un sous-groupe de $O(A)$.

Q29. Soit $N \in G$ et posons $A' = N^T A N$, qui est symétrique définie positive.

L'ensemble C est stable par G : pour $N \in G$, $N \cdot C = \{NMX ; M \in G, X \in B\}$ et $NG = G$, donc $N \cdot C = C$.

Ainsi, pour $X \in C$, on a $NX \in C$, donc $(A(NX)|NX) \leq 1$, c'est-à-dire $(A'X|X) \leq 1$: la matrice A' appartient à E .

Or $\det A' = (\det N)^2 \cdot \det A = \det A$ d'après **Q26**. La matrice A' réalise donc elle aussi le maximum, et l'unicité établie en **Q28** impose $A' = A$, c'est-à-dire

$$N^T A N = A, \text{ soit } N \in O(A).$$

G est donc un sous-groupe de $O(A)$, lequel est isomorphe à $O_n(\mathbb{R})$ (**Q24**) : tout sous-groupe compact de $GL_n(\mathbb{R})$ est isomorphe à un sous-groupe du groupe orthogonal.

Partie C · I — Croissance d'un groupe (Q30 à Q32)

G est un groupe engendré par une partie finie S , et $\ell_S(g)$ désigne la longueur minimale d'une écriture de g en générateurs. $V_S(p)$ est la boule de rayon p pour cette longueur.

- **Q30** — $\ell_S(g^{-1}) = \ell_S(g)$ et $\ell_S(gh) \leq \ell_S(g) + \ell_S(h)$.

Q30. Soit $g = s_1^{a_1} \dots s_k^{a_k}$ une écriture réalisant le minimum, donc $\sum |a_i| = \ell_S(g)$. En inversant :

$$g^{-1} = s_k^{-a_k} \dots s_1^{-a_1},$$

écriture de même longueur, d'où $\ell_S(g^{-1}) \leq \ell_S(g)$. En appliquant ce résultat à g^{-1} , on obtient l'inégalité inverse, donc l'égalité.

Pour la seconde : en concaténant une écriture minimale de g et une de h , on obtient une écriture de gh de longueur $\ell_S(g) + \ell_S(h)$. Le minimum est donc inférieur ou égal à cette valeur.

Ces deux propriétés font de ℓ_S une « longueur » au sens usuel : elle induit une distance invariante à gauche sur G .

- **Q31** — deux parties génératrices finies donnent des longueurs comparables : le degré de croissance polynomiale ne dépend pas du système choisi.

Q31. Chaque $\sigma \in \Sigma$ s'écrit à l'aide de S , puisque S engendre G . Posons $K = \max_{\{\sigma \in \Sigma\}} \ell_S(\sigma)$, fini car Σ est finie.

Si $\ell_\Sigma(g) = m$, alors g est produit de m générateurs de $\Sigma^{\{\pm 1\}}$, et la sous-additivité (Q30) donne

$$\ell_S(g) \leq K \cdot m = K \cdot \ell_\Sigma(g), \text{ soit}$$

$$\ell_\Sigma(g) \geq (1/K) \cdot \ell_S(g).$$

En échangeant les rôles de S et Σ , avec $K' = \max_{\{s \in S\}} \ell_\Sigma(s)$, on obtient $\ell_S(g) \leq K' \cdot \ell_\Sigma(g)$. Les constantes $C = 1/K$ et $C' = K'$ conviennent.

Conséquence : $V_\Sigma(p) \subset V_S(p/C)$ et $V_S(p) \subset V_\Sigma(C'p)$. Un encadrement $\alpha p^d \leq |V_S(p)| \leq \beta p^d$ se transporte donc en un encadrement de même degré d pour Σ , seules les constantes changeant : **le degré ne dépend pas du système de générateurs.**

- **Q32** — dénombrement des triplets d'entiers naturels de somme majorée, et degré de croissance de $(\mathbb{Z}^3, +)$.

Q32. Le nombre de triplets $(x, y, z) \in \mathbb{N}^3$ tels que $x + y + z \leq p$ est le nombre de quadruplets $(x, y, z, t) \in \mathbb{N}^4$ de somme exactement p , en posant $t = p - x - y - z$. C'est un problème de composition classique :

$$C(p+3, 3) = (p+1)(p+2)(p+3)/6 \sim p^3/6.$$

Pour $(\mathbb{Z}^3, +)$ engendré par $S = \{e_1, e_2, e_3\}$, on a $\ell_S((x, y, z)) = |x| + |y| + |z|$, donc $V_S(p)$ est l'ensemble des points entiers de l'octaèdre $|x| + |y| + |z| \leq p$.

En le majorant par le cube $[-p, p]^3$ et en le minorant par les huit copies signées du dénombrement précédent, on obtient

$$\alpha p^3 \leq |V_S(p)| \leq \beta p^3 \text{ avec } \alpha, \beta > 0.$$

$(\mathbb{Z}^3, +)$ est donc à croissance polynomiale de **degré 3** — et, par **Q31**, ce degré ne dépend pas du système générateur.

Partie C · II — Le groupe de Heisenberg discret (Q33 à Q41)

$n = 3$. S , T , U sont les trois matrices unipotentes de l'énoncé, A la partie qu'elles forment, et H le sous-groupe de $GL_3(\mathbb{R})$ qu'elles engendrent.

- **Q33 à Q37** — forme générale de $S^i T^j U^k$, loi de composition, centralité de U , non-commutativité de H , et la bijection $\mathbb{Z}^3 \rightarrow H$.
- **Q38 à Q40** — majoration et minoration du cardinal de $V_A(p)$, avec le dénombrement associé.
- **Q41** — conclusion : H est à croissance polynomiale de degré 4.

Q41. La question **Q38** donne $|V_A(p)| \leq \beta p^4$.

Dans l'autre sens, **Q39** montre que tous les $S^i T^j U^k$ avec $|i| + |j| \leq p$ et $|k| \leq |ij|$ appartiennent à $V_A(p)$; ils sont deux à deux distincts par l'injectivité de f (**Q37**), et **Q40** en dénombre au moins de l'ordre de $p^4/24$. D'où $\alpha p^4 \leq |V_A(p)|$.

Le groupe de Heisenberg discret est donc à croissance polynomiale de **degré 4**, degré indépendant du système de générateurs d'après **Q31**.

À retenir : H contient $\mathbb{Z}^3$ comme ensemble — la bijection f — mais croît comme p^4 et non comme p^3 . Le terme croisé de la loi de groupe coûte un degré entier de croissance.

Q33. Notons $E_{\{a,b\}}$ les matrices élémentaires : $S = I_3 + E_{\{2,3\}}$, $T = I_3 + E_{\{1,2\}}$, $U = I_3 + E_{\{1,3\}}$.

Ces trois matrices élémentaires vérifient $E_{\{1,2\}}E_{\{2,3\}} = E_{\{1,3\}}$ et tous les autres produits deux à deux sont nuls. On en déduit $S^i = I_3 + i E_{\{2,3\}}$, $T^j = I_3 + j E_{\{1,2\}}$, $U^k = I_3 + k E_{\{1,3\}}$, puis

$$S^i T^j = I_3 + j E_{\{1,2\}} + i E_{\{2,3\}} \text{ (le produit croisé } E_{\{2,3\}}E_{\{1,2\}} \text{ est nul),}$$

et enfin

$$S^i T^j U^k = \begin{bmatrix} 1 & j & k \\ 0 & 1 & i \\ 0 & 0 & 1 \end{bmatrix}.$$

Les coefficients se lisent donc directement : i en position $(2,3)$, j en $(1,2)$, k en $(1,3)$.

Q34. En multipliant les deux matrices précédentes :

$$\begin{bmatrix} 1 & j & k \\ 0 & 1 & i \\ 0 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} 1 & j' & k' \\ 0 & 1 & i' \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & j+j' & k+k'+j i' \\ 0 & 1 & i+i' \\ 0 & 0 & 1 \end{bmatrix}.$$

D'où, par identification :

$$i'' = i + i', \quad j'' = j + j', \quad k'' = k + k' + j i'.$$

C'est le terme croisé $j i'$ qui fait toute la difficulté du problème : sans lui, H serait simplement Z^3 .

Q35. $U = I_3 + E_{\{1,3\}}$ et $E_{\{1,3\}}$ annule tous les produits avec $E_{\{1,2\}}$ et $E_{\{2,3\}}$: U commute donc avec S , avec T , donc avec tout H . U est **central**.

Par ailleurs, $T^j S^i = I_3 + j E_{\{1,2\}} + i E_{\{2,3\}} + ij E_{\{1,3\}}$, tandis que

$$S^i T^j = I_3 + j E_{\{1,2\}} + i E_{\{2,3\}}. \text{ La différence est exactement } ij E_{\{1,3\}}, \text{ d'où}$$

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

Q36. Non, H n'est pas commutatif : pour $i = j = 1$, $TS = STU \neq ST$ puisque $U \neq I_3$.

Le groupe engendré par S et T contient U , car la relation précédente donne $U = T^{-1}S^{-1}TS$ — c'est le commutateur de S et T . Donc

$$\langle S, T \rangle = H.$$

Q37. f est bien définie, et **injective** : d'après **Q33**, les trois coefficients de la matrice $S^i T^j U^k$ redonnent i , j et k . Elle est **surjective** : l'ensemble des $S^i T^j U^k$ contient les générateurs, est stable par produit (**Q34**) et par passage à l'inverse, c'est donc H tout entier.

Ce n'est **pas** un isomorphisme pour la structure usuelle de Z^3 : la loi image fait apparaître le terme $j i'$, absent de l'addition.

En revanche, on peut munir Z^3 de la loi

$$(i, j, k) * (i', j', k') = (i + i', j + j', k + k' + j i'),$$

qui est associative, d'élément neutre $(0, 0, 0)$, et pour laquelle f devient un isomorphisme : c'est la loi de groupe de Heisenberg, transportée par f .

Q38. Soit $M \in H$ avec $\ell_A(M) \leq p$: M s'écrit comme un produit d'au plus p facteurs pris parmi $S^{\pm 1}$, $T^{\pm 1}$, $U^{\pm 1}$.

U étant central (**Q35**), on peut le faire glisser à droite sans contrepartie. Restent des $S^{\pm 1}$ et $T^{\pm 1}$ à réordonner : chaque échange d'un T et d'un S produit un facteur $U^{\pm 1}$ supplémentaire d'après **Q35**.

On obtient ainsi $M = S^i T^j U^{k+z}$ où i , j et k comptent les occurrences des générateurs, donc $|i| + |j| + |k| \leq p$, et où z cumule les U créés par les échanges, en nombre majoré par $|ij|$.

Le couple (i, j) vérifie $|i| + |j| \leq p$: au plus $O(p^2)$ possibilités. Le troisième exposant $k + z$ varie dans un intervalle de longueur $O(p + p^2) = O(p^2)$. D'où

$$|V_A(p)| = O(p^4).$$

Q39. Traitons le cas $i, j, k \geq 0$, les autres s'en déduisant par symétrie.

Écrivons la division euclidienne $k = a j + b$ avec $0 \leq a \leq i$ et $0 \leq b < j$ (possible dès que $k \leq ij$).

D'abord, en utilisant $T^j S^a = S^a T^j U^{aj}$ (**Q35**) :

$$S^{i-a} T^j S^a = S^{i-a} S^a T^j U^{aj} = S^i T^j U^{aj},$$

écriture de longueur $(i - a) + j + a = i + j$.

Pour le reste b , on scinde $T^j = T^b T^{j-b}$ et l'on intercale un S :

$$S^{i-a-1} T^b S T^{j-b} S^a = S^{i-a} T^b U^b T^{j-b} S^a = S^i T^j U^{aj+b},$$

de longueur $(i-a-1) + b + 1 + (j-b) + a = i + j$.

Dans les deux cas, $\ell_A(S^i T^j U^k) \leq i + j = |i| + |j| \leq p$.

Q40. Comptons les triplets $(i, j, k) \in \mathbb{N}^3$ avec $i + j \leq p$ et $k \leq ij$.

À i fixé, j parcourt $0, \dots, p - i$, et pour chaque j il y a $ij + 1 \geq ij$ valeurs de k . D'où

$$\text{card} \geq \sum_{i=0}^p \sum_{j=0}^{p-i} ij = \sum_{i=0}^p i \cdot (p-i)(p-i+1)/2 \geq \sum_{i=0}^p i(p-i)^2/2.$$

En factorisant p^3 dans chaque terme, $i(p-i)^2/2 = (p^3/2) \cdot (i/p)(1 - i/p)^2$, ce qui est exactement la minoration annoncée.

Cette somme est une somme de Riemann : quand $p \rightarrow +\infty$,

$$(1/p) \cdot \sum_{i=0}^p (i/p)(1 - i/p)^2 \rightarrow \int_0^1 x(1-x)^2 dx = 1/2 - 2/3 + 1/4 = 1/12.$$

Donc $\sum_{i=0}^p (i/p)(1-i/p)^2 \sim p/12$, et la minoration est équivalente à

$$(p^3/2) \cdot (p/12) = p^4/24.$$