Correction détaillée

Centrale-Supélec – Mathématiques 1 – MP/MPI

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

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

I. Généralités

Q1. Supposons G fini. Pour tout $x \in G$, l'ordre de x divise $|G|$ d'après le théorème de Lagrange, donc

$$x^{|G|} = e.$$

Ainsi G est d'exposant fini. De plus $\operatorname{tr} G = \{\operatorname{tr} A\,;\, A \in G\}$ est l'image d'un ensemble fini, donc est fini.

Q2. Pour $n \geq 2$, posons

$$G = \left\{ \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \oplus I_{n-2}\,;\, t \in \mathbb{R} \right\}.$$

C'est un sous-groupe de $\mathrm{GL}_n(\mathbb{R})$: le produit correspond à l'addition des paramètres t, et l'inverse au changement de t en $-t$. Il est infini, car t parcourt $\mathbb{R}$, et toutes ses matrices ont pour trace n. Ainsi

$$\operatorname{tr} G = \{n\},$$

qui est fini.

Q3. Le groupe

$$G = \bigoplus_{k \geq 1} \mathbb{Z}/2\mathbb{Z}$$

est infini, mais tout élément vérifie $x^2 = e$. Il est donc d'exposant fini, par exemple d'exposant 2.

II. Sous-groupes finis de $\mathrm{O}_2(\mathbb{R})$

On note

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

Q4. Soit $A \in \mathrm{SO}_2(\mathbb{R})$. Écrivons

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Les colonnes de A forment une base orthonormée directe. La première colonne est donc un vecteur unitaire : il existe un unique $\theta \in [0, 2\pi[$ tel que

$$a = \cos\theta, \qquad c = \sin\theta.$$

Comme la base est directe et orthonormée, la seconde colonne est nécessairement

$$\begin{pmatrix} -\sin\theta \\ \cos\theta \end{pmatrix}.$$

Ainsi $A = R_\theta$. L'unicité provient de l'unicité de l'argument dans $[0, 2\pi[$.

Q5. Soit $G = \langle R_\theta \rangle$.

a) D'après la relation $R_\alpha R_\beta = R_{\alpha+\beta}$,
$$R_\theta^k = R_{k\theta} \qquad (k \in \mathbb{Z}).$$
Donc
$$G = \{R_{k\theta}\,;\, k \in \mathbb{Z}\}.$$

b) Si $\theta = \dfrac{2\pi}{m}$, alors
$$R_\theta^m = R_{2\pi} = I_2.$$
De plus les matrices $R_0, R_\theta, \ldots, R_{(m-1)\theta}$ sont deux à deux distinctes, car les angles correspondants sont distincts modulo 2π. Ainsi
$$|G| = m.$$

c) On a $R_{k\theta} = R_{\ell\theta}$ si et seulement si $(k-\ell)\theta \in 2\pi\mathbb{Z}$. Le groupe G est fini si et seulement s'il existe $m \geq 1$ tel que $R_{m\theta} = I_2$, c'est-à-dire
$$m\theta \in 2\pi\mathbb{Z}.$$
Cela équivaut à $\theta/(2\pi) \in \mathbb{Q}$, donc à $\theta/\pi \in \mathbb{Q}$.

d) Si G est d'exposant fini, il existe $m \geq 1$ tel que, pour tout $k \in \mathbb{Z}$,
$$(R_{k\theta})^m = I_2.$$
En particulier $R_{m\theta} = I_2$, donc $m\theta \in 2\pi\mathbb{Z}$. D'après la question précédente, G est fini.

e) Pour tout $k \in \mathbb{Z}$,
$$\operatorname{tr}(R_{k\theta}) = 2\cos(k\theta).$$
Si $\operatorname{tr} G$ est fini, l'ensemble $\{\cos(k\theta)\,;\, k \in \mathbb{Z}\}$ est fini. Or
$$R_{k\theta} + R_{-k\theta} = 2\cos(k\theta) I_2.$$
Plus directement, si l'ensemble des traces est fini, la suite $(\cos(k\theta))_{k\in\mathbb{Z}}$ ne prend qu'un nombre fini de valeurs. Dans le sous-groupe compact $\mathrm{SO}_2(\mathbb{R})$, cela force l'ensemble des rotations $R_{k\theta}$ à être fini, car une rotation est déterminée par son cosinus à conjugaison près et, dans le sous-groupe cyclique, les deux angles possibles $\pm\arccos(c)$ ne donnent que deux éléments. Donc G est fini.

Q6. Soit $G = \langle R_\theta, R_{\theta'} \rangle$.

a) Par commutativité des rotations,
$$G = \{R_{a\theta+b\theta'}\,;\, (a,b) \in \mathbb{Z}^2\}.$$
Comme $R_u = R_v$ si et seulement si $u - v \in 2\pi\mathbb{Z}$, le cardinal de G est le cardinal de l'ensemble des classes de $\theta\mathbb{Z} + \theta'\mathbb{Z}$ modulo $2\pi\mathbb{Z}$:
$$|G| = \left|\left((\theta\mathbb{Z} + \theta'\mathbb{Z}) \bmod 2\pi\mathbb{Z}\right)\right|.$$
De façon équivalente, on peut prendre comme représentants les éléments de
$$(\theta\mathbb{Z} + \theta'\mathbb{Z} + 2\pi\mathbb{Z}) \cap [0, 2\pi[.$$
Le cardinal vaut $+\infty$ si cet ensemble de représentants est infini.

b) Si $p, q \in \mathbb{N}^*$ sont premiers entre eux, alors
$$\frac{\pi}{p}\mathbb{Z} + \frac{\pi}{q}\mathbb{Z} = \frac{\pi}{pq}\mathbb{Z}.$$
Modulo 2π, cela donne exactement $2pq$ classes. Donc
$$\left|\left\langle R_{\pi/p}, R_{\pi/q} \right\rangle\right| = 2pq.$$

c) Dans le cas général,
$$\frac{\pi}{p}\mathbb{Z} + \frac{\pi}{q}\mathbb{Z} = \frac{\pi}{\operatorname{ppcm}(p,q)}\mathbb{Z}.$$
Par conséquent
$$\left|\left\langle R_{\pi/p}, R_{\pi/q} \right\rangle\right| = 2\operatorname{ppcm}(p,q) = \frac{2pq}{\gcd(p,q)}.$$

Q7. Soit G un sous-groupe fini de $\mathrm{SO}_2(\mathbb{R})$. Grâce à Q4, on peut écrire

$$G = \{R_\theta \,;\, \theta \in \Theta\},$$

où Θ est une partie finie de $[0, 2\pi[$ stable modulo 2π.

Si $G = \{I_2\}$, il est cyclique. Sinon, soit α le plus petit angle strictement positif tel que $R_\alpha \in G$. Pour tout $R_\beta \in G$, avec $\beta \in [0, 2\pi[$, écrivons la division euclidienne réelle

$$\beta = q\alpha + r, \qquad q \in \mathbb{N}, \qquad 0 \leq r < \alpha.$$

Alors

$$R_r = R_\beta R_\alpha^{-q} \in G.$$

Par minimalité de α, on a $r = 0$. Ainsi tout élément de G est une puissance de R_α, donc G est monogène.

Q8. Pour $m \in \mathbb{N}^*$, soit

$$D_m = \left\langle R_{2\pi/m}, S_{\pi/2} \right\rangle.$$

a) On a

$$D_m \cap \mathrm{SO}_2(\mathbb{R}) = \langle R_{2\pi/m} \rangle = \{R_{2k\pi/m} \,;\, 0 \leq k \leq m-1\},$$

qui a cardinal m. Comme $S_{\pi/2} \notin \mathrm{SO}_2(\mathbb{R})$ et comme toute matrice de $\mathrm{O}_2(\mathbb{R})$ est soit une rotation, soit une réflexion, on obtient

$$D_m = (D_m \cap \mathrm{SO}_2(\mathbb{R})) \sqcup S_{\pi/2}(D_m \cap \mathrm{SO}_2(\mathbb{R})).$$

Les deux ensembles sont disjoints et ont même cardinal. Donc

$$|D_m| = 2m.$$

b) Soit G un sous-groupe fini de $\mathrm{O}_2(\mathbb{R})$ non inclus dans $\mathrm{SO}_2(\mathbb{R})$. Alors

$$H = G \cap \mathrm{SO}_2(\mathbb{R})$$

est le noyau du morphisme déterminant $\det : G \to \{\pm 1\}$, qui est surjectif. Ainsi H est d'indice 2 dans G.

D'après Q7, H est cyclique. Il existe donc $m \in \mathbb{N}^*$ tel que

$$H = \langle R_{2\pi/m} \rangle.$$

Choisissons une réflexion $\sigma \in G \setminus H$. Alors

$$G = H \sqcup \sigma H.$$

De plus, si $\rho = R_{2\pi/m}$, on a

$$\sigma^2 = I_2, \qquad \sigma\rho\sigma = \rho^{-1}.$$

Ce sont exactement les relations du groupe diédral D_m. L'application

$$R_{2k\pi/m} \longmapsto \rho^k, \qquad S_{\pi/2}R_{2k\pi/m} \longmapsto \sigma\rho^k$$

définit donc un isomorphisme de D_m sur G.

III. Caractérisation des sous-groupes finis de $\mathrm{O}_n(\mathbb{R})$

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

Q9. Le théorème de réduction des matrices orthogonales réelles dit que, pour toute matrice $A \in \mathrm{O}_n(\mathbb{R})$, il existe une matrice orthogonale P telle que

$$P^{-1}AP = P^TAP$$

soit diagonale par blocs, avec des blocs de taille 1 égaux à 1 ou -1, et des blocs de taille 2 de la forme

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

Autrement dit, une matrice orthogonale réelle se réduit orthogonalement en somme orthogonale de rotations planes et de symétries ± 1.

Q10. Supposons G d'exposant fini. Il existe donc $m \in \mathbb{N}^*$ tel que

$$\forall A \in G, \qquad A^m = I_n.$$

Soit $A \in G$. D'après Q9, les valeurs propres complexes de A sont parmi les racines m-ièmes de l'unité, car $A^m = I_n$. Les blocs réels possibles sont donc en nombre fini :

$$1, \qquad -1 \quad \text{si } m \text{ est pair}, \qquad R_{2k\pi/m} \quad (0 \le k < m).$$

La trace de A est une somme de n termes choisis dans l'ensemble fini des racines m-ièmes de l'unité, ou encore, dans l'écriture réelle par blocs, une somme de termes parmi

$$\{1, -1\} \cup \{2\cos(2k\pi/m)\,;\, 0 \le k < m\}.$$

Comme il n'y a que n termes, seules un nombre fini de traces peuvent apparaître. Ainsi $\operatorname{tr} G$ est fini.

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

$$(A \mid B) = \operatorname{tr}(A^TB).$$

On note $\mathcal{F} = \mathrm{Vect}(G)$ et $d = \dim \mathcal{F}$.

Q11. Par définition, $\mathcal{F}$ est engendré par la famille éventuellement infinie des éléments de G. Comme $\mathcal{F}$ est de dimension finie d, on peut extraire de cette famille génératrice une base. Il existe donc des matrices

$$A_1, \ldots, A_d \in G$$

telles que

$$\mathcal{B} = (A_1, \ldots, A_d)$$

soit une base de $\mathcal{F}$.

Q12. On pose

$$B = ((A_i \mid A_j))_{1 \le i,j \le d}.$$

On considère la matrice C des coordonnées des matrices $A_1, \ldots, A_d$ dans la base canonique de $\mathcal{M}_n(\mathbb{R})$.

a) L'espace $\mathcal{M}_n(\mathbb{R})$ est de dimension n^2. La matrice C a donc n^2 lignes et d colonnes :

$$C \in \mathcal{M}_{n^2,d}(\mathbb{R}).$$

b) La j-ième colonne de C est le vecteur des coordonnées de A_j dans la base canonique de $\mathcal{M}_n(\mathbb{R})$. Le produit scalaire usuel de $\mathcal{M}_n(\mathbb{R})$ correspond au produit scalaire canonique de $\mathbb{R}^{n^2}$. Donc

$$(C^TC)_{ij} = \mathrm{col}_i(C)^T \mathrm{col}_j(C) = (A_i \mid A_j) = B_{ij}.$$

Ainsi

$$B = C^TC.$$

c) On a toujours

$$\ker(C^TC) = \ker C.$$

En effet,

$$X^TC^TCX = \|CX\|^2.$$

Donc $B = C^TC$ et C ont même rang. Comme les colonnes de C sont les coordonnées d'une famille libre $(A_1, \dots, A_d)$, on a $\operatorname{rg} C = d$. D'où $\operatorname{rg} B = d$, et B est inversible.

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

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

On note

$$X_M = \begin{pmatrix} x_1 \\ \vdots \\ x_d \end{pmatrix}, \qquad Y_M = \begin{pmatrix} (A_1 \mid M) \\ \vdots \\ (A_d \mid M) \end{pmatrix}.$$

Pour tout $i \in \{1, \dots, d\}$,

$$(A_i \mid M) = \left(A_i \mid \sum_{j=1}^{d} x_j A_j\right) = \sum_{j=1}^{d} x_j (A_i \mid A_j).$$

Donc

$$Y_M = BX_M.$$

Comme B est inversible, on obtient

$$X_M = B^{-1}Y_M.$$

Q14. Soit $M \in G$. Pour tout i,

$$(A_i \mid M) = \operatorname{tr}(A_i^T M).$$

Comme $A_i \in \mathrm{O}_n(\mathbb{R})$, on a $A_i^T = A_i^{-1}$. Or $A_i^{-1}M \in G$, donc

$$(A_i \mid M) = \operatorname{tr}(A_i^{-1}M) \in \operatorname{tr} G.$$

L'ensemble $\operatorname{tr} G$ étant fini, chaque coordonnée de Y_M appartient à un ensemble fini. Ainsi

$$\{Y_M \,;\, M \in G\}$$

est fini. Par la relation $X_M = B^{-1}Y_M$, l'ensemble des vecteurs de coordonnées X_M est fini. Comme une matrice de $\mathcal{F}$ est déterminée par ses coordonnées dans $\mathcal{B}$, on en déduit que G est fini.

On a donc montré, pour un sous-groupe G de $\mathrm{O}_n(\mathbb{R})$,

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

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

On note $\mathcal{M}_{n,1}(\mathbb{R})$ l'espace des colonnes, muni de son produit scalaire canonique. Sur $\mathcal{M}_n(\mathbb{R})$, on utilise la norme subordonnée à la norme euclidienne de $\mathbb{R}^n$.

I. Quelques propriétés utiles

Q15. Soit $A \in \mathcal{S}_n^{++}(\mathbb{R})$. Pour $X, Y \in \mathcal{M}_{n,1}(\mathbb{R})$, posons

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

Comme A est symétrique, cette forme bilinéaire est symétrique. Comme A est définie positive,

$$\langle X, X \rangle_A = X^T A X > 0$$

pour tout $X \neq 0$. C'est donc un produit scalaire.

La boule unité fermée associée est

$$B_A = \{X \in \mathbb{R}^n \,;\, X^T A X \leq 1\}.$$

Pour obtenir la boule euclidienne fermée $B(0,r)$, il suffit de prendre

$$A = \frac{1}{r^2} I_n.$$

Alors

$$X^T A X \leq 1 \quad \Longleftrightarrow \quad \frac{\|X\|^2}{r^2} \leq 1 \quad \Longleftrightarrow \quad \|X\| \leq r.$$

Donc $B_A = B(0,r)$.

Q16. Considérons l'endomorphisme

$$u : X \longmapsto A^{-1} B X.$$

Pour tous X, Y,

$$\langle u(X), Y \rangle_A = (AA^{-1}BX \mid Y) = (BX \mid Y) = X^T B Y.$$

Comme B est symétrique,

$$X^T B Y = (X \mid BY) = \left\langle X, A^{-1}BY \right\rangle_A = \langle X, u(Y) \rangle_A .$$

Donc u est autoadjoint pour le produit scalaire $\langle \cdot, \cdot \rangle_A$.

On en déduit que $A^{-1}B$ est diagonalisable sur $\mathbb{R}$. De plus, comme $B \in \mathcal{S}_n^+(\mathbb{R})$,

$$\langle u(X), X \rangle_A = X^T B X \geq 0.$$

Les valeurs propres de $A^{-1}B$ sont donc réelles positives ou nulles.

Q17. Pour $A, B \in \mathcal{S}_n(\mathbb{R})$, on écrit $B \preceq A$ lorsque

$$\forall X \in \mathbb{R}^n, \qquad X^T B X \leq X^T A X.$$

Alors

$$B \preceq A \quad \Longleftrightarrow \quad \forall X, \quad X^T (A - B) X \geq 0 \quad \Longleftrightarrow \quad A - B \in \mathcal{S}_n^+(\mathbb{R}).$$

Q18. Soient $A, B \in \mathcal{S}_n^{++}(\mathbb{R})$. D'après Q16, $A^{-1}B$ est autoadjoint pour $\langle \cdot, \cdot \rangle_A$ et ses valeurs propres sont strictement positives.

Dans une base orthonormée pour $\langle \cdot, \cdot \rangle_A$ qui diagonalise $A^{-1}B$, si les valeurs propres sont $\lambda_1, \dots, \lambda_n > 0$, alors

$$X^T B X = \left\langle A^{-1}BX, X \right\rangle_A = \sum_{i=1}^{n} \lambda_i x_i^2,$$

et

$$X^T A X = \langle X, X \rangle_A = \sum_{i=1}^{n} x_i^2.$$

Ainsi

$$B \preceq A \iff \forall i,\ \lambda_i \leq 1 \iff \mathrm{Sp}(A^{-1}B) \subset]0, 1].$$

Q19. Sous les hypothèses de Q18, avec $B \preceq A$, les valeurs propres $\lambda_1, \dots, \lambda_n$ de $A^{-1}B$ appartiennent à $]0, 1]$. Donc

$$\frac{\det B}{\det A} = \det(A^{-1}B) = \prod_{i=1}^{n} \lambda_i \leq 1.$$

Ainsi

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

Il y a égalité si et seulement si $\prod_i \lambda_i = 1$. Comme chaque $\lambda_i \in]0, 1]$, cela équivaut à

$$\lambda_1 = \cdots = \lambda_n = 1.$$

Puisque $A^{-1}B$ est diagonalisable, cela donne $A^{-1}B = I_n$, donc $A = B$. Réciproquement, si $A = B$, l'égalité est évidente.

Q20. Pour $A \in \mathcal{S}_n^{++}(\mathbb{R})$, rappelons

$$B_A = \{X \in \mathbb{R}^n \,;\, X^T A X \leq 1\}.$$

Alors

$$B \preceq A \implies B_A \subset B_B.$$

En effet, si $X \in B_A$, alors

$$X^T B X \leq X^T A X \leq 1,$$

donc $X \in B_B$.

Réciproquement, supposons $B_A \subset B_B$. Pour $X \neq 0$, posons

$$Y = \frac{X}{\sqrt{X^T A X}}.$$

Alors $Y \in B_A$, donc $Y \in B_B$, c'est-à-dire

$$Y^T B Y \leq 1.$$

En multipliant par $X^T A X$, on obtient

$$X^T B X \leq X^T A X.$$

La propriété est aussi vraie pour $X = 0$. Donc $B \preceq A$.

Ainsi

$$B \preceq A \iff B_A \subset B_B.$$

Q21. Soit $K \subset \mathcal{S}_n^+(\mathbb{R})$.

Si K est bornée, il existe $\alpha > 0$ tel que, pour toute $A \in K$, la norme d'opérateur de A soit inférieure à α. Comme A est symétrique positive,

$$X^T A X \leq \alpha \|X\|^2 \qquad (X \in \mathbb{R}^n).$$

Donc

$$A \preceq \alpha I_n.$$

Réciproquement, s'il existe $\alpha > 0$ tel que $A \preceq \alpha I_n$ pour tout $A \in K$, alors les valeurs propres de toute matrice $A \in K$ appartiennent à $[0, \alpha]$. Les normes d'opérateur sont donc bornées par α, et K est bornée.

II. Stricte log-concavité de l'application déterminant

Q22. Soient $A, B \in \mathcal{S}_n^{++}(\mathbb{R})$ et $t \in [0,1]$. La matrice

$$tA + (1-t)B$$

est symétrique. Pour tout $X \neq 0$,

$$X^T(tA + (1-t)B)X = tX^T AX + (1-t)X^T BX > 0,$$

car $X^T AX > 0$ et $X^T BX > 0$. Donc $tA + (1-t)B \in \mathcal{S}_n^{++}(\mathbb{R})$. Ainsi $\mathcal{S}_n^{++}(\mathbb{R})$ est convexe.

Q23. Soient $A, B \in \mathcal{S}_n^{++}(\mathbb{R})$ et $t \in [0,1]$. Si $t = 0$ ou $t = 1$, l'inégalité de concavité est une égalité triviale. Supposons donc $0 < t < 1$.

On écrit

$$tA + (1-t)B = A\big(tI_n + (1-t)A^{-1}B\big).$$

D'après Q16, $A^{-1}B$ est diagonalisable sur $\mathbb{R}$ et ses valeurs propres $\lambda_1, \ldots, \lambda_n$ sont strictement positives. Donc

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

Comme ln est strictement concave sur $\mathbb{R}_+^*$,

$$\ln\big(t + (1-t)\lambda_i\big) \geq t\ln 1 + (1-t)\ln\lambda_i = (1-t)\ln\lambda_i,$$

avec égalité si et seulement si $\lambda_i = 1$.

En sommant,

$$\begin{aligned}\ln\det(tA + (1-t)B) &\geq \ln\det A + (1-t)\sum_{i=1}^{n}\ln\lambda_i \\ &= \ln\det A + (1-t)\ln\det(A^{-1}B) \\ &= t\ln\det A + (1-t)\ln\det B.\end{aligned}$$

L'égalité, pour $0 < t < 1$, impose $\lambda_1 = \cdots = \lambda_n = 1$, donc $A^{-1}B = I_n$, puisque $A^{-1}B$ est diagonalisable. Ainsi $A = B$.

Donc

$$A \longmapsto \ln\det A$$

est strictement concave sur $\mathcal{S}_n^{++}(\mathbb{R})$.

III. Groupe orthogonal associé à une matrice symétrique définie positive

Pour $A \in \mathcal{S}_n^{++}(\mathbb{R})$, on pose

$$O(A) = \{M \in \mathcal{M}_n(\mathbb{R})\,;\, M^T A M = A\}.$$

Q24. Comme $A \in \mathcal{S}_n^{++}(\mathbb{R})$, il existe $B \in \mathrm{GL}_n(\mathbb{R})$ telle que

$$A = B^T B.$$

Par exemple, on peut prendre $B = A^{1/2}$.

Pour $M \in \mathcal{M}_n(\mathbb{R})$,

$$M^T A M = A \quad \Longleftrightarrow \quad M^T B^T B M = B^T B \quad \Longleftrightarrow \quad (BMB^{-1})^T (BMB^{-1}) = I_n.$$

Ainsi

$$M \in O(A) \quad \Longleftrightarrow \quad BMB^{-1} \in \mathrm{O}_n(\mathbb{R}).$$

L'application

$$\Phi : O(A) \to \mathrm{O}_n(\mathbb{R}), \qquad M \mapsto BMB^{-1}$$

est donc un isomorphisme de groupes. En particulier $O(A)$ est un sous-groupe de $\mathrm{GL}_n(\mathbb{R})$, isomorphe à $\mathrm{O}_n(\mathbb{R})$.

Q25. D'après Q24,

$$O(A) = B^{-1}\mathrm{O}_n(\mathbb{R})B.$$

Or $\mathrm{O}_n(\mathbb{R})$ est compact : il est fermé dans $\mathcal{M}_n(\mathbb{R})$ et borné, par exemple car ses colonnes sont unitaires. L'image d'un compact par l'application continue $N \mapsto B^{-1}NB$ est compacte. Donc $O(A)$ est compact.

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

Dans cette partie, G est un sous-groupe compact de $\mathrm{GL}_n(\mathbb{R})$.

Q26. Soit $M \in G$. Comme G est un groupe, $M^k \in G$ pour tout $k \in \mathbb{Z}$. La fonction déterminant étant continue, $\det(G)$ est compact dans $\mathbb{R}^*$, donc borné.

Si $|\det M| > 1$, alors $|\det(M^k)| = |\det M|^k \to +\infty$ lorsque $k \to +\infty$, contradiction avec la bornitude de $\det(G)$.

Si $|\det M| < 1$, alors $|\det(M^{-k})| = |\det M|^{-k} \to +\infty$, même contradiction.

Donc nécessairement

$$|\det M| = 1.$$

Q27. On pose

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

où B est la boule euclidienne unité fermée de $\mathbb{R}^n$.

L'ensemble $G \times B$ est compact, et l'application

$$(M,X) \mapsto MX$$

est continue. Donc C est compact.

De plus, puisque $I_n \in G$, on a

$$B \subset C.$$

La boule unité contient une boule ouverte centrée en 0, donc 0 est un point intérieur de C.

Q28. On considère

$$E = \{A \in \mathcal{S}_n^+(\mathbb{R})\,;\, C \subset B_A\}, \qquad B_A = \{X \in \mathbb{R}^n\,;\, X^T A X \leq 1\}.$$

Non-vacuité. Comme C est compact, il est borné. Il existe donc $R > 0$ tel que

$$C \subset B(0, R).$$

D'après Q15, $B(0, R) = B_{R^{-2}I_n}$. Donc $R^{-2}I_n \in E$, et E est non vide.

Fermeture. Si (A_m) est une suite d'éléments de E convergeant vers $A \in \mathcal{S}_n^+(\mathbb{R})$, alors, pour tout $X \in C$,

$$X^T A_m X \leq 1.$$

Par passage à la limite,

$$X^T A X \leq 1,$$

donc $A \in E$. Ainsi E est fermé.

Bornitude. Comme $B \subset C$, si $A \in E$, alors $B \subset B_A$. Par Q20, cela signifie

$$A \preceq I_n.$$

D'après Q21, E est borné.

L'ensemble E est donc compact dans l'espace de dimension finie $\mathcal{S}_n(\mathbb{R})$.

Convexité. Si $A_1, A_2 \in E$ et $t \in [0, 1]$, alors pour tout $X \in C$,

$$X^T(tA_1 + (1-t)A_2)X = tX^T A_1 X + (1-t)X^T A_2 X \leq 1.$$

Donc $tA_1 + (1-t)A_2 \in E$. Ainsi E est convexe.

La fonction déterminant est continue, donc elle atteint son maximum sur le compact E. Comme E contient une matrice définie positive, le maximum est strictement positif. Toute matrice où ce maximum est atteint est donc définie positive.

Soient $A_1, A_2 \in E \cap \mathcal{S}_n^{++}(\mathbb{R})$ deux matrices de déterminant maximal. Si $A_1 \neq A_2$, alors, par convexité de E,

$$A_0 = \frac{A_1 + A_2}{2} \in E.$$

Par stricte concavité de $\ln\det$ sur $\mathcal{S}_n^{++}(\mathbb{R})$,

$$\ln\det A_0 > \frac{1}{2}\ln\det A_1 + \frac{1}{2}\ln\det A_2,$$

donc

$$\det A_0 > \det A_1,$$

ce qui contredit la maximalité. Ainsi $A_1 = A_2$.

Il existe donc une unique matrice $A \in \mathcal{S}_n^{++}(\mathbb{R})$ telle que $C \subset B_A$ et $\det A$ soit maximal.

Q29. Soit A la matrice obtenue à la question précédente. Montrons que $G \subset O(A)$.

Soit $M \in G$. On remarque d'abord que

$$MC = C.$$

En effet,

$$M(NX) = (MN)X \in C$$

pour tout $N \in G$ et $X \in B$, et l'inclusion réciproque s'obtient avec $M^{-1} \in G$.

Comme $C \subset B_A$, on a, pour tout $X \in C$,

$$MX \in C,$$

donc

$$(MX)^T A(MX) \leq 1.$$

Autrement dit

$$X^T(M^T AM)X \leq 1 \qquad (X \in C),$$

ce qui signifie

$$C \subset B_{M^T AM}.$$

Ainsi $M^T AM \in E$.

De plus, par Q26,

$$\det(M^T AM) = \det(M)^2 \det A = \det A.$$

La matrice $M^T AM$ appartient donc à E et a le déterminant maximal. Par unicité dans Q28,

$$M^T AM = A.$$

Donc $M \in O(A)$. Ainsi

$$G \subset O(A).$$

D'après Q24, $O(A)$ est isomorphe à $\mathrm{O}_n(\mathbb{R})$; par restriction, G est isomorphe à un sous-groupe compact de $\mathrm{O}_n(\mathbb{R})$.

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. On note ℓ_S la longueur associée et

$$V_S(p) = \{g \in G\,;\, \ell_S(g) \leq p\}.$$

Q30. Soit $g \in G$. Si

$$g = s_1^{\alpha_1} \cdots s_k^{\alpha_k}, \qquad s_i \in S, \qquad \alpha_i \in \mathbb{Z},$$

alors

$$g^{-1} = s_k^{-\alpha_k} \cdots s_1^{-\alpha_1}.$$

Les sommes des valeurs absolues des exposants sont les mêmes. En prenant l'infimum, on obtient

$$\ell_S(g^{-1}) = \ell_S(g).$$

De même, si g admet une écriture de longueur a et h une écriture de longueur b, alors gh admet l'écriture concaténée de longueur $a+b$. En minimisant,

$$\ell_S(gh) \leq \ell_S(g) + \ell_S(h).$$

Q31. Soit Σ une autre partie finie génératrice de G.

Pour tout $\sigma \in \Sigma$, la quantité $\ell_S(\sigma)$ est finie. Posons

$$C' = \max_{\sigma \in \Sigma} \ell_S(\sigma) > 0.$$

Si $g = \sigma_1^{\alpha_1} \cdots \sigma_k^{\alpha_k}$ est une écriture de g en générateurs de Σ, alors

$$\ell_S(g) \leq \sum_{i=1}^{k} |\alpha_i| \ell_S(\sigma_i) \leq C' \sum_{i=1}^{k} |\alpha_i|.$$

En minimisant sur les écritures selon Σ,

$$\ell_S(g) \leq C' \ell_\Sigma(g).$$

De façon symétrique, en posant

$$C'' = \max_{s \in S} \ell_\Sigma(s) > 0,$$

on obtient

$$\ell_\Sigma(g) \leq C'' \ell_S(g).$$

Ainsi il existe deux constantes strictement positives a, b telles que

$$a\ell_S(g) \leq \ell_\Sigma(g) \leq b\ell_S(g).$$

Par conséquent,

$$V_S(p) \subset V_\Sigma(bp), \qquad V_\Sigma(p) \subset V_S(C'p).$$

Les croissances polynomiales obtenues avec S et avec Σ sont donc équivalentes à changement multiplicatif de la variable près. Le degré de croissance polynomiale ne dépend pas du système fini de générateurs choisi.

Q32. On suppose ici $\mathbb{N} = \{0, 1, 2, \ldots\}$. Le nombre de triplets $(x, y, z) \in \mathbb{N}^3$ tels que

$$x + y + z \leq p$$

est le nombre de quadruplets $(x, y, z, t) \in \mathbb{N}^4$ tels que

$$x + y + z + t = p.$$

Par la méthode des barres et étoiles,

$$\mathrm{card}\{(x, y, z) \in \mathbb{N}^3 \,;\, x + y + z \leq p\} = \binom{p+3}{3}.$$

Pour $\mathbb{Z}^3$ muni de son système de générateurs canonique, la longueur d'un élément (a, b, c) est

$$|a| + |b| + |c|.$$

On a donc

$$V(p) = \{(a, b, c) \in \mathbb{Z}^3 \,;\, |a| + |b| + |c| \leq p\}.$$

Cet ensemble contient les triplets de $\mathbb{N}^3$ de somme au plus p, et il est contenu dans la réunion des 8 orthants correspondants. Ainsi

$$\binom{p+3}{3} \leq |V(p)| \leq 8\binom{p+3}{3}.$$

Comme

$$\binom{p+3}{3} \sim \frac{p^3}{6},$$

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

II. Le groupe de Heisenberg discret

On considère

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

On note $A = \{S, T, U\}$ et $H = \langle A \rangle$.

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

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

Donc

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

Q34. En utilisant la formule précédente,

$$S^i T^j U^k = \begin{pmatrix} 1 & j & k \\ 0 & 1 & i \\ 0 & 0 & 1 \end{pmatrix}, \qquad S^{i'} T^{j'} U^{k'} = \begin{pmatrix} 1 & j' & k' \\ 0 & 1 & i' \\ 0 & 0 & 1 \end{pmatrix}.$$

Le produit vaut

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

Ainsi

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

Donc

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

Q35. D'après Q34, pour tout (i, j, k),

$$(i, j, k)(0, 0, 1) = (i, j, k+1) = (0, 0, 1)(i, j, k).$$

Donc U commute avec tous les éléments de H.

Par ailleurs,

$$T^j S^i = S^0 T^j U^0 S^i T^0 U^0 = S^i T^j U^{ji}.$$

Ainsi

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

Q36. Le groupe H n'est pas commutatif. En effet,

$$TS = STU,$$

et $U \neq I_3$, donc $TS \neq ST$.

De plus, la relation précédente donne

$$U = S^{-1} T S T^{-1}.$$

Ainsi $U \in \langle S, T \rangle$, donc

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

Q37. Considérons

$$f : \mathbb{Z}^3 \to H, \qquad (i, j, k) \mapsto S^i T^j U^k.$$

D'après Q33,

$$f(i, j, k) = \begin{pmatrix} 1 & j & k \\ 0 & 1 & i \\ 0 & 0 & 1 \end{pmatrix}.$$

Cette formule montre immédiatement que f est injective.

Elle est aussi surjective : l'ensemble des matrices de la forme $S^i T^j U^k$ contient S, T, U et est stable par produit d'après Q34 ; il contient aussi les inverses, puisque

$$(S^i T^j U^k)^{-1} = S^{-i} T^{-j} U^{-k+ij}.$$

Il contient donc tout le sous-groupe H engendré par S, T, U.

L'application f n'est pas un morphisme de groupes lorsque $\mathbb{Z}^3$ est muni de sa structure additive usuelle, car H n'est pas commutatif alors que $(\mathbb{Z}^3, +)$ l'est.

En revanche, on peut munir $\mathbb{Z}^3$ de la loi

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

Alors Q34 montre exactement que

$$f(x \star y) = f(x) f(y),$$

donc f est un isomorphisme de groupes de $(\mathbb{Z}^3, \star)$ sur H.

Remarque. Dans le scan fourni, les questions Q38 et Q39 semblent contenir des coquilles si on les lit littéralement. Par exemple, l'énoncé intermédiaire de Q38 avec la contrainte $|z| \leq |ij|$ ne peut pas être vrai pour tout élément de longueur au plus p : en effet

$$S^m T^m S^{-m} T^{-m} = U^{-m^2},$$

donc $\ell_A(U^{-m^2}) \leq 4m$, alors que sa forme normale impose $i = j = 0$. La suite de la correction donne les estimations vraies et suffisantes pour établir la croissance polynomiale de degré 4.

Q38. Majorant de $|V_A(p)|$. Soit $M \in H$ tel que $\ell_A(M) \leq p$. On peut écrire M comme un mot de longueur au plus p en les lettres

$$S^{\pm 1}, \quad T^{\pm 1}, \quad U^{\pm 1}.$$

En regroupant les lettres S, T et U, on obtient une forme normale

$$M = S^i T^j U^K.$$

Les exposants i et j sont les sommes algébriques des exposants des lettres S et T dans le mot. Donc

$$|i| \leq p, \qquad |j| \leq p.$$

L'exposant central K reçoit deux contributions :

— les lettres $U^{\pm 1}$ déjà présentes dans le mot, contribution de valeur absolue au plus p ;

— les commutations nécessaires pour mettre tous les S avant tous les T. Chaque échange d'une lettre $T^{\pm 1}$ avec une lettre $S^{\pm 1}$ modifie l'exposant de U de ± 1.

Il y a au plus p^2 tels échanges. Par conséquent

$$|K| \leq p + p^2.$$

Comme la forme normale $S^i T^j U^K$ est unique d'après Q37,

$$|V_A(p)| \leq (2p+1)^2 (2(p+p^2)+1) = O(p^4).$$

Q39. Minorant par remplissage d'un rectangle. On montre le résultat utile suivant : si $i, j, k \in \mathbb{N}$, si

$$i + j \leq p \qquad \text{et} \qquad 0 \leq k \leq ij,$$

alors

$$\ell_A(S^i T^j U^k) \leq p.$$

Il suffit de montrer que l'on peut former $S^i T^j U^k$ avec un mot de longueur $i + j$ en les seules lettres S et T.

Lorsqu'on place une lettre T avant une lettre S, la remise sous forme normale utilise

$$TS = STU.$$

Ainsi l'exposant de U obtenu est le nombre d'inversions, c'est-à-dire le nombre de paires (T, S) où le T est placé avant le S.

Avec i lettres S et j lettres T, ce nombre d'inversions peut être n'importe quel entier entre 0 et ij. Si $i = 0$ ou $j = 0$, alors $k = 0$ et le mot $S^i T^j$ convient. Supposons donc $i, j \geq 1$. Écrivons

$$k = qi + r, \qquad 0 \leq r < i, \qquad 0 \leq q \leq j,$$

avec le cas $q = j$ uniquement lorsque $r = 0$. Si $q < j$, le mot

$$T^q S^{i-r} T S^r T^{j-q-1}$$

possède exactement $qi + r = k$ inversions. Si $q = j$, le mot $T^j S^i$ possède exactement $ij = k$ inversions.

Il existe donc un mot de longueur $i + j \leq p$ représentant $S^i T^j U^k$. Ainsi

$$\ell_A(S^i T^j U^k) \leq p.$$

Q40. Posons

$$E_p = \{(i,j,k) \in \mathbb{N}^3 \,;\, i+j \leq p \text{ et } 0 \leq k \leq ij\}.$$

Pour i et j fixés, le nombre de valeurs possibles de k est $ij+1$. Donc

$$\begin{aligned} |E_p| &= \sum_{i=0}^{p} \sum_{j=0}^{p-i} (ij+1) \\ &= \sum_{i=0}^{p} \left(i \sum_{j=0}^{p-i} j + (p-i+1) \right) \\ &= \sum_{i=0}^{p} \left(\frac{i(p-i)(p-i+1)}{2} + p - i + 1 \right). \end{aligned}$$

En particulier,

$$|E_p| \geq \frac{1}{2} \sum_{i=0}^{p} i(p-i)^2 = \frac{p^4}{2} \sum_{i=0}^{p} \frac{1}{p} \frac{i}{p} \left(1 - \frac{i}{p}\right)^2.$$

La somme de droite est une somme de Riemann. Elle converge vers

$$\int_0^1 x(1-x)^2 \, dx = \left[\frac{x^2}{2} - \frac{2x^3}{3} + \frac{x^4}{4} \right]_0^1 = \frac{1}{2} - \frac{2}{3} + \frac{1}{4} = \frac{1}{12}.$$

Ainsi le minorant ci-dessus est équivalent à

$$\frac{p^4}{24}.$$

On peut même calculer exactement

$$|E_p| = \frac{(p+1)(p+2)(p^2-p+12)}{24},$$

donc

$$|E_p| \sim \frac{p^4}{24}.$$

Q41. D'après Q39, pour tout $(i,j,k) \in E_p$,

$$S^i T^j U^k \in V_A(p).$$

Comme la forme normale est unique, l'application

$$(i,j,k) \mapsto S^i T^j U^k$$

est injective. Donc

$$|V_A(p)| \geq |E_p| \sim \frac{p^4}{24}.$$

En particulier, il existe $c > 0$ tel que, pour p assez grand,

$$|V_A(p)| \geq c p^4.$$

D'après Q38, il existe $C > 0$ tel que

$$|V_A(p)| \leq C p^4$$

pour p assez grand. Finalement,

$$c p^4 \leq |V_A(p)| \leq C p^4.$$

Le groupe de Heisenberg discret H est donc à croissance polynomiale de degré 4.