

CONCOURS CENTRALE-SUPÉELEC
SESSION 2026 FILIÈRE MP-MPI
CORRIGÉ DE MATHÉMATIQUES 1

m.laamoum2@gmail.com¹

Sur quelques sous-groupes de $GL_n(\mathbb{R})$

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

I – Généralités

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

- Q.1** • G est fini. D'après le théorème de Lagrange, l'ordre de tout élément de G divise $|G|$. Donc pour tout $A \in G$ on a $A^{|G|} = e$, ce qui montre que G est d'exposant fini.
- G est fini donc l'ensemble $\text{Tr}G = \{\text{Tr}A \mid A \in G\}$ l'est aussi.

Q.2 Considérons :

$$G = \left\{ \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \mid \alpha \in \mathbb{R} \right\}$$

C'est un sous-groupe infini de $GL_2(\mathbb{R})$ et $\text{Tr}G = \{2\}$.

- Q.3** Considérons $G = (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$ le groupe des suites à valeurs dans $\mathbb{Z}/2\mathbb{Z}$ muni de l'addition. G est infini et d'exposant 2.

II – Cas particulier : les sous-groupes finis de $O_2(\mathbb{R})$

- Q.4** Soit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SO_2(\mathbb{R})$. On a $A^\top A = I_2$ et $\det(A) = 1$.

On a donc le système :

$$\begin{cases} a^2 + c^2 = 1 \\ b^2 + d^2 = 1 \\ ab + cd = 0 \\ ad - bc = 1 \end{cases}$$

De $a^2 + c^2 = 1$, il existe $\theta \in [0, 2\pi[$ tel que $a = \cos(\theta)$, $c = \sin(\theta)$.

Le système devient

$$\begin{cases} b \cos(\theta) + d \sin(\theta) = 0 \\ -b \sin(\theta) + d \cos(\theta) = 1 \\ b^2 + d^2 = 1 \end{cases}$$

¹ <https://tinyurl.com/hb8n2vr9>

par suite

$$b = \frac{\begin{vmatrix} 0 & \sin(\theta) \\ 1 & \cos(\theta) \end{vmatrix}}{\begin{vmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{vmatrix}} = -\sin(\theta) \quad , \quad d = \frac{\begin{vmatrix} \cos(\theta) & 0 \\ -\sin(\theta) & 1 \end{vmatrix}}{\begin{vmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{vmatrix}} = \cos(\theta)$$

Donc $\boxed{A = R_\theta \text{ avec } \theta \in [0, 2\pi[}$.

Q.5 Soit $\theta \in \mathbb{R}$. On pose $G = \langle R_\theta \rangle$.

a) On sait que $\langle R_\theta \rangle$ est le plus petit sous-groupe de $\text{GL}_2(\mathbb{R})$ contenant R_θ et $\langle R_\theta \rangle = \{(R_\theta)^k \mid k \in \mathbb{Z}\}$.

Comme $(R_\theta)^k = R_{k\theta}$ pour tout $k \in \mathbb{Z}$, donc $\boxed{G = \langle R_\theta \rangle = \{R_{k\theta} \mid k \in \mathbb{Z}\}}$.

b) Si $\theta = \frac{2\pi}{m}$, $m \in \mathbb{N}^*$ alors $(R_\theta)^m = I_2$. Si $k, h \in \llbracket 1, m \rrbracket$, $h \neq k$ alors $(R_\theta)^k \neq (R_\theta)^h$.

Par suite $G = \{I_2, R_\theta, (R_\theta)^2, \dots, (R_\theta)^{m-1}\}$, il est donc cyclique d'ordre $|G| = m$.

c) On a $G = \langle R_\theta \rangle = \{R_{k\theta} \mid k \in \mathbb{Z}\}$.

Si G est fini alors il est d'exposant fini, il existe $m \in \mathbb{N}^*$ tel que $R_{m\theta} = I_2$, par suite $m\theta = 2k\pi$ et $k \in \mathbb{Z}$, donc $\frac{\theta}{\pi} = \frac{2k}{m} \in \mathbb{Q}$.

De la question **Q5.b)** on a l'autre implication.

Ainsi : $\boxed{G \text{ est fini si et seulement si } \frac{\theta}{\pi} \in \mathbb{Q}}$.

d) Supposons G d'exposant fini : il existe $m \in \mathbb{N}^*$ tel que $A^m = I_2$ pour tout $A \in G$, en particulier

$(R_\theta)^m = R_{m\theta} = I_2$. Cela implique $m\theta \equiv 0 \pmod{2\pi}$, donc $\frac{\theta}{\pi} \in \mathbb{Q}$, et par la question c) G est fini.

e) On a $\text{Tr}G = \{\text{Tr}R_{k\theta} \mid k \in \mathbb{Z}\} = \{2\cos(k\theta) \mid k \in \mathbb{N}\}$.

Si $\text{Tr}G$ est fini, alors il existe $n, m \in \mathbb{Z}$, tels que $n \neq m$ et $\cos(n\theta) = \cos(m\theta)$. Donc $n\theta \equiv \pm m\theta \pmod{2\pi}$, ce qui donne $\frac{\theta}{\pi} \in \mathbb{Q}$. D'après la question **Q5.c)** G est fini.

Q.6 Soient θ, θ' deux réels. $G = \langle R_\theta, R_{\theta'} \rangle$.

a) • Dans l'énoncé d'origine on demande de démontrer que : $|G| = |(\theta\mathbb{Z} + \theta'\mathbb{Z}) \cap [0, 2\pi[|$.

En général ce résultat n'est pas vrai :

Par exemple si $\theta = \frac{3\pi}{2}$ et $\theta' = 3\pi$, alors $\theta\mathbb{Z} + \theta'\mathbb{Z} = \frac{3\pi}{2}\mathbb{Z}$ et $(\theta\mathbb{Z} + \theta'\mathbb{Z}) \cap [0, 2\pi[= \{0, \frac{3\pi}{2}\}$.

Mais $\langle R_{\frac{3\pi}{2}}, R_{3\pi} \rangle = \langle R_{\frac{3\pi}{2}} \rangle = \{I_2, R_{\frac{3\pi}{2}}, R_\pi, R_{\frac{3\pi}{2}}\}$.

• Montrons que $|G| = |\overline{\theta\mathbb{Z} + \theta'\mathbb{Z}}|$:

R_θ et $R_{\theta'}$ commutent, donc

$$G = \{(R_\theta)^p (R_{\theta'})^q \mid (p, q) \in \mathbb{Z}^2\} = \{R_{(p\theta + q\theta')} \mid (p, q) \in \mathbb{Z}^2\}$$

Tout A élément de G s'écrit d'une manière unique de la forme $A = R_{\overline{(p\theta + q\theta')}}$ avec $(p, q) \in \mathbb{Z}^2$. Ce qui

définit une bijection entre G et l'ensemble $\overline{\theta\mathbb{Z} + \theta'\mathbb{Z}} = \{\overline{p\theta + q\theta'} \mid (p, q) \in \mathbb{Z}^2\}$.

$$\text{Ainsi } \boxed{|G| = |\overline{\theta\mathbb{Z} + \theta'\mathbb{Z}}|}.$$

Ce cardinal peut être infini, comme dans le cas $\theta = 1$ et $\theta' = 2$.

b) Soit p, q premiers entre eux.

On a

$$\frac{\pi}{p}\mathbb{Z} + \frac{\pi}{q}\mathbb{Z} = \frac{\pi}{pq}(q\mathbb{Z} + p\mathbb{Z})$$

comme $\text{pgcd}(p, q) = 1$ alors $q\mathbb{Z} + p\mathbb{Z} = \mathbb{Z}$, par suite

$$\frac{\pi}{p}\mathbb{Z} + \frac{\pi}{q}\mathbb{Z} = \frac{\pi}{pq}\mathbb{Z}$$

Donc

$$\overline{\frac{\pi}{p}\mathbb{Z} + \frac{\pi}{q}\mathbb{Z}} = \frac{\pi}{pq}\mathbb{Z} \cap [0, 2\pi[= \left\{ 0, \frac{\pi}{pq}, \frac{2\pi}{pq}, \dots, \frac{(2pq-1)\pi}{pq} \right\}$$

Ainsi $|G| = 2pq$.

c) On a $q\mathbb{Z} + p\mathbb{Z} = \text{pgcd}(p, q) \cdot \mathbb{Z}$, donc

$$\frac{\pi}{p}\mathbb{Z} + \frac{\pi}{q}\mathbb{Z} = \frac{\pi}{pq}(q\mathbb{Z} + p\mathbb{Z}) = \frac{\pi}{pq}\text{pgcd}(p, q) \cdot \mathbb{Z}$$

Comme $pq = \text{pgcd}(p, q) \cdot \text{ppcm}(p, q)$ alors

$$\frac{\pi}{p}\mathbb{Z} + \frac{\pi}{q}\mathbb{Z} = \frac{\pi}{\text{ppcm}(p, q)} \mathbb{Z}$$

par suite $\left| \left(\frac{\pi}{p}\mathbb{Z} + \frac{\pi}{q}\mathbb{Z} \right) \cap [0, 2\pi[\right| = 2\text{ppcm}(p, q)$.

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

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

D'après **Q4** tout élément de G s'écrit R_θ avec $\theta \in [0, 2\pi[$, donc l'ensemble $U = \{\theta \in [0, 2\pi[\mid R_\theta \in G\}$ est fini.

- Si $G = \{I_2\}$ il est monogène.

- Si $G \neq \{I_2\}$

Soit $\theta_0 = \min(U \setminus \{0\})$ (existe car U est fini non réduit à $\{0\}$). On a $R_{\theta_0} \in G$ et $\langle R_{\theta_0} \rangle \subset G$.

Soit $R_\theta \in G$ et $\theta \in [0, 2\pi[$. Posons

$$k = \left\lfloor \frac{\theta}{\theta_0} \right\rfloor \text{ et } \rho = \theta - k\theta_0 \in [0, \theta_0[$$

Alors

$$R_\rho = R_\theta \cdot R_{-k\theta_0} = R_\theta \cdot R_{k\theta_0}^{-1} \in G$$

Donc $\rho \in U$, par minimalité de θ_0 , on a $\rho = 0$.

Par suite $R_\theta = R_{\theta_0}^k \in \langle R_{\theta_0} \rangle$ donc $G \subset \langle R_{\theta_0} \rangle$.

Ainsi $G = \langle R_{\theta_0} \rangle$ est monogène.

Q.8 Soit $m \in \mathbb{N}^*$ et $\mathcal{D}_m = \left\langle R_{\frac{2\pi}{m}}, S_{\frac{\pi}{2}} \right\rangle \subset \text{O}_2(\mathbb{R})$.

a) On a

$$\mathcal{D}_m = \left\{ \prod_{i=1}^r \left(R_{\frac{2\pi}{m}} \right)^{p_i} \left(S_{\frac{\pi}{2}} \right)^{q_i} ; \prod_{i=1}^r \left(S_{\frac{\pi}{2}} \right)^{q_i} \left(R_{\frac{2\pi}{m}} \right)^{p_i} \mid r \in \mathbb{N}; p_i, q_i \in \mathbb{Z} \right\}$$

Puisque $(S_{\frac{\pi}{2}})^2 = R_0 = I_2$ alors $\mathcal{D}_m$ est de la forme

$$\mathcal{D}_m = \left\{ \prod_{i=1}^r R_{\frac{2\pi p_i}{m}} \cdot S_{\frac{\pi}{2}} ; \prod_{i=1}^r S_{\frac{\pi}{2}} R_{\frac{2\pi p_i}{m}} ; R_{\frac{2\pi q}{m}} \mid r \in \mathbb{N}; q, p_i \in \mathbb{Z} \right\}$$

Avec cette écriture le déterminant d'un élément est égal à $(-1)^r$ ou 1. Donc

$$\mathcal{D}_m \cap \text{SO}_2(\mathbb{R}) = \left\{ \prod_{i=1}^{2r} R_{\frac{2\pi p_i}{m}} \cdot S_{\frac{\pi}{2}} ; \prod_{i=1}^{2r} S_{\frac{\pi}{2}} R_{\frac{2\pi p_i}{m}} ; R_{\frac{2\pi q}{m}} \mid r \in \mathbb{N}; q, p_i \in \mathbb{Z} \right\}$$

On écrit alors

$$\mathcal{D}_m \cap \text{SO}_2(\mathbb{R}) = \left\{ \prod_{i=1}^r \left(R_{\frac{2\pi k_i}{m}} S_{\frac{\pi}{2}} R_{\frac{2\pi h_i}{m}} \cdot S_{\frac{\pi}{2}} \right) ; \prod_{i=1}^r \left(S_{\frac{\pi}{2}} \cdot R_{\frac{2\pi k_i}{m}} S_{\frac{\pi}{2}} R_{\frac{2\pi h_i}{m}} \right) ; R_{\frac{2\pi q}{m}} \mid (k_i, h_i) = (p_{2i-1}, p_{2i}) \in \mathbb{Z}^2 \right\}$$

Comme $S_\alpha R_\beta S_\alpha = R_{-\beta}$ alors

$$\mathcal{D}_m \cap \text{SO}_2(\mathbb{R}) = \left\{ R_{\frac{2\pi p}{m}} \mid p \in \mathbb{Z}^2 \right\} = \left\langle R_{\frac{2\pi}{m}} \right\rangle$$

L'application

$$\begin{aligned} \phi : \mathcal{D}_m \cap \text{SO}_2(\mathbb{R}) &\rightarrow \mathcal{D}_m \setminus \text{SO}_2(\mathbb{R}) \\ A &\mapsto S_{\frac{\pi}{2}} A \end{aligned}$$

est bijective et $\phi(\mathcal{D}_m \cap \text{SO}_2(\mathbb{R})) = S_{\frac{\pi}{2}}(\mathcal{D}_m \cap \text{SO}_2(\mathbb{R})) = \mathcal{D}_m \setminus \text{SO}_2(\mathbb{R})$.

Donc

$$|\mathcal{D}_m| = |\mathcal{D}_m \cap \text{SO}_2(\mathbb{R})| + |\mathcal{D}_m \setminus \text{SO}_2(\mathbb{R})| = 2|\mathcal{D}_m \cap \text{SO}_2(\mathbb{R})| = 2 \left| \left\langle R_{\frac{2\pi}{m}} \right\rangle \right|$$

Or $\left\langle R_{\frac{2\pi}{m}} \right\rangle$ est d'ordre m donc $|\mathcal{D}_m| = 2m$.

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

Donc G contient une symétrie S_α pour $\alpha \in \mathbb{R}$. L'ensemble $H = G \cap \text{SO}_2(\mathbb{R})$ est un sous-groupe fini de $\text{SO}_2(\mathbb{R})$, les questions **Q7** et **Q5** donnent $H = \left\langle R_{\frac{2\pi}{m}} \right\rangle$ avec $m \in \mathbb{N}^*$.

On a

$$A \in G \setminus H \text{ si et seulement si } S_\alpha A \in H$$

donc $G = \left\langle R_{\frac{2\pi}{m}} \right\rangle \cup S_\alpha \left\langle R_{\frac{2\pi}{m}} \right\rangle$. Considérons le morphisme de groupe

$$\Phi : G \rightarrow \mathcal{D}_m \text{ tel que } \Phi \left(R_{\frac{2\pi}{m}} \right) = R_{\frac{2\pi}{m}} \text{ et } \Phi(S_\alpha) = S_{\frac{\pi}{2}}.$$

Φ est surjectif par construction et $|G| = |\mathcal{D}_m|$ donc c'est un isomorphisme de groupes.

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

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

Q.9 Théorème de réduction des matrices orthogonales :

Soit $M \in \text{O}_n(\mathbb{R})$. Il existe une matrice $P \in \text{O}_n(\mathbb{R})$ et des nombres $\theta_1, \dots, \theta_r \in [0, 2\pi[$, $p, q \in \mathbb{N}$ tels que

$$M = P \cdot \text{Diag}(R_{\theta_1}, \dots, R_{\theta_r}, -I_q, I_p) \cdot P^\top$$

Q.10 Supposons G d'exposant fini : il existe $m \in \mathbb{N}^*$ tel que $A^m = I_n$ pour tout $A \in G$.

Soit $A \in G$. Par la question précédente, il existe $P \in \text{O}_n(\mathbb{R})$ et $\theta_1, \dots, \theta_r \in [0, 2\pi[$, $p, q \in \mathbb{N}$ tels que

$$A = P \cdot \text{Diag}(R_{\theta_1}, \dots, R_{\theta_r}, -I_q, I_p) \cdot P^\top$$

donc

$$A^m = I_n = P \cdot \text{Diag}(R_{m\theta_1}, \dots, R_{m\theta_r}, (-1)^m I_q, I_p) \cdot P^\top$$

par suite $m\theta_1, \dots, m\theta_r \in 2\pi\mathbb{Z}$ et $m \in 2\mathbb{N}^*$, donc pour tout $i \in \llbracket 1, r \rrbracket$ on a $\theta_i \in \frac{2\pi k_i}{m}$ avec $k_i \in \llbracket 0, m \rrbracket$.

Comme $\text{Tr}(A) = \sum_{i=1}^r 2\cos(\theta_i) + p - q$ et $2r + p + q = n$ alors

$$\text{Tr}G = \left\{ \sum_{i=1}^r 2\cos\left(\frac{2\pi k_i}{m}\right) + (2r + 2p - n) \mid r \in \llbracket 0, \frac{n}{2} \rrbracket, p \in \llbracket 0, n - 2r \rrbracket, k_i \in \llbracket 0, m \rrbracket \right\}$$

Il n'y a qu'un nombre fini d'éléments dans cet ensemble (chaque élément correspond au choix de r, p et un r -uplet de $\llbracket 0, m \rrbracket$, au maximum on a $n^2 m^r$ éléments). Ainsi $\text{Tr}G$ est fini.

On suppose que $\text{Tr}G$ est fini. On munit $\mathcal{M}_n(\mathbb{R})$ de son produit scalaire usuel :

$$\langle A \mid B \rangle = \text{Tr} (A^\top B) .$$

On note $\mathcal{F} = \text{Vect}(G)$ et $d = \dim \mathcal{F}$. Les coefficients d'une matrice M sont notés $M_{i,j}$

Q.11 On a G engendre $\mathcal{F}$ qui est de dimension d , donc le rang de G , comme famille de vecteurs, est d .

Ainsi il existe $A_1, \dots, A_d \in G$ tels que $(A_1, \dots, A_d)$ est libre et $\mathcal{F} = \text{Vect}(G) = \text{Vect}(\{A_1, \dots, A_d\})$.

Donc $\mathcal{B} = (A_1, \dots, A_d)$ est une base de $\mathcal{F}$.

Q.12 Posons $\mathcal{B}_0 = (E_{p,q})_{(p,q) \in \llbracket 1,n \rrbracket^2}$ la base canonique de $\mathcal{M}_n(\mathbb{R})$ qui est orthonormée pour le produit scalaire usuel.

Soit $B = (\langle A_i \mid A_j \rangle)_{(i,j) \in \llbracket 1,d \rrbracket^2}$ et $C = \text{Mat}_{\mathcal{B}_0}(A_1, \dots, A_d)$.

a) La longueur des colonnes de C est n^2 , donc C est de taille $n^2 \times d$ et $\boxed{C \in \mathcal{M}_{n^2,d}(\mathbb{R})}$.

b) On a $C = \text{Mat}_{\mathcal{B}_0}(A_1, \dots, A_d) = \left[\begin{array}{c|c|c} Z_1 & \dots & Z_d \end{array} \right]$, avec Z_j vecteur colonne des coordonnées de A_j dans $\mathcal{B}_0$.
Donc

$$C^\top \cdot C = \left[\begin{array}{c} Z_1^\top \\ \vdots \\ Z_d^\top \end{array} \right] \left[\begin{array}{c|c|c} Z_1 & \dots & Z_d \end{array} \right] = \left(Z_i^\top \cdot Z_j \right)_{(i,j) \in \llbracket 1,d \rrbracket^2}$$

La base $\mathcal{B}_0$ est orthonormée, donc $\langle A_i \mid A_j \rangle = Z_i^\top \cdot Z_j$ pour tout $(i,j) \in \llbracket 1,d \rrbracket$.

Ainsi $\boxed{B = C^\top C}$.

c) On a $\text{Ker}(C) \subset \text{Ker}(C^\top C)$ et si $x \in \text{Ker}(C^\top C)$ alors $x^\top C^\top C x = \|Cx\|^2 = 0$ donc $Cx = 0$, par suite $\text{Ker}(C^\top C) \subset \text{Ker}(C)$.

Donc $\text{Ker}(C^\top C) = \text{Ker}(C)$ et $\boxed{\text{rg}(B) = \text{rg}(C^\top C) = \text{rg}(C)}$.

On a $\text{rg}(C) = \text{rg}(A_1, \dots, A_d) = d$, donc $\text{rg}(B) = d$. Or $B \in \mathcal{M}_d(\mathbb{R})$ donc elle est inversible.

Q.13 Soit $M \in G$. On pose $M = \sum_{j=1}^d x_j A_j$, $X_M = (x_1, \dots, x_d)^\top$ et $Y_M = \left(\langle A_1 \mid M \rangle, \dots, \langle A_d \mid M \rangle \right)^\top$.

On a

$$(Y_M)_i = \langle A_i \mid M \rangle = \left\langle A_i \mid \sum_{j=1}^d x_j A_j \right\rangle = \sum_{j=1}^d x_j \langle A_i \mid A_j \rangle = \sum_{j=1}^d B_{i,j} x_j = (BX_M)_i$$

Donc $Y_M = BX_M$, ainsi $\boxed{X_M = B^{-1}Y_M}$ (car B est inversible).

Q.14 Soit $i \in \llbracket 1,d \rrbracket$. On a $(Y_M)_i = \langle A_i \mid M \rangle = \text{Tr}(A_i^\top M)$. Comme $A_i, M \in G \subset \text{O}_n(\mathbb{R})$, donc $A_i^\top = A_i^{-1} \in G$ et $A_i^\top M \in G$. Par suite $(Y_M)_i = \text{Tr}(A_i^\top M) \in \text{Tr}G$.

Comme $\text{Tr}G$ est fini (par hypothèse), chaque $(Y_M)_i$ prend un nombre fini de valeurs, donc

$\{Y_M \mid M \in G\} \subset (\text{Tr}G)^d$ (Y_M pris comme un d -uplet), d'où $\{Y_M \mid M \in G\}$ est fini.

Soit l'application $\varphi : G \rightarrow \{Y_M \mid M \in G\}$ avec $\varphi(A) = Y_A = BX_A$ pour $A \in G$.

Toute matrice $A \in G$ est déterminé, d'une manière unique, par ses coordonnées X_M dans la base $\mathcal{B}$.

Donc φ est bijective et $|G| = |\{Y_M \mid M \in G\}|$. Ainsi G est fini.

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

I – Quelques propriétés utiles

$\mathcal{M}_{n,1}(\mathbb{R})$ est muni de son produit scalaire canonique noté $\langle \cdot, \cdot \rangle$ et de sa norme associée $\| \cdot \|$.

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

Q.15 On pose, pour $X, Y \in \mathcal{M}_{n,1}(\mathbb{R})$: $\langle X, Y \rangle_A = \langle AX \mid Y \rangle$.

- *Bilinéarité* :

Par bilinéarité du produit scalaire $\langle \cdot, \cdot \rangle$ et linéarité de la multiplication matricielle.

- *Symétrie* :

On a : $\langle X, Y \rangle_A = \langle AX \mid Y \rangle = Y^\top AX = (Y^\top AX)^\top = X^\top A^\top Y$

or $A = A^\top$ donc $\langle X, Y \rangle_A = X^\top AY = \langle AY \mid X \rangle = \langle Y, X \rangle_A$.

- *Définition et positivité* :

On a pour $X \neq 0$: $\langle X, X \rangle_A = \langle AX \mid X \rangle = X^\top AX$,

or $A \in \mathcal{S}_n^{++}(\mathbb{R})$ donc $\langle X, X \rangle_A > 0$.

Donc $\langle \cdot, \cdot \rangle_A$ est bien un produit scalaire. La norme associée est $\|X\|_A = \sqrt{X^\top AX}$.

- On a $\mathcal{B}_A = \{X \mid \|X\|_A \leq 1\}$. Soit $r > 0$, pour $A = \frac{1}{r^2} I_n$ on obtient $\mathcal{B}(0, r) = \mathcal{B}_A$.

Q.16 On a $A \in \mathcal{S}_n^{++}(\mathbb{R})$ et $B \in \mathcal{S}_n(\mathbb{R})$, soit $g : X \mapsto A^{-1}BX$. On a pour $X, Y \in \mathcal{M}_{n,1}(\mathbb{R})$:

$$\langle g(X), Y \rangle_A = \langle A^{-1}BX, Y \rangle_A = \langle A.A^{-1}BX \mid Y \rangle = \langle BX \mid Y \rangle = \langle X \mid BY \rangle \quad (\text{car } B \in \mathcal{S}_n(\mathbb{R}))$$

de même

$$\langle X, g(Y) \rangle_A = \langle X, A^{-1}BY \rangle_A = \langle AX \mid A^{-1}BY \rangle = \langle X \mid AA^{-1}BY \rangle = \langle X \mid BY \rangle \quad (\text{car } A \in \mathcal{S}_n(\mathbb{R}))$$

Donc $\langle g(X), Y \rangle_A = \langle X, g(Y) \rangle_A$, l'endomorphisme g est bien autoadjoint pour $\langle \cdot, \cdot \rangle_A$.

Par le théorème spectral g et $A^{-1}B$ sont diagonalisables, dans une base orthonormée pour $\langle \cdot, \cdot \rangle_A$.

Q.17 Soit $A, B \in \mathcal{S}_n(\mathbb{R})$, on a

$$B \preccurlyeq A \iff \forall X, \langle BX \mid X \rangle \leq \langle AX \mid X \rangle \iff \forall X, \langle (A - B)X \mid X \rangle \geq 0 \iff A - B \in \mathcal{S}_n^+(\mathbb{R}).$$

Q.18 Soient $A, B \in \mathcal{S}_n^{++}(\mathbb{R})$. Par la question **Q.17**, $A^{-1}B$ est autoadjoint pour $\langle \cdot, \cdot \rangle_A$, donc diagonalisable dans une base orthonormée $(V_1, \dots, V_n)$ pour ce produit scalaire, avec des valeurs propres réelles $\lambda_1, \dots, \lambda_n$.

Soit $X \in \mathcal{M}_{n,1}(\mathbb{R})$ on l'écrit $X = \sum_{i=1}^n \alpha_i V_i$ donc

$$\langle A^{-1}BX, X \rangle_A = \sum_{i=1}^n \lambda_i \alpha_i^2 \quad \text{et} \quad \langle X, X \rangle_A = \sum_{i=1}^n \alpha_i^2 \tag{1}$$

Par suite

- Si $\text{Sp}(A^{-1}B) \subset]0, 1]$: les relations (1) donnent pour tout $X \in \mathcal{M}_{n,1}(\mathbb{R})$

$$\langle BX \mid X \rangle = \langle A^{-1}BX, X \rangle_A = \sum_{i=1}^n \lambda_i \alpha_i^2 \leq \sum_{i=1}^n \alpha_i^2 = \langle X, X \rangle_A = \langle AX \mid X \rangle$$

donc $B \preccurlyeq A$.

- Si $B \preccurlyeq A$.

Pour $X = V_i$ et $i \in \llbracket 1, n \rrbracket$ on a

$$\langle BX \mid X \rangle = \langle A^{-1}BX, X \rangle_A = \lambda_i \|X\|_A^2 = \lambda_i$$

et

$$\langle AX \mid X \rangle = \langle X, X \rangle_A = 1$$

donc $\lambda_i \leq 1$, comme $B \in \mathcal{S}_n^{++}(\mathbb{R})$ alors $\lambda_i > 0$. Par suite $\text{Sp}(A^{-1}B) \subset]0, 1]$.

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

Q.19 Soit $A, B \in \mathcal{S}_n^{++}(\mathbb{R})$ et $B \preccurlyeq A$.

- Par la question précédente $\text{Sp}(A^{-1}B) \subset]0, 1]$, ce qui donne

$$\det(A^{-1}B) = \frac{\det(B)}{\det(A)} = \prod_{\lambda \in \text{Sp}(A^{-1}B)} \lambda \leq 1,$$

Donc $\det(B) \leq \det(A)$.

- Cas d'égalité :

Supposons $\det(B) = \det(A)$, alors $\det(A^{-1}B) = \prod_{\lambda \in \text{Sp}(A^{-1}B)} \lambda = 1$.

On a $\text{Sp}(A^{-1}B) \subset]0, 1]$, si $\exists \lambda_0 \in \text{Sp}(A^{-1}B)$ tel que $\lambda_0 < 1$ alors $\prod_{\lambda \in \text{Sp}(A^{-1}B)} \lambda < 1$, absurde.

Donc $\text{Sp}(A^{-1}B) = \{1\}$, or $A^{-1}B$ est diagonalisable donc $A^{-1}B = I_n$ et $A = B$.

Ainsi $\boxed{\det(B) \leq \det(A) \text{ avec égalité si et seulement si } A = B}$.

Q.20 Soit $A, B \in \mathcal{S}_n^{++}(\mathbb{R})$.

- Si $B \preccurlyeq A$:

Pour $X \in \mathcal{B}_A$, on a $\|X\|_A^2 = X^\top AX \leq 1$, par suite

$$\|X\|_B^2 = X^\top BX \leq X^\top AX \leq 1$$

donc $X \in \mathcal{B}_B$. Ainsi $\mathcal{B}_A \subset \mathcal{B}_B$.

- Si $\mathcal{B}_A \subset \mathcal{B}_B$:

Soit $X \neq 0$. Posons $Y = \frac{1}{\|X\|_A} X$, on a $\|Y\|_A^2 = Y^\top AY = 1$ ce qui donne $Y \in \mathcal{B}_A \subset \mathcal{B}_B$, donc

$$Y^\top BY = \frac{1}{\|X\|_A^2} X^\top BX = \frac{X^\top BX}{X^\top AX} \leq 1$$

soit $X^\top BX \leq X^\top AX$. Pour $X = 0$, l'inégalité est triviale. Donc $B \preccurlyeq A$.

Ainsi $\boxed{B \preccurlyeq A \text{ si et seulement si } \mathcal{B}_A \subset \mathcal{B}_B}$.

Q.21 Soit $\mathcal{K}$ une partie de $\mathcal{S}_n^+(\mathbb{R})$.

$\Leftarrow$ Soit $\alpha \in \mathbb{R}_+^*$ tel que $A \preccurlyeq \alpha I_n$, pour tout $A \in \mathcal{K}$.

Donc pour tout $X \in \mathcal{M}_{n,1}(\mathbb{R})$

$$\langle AX | X \rangle \leq \alpha \|X\|^2 \tag{1}$$

On a A est diagonalisable dans une base orthonormée $(V_1, \dots, V_n)$ de $\mathcal{M}_{n,1}(\mathbb{R})$ avec $AV_i = \lambda_i V_i$.

La relation (1) donne pour tout i :

$$0 \leq \lambda_i = \langle AV_i | V_i \rangle \leq \alpha \|V_i\|^2 = \alpha$$

De plus on a

$$\|A\|^2 = \text{Tr}(A^\top A) = \text{Tr}(A^2) = \sum_{i=1}^n \lambda_i^2 \leq n\alpha^2$$

Donc $\mathcal{K} \subset \mathcal{B}(0, \alpha\sqrt{n})$ et $\mathcal{K}$ est bornée .

$\Rightarrow$ Si $\mathcal{K}$ est bornée, il existe $\alpha \in \mathbb{R}_+^*$ tel que pour tout $A \in \mathcal{K}$, $\|A\| \leq \alpha$.

Soit $A \in \mathcal{K}$, avec $\text{Sp}(A) = \{\lambda_1, \dots, \lambda_n\}$. On a $\|A\|^2 = \sum_{i=1}^n \lambda_i^2$ donc $0 \leq \lambda_i \leq \sqrt{\alpha}$ pour tout i .

Par suite la matrice $\sqrt{\alpha}I_n - A$ est symétrique réelle et

$$\text{Sp}(\alpha I_n - A) = \{\sqrt{\alpha} - \lambda_i \mid i \in \llbracket 1, n \rrbracket\} \subset \mathbb{R}_+^*,$$

donc $\sqrt{\alpha}I_n - A \in \mathcal{S}_n^+(\mathbb{R})$. D'après **Q17** on a $A \preccurlyeq \sqrt{\alpha}I_n$.

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

Ainsi $\boxed{\mathcal{K} \text{ est bornée si et seulement si } \exists \alpha \in \mathbb{R}_+^* \text{ telle que pour tout } A \in \mathcal{K}, A \preccurlyeq \alpha I_n}$.

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

Q.22 Soient $A, B \in \mathcal{S}_n^{++}(\mathbb{R})$ et $t \in [0, 1]$. La matrice $tA + (1-t)B$ est symétrique.

Pour $X \neq 0$ on a $X^\top AX > 0$ et $X^\top BX > 0$ donc

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

Par suite $tA + (1-t)B \in \mathcal{S}_n^{++}(\mathbb{R})$. Ainsi $\boxed{\mathcal{S}_n^{++}(\mathbb{R}) \text{ est convexe}}$.

De même on a $\mathcal{S}_n^+(\mathbb{R})$ est convexe.

Q.23 Soient $A, B \in \mathcal{S}_n^{++}(\mathbb{R})$ et $t \in]0, 1[$. Par la question **Q16**, $A^{-1}B$ est autoadjoint pour $\langle \cdot, \cdot \rangle_A$, donc diagonalisable avec des valeurs propres $\lambda_1, \dots, \lambda_n$ dans $\mathbb{R}_+^*$.

• On a $tA + (1-t)B \in \mathcal{S}_n^{++}(\mathbb{R})$ et

$$\det(tA + (1-t)B) = \det(A) \cdot \det(tI_n + (1-t)A^{-1}B) = \det(A) \cdot \prod_{i=1}^n (t + (1-t)\lambda_i) \quad (1)$$

ce déterminant est strictement positif, donc :

$$\ln \det(tA + (1-t)B) = \ln \det(A) + \sum_{i=1}^n \ln(t + (1-t)\lambda_i) \quad (2)$$

On a $\ln''(x) = \frac{-1}{x^2} < 0$ sur $\mathbb{R}_+^*$, donc $\ln$ est strictement concave (du cours), par suite pour $\lambda > 0$:

$$\ln(t + (1-t)\lambda) \geq t \ln 1 + (1-t) \ln \lambda = (1-t) \ln \lambda \quad (3)$$

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

Donc :

$$\ln \det(tA + (1-t)B) \geq \ln \det(A) + \sum_{i=1}^n (1-t) \ln(\lambda_i) \quad (4)$$

et on a

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

d'où

$$\ln \det(tA + (1-t)B) \geq t \ln \det A + (1-t) \ln \det B \quad (5)$$

• Cas d'égalité :

L'égalité dans (5) entraîne l'égalité dans (4), la relation (2) donne

$$\sum_{i=1}^n \ln(t + (1-t)\lambda_i) = \sum_{i=1}^n (1-t) \ln(\lambda_i)$$

soit

$$\sum_{i=1}^n (\ln(t + (1-t)\lambda_i) - (1-t) \ln(\lambda_i)) = 0 \quad (6)$$

par stricte concavité de $\ln$ on a pour tout $i \in \llbracket 1, n \rrbracket$

$$\ln(t + (1-t)\lambda_i) - (1-t)\ln(\lambda_i) \geq 0$$

la relation (6) donne

$$\ln(t + (1-t)\lambda_i) - (1-t)\ln(\lambda_i) = 0, \forall i \in \llbracket 1, n \rrbracket$$

Du cas d'égalité pour $\ln$ on a $\lambda_i = 1$ pour tout $i \in \llbracket 1, n \rrbracket$.

Or la matrice $A^{-1}B$ est diagonalisable et $\text{Sp}(A^{-1}B) = \{1\}$ donc $A^{-1}B = I_n$, soit $A = B$.

Donc $\varphi : A \mapsto \ln(\det A)$ est une fonction strictement concave sur $\mathcal{S}_n^{++}(\mathbb{R})$.

III – Groupe orthogonal associé à une matrice symétrique définie positive

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

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

Q.24 • $O(A)$ non vide :

On a $I_n^\top A I_n = A$ donc $I_n \in O(A)$ et $O(A) \neq \emptyset$.

• $O(A)$ est une partie de $\text{GL}_n(\mathbb{R})$:

Si $M \in O(A)$, on a $\det(M^\top A M) = (\det M)^2 \det A = \det A$ donc $(\det M)^2 = 1$, car $A \in \mathcal{S}_n^{++}(\mathbb{R})$.

Par suite $O(A) \subset \text{GL}_n(\mathbb{R})$.

• $O(A)$ est stable par produit et inverse :

Soit $M, N \in O(A)$, on a

$$(MN)^\top A (MN) = N^\top M^\top A M N = N^\top A N = A$$

Donc $MN \in O(A)$.

Soit $M \in O(A)$, on a

$$A = (M^{-1})^\top \cdot M^\top A M \cdot M^{-1} = (M^{-1})^\top A M^{-1}$$

Donc $M^{-1} \in O(A)$.

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

• $O(A)$ isomorphe à $O_n(\mathbb{R})$

Puisque $A \in \mathcal{S}_n^{++}(\mathbb{R})$, il existe $P \in O_n(\mathbb{R})$ et $\lambda_1, \dots, \lambda_n$ dans $\mathbb{R}_+^*$ tels que $A = P^\top \cdot \text{Diag}(\lambda_1, \dots, \lambda_n) \cdot P$.

Soit $B = P^\top \cdot \text{Diag}(\sqrt{\lambda_1}, \dots, \sqrt{\lambda_n}) \cdot P$.

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

On a

$$M \in O(A) \iff M^\top B^2 M = B^2 \iff B M^\top B^2 M B = I_n \iff (B M B^{-1})^\top (B M B^{-1}) = I_n$$

L'application $\psi : M \mapsto B M B^{-1}$ est bien définie de $O(A)$ vers $O_n(\mathbb{R})$, elle est linéaire et bijective.

Ainsi $O(A)$ isomorphe à $O_n(\mathbb{R})$.

Q.25 On a : $O_n(\mathbb{R})$ est une partie compacte de $\mathcal{M}_n(\mathbb{R})$.

En effet : il suffit de vérifier que $O_n(\mathbb{R})$ est une partie fermée et bornée de $\mathcal{M}_n(\mathbb{R})$.

L'application $f : M \mapsto M^\top M$ est continue (elle est polynomiale) et $O_n(\mathbb{R}) = f^{-1}(\{I_n\})$ est un fermé de $\mathcal{M}_n(\mathbb{R})$.

De plus pour tout $M \in O_n(\mathbb{R})$ alors $\|M\| = \sqrt{\text{Tr}(M^\top M)} = \sqrt{n}$, donc $O_n(\mathbb{R})$ est borné .

L'application $\psi^{-1} : M \mapsto B^{-1}MB$ est, linéaire en dimensions finies, donc continue de $O_n(\mathbb{R})$ vers $O(A)$.

Ainsi $O(A) = \psi^{-1}(O_n(\mathbb{R}))$ est compact dans $\mathcal{M}_n(\mathbb{R})$.

IV – Sous-groupes compacts de $GL_n(\mathbb{R})$

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

Q.26 L'application $\det : GL_n(\mathbb{R}) \rightarrow \mathbb{R}^*$ est un morphisme de groupes continu (elle est polynomiale). Donc $\det(G)$ est un sous-groupe compact de $\mathbb{R}^*$.

Pour tout $h \in \det(G)$, la famille $(h^n)_{n \in \mathbb{Z}}$ est dans $\det(G)$, donc elle est bornée.

Si $|h| \neq 1$, alors $|h^n| \xrightarrow{n \rightarrow +\infty} +\infty$ ou $|h^{-n}| \rightarrow +\infty$: contradiction avec $\det(G)$ borné.

Donc $|h| = 1$, et $\det(G) \subset \{-1, 1\}$.

Ce qui donne $|\det M| = 1$ pour tout $M \in G$.

Q.27 On pose $\mathcal{C} = \{MX \mid (M, X) \in G \times \mathcal{B}\}$.

- $G \times \mathcal{B}$ est un fermé et borné de $\mathcal{M}_n(\mathbb{R})^2$ donc compact . L'application $\phi : \mathcal{M}_n(\mathbb{R}) \times \mathcal{M}_{n,1}(\mathbb{R}) \longrightarrow \mathcal{M}_{n,1}(\mathbb{R})$ avec $\phi(M, X) = MX$, est bilinéaire en dimensions finies, donc continue. Par suite $\mathcal{C} = \phi(G \times \mathcal{B})$ est compact de $\mathcal{M}_{n,1}(\mathbb{R})$.

- On a $I_n \in G$, c'est son élément neutre . Donc $\mathcal{B} = \{I_n X \mid X \in \mathcal{B}\} \subset \mathcal{C}$, par suite la boule ouverte unité $\overset{\circ}{\mathcal{B}} = \{X \in \mathcal{M}_{n,1}(\mathbb{R}) \mid \|X\| < 1\} \subset \mathcal{C}$.

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

Q.28 Posons $\mathcal{E} = \{A \in \mathcal{S}_n^+(\mathbb{R}) \mid \mathcal{C} \subset \mathcal{B}_A\}$.

- $\mathcal{E}$ est non vide :

Puisque $\mathcal{C}$ est borné, il existe $R > 0$ tel que $\|Y\| \leq R$ pour tout $Y \in \mathcal{C}$. En posant $A = \frac{1}{R^2}I_n$, on a pour tout $Y \in \mathcal{C}$

$$\|Y\|_A^2 = Y^\top A Y = \frac{\|Y\|^2}{R^2} \leq 1$$

donc $Y \in \mathcal{B}_A$ et $\mathcal{C} \subset \mathcal{B}_A$.

Ainsi $A = \frac{1}{R^2}I_n \in \mathcal{E}$ et $\mathcal{E} \neq \emptyset$.

- $\mathcal{E}$ est compact :

Soit $(A_k)_{k \in \mathbb{N}}$ une suite d'éléments de $\mathcal{E}$.

Montrons qu'on peut en extraire une sous suite convergente dans $\mathcal{E}$.

► On a

$$\forall Y \in \mathcal{C}, \|Y\|_{A_k} = Y^\top A_k Y \leq 1$$

En particulier pour $Y \in \mathcal{B}$ ($\subset \mathcal{C}$), $Y^\top A_k Y \leq 1$ pour tout $k \in \mathbb{N}$ (1).

Soit $k \in \mathbb{N}$, on a $A_k \in \mathcal{S}_n^+(\mathbb{R})$, donc elle est diagonalisable dans une base orthonormée $(V_1, \dots, V_n)$ de $\mathcal{M}_{n,1}(\mathbb{R})$ avec $A_k V_i = \lambda_i V_i$ et $V_i \in \mathcal{B}$ pour tout i .

La relation (1) donne pour tout i :

$$0 \leq \lambda_i = V_i^\top A_k V_i \leq 1$$

De plus on a

$$\|A_k\|^2 = \text{Tr}(A_k^\top A_k) = \text{Tr}(A_k^2) = \sum_{i=1}^n \lambda_i^2 \leq n$$

Donc la suite $(A_k)_{k \in \mathbb{N}}$ est bornée dans $\mathcal{M}_n(\mathbb{R})$. D'après le théorème de Bolzano et Weierstrass (valable en dimension finie) on peut en extraire une sous suite $(A_{\varphi(k)})_{k \in \mathbb{N}}$ convergente vers $L \in \mathcal{M}_n(\mathbb{R})$.

► Montrons que $L \in \mathcal{S}_n^+(\mathbb{R})$ et $L \in \mathcal{E}$:

L'application $M \mapsto M^\top$ est continue, donc $A_{\varphi(k)} = (A_{\varphi(k)})^\top \xrightarrow{k \rightarrow +\infty} L^\top$, par unicité de la limite $L = L^\top$ donc $L \in \mathcal{S}_n(\mathbb{R})$.

Pour $X \in \mathcal{M}_{n,1}(\mathbb{R})$ l'application $\phi_X : A \rightarrow X^\top A X$ est continue de $\mathcal{M}_n(\mathbb{R})$ vers $\mathbb{R}$.

On a pour tout $k \in \mathbb{N}$:

$$\forall X \in \mathcal{M}_{n,1}(\mathbb{R}) \quad X^\top A_k X \geq 0 \quad \text{et} \quad \forall Y \in \mathcal{C} \quad \|Y\|_{A_k} = Y^\top A_k Y \leq 1$$

Par passage à la limite on obtient :

$$\forall X \in \mathcal{M}_{n,1}(\mathbb{R}) \quad X^\top L X \geq 0 \quad \text{et} \quad \forall Y \in \mathcal{C} \quad \|Y\|_L \leq 1$$

Donc $L \in \mathcal{S}_n^+(\mathbb{R})$ et $\mathcal{C} \subset \mathcal{B}_L$, d'où $L \in \mathcal{E}$. Ainsi $\boxed{\mathcal{E} \text{ est compact}}$.

• $\mathcal{E}$ est convexe :

Soient $A, B \in \mathcal{E}$ et $t \in [0, 1]$. Pour tout $X \in \mathcal{C}$, on a $tA + (1-t)B \in \mathcal{S}_n^+(\mathbb{R})$ (qui est convexe **Q22**) et

$$X^\top (tA + (1-t)B) X = t.X^\top A X + (1-t).X^\top B X = t.\underbrace{\|X\|_A^2}_{\leq 1} + (1-t).\underbrace{\|X\|_B^2}_{\leq 1} \leq 1$$

Ainsi $tA + (1-t)B \in \mathcal{E}$, donc $\boxed{\mathcal{E} \text{ est convexe}}$.

• Existence et unicité de la matrice $A \in \mathcal{S}_n^{++}(\mathbb{R})$:

► L'application $\det$ est continue sur le compact $\mathcal{E}$, donc elle est bornée et y admet un maximum A ($\det(A) = \max_{M \in \mathcal{E}} \det(M)$).

On a vu que $\mathcal{E}$ contient une matrice de la forme kI_n avec $k > 0$, donc $\det A > 0$.

On a $A \in \mathcal{S}_n^+(\mathbb{R})$ et $\det A > 0$ donc $A \in \mathcal{S}_n^{++}(\mathbb{R})$.

► Supposons qu'il existe $B \in \mathcal{E}$ maximisant $\det$. On a donc $\det B = \det A$ et $B \in \mathcal{S}_n^{++}(\mathbb{R})$.

Par stricte concavité de la fonction $\ln \det$ sur $\mathcal{S}_n^{++}(\mathbb{R})$ (**Q23**), on a :

$$\ln \left(\det \left(\frac{1}{2}A + \frac{1}{2}B \right) \right) \geq \frac{1}{2} \ln(\det A) + \frac{1}{2} \ln(\det B) = \ln(\det A) \quad (1)$$

Donc $\det \left(\frac{1}{2}A + \frac{1}{2}B \right) \geq \det A$, la maximalité de $\det A$ donne $\det \left(\frac{1}{2}A + \frac{1}{2}B \right) = \det A$. On a donc égalité dans (1), la stricte concavité de $\ln \det$ donne $A = B$.

Ainsi $\boxed{\text{il existe } A \in \mathcal{S}_n^{++}(\mathbb{R}) \text{ unique tel que } \det(A) = \max_{M \in \mathcal{E}} \det(M)}$.

Q.29 Soit $M \in G$. Soit $\phi_M : B \mapsto MB$ isomorphisme de $\mathcal{M}_n(\mathbb{R})$.

On a $\phi_M(G) = G$ et $\phi_M(\mathcal{C}) = \mathcal{C}$. Considérons $A' = M^\top A M$ avec A la matrice définie dans **Q28**.

Pour $Y \in \mathcal{C}$

$$\|Y\|_{A'}^2 = Y^\top M^\top A M Y = \|MY\|_A^2$$

Or $MY \in \phi_M(\mathcal{C}) = \mathcal{C} \subset \mathcal{B}_A$, donc $\|MY\|_A \leq 1$, soit $\|Y\|_{A'} \leq 1$. Donc $\mathcal{C} \subset \mathcal{B}_{A'}$, ce qui donne $A' \in \mathcal{E}$.

D'après **Q26** $|\det M| = 1$ donc $\det A' = (\det M)^2 \det A = \det A$. Par unicité du maximum de $\det$ sur $\mathcal{E}$ on a $A' = A$, donc $M^\top A M = A$ d'où $M \in O(A)$.

Donc $G \subset O(A)$. Ainsi $\boxed{G \text{ est un sous groupe de } O(A)}$.

Partie C – Croissance du groupe de Heisenberg discret

I – Croissance d'un groupe

Soit G un groupe engendré par $\mathcal{S} = \{s_i\}_{i \in \llbracket 1, N \rrbracket}$.

Q.30 • Soit $g \in G$, $\ell_{\mathcal{S}}(g)$ est un minimum d'une partie non vide de $\mathbb{N}$ donc il est atteint .

Si $g = s_1^{a_1} \cdots s_k^{a_k}$ avec $\sum_{i=1}^k |a_i| = \ell_{\mathcal{S}}(g)$, alors $g^{-1} = s_k^{-a_k} \cdots s_1^{-a_1}$ donc $\ell_{\mathcal{S}}(g^{-1}) \leq \ell_{\mathcal{S}}(g)$.

Par symétrie, $\ell_{\mathcal{S}}(g) = \ell_{\mathcal{S}}((g^{-1})^{-1}) \leq \ell_{\mathcal{S}}(g^{-1})$. Donc $\boxed{\ell_{\mathcal{S}}(g^{-1}) = \ell_{\mathcal{S}}(g)}$.

• Si $g = s_{i_1}^{a_1} \cdots s_{i_p}^{a_p}$ et $h = s_{j_1}^{b_1} \cdots s_{j_q}^{b_q}$ avec $\sum_{i=1}^p |a_i| = \ell_{\mathcal{S}}(g)$ et $\sum_{i=1}^q |b_i| = \ell_{\mathcal{S}}(h)$. Alors $gh = s_{i_1}^{a_1} \cdots s_{i_p}^{a_p} s_{j_1}^{b_1} \cdots s_{j_q}^{b_q}$ par suite

$$\boxed{\ell_{\mathcal{S}}(gh) \leq \ell_{\mathcal{S}}(g) + \ell_{\mathcal{S}}(h)} .$$

Q.31 • Soit $\Sigma = \{t_i\}_{i \in \llbracket 1, N' \rrbracket}$ une autre partie finie génératrice de G .

Soit $g = s_{i_1}^{a_1} \cdots s_{i_p}^{a_p}$ avec $\sum_{i=1}^k |a_i| = \ell_{\mathcal{S}}(g)$. Chaque $s_i \in \mathcal{S}$ s'exprime en fonction des éléments de Σ :

$s_i = t_{j_1}^{b_1(i)} \cdots t_{j_q}^{b_q(i)}$ avec $\sum_{j=1}^q |b_j(i)| = \ell_{\Sigma}(s_i)$. Posons $L = \max_i \ell_{\Sigma}(s_i)$ (qui est fini). Alors

$$\ell_{\Sigma}(g) \leq \sum_i |a_i| \sum_j |b_j(i)| \leq \sum_i |a_i| \ell_{\Sigma}(s_i) \leq L \sum_i |a_i| = L \ell_{\mathcal{S}}(g).$$

Par symétrie, $\ell_{\mathcal{S}}(g) \leq L' \ell_{\Sigma}(g)$ pour $L' = \max_{\sigma \in \Sigma} \ell_{\mathcal{S}}(\sigma)$.

Pour $C = 1/L'$ et $C' = L$ on a $\boxed{C \ell_{\mathcal{S}}(g) \leq \ell_{\Sigma}(g) \leq C' \ell_{\mathcal{S}}(g)} \quad (1)$.

• On déduit de l'inégalité (1) : pour tout $p \geq 1$

$$\mathcal{V}_{\mathcal{S}} \left(\left\lfloor \frac{p}{C'} \right\rfloor \right) \subset \mathcal{V}_{\Sigma}(p) \subset \mathcal{V}_{\mathcal{S}} \left(\left\lfloor \frac{p}{C} \right\rfloor \right) \quad (2)$$

Par définition de C et C' on a $C' \geq 1$ et $C \leq 1$.

Si G est à croissance polynomiale de degré d pour $\mathcal{S}$, alors $\alpha p^d \leq |\mathcal{V}_{\mathcal{S}}(p)| \leq \beta p^d$ pour α et β dans $\mathbb{R}_+^*$.

► Si $p \geq C'$ alors $\left\lfloor \frac{p}{C'} \right\rfloor \geq 1$. On a de la relation (2)

$$\alpha \cdot \left\lfloor \frac{p}{C'} \right\rfloor^d \leq |\mathcal{V}_{\Sigma}(p)| \leq \beta \cdot \left\lfloor \frac{p}{C} \right\rfloor^d$$

Comme

$$1 \leq \left\lfloor \frac{p}{C'} \right\rfloor \leq \frac{p}{C'} \leq \left\lfloor \frac{p}{C'} \right\rfloor + 1 \leq 2 \left\lfloor \frac{p}{C'} \right\rfloor$$

alors

$$\frac{\alpha}{(2C')^d} \cdot p^d \leq |\mathcal{V}_{\Sigma}(p)| \leq \beta \cdot \left(\frac{p}{C} \right)^d$$

► Si $1 \leq p < C'$, soit $m_0 = \min_{1 \leq p < C'} \left(\frac{|\mathcal{V}_{\Sigma}(p)|}{p^d} \right)$, $m_1 = \max_{1 \leq p < C'} \left(\frac{|\mathcal{V}_{\Sigma}(p)|}{p^d} \right)$, on a

$$m_0 \cdot p^d \leq |\mathcal{V}_{\Sigma}(p)| \leq m_1 \cdot p^d$$

Posons

$$A = \min \left(\frac{\alpha}{(2C')^d}, m_0 \right) \text{ et } B = \max \left(\frac{\beta}{C^d}, m_1 \right)$$

On a donc $A, B \in \mathbb{R}_+^*$ et pour $p \geq 1$

$$A \cdot p^d \leq |\mathcal{V}_{\Sigma}(p)| \leq B \cdot p^d$$

Ainsi G est à croissance polynomiale de degré d pour Σ .

Le degré d ne dépend donc pas du choix du système générateur.

Q.32 • On a

$$\{(x, y, z) \in \mathbb{N}^3 \mid x + y + z \leq p\} = \{(x, y, z) \in \mathbb{N}^3 \mid 0 \leq x \leq p, 0 \leq y \leq p - x \text{ et } 0 \leq z \leq p - x - y\}$$

donc

$$\text{Card} \{(x, y, z) \in \mathbb{N}^3 \mid x + y + z \leq p\} = \sum_{i=0}^p \sum_{j=0}^{p-i} \sum_{l=0}^{p-i-j} 1$$

On a

$$\begin{aligned} \sum_{i=0}^p \sum_{j=0}^{p-i} \sum_{l=0}^{p-i-j} 1 &= \sum_{i=0}^p \sum_{j=0}^{p-i} (p - i - j + 1) \\ &= \sum_{i=0}^p \sum_{k=p-i-j+1}^{p-i+1} k \\ &= \frac{1}{2} \sum_{i=0}^p (p - i + 1)(p - i + 2) \\ &= \sum_{i=1}^{p+1} \frac{1}{2} k(k+1) \\ &= \frac{(p+1)(p+2)(2p+3)}{12} + \frac{(p+1)(p+2)}{4} \\ &= \frac{(p+1)(p+2)(p+3)}{6} \end{aligned}$$

Ainsi $\boxed{\text{Card} \{(x, y, z) \in \mathbb{N}^3 \mid x + y + z \leq p\} = \frac{(p+1)(p+2)(p+3)}{6}}.$

Autre méthode : Soit $a_n = \text{Card} \{(x, y, z) \in \mathbb{N}^3 \mid x + y + z = n\}$ et $N_p = \text{Card} \{(x, y, z) \in \mathbb{N}^3 \mid x + y + z \leq p\}$.

On a $N_p = \sum_{n=0}^p a_n$. Pour $t \in]-1, 1[$, par convergence absolue et sommabilité, on peut écrire :

$$\frac{1}{(1-t)^3} = \left(\sum_{n=0}^{+\infty} t^n \right)^3 = \sum_{k=0}^{+\infty} \sum_{h=0}^{+\infty} \sum_{l=0}^{+\infty} t^{k+h+l} = \sum_{n=0}^{+\infty} a_n t^n$$

Le théorème du produit de Cauchy donne

$$\sum_{p=0}^{+\infty} N_p t^p = \frac{1}{1-t} \sum_{n=0}^{+\infty} a_n t^n = \frac{1}{(1-t)^4}$$

En utilisant la formule du développement en série entière

$$\frac{1}{(1-t)^d} = \sum_{n=0}^{+\infty} \binom{n+d-1}{d-1} t^n \quad \text{pour } t \in]-1, 1[$$

on obtient

$$N_p = \binom{p+3}{3} = \frac{(p+3)(p+2)(p+1)}{6}$$

- Soit $\mathcal{S} = (e_1, e_2, e_3)$ la base canonique de $\mathbb{R}^3$ qui engendre aussi $\mathbb{Z}^3$. Alors si $g = (x, y, z) = xe_1 + ye_2 + ze_3$ on a $\ell_{\mathcal{S}}(g) = |x| + |y| + |z|$.

D'après ce qui précède, on a pour tout $p \geq 1$

$$|\mathcal{V}_{\mathcal{S}}(p)| = \text{Card} \{(x, y, z) \in \mathbb{N}^3 \mid x + y + z \leq p\} = \frac{(p+1)(p+2)(p+3)}{6}$$

Pour $p \geq 1$ on a $p + 1 \leq 2p$, $p + 2 \leq 3p$ et $p + 3 \leq 4p$ donc :

$$\frac{1}{6}p^3 \leq |\mathcal{V}_S(p)| \leq 4p^3$$

Ainsi $\boxed{\mathbb{Z}^3 \text{ est à croissance polynomiale de degré } 3}$.

II – Le groupe de Heisenberg discret

On considère $n = 3$ et les matrices :

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

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

Q.33 On a par récurrence :

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

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

Q.34 Pour $(i, j, k, i', j', k') \in \mathbb{Z}^6$, on a d'après **Q.33** :

$$S^i T^j U^k S^{i'} T^{j'} U^{k'} = \begin{pmatrix} 1 & j & k \\ 0 & 1 & i \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & j' & k' \\ 0 & 1 & i' \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & j+j' & k+k'+ji' \\ 0 & 1 & i'+i \\ 0 & 0 & 1 \end{pmatrix}$$

Donc $S^i T^j U^k S^{i'} T^{j'} U^{k'} = S^{i''} T^{j''} U^{k''}$ avec $\boxed{i'' = i + i', \quad j'' = j + j', \quad k'' = k + k' + ji'}$.

Q.35 • Pour $(i, j, k, i', j', k') = (1, 0, 1, 0, 0, 0)$ et $(i, j, k, i', j', k') = (0, 0, 1, 1, 0, 0)$ on a

$$SU = US = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

Pour $(i, j, k, i', j', k') = (0, 1, 1, 0, 0, 0)$ et $(i, j, k, i', j', k') = (0, 0, 1, 0, 1, 0)$ on a

$$TU = UT = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Comme $\mathbb{H} = \langle U, S, T \rangle$ alors U commute avec tous les éléments de $\mathbb{H}$.

• Pour $(i, j) \in \mathbb{Z}^2$, par les calculs précédents

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

Q.36 • On a

$$ST = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} = TS.$$

donc $\mathbb{H}$ n'est pas commutatif.

- D'après **Q35** $U = T^{-1}S^{-1}TS \in \langle S, T \rangle$ donc $\boxed{\langle S, T \rangle = \mathbb{H}}$.

Q.37 Soit $f : \mathbb{Z}^3 \rightarrow \mathbb{H}$ et $f(i, j, k) = S^i T^j U^k$.

- On a $\mathbb{H} = \langle S, T, U \rangle$ donc f est bien définie.

D'après **Q33**, $S^i T^j U^k = \begin{pmatrix} 1 & i & ij+k \\ 0 & 1 & j \\ 0 & 0 & 1 \end{pmatrix}$. Si $f(i, j, k) = f(i', j', k')$ alors $(i, j, k) = (i', j', k')$. Donc f est injective.

D'après **Q34**, tout élément de $\mathbb{H}$ se réduit à la forme $S^i T^j U^k$, donc f est surjective.

Ainsi f est bijective et tout élément de $\mathbb{H}$ s'écrit d'une manière unique sous la forme $S^i T^j U^k$.

- On a d'après **Q34**

$$f(i + i', j + j', k + k') = S^{i+i'} T^{j+j'} U^{k+k'} \text{ et } f(i, j, k) \cdot f(i', j', k') = S^{i+i'} T^{j+j'} U^{k+k'+ji'}$$

Ces deux termes coïncident seulement si $i'j = 0$, ce qui est faux en général ($f(1, 1, 1) \cdot f(1, 1, 1) \neq f(2, 2, 2)$).

Donc f n'est pas un isomorphisme de groupes pour la structure usuelle de $\mathbb{Z}^3$.

- A l'aide de **Q34**, on munit $\mathbb{Z}^3$ de la loi de composition interne :

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

On vérifie que :

- $\star$ est associative :

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

- $(0, 0, 0)$ est l'élément neutre de $\star$ et pour (x, y, z) on a

$$(x, y, z) \star (x', y', z') = (0, 0, 0) \Leftrightarrow (x', y', z') = (-x, -y, -z + xy)$$

donc tout élément admet un symétrique pour $\star$.

Ainsi, $(\mathbb{Z}^3, \star)$ est bien un groupe et f est un isomorphisme de $(\mathbb{Z}^3, \star)$ vers $(\mathbb{H}, \times)$.

Q.38 • Soit $M \in \mathbb{H}$ et $p \in \mathbb{N}^*$. On suppose que $\ell_{\mathcal{A}}(M) \leq p$.

Dans la question d'origine on demande de montrer que : « 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 $|z| \leq |ij|$ ».

Ce qui est faux en général:

Pour $d > 4$ on a $T^{-d} S^{-d} T^d S^d = U^{d^2}$, alors $\ell_{\mathcal{A}}(U^{d^2}) \leq 4d$. On prend $p = 4d$ et $M = U^{d^2}$, par **Q37** $(i, j, k) = (0, 0, d^2)$ et $z = 0$. Mais $|i| + |j| + |k| = d^2 > p$.

- Montrons que : « 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 $|z| \leq p^2$ ».

Par commutativité de U avec S et T , prenons $M = S^{i_1} T^{j_1} S^{i_2} T^{j_2} \dots S^{i_r} T^{j_r} U^k$ avec

$$\sum_{l=1}^r (|i_l| + |j_l|) + |k| = \ell_{\mathcal{A}}(M) \leq p.$$

Par **Q35**, on a $T^{j_1} S^{i_2} = S^{i_2} T^{j_1} U^{i_2 j_1}$ donc

$$M = S^{i_1} (S^{i_2} T^{j_1} U^{i_2 j_1}) T^{j_2} S^{i_3} \dots S^{i_r} T^{j_r} U^k = S^{i_1 + i_2} T^{j_1 + j_2} S^{i_3} T^{j_3} \dots S^{i_r} T^{j_r} U^{k + i_2 j_1}$$

Par récurrence on obtient

$$M = S^i T^j U^{k+z} \text{ avec } i = \sum_{h=1}^r i_h, j = \sum_{h=1}^r j_h \text{ et } z = \sum_{h=2}^r i_h(j_1 + \dots + j_{h-1})$$

On a donc

$$|z| \leq \sum_{h=2}^r |i_h| (|j_1| + \dots + |j_{h-1}|) \leq \sum_{h=1}^r |i_h| \sum_{h=1}^r |j_h| \leq p^2$$

Ainsi $\boxed{M = S^i T^j U^{k+z} \text{ avec } |i| + |j| + |k| \leq p \text{ et } |z| \leq p^2}$.

• On a donc

$$\mathcal{V}_{\mathcal{A}}(p) = \{M \in \mathbb{H} \mid \ell_{\mathcal{A}}(M) \leq p\} \subset \{M = S^i T^j U^{k+z} \mid |i| + |j| + |k| \leq p \text{ et } |z| \leq p^2\}.$$

Puisque le triplet $(i, j, k+z)$ est unique pour chaque M alors

$$\mathcal{V}_{\mathcal{A}}(p) \subset \{M = S^i T^j U^m \mid |i| + |j| \leq p \text{ et } |m| \leq p + p^2\}.$$

Par suite

$$|\mathcal{V}_{\mathcal{A}}(p)| \leq |\llbracket -p, p \rrbracket^2 \times \llbracket -p - p^2, p + p^2 \rrbracket| \leq 8p^2(p + p^2)$$

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

Q.39 Montrons que:

«Il existe $C > 0$ tel que pour tout $(i, j, k) \in \mathbb{Z}^3$, si $|i| + |j| \leq p$ et $|k| \leq |ij|$, alors $\ell_{\mathcal{A}}(S^i T^j U^k) \leq Cp$ ».

• Pour $|d| \geq 1$ on a $T^{-d} S^{-d} T^d S^d = U^{d^2}$, donc $\boxed{\ell_{\mathcal{A}}(U^{d^2}) \leq 4d}$.

Soit $m \geq 1$, posons $d = \lfloor \sqrt{m} \rfloor$, donc $d^2 \leq m < (d+1)^2$ et $m = d^2 + h$ avec $h \in \llbracket 0, 2d \rrbracket$.

De la relation

$$U^m = U^{d^2} U^h = T^{-d} S^{-d} T^d S^d U^h$$

on déduit $\ell_{\mathcal{A}}(U^m) \leq 4d + h \leq 6d$, soit $\boxed{\ell_{\mathcal{A}}(U^m) \leq 6 \lfloor \sqrt{m} \rfloor}$.

Comme $\ell_{\mathcal{A}}(U^{-m}) = \ell_{\mathcal{A}}(U^m)$ alors pour tout $m \in \mathbb{Z}$ $\boxed{\ell_{\mathcal{A}}(U^m) \leq 6 \lfloor \sqrt{|m|} \rfloor}$.

• Soit $(i, j, k) \in \mathbb{Z}^3$, si $|i| + |j| \leq p$ et $|k| \leq |ij|$. On a donc

$$|k| \leq |ij| \leq \frac{(|i| + |j|)^2}{4} \leq \frac{p^2}{4}$$

par suite

$$\ell_{\mathcal{A}}(S^i T^j U^k) \leq \ell_{\mathcal{A}}(S^i) + \ell_{\mathcal{A}}(T^j) + \ell_{\mathcal{A}}(U^k) \leq |i| + |j| + 6 \lfloor \sqrt{|k|} \rfloor \leq 4p$$

Ainsi $\boxed{\forall (i, j, k) \in \mathbb{Z}^3, \text{ si } |i| + |j| \leq p \text{ et } |k| \leq |ij|, \text{ alors } \ell_{\mathcal{A}}(S^i T^j U^k) \leq 4p}$.

Q.40 • On a

$$\text{Card} \{(i, j, k) \in \mathbb{N}^3 \mid i + j \leq p \text{ et } k \leq ij\} = \sum_{\substack{i, j \geq 0 \\ i+j \leq p}} \sum_{0 \leq k \leq ij} 1 = \sum_{i=0}^p \sum_{j=0}^{p-i} (ij + 1) \geq \sum_{i=0}^p \sum_{j=0}^{p-i} ij$$

simplifions cette somme

$$\sum_{i=0}^p \sum_{j=0}^{p-i} ij = \sum_{i=0}^p i \frac{(p-i)(p-i+1)}{2} \geq \sum_{i=0}^p i \frac{(p-i)^2}{2}$$

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

- Dans cette expression on a la somme de Riemann :

$$\frac{1}{p} \sum_{i=0}^p \frac{i}{p} \left(1 - \frac{i}{p}\right)^2 \xrightarrow{p \rightarrow +\infty} \int_0^1 x(1-x)^2 dx$$

Puisque $\int_0^1 x(1-x)^2 dx = \frac{1}{12}$ alors $\boxed{\frac{p^3}{2} \sum_{i=0}^p \frac{i}{p} \left(1 - \frac{i}{p}\right)^2 \underset{p \rightarrow +\infty}{\sim} \frac{p^4}{24}}$.

Q.41 • D'après **Q38**, il existe une constante $C_1 > 0$ telle que $|\mathcal{V}_{\mathcal{A}}(p)| \leq C_1 p^4$.

- D'après **Q39** on a

$$\left\{ S^i T^j U^k \mid (i, j, k) \in \mathbb{Z}^3 \mid |i| + |j| \leq \frac{p}{4} \text{ et } |k| \leq |ij| \right\} \subset \mathcal{V}_{\mathcal{A}}(p)$$

donc

$$\text{Card} \left\{ (i, j, k) \in \mathbb{Z}^3 \mid |i| + |j| \leq \frac{p}{4} \text{ et } |k| \leq |ij| \right\} \leq |\mathcal{V}_{\mathcal{A}}(p)|$$

par suite

$$|\mathcal{V}_{\mathcal{A}}(p)| \geq \text{Card} \left\{ (i, j, k) \in \mathbb{N}^3 \mid i + j \leq p \text{ et } k \leq ij \right\}$$

D'après **Q40**

$$|\mathcal{V}_{\mathcal{A}}(p)| \geq \frac{p^4}{24 \cdot 4^4} (1 + o(1))$$

Il existe donc $C_2 > 0$ tel que $|\mathcal{V}_{\mathcal{A}}(p)| \geq C_2 p^4$.

Finalement, il existe $C_1, C_2 > 0$ tels que $C_2 p^4 \leq |\mathcal{V}_{\mathcal{A}}(p)| \leq C_1 p^4$ pour tout $p \geq 1$.

Ainsi $\mathbb{H}$ est un groupe à croissance polynomiale de degré 4.