

Ecrit par Fabrice Castel, lycée Fénelon Sainte-Marie.

REM. Je remercie François Dion pour nos échanges au sujet des erreurs rencontrées dans ce sujet. Les énoncés des questions **6.a)**, **38** et **39** nous ont semblé erronés.

Nous les redonnons tels que posés le jour du concours et expliquons les absurdités rencontrées. Puis pour chacune d'elles, nous proposons une version modifiée de l'énoncé initial, permettant d'atteindre le but fixé par le problème, notamment celui de la partie **C**.

Correction de l'épreuve :

Centrale – MP – 2026 – sujet 1

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

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

- $\mathcal{M}_n(\mathbb{R})$ l'ensemble des matrices de taille $n \times n$ à coefficients dans $\mathbb{R}$, I_n sa matrice identité.
- $\mathcal{GL}_n(\mathbb{R})$ 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).
- $\mathcal{O}_n(\mathbb{R})$ le groupe des matrices orthogonales de $\mathcal{M}_n(\mathbb{R})$, et $\mathcal{SO}_n(\mathbb{R})$ celui des matrices orthogonales de déterminant 1.
- La transposée d'une matrice $M \in \mathcal{M}_n(\mathbb{R})$ sera notée M^T et sa trace $\text{tr} M$.
- On note $|X|$ le cardinal d'un ensemble X , en convenant que $|X| = +\infty$ si X est un ensemble infini.
- Si $\mathcal{A}$ est une partie finie d'un groupe G , on note $\langle \mathcal{A} \rangle$ le sous-groupe de G engendré par $\mathcal{A}$.

Le problème comporte trois parties indépendantes.

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

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

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

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

$$\text{tr} G = \{\text{tr} A ; A \in G\}.$$

I Généralités

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

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

Soit m le PPCM des ordres de tous les éléments de G .

Puisque G est fini, ce PPCM existe.

Alors, pour tout $x \in G$, $x^m = e$.

REM. Il est également possible de prendre m le cardinal du groupe G .

Alors d'après un théorème du cours (corollaire du théorème de Lagrange), pour tout $x \in G$, $x^m = e$.

Donc G est d'exposant fini.

De plus la forme linéaire tr induit une surjection de G sur $\text{tr} G$,

or G est fini, donc $\text{tr} G$ est fini.

2. Donner un exemple de sous-groupe infini de $\mathcal{G}\ell_n(\mathbb{R})$ dont la trace soit finie.

Soit $n \geq 2$.

Pour tout $\lambda \in \mathbb{R}$, notons $T_\lambda = I_n + \lambda E_{12}$.

Alors $G = \{T_\lambda ; \lambda \in \mathbb{R}\}$ est un sous-groupe de $\mathcal{G}\ell_n(\mathbb{R})$ de cardinal infini tandis que $\text{tr } G = \{1\}$ est finie.

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

Le groupe produit $((\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}, +)$ est infini, d'exposant fini ;

car tous ses éléments non neutres sont d'ordre 2.

Il s'agit en fait d'un $(\mathbb{Z}/2\mathbb{Z})$ -espace vectoriel.

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

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

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

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

$$R_\theta R_\varphi = R_{\theta+\varphi}, \quad R_\theta S_\varphi = S_{\theta+\varphi}, \quad S_\varphi R_\theta = S_{\varphi-\theta}, \quad S_\theta S_\varphi = R_{\theta-\varphi}.$$

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

Notons $(A_1|A_2) = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = A$ les colonnes et coefficients de A .

La première colonne est de norme 1, donc il existe $\theta \in]-\pi, \pi]$ tel que $(a_{11}, a_{21}) = (\cos(\theta), \sin(\theta))$.

REM. S'il fallait le prouver, rappelons qu'il suffit de prendre $\theta = \text{sgn}(a_{21})\text{Arccos}(a_{11})$ où sgn est la fonction signe, valant +1 sur $\mathbb{R}_+$ et -1 sur $\mathbb{R}_-^*$.

• Puis, comme $A \in \mathcal{SO}_2(\mathbb{R})$, A_1 et A_2 sont orthogonales, il existe λ tel que $(a_{12}, a_{22}) = \lambda(-a_{21}, a_{11})$.

On s'aperçoit alors que $\det(A) = \det \begin{pmatrix} \cos(\theta) & -\lambda \sin(\theta) \\ \sin(\theta) & \lambda \cos(\theta) \end{pmatrix} = \lambda$,

or $\det(A) = 1$, donc $\lambda = 1$.

Finalement, $\boxed{\text{il existe bien } \theta \text{ tel que } A = R_\theta}$.

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

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

Par définition, $G = \langle R_\theta \rangle = \{R_\theta^k ; k \in \mathbb{Z}\}$.

Pour $k = 0$, $R_\theta^k = I_2 = R_{0\theta}$.

Soit $k \geq 0$. Supposons que $R_\theta^k = R_{k\theta}$.

Alors, d'après les relations données par l'énoncé :

$$R_\theta^{k+1} = R_\theta^k \times R_\theta = R_{k\theta} \times R_\theta = R_{(k+1)\theta}.$$

Nous avons ainsi montré par récurrence que pour tout $k \in \mathbb{N}$, $R_\theta^k = R_{k\theta}$.

Enfin, pour tout $k \in \mathbb{Z}^-$,

$$R_\theta^k = ((R_\theta)^{|k|})^{-1} = R_{|k|\theta}^{-1} = R_{-|k|\theta}^T = R_{k\theta}.$$

Donc, $\boxed{\text{pour tout } k \in \mathbb{Z}, R_\theta^k = R_{k\theta}}$, donc $\boxed{G = \{R_{k\theta} ; k \in \mathbb{Z}\}}$.

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

Nous utilisons la 2π -périodicité des fonctions cos et sin.

Pour tout $k \in \mathbb{Z}$, $\frac{2k\pi}{m} \equiv \frac{2r\pi}{m} [2\pi]$ où r est le reste de la division euclidienne de k par m .

Donc, en utilisant la question **5.a)**, il vient :

$$G = \{R_{\frac{2k\pi}{m}} ; k \in \llbracket 0, m-1 \rrbracket\}.$$

Par ailleurs, la fonction $\theta \mapsto (\cos(\theta), \sin(\theta))$ est injective sur $[0, 2\pi[$, donc aucun élément de G n'est répété dans l'énumération ci-dessus.

Donc $\boxed{|G| = m}$.

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

• Supposons que $\frac{\theta}{\pi} \in \mathbb{Q}$.

Soit $(k, m) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $\frac{\theta}{\pi} = \frac{k}{m}$. Alors $\theta = \frac{2k\pi}{2m}$.

Donc, comme on l'a vu question **5.a)**, $R_\theta \in \langle R_{\frac{2\pi}{2m}} \rangle$.

Donc, G est inclus dans $\langle R_{\frac{2\pi}{2m}} \rangle$.

Et nous avons vu question **5.b)** que ce groupe était fini.

Donc a fortiori, $\boxed{G \text{ est fini}}$.

• Réciproquement, supposons que G est fini. Soit m son ordre.

Alors l'ordre de R_θ divise le cardinal du groupe G , donc divise m .

Donc il existe m tel que $R_\theta^m = I_2$. Donc $R_{m\theta} = I_2$.

Donc $(\cos(m\theta), \sin(m\theta)) = (1, 0)$.

Donc $m\theta \equiv 0 [2\pi]$.

Donc il existe $k \in \mathbb{Z}$ tel que $m\theta = k2\pi$, donc $\boxed{\frac{\theta}{\pi} \in \mathbb{Q}}$.

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

Supposons que G est d'exposant fini.

Soit $m \in \mathbb{N}^*$ tel que pour tout $A \in G$, $A^m = I_2$.

En particulier, $R_\theta^m = I_2$, donc $R_{m\theta} = I_2$, donc $m\theta \equiv 0[2\pi]$.

Donc $\frac{\theta}{\pi} \in \mathbb{Q}$, donc d'après la question **5.c)**, G est fini.

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

Supposons que $\text{tr } G$ est fini. Tout d'abord,

$$G \subset \{A \in \mathcal{SO}_2(\mathbb{R}) ; \text{tr } A \in \text{tr } G\}.$$

Or, dans $\mathcal{SO}_2(\mathbb{R})$, la trace est le double du coefficient d'indice (1,1). Donc, en notant $\frac{1}{2} \text{tr } G = \{\frac{t}{2} ; t \in \text{tr } G\}$, l'inclusion précédente s'écrit :

$$G \subset \{A \in \mathcal{SO}_2(\mathbb{R}) ; E_1^T A E_1 \in \frac{1}{2} \text{tr } G\}.$$

Or pour tout $c \in [-1, 1]$, il n'existe au plus que deux matrices A de $\mathcal{SO}_2(\mathbb{R})$ telles que $E_1^T A E_1 = c$, à savoir $R_{\pm\theta}$ avec $\theta = \text{Arccos}(c)$.

Donc G est fini et $|G| \leq 2|\text{tr } G|$.

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

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

L'égalité demandée est fausse.

Comme $\mathcal{SO}_2(\mathbb{R})$ est commutatif,

$$\begin{aligned} \langle R_\theta, R_{\theta'} \rangle &= \{R_\theta^k \times R_{\theta'}^\ell ; (k, \ell) \in \mathbb{Z}^2\} \\ &= \{R_{k\theta + \ell\theta'} ; (k, \ell) \in \mathbb{Z}^2\}. \\ &= \{R_\varphi ; \varphi \in \theta\mathbb{Z} + \theta'\mathbb{Z}\}. \end{aligned}$$

Etudions le sous-groupe $H = \theta\mathbb{Z} + \theta'\mathbb{Z}$ de $\mathbb{R}$.

Nous allons utiliser le fait que tout sous-groupe de $\mathbb{R}$ est soit discret, soit dense.

- Si H n'est pas discret, alors H est dense. Dans ce cas là,

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

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

- Si H est discret, il existe $\alpha > 0$ tel que $\theta\mathbb{Z} + \theta'\mathbb{Z} = \alpha\mathbb{Z}$.

Alors :

$$|(\theta\mathbb{Z} + \theta'\mathbb{Z}) \cap [0, 2\pi[| = |\alpha\mathbb{Z} \cap [0, 2\pi[| = 1 + \left\lfloor \frac{2\pi}{\alpha} \right\rfloor.$$

Dans ce cas, il n'y a aucun rapport entre $|G|$ et $|(\theta\mathbb{Z} + \theta'\mathbb{Z}) \cap [0, 2\pi[|$.

— Voici un contre-exemple : $(\theta = 4, \theta' = 0)$.

Alors $G = \langle R_\theta, R_{\theta'} \rangle = \langle R_\theta \rangle$ est un groupe infini,

mais $|(\theta\mathbb{Z} + \theta'\mathbb{Z}) \cap [0, 2\pi[| = 1$.

— Voici un second contre-exemple : $(\theta = \theta' = \frac{3\pi}{2})$.

Alors $G = \langle R_\theta, R_{\theta'} \rangle = \langle R_\theta \rangle$ est un groupe de cardinal 4,

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

6.a) [*Proposition alternative*]

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

Posons $f : [0, 2\pi[\longrightarrow \mathcal{SO}_2(\mathbb{R})$, bijective d'après la question 4.

$$x \longmapsto R_x$$

Notons $\Theta = (\theta\mathbb{Z} + \theta'\mathbb{Z} + 2\pi\mathbb{Z}) \cap [0, 2\pi[$.

Nous allons montrer que $f(\Theta) = G$:

- Pour tout $x \in \Theta$, il existe $k, \ell, m \in \mathbb{R}$ tel que $x = k\theta + \ell\theta' + 2m\pi$.
Alors $f(x) = R_{k\theta + \ell\theta' + 2m\pi} = R_{k\theta + \ell\theta'} = R_\theta^k R_{\theta'}^\ell$.
Donc $f(\Theta) \subset G$.
- Pour tout $M \in G$, il existe $k, \ell \in \mathbb{Z}$ tel que $M = R_\theta^k R_{\theta'}^\ell = R_{k\theta + \ell\theta'}$.
Soit $m = \lfloor \frac{k\theta + \ell\theta'}{2\pi} \rfloor$ de sorte que : $0 \leq k\theta + \ell\theta' - m2\pi < 2\pi$. Alors $k\theta + \ell\theta' - m2\pi \in \Theta$.
Puis $f(k\theta + \ell\theta' - m2\pi) = R_{k\theta + \ell\theta' - m2\pi} = R_{k\theta + \ell\theta'} = M$.
Donc $G \subset f(\Theta)$.

Ainsi, Θ envoie bijectivement Θ sur G , ces deux ensembles ont même cardinal.

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

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

- *Preuve s'appuyant sur l'énoncé rectifié de la question 6.a).*

$$\begin{aligned} \left| \langle R_{\frac{\pi}{p}}, R_{\frac{\pi}{q}} \rangle \right| &= \left| \left(\frac{\pi}{p}\mathbb{Z} + \frac{\pi}{q}\mathbb{Z} + 2\pi\mathbb{Z} \right) \cap [0, 2\pi[\right| \quad \text{d'après la question 6.a)} \\ &= \left| \left(\frac{\pi}{p}\mathbb{Z} + \frac{\pi}{q}\mathbb{Z} \right) \cap [0, 2\pi[\right| \quad \text{car } 2\pi\mathbb{Z} \subset \frac{\pi}{p}\mathbb{Z} \\ &= \left| (q\mathbb{Z} + p\mathbb{Z}) \cap [0, 2pq[\right| \quad \text{car } x \mapsto \frac{pq}{\pi}x \text{ est bijective de } \mathbb{R} \text{ sur } \mathbb{R} \\ &= \left| (p \wedge q)\mathbb{Z} + p\mathbb{Z} \cap [0, 2pq[\right| \quad \text{par définition du PGCD par les idéaux de } \mathbb{Z} \\ &= \left| pq\mathbb{Z} \cap [0, 2pq[\right| \quad \text{car } p \text{ et } q \text{ sont premiers entre eux.} \\ &= 2pq \end{aligned}$$

$$\text{Ainsi, } \left| \langle R_{\frac{\pi}{p}}, R_{\frac{\pi}{q}} \rangle \right| = \left| \langle R_{\frac{2\pi}{2pq}} \rangle \right| = 2pq.$$

- *Preuve directe, sans passer par la question 6.a).*

Soient p et q deux entiers non nuls premiers entre eux.

D'une part, $\langle R_{\frac{\pi}{p}} \rangle$ et $\langle R_{\frac{\pi}{q}} \rangle$ sont des sous-groupes de $\langle R_{\frac{\pi}{pq}} \rangle$, donc

$$\langle R_{\frac{\pi}{p}}, R_{\frac{\pi}{q}} \rangle \subset \langle R_{\frac{\pi}{pq}} \rangle.$$

D'autre part, puisque p et q sont premiers entre eux, il existe $u, v \in \mathbb{Z}$ tel que $up + vq = 1$.

Alors $u\frac{\pi}{q} + v\frac{\pi}{p} = \frac{\pi}{pq}$. Donc :

$$\langle R_{\frac{\pi}{p}}, R_{\frac{\pi}{q}} \rangle \supset \langle R_{\frac{\pi}{pq}} \rangle.$$

Ainsi,

$$\langle R_{\frac{\pi}{p}}, R_{\frac{\pi}{q}} \rangle = \langle R_{\frac{\pi}{pq}} \rangle.$$

$$\text{Alors, } \left| \langle R_{\frac{\pi}{p}}, R_{\frac{\pi}{q}} \rangle \right| = \left| \langle R_{\frac{2\pi}{2pq}} \rangle \right| = 2pq.$$

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

D'une part, $\langle R_{\frac{\pi}{p}} \rangle$ et $\langle R_{\frac{\pi}{q}} \rangle$ sont des sous-groupes de $\langle R_{\frac{\pi}{p \vee q}} \rangle$, donc

$$\langle R_{\frac{\pi}{p}}, R_{\frac{\pi}{q}} \rangle \subset \langle R_{\frac{\pi}{p \vee q}} \rangle.$$

D'autre part, puisque $\frac{p}{p \wedge q} \wedge \frac{q}{p \wedge q} = 1$, il existe $u, v \in \mathbb{Z}$ tel que $u \frac{p}{p \wedge q} + v \frac{q}{p \wedge q} = 1$.

Alors, en multipliant ceci par $\frac{\pi}{p \vee q}$, $u \frac{\pi}{q} + v \frac{\pi}{q} = \frac{\pi}{p \vee q}$. Donc :

$$\langle R_{\frac{\pi}{p}}, R_{\frac{\pi}{q}} \rangle \supset \langle R_{\frac{\pi}{p \vee q}} \rangle.$$

Finalement, nous avons montré la double inclusion. Donc :

$$\left| \left\langle R_{\frac{\pi}{p}}, R_{\frac{\pi}{q}} \right\rangle \right| = \left| \langle R_{\frac{2\pi}{2(p \vee q)}} \rangle \right| = 2(p \vee q).$$

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

Soit $m = |G|$. Alors pour tout $A \in G$, $A^m = I_2$.

Or pour tout $\theta \in [0, 2\pi[$,

$$\begin{aligned} R_\theta^m = I_2 &\iff R_{m\theta} = I_2 \\ &\iff m\theta \equiv 0[2\pi] \\ &\iff \theta \in \frac{2\pi}{m}\mathbb{Z} \\ &\iff \theta \in \frac{2\pi}{m}\mathbb{Z} \cap [0, 2\pi[\\ &\iff \theta \in \left\{ \frac{2k\pi}{m} ; k \in \llbracket 0, m-1 \rrbracket \right\} \end{aligned}$$

Donc $G \subset \{R_{\frac{2k\pi}{m}} ; k \in \llbracket 0, m-1 \rrbracket\}$.

Or $|G| = m = |\{R_{\frac{2k\pi}{m}} ; k \in \llbracket 0, m-1 \rrbracket\}|$, donc $G = \{R_{\frac{2k\pi}{m}} ; k \in \llbracket 0, m-1 \rrbracket\}$.

Or $\{R_{\frac{2k\pi}{m}} ; k \in \llbracket 0, m-1 \rrbracket\} = \langle R_{\frac{2\pi}{m}} \rangle$.

Ainsi, G est monogène.

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

8.a) Déterminer le cardinal de $\mathcal{D}_m$.

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

Pour plus de clarté, notons $R = R_{\frac{2\pi}{m}}$ et $S = S_{\frac{\pi}{2}}$.

- D'une part, $\mathcal{D}_m$ contient le sous-groupe $N = \langle R \rangle$ de cardinal m .

D'autre part, la bijection $L_S : \mathcal{D}_m \longrightarrow \mathcal{D}_m$ envoie N sur un ensemble SN de même

$$A \longmapsto SA$$

cardinal m et disjoint de N (puisque hors de $\mathcal{SO}_2(\mathbb{R})$).

A ce stade,

$$\mathcal{D}_m \supset N \sqcup SN \text{ et } \text{Card}(\mathcal{D}_m) \geq 2m.$$

- Comme S est d'ordre 2, un élément quelconque de $\mathcal{D}_m$ s'écrit a priori sous la forme :

$$R^{a_0} S R^{a_1} S R^{a_2} \dots S R^{a_n}$$

où $n \in \mathbb{N}$ et les a_i sont des entiers de $\llbracket 0, m-1 \rrbracket$.

Mais d'après les relations données par l'énoncé,

$$\forall a \in \llbracket 0, m-1 \rrbracket, R^a S = S R^{m-a},$$

donc, par récurrence sur n , un tel un élément de $\mathcal{D}_m$ peut s'écrire sous la forme :

$$S^\varepsilon R^a \text{ avec } \varepsilon \in \{0, 1\} \text{ et } a \in \llbracket 0, m-1 \rrbracket$$

Donc :

$$\mathcal{D}_m = N \sqcup SN \text{ et } \boxed{\text{Card}(\mathcal{D}_m) = 2m}.$$

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

Notons $N = G \cap \mathcal{SO}_2(\mathbb{R})$.

D'après la question 7, N est monogène.

Soit m l'ordre. On a vu qu'alors $N = \langle R_{\frac{2\pi}{m}} \rangle$.

Puisque $G \not\subset \mathcal{SO}_2(\mathbb{R})$, il existe $S \in G \setminus N$.

Comme avant, $SN \subset G \setminus N$ (à cause du déterminant) et nous en déduisons :

$$G \supset N \sqcup NS.$$

La bijection $\begin{array}{ccc} G & \longrightarrow & G \\ A & \longmapsto & SA \end{array}$ échange les parties $G \cap \mathcal{SO}_2(\mathbb{R})$ et $G \setminus \mathcal{SO}_2(\mathbb{R})$ en raison du déterminant.

Donc $|G \setminus \mathcal{SO}_2(\mathbb{R})| = |G \cap \mathcal{SO}_2(\mathbb{R})| = m$.

Donc $G \setminus \mathcal{SO}_2(\mathbb{R}) = SN$. Donc :

$$G = N \sqcup NS.$$

Pour conclure, soit φ tel que $S_\varphi = S$. Notons la bijection suivante :

$$\Psi : \begin{array}{ccc} \mathcal{D}_m & \longrightarrow & G \\ S_{\frac{\pi}{2}}^\varepsilon R_{\frac{2\pi}{m}}^a & \longmapsto & S_\varphi^\varepsilon R_{\frac{2\pi}{m}}^a \end{array} .$$

définie ainsi pour tout $\varepsilon \in \{0, 1\}$ et $a \in \llbracket 0, m-1 \rrbracket$.

Il reste à vérifier que Ψ est un morphisme. Or pour tout θ :

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

Nous en déduisons que pour tous ε et tous θ_1, θ_2 , dans $\frac{2\pi}{m}\mathbb{Z}$,

$$\begin{aligned} \Psi(S_{\frac{\pi}{2}}^\varepsilon R_{\theta_1} S_{\frac{\pi}{2}}^\varepsilon R_{\theta_2}) &= \Psi(S_{\frac{\pi}{2}}^{\varepsilon+1} R_{-\theta_1} R_{\theta_2}) \\ &= S_\varphi^{\varepsilon+1} R_{-\theta_1} R_{\theta_2} \\ &= S_\varphi^\varepsilon R_{\theta_1} S_\varphi R_{\theta_2} \\ &= \Psi(S_{\frac{\pi}{2}}^\varepsilon R_{\theta_1}) \Psi(S_{\frac{\pi}{2}}^\varepsilon R_{\theta_2}) \end{aligned}$$

Ainsi, Ψ est un isomorphisme et G est isomorphe à $\mathcal{D}_m$.

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

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

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

9. Rappeler le théorème de réduction des matrices orthogonales.

Soit $O \in \mathcal{O}_n(\mathbb{R})$. Alors, il existe $P \in \mathcal{O}_n(\mathbb{R})$ telle que :

$$P^T O P = \begin{pmatrix} I_r & & & (0) \\ & -I_s & & \\ & & R_{\theta_1} & \\ & & & \ddots \\ (0) & & & & R_{\theta_t} \end{pmatrix} \text{ où } \begin{cases} r, s, t \in \mathbb{N}, \\ r + s + 2t = n, \\ \theta_1, \dots, \theta_t \in \mathbb{R}. \end{cases}$$

10. On suppose dans cette question que G est d'exposant fini.

Montrer, en utilisant le théorème de réduction précédent, que $\text{tr} G$ est fini.

Si G est d'exposant fini, il existe $m \in \mathbb{N}^*$ tel que pour tout $A \in G$, $A^m = I_n$.

Donc, la matrice diagonale par blocs ci-dessus n'a que des blocs de rotation dont l'angle appartient à l'ensemble $E_m = \{\frac{2\pi}{m}, \frac{4\pi}{m}, \dots, \frac{2(m-1)\pi}{m}\}$ modulo 2π . Donc :

$$\text{tr} A = r - s + \sum_{k=1}^t 2 \cos(\theta_k) \text{ avec } \begin{cases} r, s, t \in \mathbb{N} \text{ et } r + s + 2t = n, \\ \theta_1, \dots, \theta_m \in E_m. \end{cases}$$

Alors, $(r, s, t) \in \llbracket 1, n \rrbracket^3$, de cardinal n^3 .

Et pour chacun d'eux, $(\theta_1, \dots, \theta_t) \in E_m^t$, de cardinal $m^t \leq m^n$.

Ainsi :

le nombre de traces possibles dans A est majoré par $n^3 m^n$, donc est fini.

Jusqu'à la fin de cette partie, on suppose maintenant que $\text{tr} G$ est fini.

On munit $\mathcal{M}_n(\mathbb{R})$ de son produit scalaire usuel :

$$(A | B) = \text{tr} A^T B$$

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

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

Par le théorème de la base extraite appliqué à la famille G génératrice de $\mathcal{F}$,

il existe une famille $\mathcal{B}$ de matrices de G qui forme une base de $\mathcal{F}$.

12. Soit $B = ((A_i | A_j))_{(i,j) \in \llbracket 1, d \rrbracket^2}$. 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 ?

La matrice C appartient à $\boxed{\mathcal{M}_{n^2, d}(\mathbb{R})}$.

b) Montrer que $B = C^T C$.

Pour tout $i \in \llbracket 1, d \rrbracket$, la colonne $CE_i \in \mathcal{M}_{n^2, 1}(\mathbb{R})$ est le vecteur des coordonnées de A_i . Comme la base canonique de $\mathcal{M}_n(\mathbb{R})$ est orthonormée,

$$\forall i, j \in \llbracket 1, d \rrbracket^2, E_i^T B E_j = (A_i | A_j) = (CE_i)^T (CE_j) = E_i^T (C^T C) E_j.$$

Donc $\boxed{B = C^T C}$.

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

Comme $\text{Im}(C^T C) \subset \text{Im}(C)$, on a l'inégalité $\text{rg}(B) = \text{rg}(C^T C) \leq \text{rg}(C)$.

Comparons $\text{Ker}(B)$ et $\text{Ker}(C)$.

Soit $X \in \text{Ker}(C^T C)$.

Alors $X^T C^T C X = 0$, autrement dit $\|CX\| = 0$ pour la norme euclidienne de $\mathcal{M}_{n^2, 1}(\mathbb{R})$.

Donc $CX = 0$, donc $X \in \text{Ker}(C)$.

Ainsi, $\text{Ker}(C^T C) \subset \text{Ker}(C)$.

Donc par le théorème du rang, $\text{rg}(C) \leq \text{rg}(C^T C)$.

Ainsi, $\boxed{\text{rg}(C) = \text{rg}(C^T C) = \text{rg}(B)}$.

Or $\text{rg}(C) = d$, puisque C est la matrice d'une famille libre de d vecteurs.

Donc $\text{rg}(B) = d$. Donc $\boxed{B \in \mathcal{GL}_d(\mathbb{R})}$.

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

Pour tout $i \in \llbracket 1, d \rrbracket$,

$$E_i^T B X_M = \sum_{j=1}^d x_j E_i^T B E_j = \sum_{j=1}^d x_j (A_i | A_j) = (A_i | \sum_{j=1}^d x_j A_j) = (A_i | M).$$

Donc $B X_M = Y_M$. Donc $\boxed{X_M = B^{-1} Y_M}$.

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

• Soit $M \in G$.

Pour tout $i \in \llbracket 1, d \rrbracket$, $A_i^{-1} \in G$, or $G \subset \mathcal{O}_n(\mathbb{R})$, donc $A_i^T \in G$.

Donc pour tout $i \in \llbracket 1, d \rrbracket$, $A_i^T M \in G$, donc $\text{tr}(A_i^T M) \in \text{tr}(G)$.

Donc pour tout $i \in \llbracket 1, d \rrbracket$, $(A_i | M) \in \text{tr}(G)$.

Donc, en identifiant $\mathcal{M}_d(\mathbb{R})$ et $\mathbb{R}^d$, $Y_M \in (\text{tr}(G))^d$. Donc :

$$\boxed{\{Y_M \mid M \in G\} \text{ est un ensemble fini (de cardinal inférieur à } |\text{tr}(G)|^d \text{)}}.$$

• Notons $E = \{Y_M \mid M \in G\}$ qui est donc un ensemble fini.

Pour tout $M \in G$,

$$M = \sum_{j=1}^d x_j A_j = (A_1 | \cdots | A_d) X_M = (A_1 | \cdots | A_d) B^{-1} Y_M.$$

Donc :

$$G \subset \{(A_1 | \cdots | A_d) B^{-1} Y \mid Y \in E\}.$$

Puisque E est fini, $\boxed{G \text{ est fini}}$.

Partie B : Sous-groupes compacts de $\mathcal{G}\ell_n(\mathbb{R})$

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 $\langle \cdot | \cdot \rangle$ et de sa norme associée $\| \cdot \|$. Pour $r \geq 0$, on note $\mathcal{B}(0, r)$ la boule fermée de centre 0 et de rayon r de $\mathcal{M}_{n,1}(\mathbb{R})$ pour cette norme, et $\mathcal{B} = \mathcal{B}(0, 1)$ la boule unité fermée.

I Quelques propriétés utiles

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

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

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

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

* La bilinéarité de $\langle \cdot, \cdot \rangle_A$ est évidente.

* La symétrie de $\langle \cdot, \cdot \rangle_A$ vient du fait que A est symétrique :

$$\forall X, Y \in \mathcal{M}_{n,1}(\mathbb{R}), \langle X, Y \rangle_A = (AX)^T Y = X^T A Y = \langle Y, X \rangle_A.$$

* La positivité de $\langle \cdot, \cdot \rangle_A$ vient du fait que $A \in \mathcal{S}_n^+(\mathbb{R})$.

* Enfin, $\langle \cdot, \cdot \rangle_A$ est définie positive, grâce au fait que $A \in \mathcal{S}_n^{++}(\mathbb{R})$:

$$\forall X \in \mathcal{M}_{n,1}(\mathbb{R}) \setminus \{0\}, \langle X, X \rangle_A = X^T A X > 0$$

Donc $\boxed{\langle \cdot, \cdot \rangle_A \text{ est un produit scalaire sur } \mathcal{M}_{n,1}(\mathbb{R})}$.

On note alors $\|\cdot\|_A$ la norme associée à ce produit scalaire et $\mathcal{B}_A$ la boule unité fermée pour cette norme.

b) Existe-t-il une matrice A telle que $\mathcal{B}(0, r) = \mathcal{B}_A$?

Pour tout $r > 0$, En prenant $A = \frac{1}{r^2} I_n$, alors $A \in \mathcal{S}_n^{++}(\mathbb{R})$ et pour tout $X \in \mathcal{M}_{n,1}(\mathbb{R})$,

$$\begin{aligned} \|X\|_A \leq 1 &\iff X^T A X \leq 1 \\ &\iff \frac{1}{r^2} X^T X \leq 1 \\ &\iff \|X\|^2 \leq r^2 \\ &\iff \|X\| \leq r. \end{aligned}$$

Ainsi, En prenant $A = \frac{1}{r^2} I_n$, on a : $\mathcal{B}(0, r) = \mathcal{B}_A$.

16. Vérifier que $X \mapsto A^{-1}BX$ est autoadjoint pour le produit scalaire $\langle \cdot, \cdot \rangle_A$.

Que peut-on en déduire pour la matrice $A^{-1}B$?

• Les matrices car B puis A étant symétriques, elles induisent des applications linéaires sur $\mathcal{M}_{n,1}(\mathbb{R})$ auto-adjointes pour le produit scalaire canonique.

Ceci intervient aux endroits (*) ci-dessous.

Pour tous $X, Y \in \mathcal{M}_{n,1}(\mathbb{R})$,

$$\begin{aligned} \langle A^{-1}BX, Y \rangle_A &= \langle BX, Y \rangle \\ &= (X | BY) \\ (*) &= (X | AA^{-1}BY) \\ &= (AX | A^{-1}BY) \\ (*) &= \langle X, A^{-1}BY \rangle_A \end{aligned}$$

Donc $X \mapsto A^{-1}BX$ est auto-adjointe pour le produit scalaire $\langle \cdot, \cdot \rangle_A$.

• Alors d'après le théorème spectral, cette application est diagonalisable en base $\langle \cdot, \cdot \rangle_A$ -orthonormale.

En particulier, $A^{-1}B$ est diagonalisable dans $\mathcal{M}_n(\mathbb{R})$.

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

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

Rappelons que $A - B \in \mathcal{S}_n(\mathbb{R})$. Sachant cela,

$$\begin{aligned} B \preccurlyeq A &\iff \forall X \in \mathcal{M}_{n,1}(\mathbb{R}), (BX | X) \leq (AX | X) \\ &\iff \forall X \in \mathcal{M}_{n,1}(\mathbb{R}), ((A - B)X | X) \geq 0 \\ &\iff \forall X \in \mathcal{M}_{n,1}(\mathbb{R}), X^T (A - B) X \geq 0 \\ &\iff (A - B) \in \mathcal{S}_n^+(\mathbb{R}). \end{aligned}$$

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

- 18.** 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 $\langle \cdot, \cdot \rangle_A$ bien choisie.

Puisque $A, B \in \mathcal{S}_n^{++}(\mathbb{R})$, $A^{-1}B \in \mathcal{G}\ell_n(\mathbb{R})$, dont les valeurs propres de $A^{-1}B$ sont non nulles. Rappelons que d'après la question **17**, $A^{-1}B$ est diagonalisable.

$\Rightarrow$ Supposons que $B \preccurlyeq A$.

Alors pour tout X vecteur propre de $A^{-1}B$ de valeur propre λ ,

$$(BX|X) \leq (AX|X) = (BB^{-1}AX|X) = \frac{1}{\lambda}(BX|X).$$

Or $(BX|X) \neq 0$ car $X \neq 0$ et $B \in \mathcal{S}_n^{++}(\mathbb{R})$.

Donc $\frac{1}{\lambda} \geq 1$, donc $\lambda \in]0, 1]$.

Donc $\boxed{\text{Sp}(A^{-1}B) \subset]0, 1]}$.

$\Leftarrow$ Supposons que $\text{Sp}(A^{-1}B) \subset]0, 1]$.

Soient $(U_1, \dots, U_n)$ une base $\langle \cdot, \cdot \rangle_A$ -orthonormale de $\mathcal{M}_{n,1}(\mathbb{R})$ de vecteurs propres de $A^{-1}B$ et $(\lambda_1, \dots, \lambda_n) \in]0, 1]^n$ les valeurs propres associées.

Soit $X \in \mathcal{M}_{n,1}(\mathbb{R})$.

Soit $(x_1, \dots, x_n) \in \mathbb{R}^n$ tel que $X = \sum_{i=1}^n x_i U_i$.

Alors, comme $(U_1, \dots, U_n)$ est une base $\langle \cdot, \cdot \rangle_A$ -orthonormale,

$$\langle A^{-1}BX, X \rangle_A = \sum_{i=1}^n x_i^2 \lambda_i \leq \sum_{i=1}^n x_i^2 = \langle X, X \rangle_A.$$

En revenant au produit scalaire canonique sur $\mathcal{M}_{n,1}(\mathbb{R})$, nous obtenons :

$$(BX | X) \leq (AX | X).$$

Donc $\boxed{B \preccurlyeq A}$.

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

D'après les questions **16** et **18**, $\text{Sp}_{\mathbb{C}}(A^{-1}B) \subset]0, 1]$.

Donc $\det(A^{-1}B) \in]0, 1]$, donc $\boxed{\det(A) \geq \det(B)}$.

Si $\det(A) = \det(B)$, alors d'après ce qui précède, $\text{Sp}(A^{-1}B) = \{1\}$.

Or $A^{-1}B$ est diagonalisable (question **16**),

donc $A^{-1}B$ est semblable à I_n , donc est égale à I_n .

Donc sous l'hypothèse $B \preccurlyeq A$, $\boxed{\det B = \det A \iff A = B}$.

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

$$\begin{aligned}
B \preccurlyeq A &\iff \forall X, (BX | X) \leq (AX | X) \\
&\iff \forall X \neq 0, \left(B \frac{X}{\|X\|_A} \middle| \frac{X}{\|X\|_A} \right) \leq 1 \\
&\iff (\forall X, \|X\|_A \leq 1 \Rightarrow (BX | X) \leq 1) \\
&\iff (\forall X, (AX | X) \leq 1 \Rightarrow (BX | X) \leq 1) \\
&\iff (\forall X, X \in \mathcal{B}_A \Rightarrow X \in \mathcal{B}_B) \\
&\iff \mathcal{B}_A \subset \mathcal{B}_B
\end{aligned}$$

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

$\Rightarrow$ Si $\mathcal{K}$ est bornée, soit $\alpha = \{\|S\| ; S \in \mathcal{S}_n(\mathbb{R})\}$.

Notons $\|\cdot\|$ la norme sur $\mathcal{M}_n(\mathbb{R})$ subordonnée à la norme $\|\cdot\|$ de $\mathcal{M}_{n,1}(\mathbb{R})$.

Alors, pour tout $A \in \mathcal{S}_n^+(\mathbb{R})$ et tout $X \in \mathcal{M}_{n,1}(\mathbb{R})$,

$$(AX | X) \leq \|AX\| \|X\| \leq \|A\| \|X\|^2 \leq \alpha \|X\|^2 = (\alpha I_n X | X).$$

Donc $\boxed{\text{pour tout } A \in \mathcal{K}, A \preccurlyeq \alpha I_n}$.

$\Leftarrow$ Supposons que pour tout $A \in \mathcal{K}$, $(AX | X) \leq \alpha \|X\|^2$.

Lorsque X est un vecteur propre de A de norme 1, $(AX | X)$ est la valeur propre associée.

Donc $\text{Sp}(A) \subset [0, \alpha]$.

Par le théorème spectral, il existe $P \in \mathcal{O}_n(\mathbb{R})$ et $(\lambda_1, \dots, \lambda_n) \in [0, \alpha]^n$ tels que :

$$A = P \text{diag}(\lambda_1, \dots, \lambda_n) P^T.$$

Alors, en considérant la « norme 2 » sur $\mathcal{M}_n(\mathbb{R})$, pour tout $A \in \mathcal{K}$,

$$\|A\|^2 = \sqrt{\text{tr}(A^T A)} = \sqrt{\text{tr}(P^T \text{diag}(\lambda_1^2, \dots, \lambda_n^2) P)} = \sqrt{\sum_{i=1}^n \lambda_i^2} \leq \alpha \sqrt{n}.$$

Donc $\boxed{\mathcal{K} \text{ est borné}}$.

II Stricte log-concavité de l'application $\det$

Soit $\mathcal{C}$ une partie convexe de $\mathcal{M}_n(\mathbb{R})$ et $\varphi : \mathcal{C} \rightarrow \mathbb{R}$ une fonction.

On dit que φ est strictement concave si et seulement si :

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

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

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

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

Alors $tA + (1-t)B \in \mathcal{S}_n(\mathbb{R})$ (puisque $\mathcal{S}_n(\mathbb{R})$ est un $\mathbb{R}$ -espace vectoriel).

Pour tout $X \in \mathcal{M}_{n,1}(\mathbb{R}) \setminus \{0\}$,

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

donc $tA + (1-t)B \in \mathcal{S}_n^{++}(\mathbb{R})$.

Donc $\boxed{\mathcal{S}_n^{++}(\mathbb{R}) \text{ est une partie convexe de } \mathcal{M}_n(\mathbb{R})}$.

23. 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 **16**.

• *Montrons la concavité de φ .*

Par concavité de la fonction $\ln$ sur $\mathbb{R}_+^*$,

$$\forall \lambda \in \mathbb{R}_+^*, \forall t \in [0, 1], \ln(t\lambda + (1-t) \cdot 1) \geq t \ln(\lambda) + (1-t) \ln(1) = t \ln(\lambda).$$

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

D'après la question **16**, $B^{-1}A$ est diagonalisable dans $\mathcal{M}_n(\mathbb{R})$.

Soient $\lambda_1, \dots, \lambda_n$ les n racines de $\chi_{B^{-1}A}$. Alors :

$$\forall t \in [0, 1], \ln \left(\prod_{i=1}^n (t\lambda_i + 1 + t) \right) \leq t \ln \left(\prod_{i=1}^n \lambda_i \right).$$

donc :

$$\forall t \in [0, 1], \ln(\det(tB^{-1}A + (1-t)I_n)) \leq t \ln(\det(B^{-1}A)).$$

puis, en ajoutant $\ln(\det(B))$ à gauche et à droite :

$$\forall t \in [0, 1], \ln(\det(tA + (1-t)B)) \leq t \ln(\det(A)) + (1-t) \ln(\det(B)).$$

Donc la fonction $\varphi = \ln \circ \det$ est concave sur $\mathcal{S}_n^{++}(\mathbb{R})$.

• *Montrons la stricte concavité de φ .*

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

Le cas d'égalité de l'inégalité de concavité de φ

$$\ln(\det(tA + (1-t)B)) = t \ln(\det(A)) + (1-t) \ln(\det(B)).$$

est obtenu d'après nos calculs précédents lorsque :

$$\forall \lambda \in \text{Sp}(B^{-1}A), \ln(t\lambda + (1-t) \cdot 1) = t \ln(\lambda) + (1-t) \ln(1).$$

Mais d'après la stricte concavité de $\ln$ sur $\mathbb{R}_+^*$ (cf. ci-après),

puisque $t \in]0, 1[$, cela signifie que $\text{Sp}(B^{-1}A) = \{1\}$.

Or la matrice $B^{-1}A$ est diagonalisable, donc elle est semblable à I_n , donc égale à I_n .

Donc $A = B$.

D'où la stricte concavité de φ .

• *Montrons la stricte concavité de $\ln$ sur $\mathbb{R}_+^*$.*

Nous partons du fait que $\ln'' : t \mapsto \frac{-1}{t^2}$ est strictement négative sur $\mathbb{R}_+^*$.

Soient $a, b \in \mathbb{R}_+^*$ avec $b > a$ et $t \in]0, 1[$. Soit $m = ta + (1-t)b$.

Puisque $a < m$, on a : $\int_m^a \underbrace{(a-m)}_{<0} \underbrace{\ln''(t)}_{<0} dt < 0$,

donc, d'après la formule de Taylor avec reste intégrale sur $[a, m]$ basée en m :

$$\ln(a) < \ln(m) + \ln'(m)(a-m) \tag{1}$$

De façon similaire, puisque $b > m$, on a : $\int_m^b \underbrace{(b-m)}_{>0} \underbrace{\ln''(t)}_{<0} dt < 0$, donc :

$$\ln(b) < \ln(m) + \ln'(m)(b-m). \tag{2}$$

En calculant $t \times (1) + (1-t) \times (2)$, il vient :

$$t \ln(a) + (1-t) \ln(b) < 1 \times \ln(m) + \ln'(m) \times 0.$$

autrement dit :

$$\ln(ta + (1-t)b) > t \ln(a) + (1-t) \ln(b).$$

Donc $\ln$ est strictement concave sur $\mathbb{R}_+^*$.

REM. Les inégalités (1) et (2) traduisent le fait que, sauf au point m , la courbe de $\ln$ est située strictement sous sa tangente basée en m .

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 :

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

24. Montrer que $\mathcal{O}(A)$ est un sous-groupe de $\mathcal{GL}_n(\mathbb{R})$, isomorphe à $\mathcal{O}_n(\mathbb{R})$.

*On pourra montrer qu'il existe une matrice B telle que $A = B^T B$,
et chercher un isomorphisme sous la forme $M \mapsto B^{-1} M B$.*

- Puisque $A \in \mathcal{S}_n^{++}(\mathbb{R})$, il existe $P \in \mathcal{O}_n(\mathbb{R})$ et $(\lambda_1, \dots, \lambda_n) \in (\mathbb{R}_+^*)^n$ tel que :

$$A = P \text{diag}(\lambda_1, \dots, \lambda_n) P^T.$$

Posons

$$B = P \text{diag}(\sqrt{\lambda_1}, \dots, \sqrt{\lambda_n}) P^T.$$

Alors $B \in \mathcal{S}_n^{++}(\mathbb{R})$ et $A = B^2 = B^T B$.

- Soit $\Phi : \mathcal{GL}_n(\mathbb{R}) \longrightarrow \mathcal{GL}_n(\mathbb{R})$ un automorphisme de $\mathcal{GL}_n(\mathbb{R})$.

$$M \longmapsto B M B^{-1}$$

Alors, pour tout $M \in \mathcal{O}(A)$,

$$\begin{aligned} M \in \mathcal{O}(A) &\iff M^T A M = A \\ &\iff M^T B^T B M = B^T B \\ &\iff (B^T)^{-1} M^T B^T B M B^{-1} = I_n \\ &\iff (B M B^{-1})^T (B M B^{-1}) = I_n \\ &\iff \Phi(M) \in \mathcal{O}_n(\mathbb{R}). \end{aligned}$$

Donc $\mathcal{O}(A) = \Phi(\mathcal{O}_n(\mathbb{R}))$.

Or Φ est morphisme de groupes et $\mathcal{O}_n(\mathbb{R})$ est un sous-groupe de $\mathcal{GL}_n(\mathbb{R})$,

donc $\mathcal{O}(A)$ est un sous-groupe de $\mathcal{GL}_n(\mathbb{R})$.

et comme Φ est un isomorphisme, $\mathcal{O}(A)$ est isomorphe à $\mathcal{O}_n(\mathbb{R})$.

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

Notons $\Psi : \mathcal{M}_n(\mathbb{R}) \longrightarrow \mathcal{M}_n(\mathbb{R})$ est linéaire en dimension finie, donc continue.

$$M \longmapsto B M B^{-1}$$

Or $\mathcal{O}(A) = \Psi(\mathcal{O}_n(\mathbb{R}))$, donc $\mathcal{O}(A)$ est compact comme image d'un compact par une application continue.

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

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

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

L'application $|\det|$ est un morphisme continu de $\mathcal{GL}_n(\mathbb{R})$ dans $\mathbb{R}_+^*$.

Donc elle envoie G , sous-groupe de $\mathcal{GL}_n(\mathbb{R})$ compact sur un sous-groupe compact de $\mathbb{R}_+^*$.

Or tout sous-groupe de $\mathbb{R}_+^*$ non trivial contient un élément $a \neq 1$, donc contient $\{a^k ; k \in \mathbb{Z}\}$ qui est non borné, donc non compact.

Donc l'image de G par $|\det|$ ne peut être que $\{1\}$.

Donc pour tout $M \in G$, $\det(M) = 1$.

27. On pose :

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

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

Notons $f : \mathcal{M}_n(\mathbb{R})^2 \longrightarrow \mathcal{M}_n(\mathbb{R})$ continue, car bilinéaire en dimension finie.
 $(M, X) \longmapsto MX$

Or $G \times \mathcal{B}$ est compact comme produit de compacts.

Donc $\mathcal{C}$ est compact.

La partie $\mathcal{C}$ contient $\{I_n X ; X \in \mathcal{B}\} = \mathcal{B}$ car $I_n \in G$.

Donc $\mathcal{C}$ contient la boule ouverte de rayon 1 centrée en 0.

Donc 0 est un point intérieur à $\mathcal{C}$.

28. Montrer qu'il existe une unique matrice $A \in \mathcal{S}_n^{++}(\mathbb{R})$ telle que $\mathcal{C} \subset \mathcal{B}_A$ et qui soit de déterminant maximal. On pourra commencer par montrer que $\mathcal{E} = \{A \in \mathcal{S}_n^+(\mathbb{R}) ; \mathcal{C} \subset \mathcal{B}_A\}$ est non vide, compact et convexe, puis utiliser la question **23** pour démontrer l'unicité.

Posons $\mathcal{E} = \{A \in \mathcal{S}_n^+(\mathbb{R}) ; \mathcal{C} \subset \mathcal{B}_A\}$.

- Comme $\mathcal{C}$ est compact, il existe $R > 0$ tel que $\mathcal{C} \subset \mathcal{B}(0, R)$.

Alors, pour tout $X \in \mathcal{B}(0, R)$, $(\frac{1}{R^2} I_n X \mid X) = \left(\frac{\|X\|}{R}\right)^2 \leq 1$.

Donc $\mathcal{B}(0, R) \subset \mathcal{B}_{\frac{1}{R^2} I_n}$

Donc $\frac{1}{R^2} I_n \in \mathcal{E}$.

Donc $\mathcal{E}$ est non vide.

- Pour tout $A \in \mathcal{E}$, $\mathcal{B}_{I_n} = \mathcal{B} \subset \mathcal{C} \subset \mathcal{B}_A$,

donc d'après la question **20**, $A \preceq I_n$.

donc d'après la question **21**, $\mathcal{E}$ est borné.

- Montrons que $\mathcal{E}$ est fermé.

Soit une suite $(A_k)_k \in \mathcal{E}^{\mathbb{N}}$ convergeant vers une matrice $A \in \mathcal{M}_n(\mathbb{R})$.

Alors $A \in \mathcal{S}_n^+(\mathbb{R})$ car $\mathcal{S}_n^+(\mathbb{R})$ est fermé.

Justifions que $\mathcal{S}_n^+(\mathbb{R})$ est fermé.

Tout d'abord, $\mathcal{S}_n(\mathbb{R})$ est fermé comme sous-espace vectoriel (de dimension finie) de $\mathcal{M}_n(\mathbb{R})$. Pour tout $X \in \mathcal{M}_{n,1}(\mathbb{R})$, soit $f_X : \mathcal{M}_n(\mathbb{R}) \rightarrow \mathbb{R}$
 $M \mapsto (MX | X)$.

Ces applications sont continues car linéaires en dimension finie.

Donc pour tout $X \in \mathcal{M}_{n,1}(\mathbb{R})$, $f_X^{-1}(\mathbb{R}_+)$ est fermé.

Enfin, $\mathcal{S}_n^+(\mathbb{R}) = \mathcal{S}_n(\mathbb{R}) \cap \left(\bigcap_{X \in \mathcal{M}_{n,1}(\mathbb{R})} f_X^{-1}(\mathbb{R}_+) \right)$,

donc $\mathcal{S}_n^+(\mathbb{R})$ est fermé comme intersection de fermés.

Or, pour tout $k \in \mathbb{N}$, $\mathcal{C} \subset \mathcal{B}_{A_k}$, donc pour tout $X \in \mathcal{C}$, $(A_k X | X) \leq 1$.

Or l'application $\mathcal{M}_n(\mathbb{R}) \rightarrow \mathbb{R}$ est continue,
 $M \mapsto (MX | X)$

donc à la limite, $(AX | X) = \lim_{k \rightarrow \infty} (A_k X | X) \leq 1$.

Donc $A \in \mathcal{E}$.

Ainsi, $\boxed{\mathcal{E} \text{ est fermé}}$.

• *Montrons que $\mathcal{E}$ est convexe.*

Si A et B sont dans $\mathcal{E}$ et $t \in [0, 1]$,

alors pour tout $X \in \mathcal{C}$, $(AX | X) \leq 1$ et $(BX | X) \leq 1$,

donc pour tout $X \in \mathcal{C}$, $((tA + (1-t)B)X | X) \leq 1$.

Donc $tA + (1-t)B \in \mathcal{S}_n^+(\mathbb{R})$ et $\mathcal{C} \subset \mathcal{B}_{tA+(1-t)B}$.

Donc $\boxed{\mathcal{E} \text{ est convexe}}$.

• *Montrons l'existence du maximum de $\det$ sur $\mathcal{E} \cap \mathcal{S}_n^{++}(\mathbb{R})$.*

Puisque $\mathcal{E}$ est un compact non vide et que l'application $\det$ est continue,

$\max\{\det(A) ; A \in \mathcal{E}\}$ existe et est atteint en une matrice $A_0 \in \mathcal{E}$.

Rappelons que $\frac{1}{R^2}I_n \in \mathcal{E}$. Or $\det(\frac{1}{R^2}I_n) > 0$, donc $\det(A_0) > 0$.

Or $A_0 \in \mathcal{S}_n^+(\mathbb{R})$, donc $A_0 \in \mathcal{S}_n^{++}(\mathbb{R})$.

D'où $\boxed{\text{l'existence de la matrice } A \in \mathcal{S}_n^{++}(\mathbb{R}) \text{ de déterminant maximal telle que } \mathcal{C} \subset \mathcal{B}_A}$.

• *Montrons l'unicité.*

S'il y avait deux matrices A et B dans $\mathcal{C}$ maximisant le déterminant,

alors $A, B \in \mathcal{S}_n^{++}(\mathbb{R})$ et $\frac{A+B}{2} \in \mathcal{E}$ et l'on aurait :

$$\det\left(\frac{A+B}{2}\right) \leq \det(A) = \det(B).$$

D'où :

$$\ln(\det(\frac{A+B}{2})) \leq \frac{1}{2} \ln(\det(A)) + \frac{1}{2} \ln(\det(B))$$

mais c'est absurde, car ceci enfreint la stricte concavité de la fonction $\varphi = \ln \circ \det$ vue à la question 23.

D'où $\boxed{\text{l'unicité de la matrice } A \in \mathcal{S}_n^{++}(\mathbb{R}) \text{ de déterminant maximal telle que } \mathcal{C} \subset \mathcal{B}_A}$.

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

Soit A la matrice fournie par la question **28**.

Puisque A appartient à l'ensemble $\mathcal{E}$ introduit à la question **28**,

$$\forall R \in G, \forall X \in \mathcal{B}, (ARX | RX) \leq 1.$$

Donc, pour tous $M, N \in G$ et $X \in \mathcal{B}$,

$$(M^T AMNX | NX) = (A(MN)X | (MN)X) \leq 1.$$

De plus, $M^T AM \in \mathcal{S}_n^{++}(\mathbb{R})$, donc $M^T AM \in \mathcal{E}$.

Enfin, d'après la question **26**, $\det(M) = 1$, donc $\det(M^T AM) = \det(A)$.

Ainsi, $M^T AM$ maximise $\det$ sur $\mathcal{E}$, donc d'après la question **28**, $M^T AM = A$.

Donc $M \in \mathcal{O}(A)$.

Ainsi, G est un sous-groupe de $\mathcal{GL}_n(\mathbb{R})$ est inclus dans le sous-groupe $\mathcal{O}(A)$,

donc G est un sous-groupe de $\mathcal{O}(A)$.

Partie C : Croissance du groupe de Heisenberg discret

I Croissance d'un groupe

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

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

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

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

$\mathcal{V}_{\mathcal{S}}(p)$ est l'ensemble des éléments de G s'obtenant à partir d'au maximum p éléments de $\mathcal{S}$. Nous dirons que G est un groupe à croissance polynomiale de degré $d \in \mathbb{N}$ si et seulement s'il existe deux réels strictement positifs α et β tels que, pour tout $p \geq 1$:

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

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

Soient $k = \ell_{\mathcal{S}}(g)$ et $\ell = \ell_{\mathcal{S}}(h)$.

Il existe $s_1, \dots, s_k, t_1, \dots, t_{\ell} \in \mathcal{S}$ et $a_1, \dots, a_k, b_1, \dots, b_{\ell} \in \mathbb{Z}$ tels que :

$$g = s_1^{a_1} \dots s_k^{a_k} \text{ et } h = t_1^{b_1} \dots t_{\ell}^{b_{\ell}}.$$

Alors $g^{-1} = s_k^{-a_k} \dots s_1^{-a_1}$, donc $\ell_{\mathcal{S}}(g^{-1}) \leq \ell_{\mathcal{S}}(g)$.

Or, on a de même $\ell_{\mathcal{S}}((g^{-1})^{-1}) \leq k = \ell_{\mathcal{S}}(g^{-1})$, donc $\ell_{\mathcal{S}}(g^{-1}) = \ell_{\mathcal{S}}(g)$.

De même, $gh = s_1^{a_1} \dots s_k^{a_k} t_1^{b_1} \dots t_{\ell}^{b_{\ell}}$, donc $\ell_{\mathcal{S}}(gh) \leq k + \ell = \ell_{\mathcal{S}}(g) + \ell_{\mathcal{S}}(h)$.

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

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

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

- Soit $M = \max(\{\ell_{\mathcal{S}}(\sigma) ; \sigma \in \Sigma\})$.

Soit $g \in G$ quelconque. Soit $k = \ell_{\Sigma}(g)$.

Alors g peut s'écrire sous la forme $g = \sigma_1^{a_1} \dots \sigma_k^{a_k}$.

Or, pour tout $i \in \llbracket 1, k \rrbracket$, $\ell_{\mathcal{S}}(\sigma_i) \leq M$.

Donc, d'après la question **30**, $\ell_{\mathcal{S}}(g) \leq \sum_{i=1}^k M|a_i| = M\ell_{\Sigma}(g)$.

Donc en prenant $C = M^{-1} > 0$, nous avons démontré que :

$$\boxed{C\ell_{\mathcal{S}}(g) \leq \ell_{\Sigma}(g)}.$$

Symétriquement, il existe $C' > 0$ tel que :

$$\boxed{\ell_{\Sigma}(g) \leq C'\ell_{\mathcal{S}}(g)}.$$

- Supposons que G soit un groupe à croissance polynomiale de degré d vis-à-vis de $\mathcal{S}$.

Il existe donc $\alpha, \beta \in \mathbb{R}_+^*$ tels que, pour tout $p \geq 1$:

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

Soient $q > 0$ et $p = \frac{q}{C}$.

Alors, pour tout $g \in \mathcal{V}_{\mathcal{S}}(p)$, $\ell_{\mathcal{S}}(g) \leq p$, donc $\ell_{\Sigma}(g) \leq C'\ell_{\mathcal{S}}(g) \leq C'p = q$.

Donc $g \in \mathcal{V}_{\Sigma}(q)$. Ainsi, $\mathcal{V}_{\mathcal{S}}(p) \subset \mathcal{V}_{\Sigma}(q)$.

Or $|\mathcal{V}_{\mathcal{S}}(p)| \geq \alpha p^d$, donc $\boxed{|\mathcal{V}_{\Sigma}(q)| \geq \alpha p^d = \left(\frac{\alpha}{C'^d}\right)q^d}$.

Soient $q > 0$ et $p = \frac{q}{C}$.

Alors, pour tout $g \in \mathcal{V}_{\Sigma}(q)$, $\ell_{\Sigma}(g) \leq q$, donc $\ell_{\mathcal{S}}(g) \leq C^{-1}\ell_{\Sigma}(g) \leq \frac{q}{C}$.

Donc $g \in \mathcal{V}_{\mathcal{S}}(\frac{q}{C})$. Ainsi, $\mathcal{V}_{\Sigma}(q) \subset \mathcal{V}_{\mathcal{S}}(\frac{q}{C})$.

Or $|\mathcal{V}_{\mathcal{S}}(\frac{q}{C})| \leq \beta \left(\frac{q}{C}\right)^d$, donc $\boxed{|\mathcal{V}_{\Sigma}(q)| \leq \beta p^d = \left(\frac{\beta}{C^d}\right)q^d}$.

Donc $\boxed{G \text{ est également à croissance polynomiale de degré } d \text{ vis-à-vis de } \Sigma}$.

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

- Soit $A_p = \{(x, y, z) \in \mathbb{N}^3 ; x + y + z \leq p\}$. Alors :

$$|A_p| = \sum_{x=0}^p \sum_{y=0}^{p-x} \sum_{z=0}^{p-x-y} 1 = \sum_{x=0}^p \sum_{y=0}^{p-x} (p - x - y + 1) = \sum_{x=0}^p \frac{(p - x + 1)(p - x + 2)}{2}.$$

En posant $k = p - x + 2$, il vient :

$$|A_p| = \sum_{k=2}^{p+2} \frac{k(k-1)}{2} = \sum_{k=2}^{p+2} \binom{k}{2} = \sum_{x=2}^{p+2} \left(\binom{k+1}{3} - \binom{k}{3} \right) = \binom{p+3}{3} - \binom{2}{3}.$$

Donc :

$$|\{(x, y, z) \in \mathbb{N}^3 ; x + y + z \leq p\}| = \frac{(p+3)(p+2)(p+1)}{6}.$$

- Soit $\mathcal{S} = \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\}$ un système de générateur de $\mathbb{Z}^3$.

Un élément quelconque $g = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$ de $\mathbb{Z}^3$ peut s'écrire : $x \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + y \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + z \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$,

donc sa longueur vis-à-vis de $\mathcal{S}$ est au plus $|x| + |y| + |z|$.

Toute autre combinaison d'entiers x', y', z' avec $|x'| + |y'| + |z'| < |x| + |y| + |z|$ ne peut reconstituer g , par unicité de l'expression de g dans la base $\mathcal{S}$, lorsque $\mathbb{Z}^3$ vu comme un sous-groupe du $\mathbb{Q}$ -espace vectoriel $\mathbb{Q}^3$.

Alors :

$$\mathcal{V}_{\mathcal{S}}(p) = \left\{ \begin{pmatrix} x \\ y \\ z \end{pmatrix} ; |x| + |y| + |z| \leq p \right\}.$$

Si on ne comptait que les termes de $\mathbb{N}^3$ de longueur inférieure à p , on en aurait $\binom{p+3}{3}$.

Donc $\binom{p+3}{3}$ est un minorant de $|\mathcal{V}_{\mathcal{S}}(p)|$.

Mais en tenant compte du signe, chaque triplet $(|x|, |y|, |z|)$ de $\mathbb{N}^3$ peut correspondre jusqu'à huit triplets (x, y, z) de $\mathbb{Z}^3$.

Donc $8\binom{p+3}{3}$ est un majorant de $|\mathcal{V}_{\mathcal{S}}(p)|$. Ainsi :

$$\frac{p^3}{6} \leq \binom{p+3}{3} \leq |\mathcal{V}_{\mathcal{S}}(p)| \leq 8\binom{p+3}{3} = \frac{4}{3}(p^3 + 6p^2 + 11p + 6) \leq 32p^3.$$

(Pour la dernière majoration, on a utilisé le fait que $1 \leq p \leq p^2 \leq p^3$).

Cet encadrement justifie que $\boxed{\mathbb{Z}^3 \text{ est un groupe à croissance polynomiale de degré } 3}.$

II Le groupe de Heisenberg discret

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

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

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

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

Grâce au binôme de Newton, parce que I_3 et E_{23} commutent,

$$S^i = (I_3 + E_{23})^i = \sum_{k=0}^i \binom{i}{k} (E_{23})^k = I_3 + iE_{23}.$$

De même pour T^j et U^k de sorte que :

$$S^i T^j U^k = (I_3 + iE_{23})(I_3 + jE_{12})(I_3 + kE_{13}) = I_3 + iE_{23} + jE_{12} + kE_{13}.$$

Ainsi,

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

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

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

$$\begin{aligned} S^i T^j U^k S^{i'} T^{j'} U^{k'} &= (I_3 + iE_{23} + jE_{12} + kE_{13})(I_3 + i'E_{23} + j'E_{12} + k'E_{13}) \\ &= I_3 + (i + i')E_{23} + (j + j')E_{12} + (k + k')E_{13} + i'jE_{12}E_{23} \\ &= I_3 + (i + i')E_{23} + (j + j')E_{12} + (k + k' + i'j)E_{13} \\ &= S^{i+i'} T^{j+j'} U^{k+k'+i'j} \end{aligned}$$

Le triplet attendu est donc $(i'', j'', k'') = (i + i'), (j + j'), (k + k' + i'j)$.

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

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

• E_{13} commute avec E_{12} et avec E_{23} , donc en ajoutant I_3 qui est central, U commute avec S et T , donc U est un élément central de $\mathbb{H}$.

• On utilise la question **34** pour la seconde partie de la question :

$$T^j S^i = (S^0 T^j U^0)(S^i T^0 U^0) = S^i T^j U^{ij}.$$

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

- Le groupe $\boxed{\mathbb{H} \text{ n'est pas commutatif}}$, puisque d'après la question **35**,

$$TS = STU \neq ST.$$
- Remarquons que $U = T^{-1}S^{-1}STU = T^{-1}S^{-1}TS$.
Donc $\boxed{\langle S, T \rangle_{\mathbb{H}} = \langle S, T, U \rangle_{\mathbb{H}} = \mathbb{H}}.$

37. Montrer que l'application f définie par :

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

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?

- D'après la question **33**, cette application f est l'application :

$$\begin{aligned} f : \quad \mathbb{Z}^3 &\longrightarrow \mathbb{H} \\ (i, j, k) &\longmapsto \begin{pmatrix} 1 & j & k \\ 0 & 1 & i \\ 0 & 0 & 1 \end{pmatrix} \end{aligned}$$

qui atterrit bien dans $\mathbb{H}$ par stabilité du produit dans le groupe $\mathbb{H}$.

- Elle est $\boxed{\text{injective}}$, car $(I_3, E_{23}, E_{23}, E_{13})$ est libre.
- Pour montrer qu'elle est surjective on peut raisonner par récurrence sur la longueur d'un mot relativement à $\mathcal{A} = \{S, T, U\}$ et montrer que tout élément dans $\mathbb{H}$ peut s'écrire (de façon unique, d'après l'injectivité de f) sous la forme $S^i T^j U^k$:
- C'est vrai pour le mot trivial : $I_3 = S^0 T^0 U^0$ de longueur nulle.
- Soit $k \geq 0$.

Supposons que le résultat est vrai pour tout élément de $\mathbb{H}$ de longueur k .

Soit $M \in \mathbb{H}$ de longueur de $k + 1$.

Il existe donc N de longueur k tel que $M \in \{SN, S^{-1}N, TN, T^{-1}N, UN, U^{-1}N\}$.

Par hypothèse de récurrence, N s'écrit sous la forme $S^i T^j U^k$.

Les cas SN et $S^{-1}N$ mènent directement au résultat attendu.

Les cas UN et $U^{-1}N$ y mènent également par commutativité de U avec S et T .

Restent les cas $T^\varepsilon N$ avec $\varepsilon \in \{\pm 1\}$. Avec la question **35**, on a :

$$T^\varepsilon N = T^\varepsilon S^i T^j U^k = S^i T^\varepsilon U^{\varepsilon i} T^j U^k = S^i T^{j+\varepsilon} U^{k+\varepsilon i}.$$

Ceci clôt la récurrence et prouve que $\boxed{f \text{ est bien surjective}}$.

- $\boxed{\text{Il ne s'agit pas d'un isomorphisme de groupes}}$ puisque $\mathbb{Z}^3$ est abélien alors que $\mathbb{H}$ ne l'est pas.

- Si l'on munit $\mathbb{Z}^3$ de la loi issue de $\mathbb{H}$ par « tiré en arrière par f » :

$$(a, b, c) \oplus (a', b', c') := f^{-1}(f(a, b, c) \times f(a', b', c')) = (a + a', b + b', c + c' + ba').$$

alors $\boxed{(\mathbb{Z}^3, \oplus) \text{ est un groupe isomorphe à } \mathbb{H}}$.

Cette loi $\oplus$ vérifie bien les axiomes d'une loi de groupe, à savoir :

- $\oplus$ est une loi de composition interne associative ;
- l'élément $(0, 0, 0)$ est le neutre de $\oplus$;
- l'élément (a, b, c) a pour inverse $(-a, -b, -c + ab)$;

puisque ces propriétés sont vraies dans $\mathbb{H}$ et sont transportées telles quelles dans $\mathbb{Z}^3$ par la bijection f^{-1} .

38. Soit $M \in \mathbb{H}$ et $p \in \mathbb{N}^*$. Montrer que si $\ell_{\mathcal{A}}(M) \leq p$, alors il existe $(i, j, k, z) \in \mathbb{Z}^4$ tels que $M = S^i T^j U^{k+z}$ avec $|i| + |j| + |k| \leq p$ et $|z| \leq |ij|$. En déduire que $|\mathcal{V}_{\mathcal{A}}(p)| = O(p^4)$ quand p tend vers $+\infty$.

On pourra utiliser les résultats de la question 35.

Les deux parties de cette question sont impossibles !

• On s'attendrait à devoir faire une récurrence sur p , mais on trouve des contre-exemples. En effet, considérons $M = T^{-1}S^3T$. Alors $\ell_{\mathcal{A}}(M) \leq 5$.

Pourtant, l'unique triplet (i, j, k) tel que $M = S^i T^j U^k$ est $(3, 0, -3)$:

$$T^{-1}S^3T = S^3T^{-1}U^{-3}T = S^3T^0U^{-3}.$$

Et comme on le voit, $i = 3, j = 0$, donc $ij = 0$, donc $z = 0$ (car $|z| \leq |ij|$), donc $k = -3$, mais alors $|i| + |j| + |k| \geq 6$.

• Notons $A_p = \{(i, j, k, z) \in \mathbb{N}^4 ; i + j + k \leq p \text{ et } z \leq ij\}$.

$$|A_p| \leq |\mathcal{V}_{\mathcal{A}}(p)| \leq 16|A_p|.$$

Il s'agit donc de montrer que $|A_p| \underset{p \rightarrow +\infty}{=} O(p^4)$.

$$|A_p| = \sum_{i=0}^p \sum_{j=0}^{p-i} \sum_{k=0}^{p-i-j} (1 + ij).$$

En minorant les « 1+ » par 0 et après changement de variables en $i' = p - i$, on obtient :

$$|A_p| \geq \sum_{i=0}^p (p-i) \underbrace{\left(i \frac{i(i+1)}{2} - \frac{i(i+1)(2i+1)}{6} \right)}_{\frac{i^3 - i}{6}}.$$

Or, en reconnaissant des sommes de Riemann,

$$\begin{aligned} * \sum_{i=0}^p p i^3 &= p^5 \times \frac{1}{p} \sum_{i=0}^p \left(\frac{i}{p}\right)^3 \underset{p \rightarrow \infty}{=} p^5 \left(\int_0^1 x^3 dx + o(1) \right) \underset{p \rightarrow \infty}{=} \frac{p^5}{4} + o(p^5); \\ * \sum_{i=0}^p i^4 &= p^5 \times \frac{1}{p} \sum_{i=0}^p \left(\frac{i}{p}\right)^4 \underset{p \rightarrow \infty}{=} p^5 \left(\int_0^1 x^4 dx + o(1) \right) \underset{p \rightarrow \infty}{=} \frac{p^5}{5} + o(p^5); \\ * \sum_{i=0}^p (p-i)i &\leq p^3 \underset{p \rightarrow \infty}{=} o(p^5), \text{ donc } \sum_{i=0}^p (p-i)i \underset{p \rightarrow \infty}{=} o(p^5). \end{aligned}$$

Donc :

$$\sum_{i=0}^p (p-i) \frac{i^3 - i}{6} \underset{p \rightarrow \infty}{\sim} \frac{p^5}{120}.$$

Ainsi,

$$p^5 \underset{p \rightarrow \infty}{=} O(|A_p|).$$

ce qui est contraire à la conclusion attendue.

38. [*Proposition alternative*]

Soit $M \in \mathbb{H}$ et $p \in \mathbb{N}^*$. Montrer que si $\ell_{\mathcal{A}}(M) \leq p$, alors il existe $(i, j, k) \in \mathbb{Z}^4$ tels que $M = S^i T^j U^k$ avec $|i| \leq p$, $|j| \leq p$ et $|k| \leq p^2$.

En déduire que $|\mathcal{V}_{\mathcal{A}}(p)| = O(p^4)$ quand p tend vers $+\infty$.

Notons $A_p = \{(i, j, k) \in \mathbb{Z}^3 ; |i| \leq p, |j| \leq p, |k| \leq p^2\}$.

Pour tout $p \in \mathbb{N}$, notons $\mathcal{P}_p : \ll \forall M \in \mathbb{H}, \ell_{\mathcal{A}}(M) \leq p \Rightarrow \exists (i, j, k) \in A_p \mid M = S^i T^j U^k. \gg$

- Nous le montrons par récurrence sur p .

Si $p = 0$, $M = I_n = S^0 T^0 U^0$ et $(0, 0, 0) \in A_0$. Donc $\mathcal{P}_0$ est vérifié.

Soit $p \geq 0$. Supposons que pour tout mot de longueur au plus p , il existe

$(i, j, k) \in \mathbb{Z}^4$ tels que $M = S^i T^j U^k$ avec $|i| \leq p$, $|j| \leq p$ et $|k| \leq p^2$.

Soit M de longueur $p+1$. Soient $A \in \mathcal{A}$, $\varepsilon \in \{\pm 1\}$ et $N \in \mathbb{H}$ de longueur p tels que $M = A^\varepsilon N$.

Alors par hypothèse de récurrence, il existe $(i, j, k) \in A_p$ tels que $N = S^i T^j U^k$.

- Si $A = S$, alors $N = S^{i+\varepsilon} T^j U^k$ et $(i + \varepsilon, j, k) \in A_{p+1}$.
- Si $A = U$, alors $N = U^\varepsilon S^i T^j U^k = S^i T^j U^{k+\varepsilon}$ et $(i, j, k + \varepsilon) \in A_{p+1}$.
- Si $A = T$, alors $N = T^\varepsilon S^i T^j U^k = S^i T^{j+\varepsilon} U^{k+\varepsilon i}$.

Or $|i| \leq p$, donc $|i| \leq p+1$; $|j| \leq p$, donc $|j + \varepsilon| \leq p+1$; et $|k + \varepsilon i| \leq p^2 + p \leq (p+1)^2$.

Donc, il existe $(i', j', k') \in A_{p+1}$ tels que $A = S^{i'} T^{j'} U^{k'}$, d'où $\mathcal{P}_{p+1}$.

Ainsi, $\boxed{\forall p \in \mathbb{N}, \forall M \in \mathbb{H}, \ell_{\mathcal{A}}(M) \leq p \Rightarrow \exists (i, j, k) \in A_p \mid M = S^i T^j U^k.}$

- Nous venons de démontrer que $\mathcal{V}_{\mathcal{A}}(p) \subset \{S^i T^j U^k ; (i, j, k) \in A_p\}$.

Donc $|\mathcal{V}_{\mathcal{A}}(p)| \leq |A_p| = (2p+1) \cdot (2p+1) \cdot (2p^2+1) \leq (3p) \cdot (3p) \cdot (3p^2) = 27p^4$.

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

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

Cette question est impossible !

Soit $M = STU^{-1}$. Alors $(i, j, k) = (1, 1, -1)$ et vérifie les hypothèses de l'énoncé avec $p = 2$. Pourtant, $\ell_{\mathcal{A}}(M) = 3$ (aucun élément de longueur 2 ne vaut STU^{-1}).

39. [*Proposition alternative*]

Montrer que, pour tout $(i, j, k) \in \mathbb{N}^3$, si $i + j \leq p$ et $k \leq ij$, alors $\ell_{\mathcal{A}}(S^i T^j U^k) \leq 2p$.

Soit $(i, j, k) \in \mathbb{N}^3$ tel que $i + j \leq p$ et $k \leq ij$.

Soit $B = \{(i', j') \in \llbracket 1, i \rrbracket \times \llbracket 1, j \rrbracket ; i' j' \leq k\}$.

Soient $k' = \max(B)$ et $(i', j') \in B$ tel que $i' j' = k'$.

Notons i'', j'', k'' tels que $i = i' + i'', j = j' + j'', k = k' + k''$.

Par définition de k' , on a : $(i' + 1)j' > k = k' + k'' = i' j' + k''$, donc $k'' < j'$.

De même, $i'(j' + 1) > k$ fournit $k'' < i'$.

Si $i'' = j'' = 0$, alors $k' = i' j' = ij$, donc $ij = k$ et $k'' = 0$.

Sinon, $i'' > 0$ ou $j'' > 0$.

$$\begin{aligned}
 S^i T^j U^k &= S^{i'+i''} T^{j'+j''} U^{k'+k''} \\
 &= S^{i''} (S^{i'} T^{j'} U^{i' j'}) T^{j''} U^{k''} \\
 &= S^{i''} (T^{j'} S^{i'}) T^{j''} U^{k''} \\
 &= \begin{cases} S^{i''} (T^{j'} S^{i'}) T^{j''} & \text{si } i'' = j'' = 0 \\ S^{i''-1} (S T^{k''} U^{k''}) T^{j'-k''} S^{i'} T^{j''} & \text{si } i'' > 0 \\ S^{i''} T^{j'} S^{i'-k''} (S^{k''} T U^{k''}) T^{j''-1} & \text{si } j'' > 0 \end{cases} \\
 &= \begin{cases} S^{i''} (T^{j'} S^{i'}) T^{j''} & \text{si } i'' = j'' = 0 \\ S^{i''-1} (T^{k''} S) T^{j'-k''} S^{i'} T^{j''} & \text{si } i'' > 0 \\ S^{i''} T^{j'} S^{i'-k''} (T S^{k''}) T^{j''-1} & \text{si } j'' > 0 \end{cases}
 \end{aligned}$$

Dans les trois cas, le nombre de générateurs employés ultimement est égal à

$$(i'' - 1) + k'' + 1 + (j' - k'') + i' + j'' = i'' + j' + i' + j'' = i + j.$$

Ainsi, $\ell_{\mathcal{A}}(S^i T^j U^k) \leq p$ lorsque $i, j, k \geq 0$, $i + j \leq p$ et $k \leq ij$.

40. Montrer que :

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

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

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

Alors :

$$\begin{aligned} |A_p| &= \sum_{i=0}^p \sum_{j=0}^{p-i} \sum_{k=0}^{ij} 1 \\ &= \sum_{i=0}^p \sum_{j=0}^{p-i} (ij + 1) \\ &= \sum_{i=0}^p \left((p-i+1) + i \frac{(p-i)(p-i+1)}{2} \right) \\ &= \frac{p^3}{2} \sum_{i=0}^p \left(\left(\frac{i}{p} \right)^3 + \left(-2 + \frac{1}{p} \right) \left(\frac{i}{p} \right)^2 + \left(1 - \frac{1}{p} \right) \left(\frac{i}{p} \right) + \left(1 + \frac{1}{p} \right) \frac{2}{p} \right) \\ &\stackrel{(1)}{\geq} \frac{p^3}{2} \sum_{i=0}^p \left(\left(\frac{i}{p} \right)^3 - 2 \left(\frac{i}{p} \right)^2 + \left(\frac{i}{p} \right) \right) \\ &\geq \frac{p^3}{2} \sum_{i=0}^p \frac{i}{p} \left(1 - \frac{i}{p} \right)^2 \end{aligned}$$

(1) car $0 \leq \frac{i}{p} \leq 1$ et donc $\left(1 + \frac{1}{p} \right) \frac{2}{p}$ compense le terme $-\frac{1}{p} \frac{i}{p}$.

- Par continuité de l'application $x \mapsto x(1-x^2)$ sur $[0, 1]$,

$$\frac{1}{p} \sum_{i=1}^p \frac{i}{p} \left(1 - \frac{i}{p} \right)^2 \xrightarrow{p \rightarrow \infty} \int_0^1 x(1-x)^2 dx = \frac{1}{12}.$$

Donc $\boxed{|A_p| \underset{p \rightarrow \infty}{\sim} \frac{p^4}{24}}.$

41. En d  duire que $\mathbb{H}$ est un groupe    croissance polynomiale de degr   4 .

Nous nous appuyons sur les   nonc  s (probablement erron  s) des questions 38 et 39.

Nous notons    nouveau $A_p = \{(i, j, k) \in \mathbb{N}^3 ; i + j \leq p \text{ et } k \leq ij\}$.

Les questions 39 et 40 fournissent un sens de l'in  galit   (asymptotiquement seulement) :

$$|\mathcal{V}_{\mathcal{A}}(p)| \geq |A_p| \underset{p \rightarrow \infty}{\sim} \frac{p^4}{8}.$$

La fin de la question 38 fournit l'autre sens de l'in  galit   (asymptotiquement seulement) :

$$|\mathcal{V}_{\mathcal{A}}(p)| \underset{p \rightarrow \infty}{=} O(p^4).$$

Il existe donc $\alpha, \beta > 0$ (avec $\alpha = \frac{1}{16}$, par exemple) et $N \in \mathbb{N}$ tels que :

$$\forall p \geq N, \alpha p^4 \leq |\mathcal{V}_{\mathcal{A}}(p)| \leq \beta p^4.$$

Soient $\alpha' = \min \left\{ \frac{|\mathcal{V}_{\mathcal{A}}(p)|}{p^4} ; p \in \llbracket 1, N \rrbracket \right\} > 0$ et $\beta' = \max \left\{ \frac{|\mathcal{V}_{\mathcal{A}}(p)|}{p^4} ; p \in \llbracket 1, N \rrbracket \right\} > 0$.

Alors :

$$\forall p \in \llbracket 1, N \rrbracket, \alpha' p^4 \leq |\mathcal{V}_{\mathcal{A}}(p)| \leq \beta' p^4.$$

Finalement,

$$\forall p \in \mathbb{N}^*, \min(\alpha, \alpha') p^4 \leq |\mathcal{V}_{\mathcal{A}}(p)| \leq \max(\beta, \beta') p^4.$$

Donc $\mathbb{H}$ est un groupe    croissance polynomiale de degr   4.

FIN DU PROBL  ME