Correction de la composition de *Mathématiques générales* Agrégation 1998

Partie I. Il n'existe pas de partition du plan en cercles de diamètre non nul.

Question 1. Notons Ω_i le centre du cercle C_i. Puisque $(C_j)_{j\in I}$ est une partition de $\mathcal{E}$, il existe un unique élément de I, que nous notons $f(i)$, tel que $\Omega_i \in C_{f(i)}$. Cela définit une application $f : I \to I$. Nous allons montrer le résultat suivant :

$$(*) \qquad D_{f(i)} \subset D_i \quad \text{et} \quad r_{f(i)} \leqslant \frac{1}{2} r_i.$$

> *Preuve* - Tout d'abord, le fait que $D_{f(i)} \subset D_i$ découle de ce que C_i et $C_{f(i)}$ ne s'intersectent pas et que $C_{f(i)}$ contient un point de D_i. Montrons maintenant l'inégalité. Soit x le point de $C_{f(i)}$ diamétralement opposé à Ω_i. Alors la distance d de Ω_i à x vérifie $d = 2r_{f(i)}$. Mais $x \in D_{f(i)} \subset D_i$, donc $d \leqslant r_i$. D'où le résultat. $\square$

Fixons maintenant $i_0 \in I$ et notons $(i_n)_{n\in\mathbb{N}}$ la suite définie par récurrence par $i_{n+1} = f(i_n)$. Alors on a, d'après $(*)$,

$$D_{i_{n+1}} \subset D_{i_n} \quad \text{et} \quad r_{i_{n+1}} \leqslant \frac{1}{2} r_{i_n}$$

pour tout n.

Question 2. Notons que la suite numérique $(r_{i_n})_{n\in\mathbb{N}}$ tend vers 0 (un raisonnement par récurrence immédiat montre que $r_{i_n} \leqslant \dfrac{r_{i_0}}{2^n}$ pour tout n). Par conséquent, la suite $(D_{i_n})_{n\in\mathbb{N}}$ est une suite de fermés emboités de $\mathcal{E}$ de diamètre tendant vers 0. Puisque $\mathcal{E}$ est complet, l'intersection $\displaystyle\bigcap_{n\in\mathbb{N}} D_{i_n}$ est non vide et réduite à un point.

Question 3. Soit p l'unique élément de $\displaystyle\bigcap_{n\in\mathbb{N}} D_{i_n}$ (voir la question **I.2**). Notons i l'unique élément de I tel que $p \in C_i$. Puisque $r_i > 0$, il existe $n \in \mathbb{N}$ tel que $r_{i_n} < r_i$. Puisque $p \in C_i$ et $p \in D_{i_n}$ et puisque C_i et C_{i_n} ne s'intersectent pas, on a $D_i \subset D_{i_n}$, ce qui contredit le fait que $r_i > r_{i_n}$.

Conclusion : il n'existe pas de partition du plan $\mathcal{E}$ par des cercles de rayon strictement positif.

Partie II. Il existe une partition de l'espace en cercles de diamètre non nul.

Question 1. Notons $\mathcal{P}$ le plan de $\mathcal{E}$ contenant C. Soient Δ_p et Δ_q les droites tangentes à C en p et q et soit x leur point d'intersection (si Δ_p et Δ_q sont parallèles, la solution sera dessinée mais la preuve ne sera pas détaillée car elle fonctionne en gros sur les mêmes principes).

Notons I l'ensemble des droites passant par x. Alors $(\Delta - \{x\})_{\Delta \in I}$ est une partition de $\mathcal{P} - \{x\}$. Notons I_0 l'ensemble des droites passant par x et rencontrant D. Puisque $x \notin D$, $((\Delta - \{x\}) \cap D)_{\Delta \in I_0}$ est une partition de D. Or, si $\Delta \in I_0$, on a $\Delta \cap D = (\Delta - \{x\}) \cap D$. Donc $(\Delta \cap D)_{\Delta \in I_0}$ est une partition de D.

Posons maintenant $I_1 = I_0 - \{\Delta_p, \Delta_q\}$. Puique $\Delta_p \cap D = \{p\}$ et $\Delta_q \cap D = \{q\}$ (rappelons que Δ_p et Δ_q sont tangentes à C), la famille $(\Delta \cap D)_{\Delta \in I_1}$ est une partition de $D - \{p, q\}$. Or il n'y a que deux droites tangentes à C issues de x (ce sont Δ_p et Δ_q). Donc, si $\Delta \in I_1$, $\Delta \cap C$ contient deux points distincts, et donc $\Delta \cap D$ est un segment de droite de longueur non nulle.

Question 2. Notons $\mathcal{P}_p$ et $\mathcal{P}_q$ les plans tangents à S en p et q respectivement. Notons Δ l'intersection de $\mathcal{P}_p$ et $\mathcal{P}_q$ (encore une fois, le cas où $\mathcal{P}_p$ et $\mathcal{P}_q$ sont parallèles admet une solution légèrement différente mais dont la preuve est similaire).

Notons I l'ensemble des plans de $\mathcal{E}$ contenant Δ. Notons I_0 l'ensemble des $\mathcal{P} \in I$ rencontrant S. Soit $I_1 = I - \{\mathcal{P}_p, \mathcal{P}_q\}$. Alors, par les mêmes arguments qu'à la question **II.1**, $(\mathcal{P} \cap S)_{\mathcal{P} \in I_1}$ est une partition de S et, si $\mathcal{P} \in I_1$, alors $\mathcal{P} \cap S$ est un disque de diamètre strictement positif. D'où le résultat.

Question 3. Notons $\mathcal{P}$ un plan contenant Δ. Choisissons un vecteur directeur $\vec{v}$ de Δ de norme 1 et notons O_m le point de Δ tel que $O_m - O = (4m+1)\vec{v}$ (pour $m \in \mathbb{Z}$). Notons C_m le cercle de centre O_m et de rayon 1 contenu dans $\mathcal{P}$. Notons que $C_m \cap C_n = \varnothing$ si $m \neq n$.

Soit maintenant S une sphère de centre O. Notons C le cercle $S \cap \mathcal{P}$. Puisque $C_m \subset \mathcal{P}$ pour tout m, il suffit de montrer que le cardinal de $C \cap \bigcup_{m \in \mathbb{Z}} C_m$ est égal à 2 (donc de travailler dans le plan $\mathcal{P}$).

Notons r le rayon de C. Si $r = 4n$, avec $n \in \mathbb{N}^*$, alors C rencontre les cercles C_{n+1} et C_{-n} en un point chacun et ne rencontrent pas les autres cercles. Si $r = 4n+2$ avec $n \in \mathbb{N}$, alors C rencontre les cercles C_n et C_{-n-1} en un point chacun et ne rencotrent pas les autres cercles. Maintenant, si $r \notin 2\mathbb{N}^*$, notons n la partie entière de $r/2$. Si n est impair, alors C rencontre $C_{-(n+1)/2}$ en deux points et ne rencotrent pas les autres cercles. Si n est pair, alors C rencontre $C_{n/2}$ en deux points et ne rencotrent pas les autres cercles.

Question 4. La famille $(S(O,r))_{r>0}$ est une partition de $\mathcal{E} - \{O\}$. Notons $(C_m)_{m \in \mathbb{Z}}$ la famille de cercles construite à la question **II.3** et posons $X = \bigcup_{m \in \mathbb{C}} C_m$. Si $r > 0$, notons $S(O,r) \cap X = \{p_r, q_r\}$ (voir question **II.3**). Puisque $O \in C_0 \subset X$, $(S(O,r) - \{p_r, q_r\})_{r>0}$ est une partition de $\mathcal{E} - X$. Puisque $(C_m)_{m \in \mathbb{Z}}$ est une partition de X et puisque, pour tout $r > 0$, $S(O,r) - \{p_r, q_r\}$ est une réunion disjointe de cercles (voir question **II.2**), on en déduit que $\mathcal{E}$ est une réunion disjointe de cercles.

Partie III. Action de $\mathbf{GL}_n(\mathbb{R})$ sur les réseaux.

Question 1. Soit $M \in \mathbf{GL}_n(\mathbb{R})$. Notons M_i la i-ième colonne de M. La famille $(M_1, \ldots, M_n)$ forme une base de l'espace vectoriel $\mathbb{R}^n$ (identifié à l'espace des vecteurs colonnes de taille $n \times 1$). Le théorème d'orthonormalisation nous dit qu'il existe une base orthonormée $(K_1, \ldots, K_n)$ de $\mathbb{R}^n$ telle que K_i appartienne à l'espace engendré par $(M_1, \ldots, M_i)$ pour tout i et telle que ${}^tK_iM_i \in \mathbb{R}_+^*$. Notons K la matrice dont les colones sont $(K_1, \ldots, K_n)$ et A la matrice de passage de la base $(K_1, \ldots, K_n)$ à la base $(M_1, \ldots, M_n)$, de sorte que $M = KA$. lors A est triangulaire supérieure et, si on note $(d_1, \ldots, d_n)$ les coefficients diagonaux de A, alors $d_i = {}^tK_iM_i > 0$ (en effet, $M_i = dK_i \in \langle K_1, \ldots, K_{i-1}\rangle$ et ${}^tK_iK_j = 0$ si $i \neq j$). Notons $D = \operatorname{diag}(d_1, \ldots, d_n)$ et $T = D^{-1}A$. Alors T est unipotente et triangulaire supérieure, D est diagonale à coefficients strictement positifs, K est orthogonale et

$$M = KDT.$$

Pour montrer l'unicité de la décomposition précédente, on pourrait utiliser l'unicité déjà présente dans le théorème d'orthonormalisation. Nous allons ici en donner une preuve plus directe. Soient donc K et K' deux matrices orthogonales, D et D' deux matrices diagonales à coefficients positifs, T et T' deux matrices unipotentes triangulaires supérieures et supposons que

$$KDT = K'D'T'.$$

Alors $K'^{-1}K = D'T'T^{-1}D^{-1}$. Notons $S = K'^{-1}K$. L'égalité précédente montre d'une part que S est orthogonale (donc que $S^{-1} = {}^tS$) et d'autre part que S est triangulaire supérieure à coefficients positifs. Donc S est la matrice identité. Cela montre que $K = K'$ et que $DT = D'T'$.

La comparaison des coefficients diagonaux dans cette dernière égalité montre que $D = D'$, et finalement que $T = D^{-1}DT = D'^{-1}D'T' = T'$, ce qui termine la preuve de l'unicité dans la décomposition d'Iwasawa.

Question 2. Si $M \in \mathbf{GL}_n(\mathbb{Z})$, alors M^{-1} est une matrice à coefficients entiers et donc $\det(M)$ et $\det(M^{-1}) = (\det M)^{-1}$ sont des entiers. Cela force $\det(M)$ à être égal à ± 1, comme attendu.

Réciproquement, soit M une matrice à coefficients entiers de déterminant ± 1. Notons N la transposée de la comatrice de M. Puisque M est à coefficients entiers, N est à coefficients entiers. D'autre part, $M^{-1} = (\det M)^{-1}N = \pm N$ donc M^{-1} est à coefficients entiers, c'est-à-dire $M \in \mathbf{GL}_n(\mathbb{Z})$.

Question 3. Il existe une structure de groupe sur $\mathcal{X}_n$ telle que π_n soit un morphisme de groupes si et seulement si $\mathbf{GL}_n(\mathbb{Z})$ est distingué dans $\mathbf{GL}_n(\mathbb{R})$. Nous allons montrer que c'est le cas si et seulement si $n = 1$.

Tout d'abord, $\mathbf{GL}_1(\mathbb{R}) \simeq \mathbb{R}^*$ est abélien, donc tous ses sous-groupes sont distingués.

Supposons maintenant que $n = 2$. On a

$$M = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \in \mathbf{GL}_2(\mathbb{Z}) \quad \text{et} \quad N = \begin{pmatrix} 1 & 1/3 \\ 0 & 1 \end{pmatrix} \in \mathbf{GL}_2(\mathbb{R}),$$

alors que

$$NMN^{-1} = \begin{pmatrix} 1 & -2/3 \\ 0 & 1 \end{pmatrix} \notin \mathbf{GL}_2(\mathbb{Z}).$$

Donc $\mathbf{GL}_2(\mathbb{Z})$ n'est pas distingué dans $\mathbf{GL}_2(\mathbb{R})$.

Supposons maintenant $n > 2$. Soit M' (respectivement N') la matrice diagonale par blocs dont le premier bloc est la matrice identité de taille $n-2$ et le deuxième bloc est la matrice M (respectivement N) ci-dessus. Alors $M' \in \mathbf{GL}_n(\mathbb{Z})$, $N' \in \mathbf{GL}_2(\mathbb{R})$ et le calcul précédent montre que $N'M'N'^{-1} \notin \mathbf{GL}_n(\mathbb{Z})$.

Question 4. Commençons par introduire quelques notations et r'esultats préliminaires. Si $\mathcal{C} = (f_1, \ldots, f_n)$ est une base de $\mathbb{R}^n$, notons $\Gamma_{\mathcal{C}}$ le réseau de base $\mathcal{C}$, c'est-à-dire

$$\Gamma_{\mathcal{C}} = \{a_1 f_1 + \cdots + a_n f_n \mid a_1, \ldots, a_n \in \mathbb{Z}\}.$$

Nous noterons $\mathcal{B}_{\mathrm{can}}$ la base canonique de $\mathbb{R}^n$. On a alors

$$\Gamma_{\mathcal{B}_{\mathrm{can}}} = \mathbb{Z}^n.$$

Le résultat suivant est immédiat :

> LEMME A - *Si $M \in \mathbf{GL}_n(\mathbb{R})$ et si $\mathcal{C}$ est une base de $\mathbb{R}^n$, alors*
>
> $$M(\Gamma_{\mathcal{C}}) = \Gamma_{M(\mathcal{C})}.$$

Cela montre que l'application

$$\begin{array}{rccc} \tau_n : & \mathbf{GL}_n(\mathbb{R}) & \longrightarrow & \mathcal{R}_n \\ & M & \longmapsto & M(\mathbb{Z}^n) \end{array}$$

est bien définie car $M(\mathbb{Z}^n) = \Gamma_{M(\mathcal{B}_{\mathrm{can}})}$ est bien un réseau. Comme autre conséquence du lemme A, on obtient :

> COROLLAIRE B - *Soit $M \in \mathbf{GL}_n(\mathbb{R})$. Alors $M \in \mathbf{GL}_n(\mathbb{Z})$ si et seulement si $M(\mathbb{Z}^n) = \mathbb{Z}^n$.*
>
> *Preuve* - Rappelons que $\mathcal{B}_{\mathrm{can}}$ est la base canonique de $\mathbb{R}^n$. D'après le lemme A, $M(\mathbb{Z}^n) \subset \mathbb{Z}^n$ si et seulement si $M(\mathcal{B}_{\mathrm{can}})$ est formée de vecteurs à coordonnées dans $\mathbb{Z}$, c'est-à-dire si et seulement si M est à coefficients dans $\mathbb{Z}$. Le résultat découle de cette observation et du fait que $M(\mathbb{Z}^n) = \mathbb{Z}^n$ si et seulement si $M(\mathbb{Z}^n) \subset \mathbb{Z}^n$ et $M^{-1}(\mathbb{Z}^n) \subset \mathbb{Z}^n$. ■

Si $M \in \mathbf{GL}_n(\mathbb{R})$ et $A \in \mathbf{GL}_n(\mathbb{Z})$, alors $A(\mathbb{Z}^n) = \mathbb{Z}^n$ (voir corollaire B) donc $M(\mathbb{Z}^n) = MA(\mathbb{Z}^n)$. Cela montre que l'application τ_n se factorise à travers π_n en une application $\psi_n : \mathcal{X}_n \to \mathcal{R}_n$ rendant le diagramme

$$\begin{tikzcd} \mathbf{GL}_n(\mathbb{R}) \arrow[r, "\tau_n"] \arrow[d, "\pi_n"'] & \mathcal{R}_n \\ \mathcal{X}_n \arrow[ur, "\psi_n"'] & \end{tikzcd}$$

commutatif. Nous allons montrer que ψ_n est bijective.

Puisque $\mathbf{GL}_n(\mathbb{R})$ agit transitivement sur les bases de $\mathbb{R}^n$, on déduit du lemme A que τ_n est surjective. En particulier, ψ_n est surjective. Le corollaire B montre l'injectivité de ψ_n. Donc $\psi_n : \mathcal{X}_n \to \mathcal{R}_n$ est bijective.

Question 5. Soit Γ un réseau de $\mathbb{R}^n$ et soit $M \in \mathbf{GL}_n(\mathbb{R})$ telle que $\Gamma = M(\mathbb{Z}^n)$. Posons $\nu(\Gamma) = |\det(M)|$. Nous allons montrer que $\nu : \mathcal{R}_n \to \mathbb{R}_+^*$ est bien définie (c'est-à-dire ne dépend pas du choix de M telle que $\Gamma = M(\mathbb{Z}^n)$). Soit donc $M' \in \mathbf{GL}_n(\mathbb{R})$ telle que $\Gamma = M'(\mathbb{Z}^n)$. D'après la question **III.4**, $M' = MA$ pour une matrice $A \in \mathbf{GL}_n(\mathbb{Z})$. Mais alors $|\det(M')| = |\det(M)| \cdot |\det(A)|$. Comme $\det(A) = \pm 1$ d'après la question **III.2**, on en déduit que $|\det(M)| = |\det(M')|$.

Si $(v_1, \ldots, v_n)$ est une $\mathbb{Z}$-base du réseau Γ, alors $\nu(\Gamma)$ est le volume d'une maille fondamentale de Γ, par exemple le volume de

$$\{t_1 v_1 + \cdots + t_n v_n \mid (t_1, \ldots, t_n) \in [0,1]^n\}.$$

Question 6. Avant de montrer le résultat, nous allons rappeler une démonstration du lemme suivant :

> Lemme C - *Soit Γ un réseau de $\mathbb{R}^n$. Alors Γ est fermé et discret.*
>
> *Preuve* - Soit $M \in \mathbf{GL}_n(\mathbb{R}^n)$ telle que $\Gamma = M(\mathbb{Z}^n)$ (il en existe d'après la question **III.4**). L'application $M : \mathbb{R}^n \to \mathbb{R}^n$ est linéaire donc continue et son inverse étant aussi linéaire, M est un homéomorphisme. Puisque $\Gamma = M(\mathbb{Z}^n)$, il suffit de montrer que $\mathbb{Z}^n$ est fermé et discret dans $\mathbb{R}^n$, ce qui est facile. ■

Soit $c \in \mathbb{R}^n$ et $r > 0$. Notons $\overline{B}(c,r) = \{p \in \mathbb{R}^n \mid ||p - c|| \leqslant r\}$. Pour montrer que $\Gamma \cap B(c,r)$ est fini, il suffit de montrer que $\Gamma \cap \overline{B}(c,r)$ est fini. Mais, d'après le lemme C, ce dernier ensemble est discret (car contenu dans Γ) et compact (car fermé et contenu dans un compact). Donc il est fini.

Question 7. Soit $M_0 \in \mathcal{M}$. On a $\mathcal{M} = M_0.\mathbf{GL}_n(\mathbb{Z})$. Posons $r_0 = ||M_0(e)||$. Posons $E = \{M(e) \mid M \in \mathcal{M}\}$ et notons Γ_0 le réseau $M_0(\mathbb{Z}^n)$. Pour montrer que φ atteint son minimum sur $\mathcal{M}$, il suffit de montrer que $E \cap B(0, r_0)$ est fini (en effet, $\varphi(\mathcal{M}) = \{||x|| \mid x \in E\}$). Mais,

$$E = \{M_0 A(e) \mid A \in \mathbf{GL}_n(\mathbb{Z})\} \subset M_0(\mathbb{Z}^n) = \Gamma_0$$

car $A(e) \in \mathbb{Z}^n$ pour tout $A \in \mathbf{GL}_n(\mathbb{Z})$. Par conséquent, $E \cap B(0, r_0) \subset \Gamma_0 \cap B(0, r_0)$, donc $E \cap B(0, r_0)$ est fini d'après la question **III.6**. D'où le résultat.

Question 8. On a

$$\varphi(M) = ||M(e)|| = ||KDT(e)||.$$

Mais $T(e) = e$ et, K étant orthogonale, on a $||KDT(e)|| = ||DT(e)||$. Donc $||M(e)|| = ||D(e)|| = d_1(M)$ car $D(e) = d_1(M)e$. En d'autres termes,

$$\varphi(M) = d_1(M).$$

Question 9. Notons t le coefficient de la première ligne et de la deuxième colonne de DT et posons pour simplifier $d_i = d_i(M)$. Puisque M est minimale on a, pour tout $r \in \mathbb{Z}$, $||MU_r(e)||^2 \geqslant d_1^2$, où U_r est la matrice appartenant à $\mathbf{GL}_n(\mathbb{Z})$ égale à

$$U_r = \begin{pmatrix} r & 1 & 0 & \cdots & 0 \\ 1 & 0 & 0 & & 0 \\ 0 & 0 & 1 & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \dots & \dots & 0 & 1 \end{pmatrix}$$

Alors $||MU_r(e)||^2 = (t + rd_1)^2 + d_2^2$. Donc, pour tout $r \in \mathbb{Z}$, on a

$$(t + rd_1)^2 + d_2^2 \geqslant d_1^2.$$

Or, il existe $r \in \mathbb{Z}$ tel que $|t + rd_1| \leqslant d_1/2$. Par suite,

$$\frac{d_1^2}{4} + d_2^2 \geqslant d_1^2.$$

D'où $d_1 \leqslant \dfrac{2}{\sqrt{3}} d_2$.

Question 10. (a) Écrivons

$$DT = \begin{pmatrix} d_1 & a_2 & \cdots & a_n \\ 0 & & & \\ \vdots & & B' & \\ 0 & & & \end{pmatrix}.$$

Puisque l'on suppose que $\pi_{n-1}(\mathcal{T}_{n-1}) = \mathcal{X}_{n-1}$, il existe une matrice $C' \in \mathcal{T}_{n-1}$ telle que $C'(\mathbb{Z}^{n-1}) = B'(\mathbb{Z}^{n-1})$. Donc, d'après la question **III.4**, si on pose $A' = B'^{-1}C'$, on a $A' \in \mathbf{GL}_{n-1}(\mathbb{Z})$ et $B'A' = C' \in \mathcal{T}_{n-1}$. Posons maintenant

$$A = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & A' & \\ 0 & & & \end{pmatrix}.$$

Alors DTA est de la forme annoncée.

(b) Soit (K', D', T') la décomposition d'Iwasawa de M'. Posons

$$K_0 = K \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & K' & \\ 0 & & & \end{pmatrix}, \quad D_0 = \begin{pmatrix} d_1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & D' & \\ 0 & & & \end{pmatrix}$$

et

$$T_0 = \begin{pmatrix} 1 & b_2/d_1 & \dots & b_n/d_1 \\ 0 & & & \\ \vdots & & T' & \\ 0 & & & \end{pmatrix}.$$

Alors K_0 est orthogonale, D_0 est diagonale à coefficients positifs, T_0 est unipotente triangulaire supérieure et un calcul immédiat montre que $MA = KDTA = K_0 D_0 T_0$, ce qui montre que (K_0, D_0, T_0) est la décomposition d'Iwasawa de MA.

Question 11. Montrons par récurrence sur n que $\pi_n(\mathcal{T}_n) = \mathcal{X}_n$. L'égalité $\pi_1(\mathcal{T}_1) = \mathcal{X}_1$ est immédiate (car $\mathcal{T}_1 = \mathbf{GL}_1(\mathbb{R})$).

Supposons maintenant $n \geqslant 2$ et supposons que $\pi_{n-1}(\mathcal{T}_{n-1}) = \mathcal{X}_{n-1}$. Nous voulons montrer que $\pi_n(\mathcal{T}_n) = \mathcal{X}_n$. Soit donc $M \in \mathbf{GL}_n(\mathbb{R})$. Il nous faut montrer qu'il existe une matrice $A \in \mathbf{GL}_n(\mathbb{Z})$ telle que $MA \in \mathcal{T}_n$. Pour cela, on peut supposer M minimale. Soit (K, D, T) la décomposition d'Iwasawa de M. D'après la question **III.11 (a)** (et grâce à l'hypothèse de récurrence), il existe $A \in \mathbf{GL}_n(\mathbb{Z})$ de la forme

$$A = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & A' & \\ 0 & & & \end{pmatrix}$$

telle que DTA soit de la forme décrite à la question **III.11 (a)**. Puisque $M(e) = MA(e)$ (et donc $\varphi(M) = \varphi(MA)$), la matrice MA est aussi minimale. D'après la question **III.11 (b)**, si on note (K_0, D_0, T_0) la décomposition d'Iwasawa de MA, alors $d_1(MA) \leqslant 2d_2(MA)/\sqrt{3}$ car MA est minimale (voir question **III.9**). De plus, si $i \geqslant 2$, alors $d_i(MA) \leqslant 2d_{i+1}(MA)/\sqrt{3}$ (voir question **III.10 (b)**). Donc $MA \in \mathcal{T}_n$, ce qui termine la démonstration par récurrence.

Question 12. *Il y a une erreur dans l'énoncé. Il faut lire : "On définit les applications* $m : \mathcal{R}_n \to \mathbb{R}$ *et* $\gamma : \mathcal{R}_n \to \mathbb{R}$ *en posant,..."*

Puisque Γ est discret (voir Lemme C de la question **III.6**), il existe $r > 0$ tel que $B(0, r) \cap \Gamma = \{0\}$. Cela montre que $m(\Gamma) \geqslant r > 0$.

D'autre part, d'après la question **III.11**, il existe $M \in \mathcal{T}_n$ telle que $M(\mathbb{Z}^n) = \Gamma$. Par suite,

$$m(\Gamma)^2 \leqslant ||M(e)||^2 \leqslant d_1(M)^2. \tag{1}$$

D'autre part, si on note (K, D, T) la décomposition d'Iwasawa de M, alors

$$\nu(\Gamma) = |\det(M)| = |\det(K)| \cdot |\det(D)| \cdot |\det(T)| = |\det(D)| = d_1(M) \cdots d_n(M).$$

Donc, par définition de $\mathcal{T}_n$, on obtient

$$\nu(\Gamma)^{2/n} \geqslant d_1(M) \cdot \Big(\frac{\sqrt{3}}{2} d_1(M)\Big) \cdots \Big(\Big(\frac{\sqrt{3}}{2}\Big)^{n-1} d_1(M)\Big).$$

En d'autres termes,

$$\nu(\Gamma)^{2/n} \geqslant \Big(\Big(\frac{\sqrt{3}}{2}\Big)^{n(n-1)/2} d_1(M)^n\Big)^{2/n} = \Big(\frac{\sqrt{3}}{2}\Big)^{n-1} d_1(M)^2. \tag{2}$$

Le résultat découle des inégalités (1) et (2).

Remarque - Si $\lambda \in \mathbb{R}^\times$ et si Γ est un réseau de $\mathbb{R}^n$, alors $\lambda\Gamma$ est aussi un réseau de $\mathbb{R}^n$ et on a

$$\nu(\lambda\Gamma) = |\lambda|^n \nu(\Gamma) \quad \text{et} \quad m(\lambda\Gamma) = |\lambda| m(\Gamma).$$

En particulier, $\gamma(\lambda\Gamma) = \gamma(\Gamma)$. $\square$

Question 13. On a
$$m(\mathbb{Z}^n) = 1 \quad \text{et} \quad \nu(\Gamma) = 1, \quad \text{donc} \quad \gamma(\Gamma) = 1.$$

Soit maintenant $\gamma = \mathbb{Z}(1,0) \oplus \mathbb{Z}(1/2, \sqrt{3}/2)$. Alors
$$m(\Gamma) = 1 \quad \text{et} \quad \nu(\Gamma) = \det \begin{pmatrix} 1 & 1/2 \\ 0 & \sqrt{3}/2 \end{pmatrix} = \frac{\sqrt{3}}{2}, \quad \text{donc} \quad \gamma(\Gamma) = \frac{2}{\sqrt{3}}.$$
Le fait que $m(\Gamma) = 1$ découle des deux faits suivants : tout d'abord, $||(1,0)|| = 1$ et, si $(a,b) \in \mathbb{Z}^2$, alors $||a(1,0) + b(1/2, \sqrt{3}/2)||^2 = a^2 + ab + b^2 \geqslant 1$ dès que $(a,b) \neq (0,0)$ car ce sont des entiers.

Question 14. Nous allons commencer par montrer par récurrence le lemme suivant :

Lemme D - *Soit T une matrice unipotente triangulaire supérieure. Alors il existe une matrice T_0 unipotente triangulaire supérieure à coefficients dans $\mathbb{Z}$ telle que les coefficients non diagonaux de TT_0 soient de valeur absolue $\leqslant 1/2$.*

Preuve - Nous allons montrer ce résultat par récurrence sur n en suivant le même principe que lors de la question **III.10 (b)**. Notons (P_n) la propriété énoncé dans le lemme D. Alors (P_1) est évidente.

Supposons donc $n \geqslant 2$ et (P_{n-1}) vraie. Soit $T \in \mathbf{GL}_n(\mathbb{R})$ unipotente et triangulaire supérieure. Écrivons
$$T = \begin{pmatrix} 1 & a_2 & \dots & a_n \\ 0 & & & \\ \vdots & & T' & \\ 0 & & & \end{pmatrix},$$
où $T' \in \mathbf{GL}_{n-1}(\mathbb{R})$ est une matrice unipotente et triangulaire supérieure et les a_i sont des réels. Par hypothèse de récurrence, il existe une matrice $T_0' \in \mathbf{GL}_{n-1}(\mathbb{Z})$ unipotente et triangulaire supérieure telle que les coefficients non diagonaux de $T'T_0'$ soient de valeur absolue $\leqslant 1/2$.

Posons
$$T_1 = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & T_0' & \\ 0 & & & \end{pmatrix}.$$
Alors
$$TT_1 = \begin{pmatrix} 1 & b_2 & \dots & b_n \\ 0 & & & \\ \vdots & & T'T_0' & \\ 0 & & & \end{pmatrix},$$
où les b_i sont des réels. Il existe des entiers relatifs $r_2, \dots, r_n$ tels que $|b_i - r_i| \leqslant 1/2$ pour tout i. Posons maintenant
$$T_0 = T_1 \begin{pmatrix} 1 & -r_2 & \dots & -r_n \\ 0 & & & \\ \vdots & & I_{n-1} & \\ 0 & & & \end{pmatrix},$$

où I_{n-1} est la matrice identité de taille $n-1$. Alors $T_0 \in \mathbf{GL}_n(\mathbb{Z})$ est unipotente et triangulaire supérieure. De plus

$$TT_0 = \begin{pmatrix} 1 & b_2 - r_2 & \dots & b_n - r_n \\ 0 & & & \\ \vdots & & T'T_0' & \\ 0 & & & \end{pmatrix},$$

donc les coefficients non diagonaux de $T'T_0'$ soient de valeur absolue $\leqslant 1/2$.

Cela montre (P_n) et conclut la preuve par récurrence du lemme D. ■

Soit $\mathcal{M} \in \mathcal{X}_n$ et soit $M \in \mathcal{M} \cap \mathcal{T}_n$ (il en existe d'après la question **III.11**). Soit (K, D, T) la décomposition d'Iwasawa de M et soit T_0 une matrice unipotente triangulaire supérieure à coefficients dans $\mathbb{Z}$ telle que les coefficients non diagonaux de TT_0 soient de valeur absolue $\leqslant 1/2$ (il en existe d'après le lemme D). Alors $MT_0 \in \mathcal{M}$ car $T_0 \in \mathbf{GL}_n(\mathbb{Z})$ et (K, D, TT_0) est la décomposition d'Iwasawa de MT_0. Par suite, $\mathcal{M} = \pi_n(MT_0)$, donc $\pi_n(\mathcal{S}_n) = \mathcal{X}_n$.

Partie IV. Topologie de $\mathcal{R}_n$

*En toute rigueur, il FAUDRAIT montrer que la topologie de $\mathcal{R}_n$ définie dans l'énoncé est BIEN une topologie. C'est ce que nous allons faire en préambule à cette partie. D'autre part, pour éviter l'ambiguïté du début de l'énoncé de cette partie, nous noterons $\tau_n : \mathbf{GL}_n(\mathbb{R}) \to \mathcal{R}_n$ l'application définie dans la question **III.4** et nous utiliserons cette application plutôt que π_n dans l'énoncé. Par exemple, on munit $\mathcal{R}_n$ de la topologie dont les ouverts sont les $\tau_n(U)$, pour U un ouvert de $\mathbf{GL}_n(\mathbb{R})$.*

Pour cela, montrons tout d'abord le lemme suivant :

Lemme E - *Soit $U \in \mathcal{R}_n$. Alors U est ouvert dans $\mathcal{R}_n$ si et seulement si $\tau_n^{-1}(U)$ est ouvert dans $\mathbf{GL}_n(\mathbb{R})$.*

Preuve - Puisque τ_n est surjective, on a $U = \tau_n(\tau_n^{-1}(U))$. Donc, si $\tau_n^{-1}(U)$ est un ouvert de $\mathbf{GL}_n(\mathbb{R})$, alors U est un ouvert de $\mathcal{R}_n$ par définition.

Réciproquement, si U est un ouvert de $\mathcal{R}_n$, alors il existe un ouvert V de $\mathbf{GL}_n(\mathbb{R})$ tel que $\tau_n(V) = U$. Or, d'après la question **III.4**, on a

$$\tau_n^{-1}(U) = \bigcup_{g \in \mathbf{GL}_n(\mathbb{R})} Vg.$$

Mais l'application $\mathbf{GL}_n(\mathbb{R}) \to \mathbf{GL}_n(\mathbb{R})$, $x \mapsto xg$ est un homéomorphisme, donc Vg est un ouvert de $\mathbf{GL}_n(\mathbb{R})$ pour tout $g \in \mathbf{GL}_n(\mathbb{Z})$. Par suite, $\tau_n^{-1}(U)$ est une réunion d'ouvert, donc c'est un ouvert. ■

Corollaire F - *L'ensemble $\{\tau_n(U) \mid U \text{ ouvert de } \mathbf{GL}_n(\mathbb{R})\}$ définit bien une topologie sur $\mathcal{R}_n$.*

Preuve - D'apr'es le lemme E, il suffit de rappeler que, si $(E_i)_{i \in I}$ est une famille de parties de $\mathcal{R}_n$, alors

$$\tau_n^{-1}\Big(\bigcup_{i \in I} E_i\Big) = \bigcup_{i \in I} \tau_n^{-1}(E_i)$$

et

$$\tau_n^{-1}\Big(\bigcap_{i\in I} E_i\Big) = \bigcap_{i\in I} \tau_n^{-1}(E_i),$$

et de revenir à la définition d'une topologie. ■

Question 1. Le fait que τ_n est continue découle immédiatement du lemme E.

Montrons maintenant que $\mathcal{R}_n$ est séparé. Puisque $\mathrm{Mat}_n(\mathbb{Z})$ est un réseau de $\mathrm{Mat}_n(\mathbb{R})$, c'est un fermé de $\mathrm{Mat}_n(\mathbb{R})$. D'autre part, l'application $\det : \mathrm{Mat}_n(\mathbb{R}) \to \mathbb{R}$ étant continue, l'image inverse $\det^{-1}(\{1,-1\})$ est un fermé de $\mathrm{Mat}_n(\mathbb{R})$. Donc, puisque $\mathbf{GL}_n(\mathbb{Z}) = \mathrm{Mat}_n(\mathbb{Z}) \cap \det^{-1}(\{1,-1\})$ d'après la question **III.2**, on en déduit que :

LEMME G - $\mathbf{GL}_n(\mathbb{Z})$ *est fermé dans* $\mathrm{Mat}_n(\mathbb{R})$*, donc dans* $\mathbf{GL}_n(\mathbb{R})$.

Fixons maintenant Γ et Γ' deux réseaux différents de $\mathbb{R}^n$. Soient M et M' deux éléments de $\mathbf{GL}_n(\mathbb{R})$ tels que $\Gamma = M(\mathbb{Z}^n) = \tau_n(M)$ et $\Gamma' = M'(\mathbb{Z}^n) = \tau_n(M')$. D'après la question **III.4**, on a $M^{-1}M' \notin \mathbf{GL}_n(\mathbb{Z})$. Notons

$$\begin{array}{rccc} \mu : & \mathbf{GL}_n(\mathbb{R}) \times \mathbf{GL}_n(\mathbb{R}) & \longrightarrow & \mathbf{GL}_n(\mathbb{R}) \\ & (A,B) & \longmapsto & A^{-1}B. \end{array}$$

Alors μ est continue (les coordonnées de $A^{-1}B$ sont des fractions rationnelles en les coefficients de A et B). Par suite, $U = \mu^{-1}\big(\mathbf{GL}_n(\mathbb{R}) - \mathbf{GL}_n(\mathbb{Z})\big)$ est un ouvert de $\mathbf{GL}_n(\mathbb{R}) \times \mathbf{GL}_n(\mathbb{R})$ car $\mathbf{GL}_n(\mathbb{R}) - \mathbf{GL}_n(\mathbb{Z})$ est un ouvert de $\mathbf{GL}_n(\mathbb{R})$ d'après le lemme G. Or, $(M, M') \in U$. Par définition de la topologie produit, il existe des ouverts V et V' de $\mathbf{GL}_n(\mathbb{R})$ contenant M et M' respectivement et tels que $V \times V' \subset U$. En d'autres termes, on a $A^{-1}B \notin \mathbf{GL}_n(\mathbb{Z})$ pour tous $A \in V$ et $B \in V'$, ce qui siginife exactement que $\tau_n(V) \cap \tau_n(V') = \varnothing$. Par définition, $\tau_n(V)$ et $\tau_n(V')$ sont des voisinages ouverts de Γ et Γ' respectivement, ce qui montre que $\mathcal{R}_n$ est séparé.

Question 2. Soit U un ouvert de $\mathbb{R}_+^*$. Pour montrer que ν est continue, il faut montrer que $\nu^{-1}(U)$ est un ouvert de $\mathcal{R}_n$. D'après le lemme E, cela revient à montrer que $\tau_n^{-1}(\nu^{-1}(U))$ est un ouvert de $\mathbf{GL}_n(\mathbb{R})$. Or, $\nu \circ \tau_n = |\det|$. Donc $\tau_n^{-1}(\nu^{-1}(U)) = |\det|^{-1}(U)$ est bien ouvert car $|\det| : \mathbf{GL}_n(\mathbb{R}) \to \mathbb{R}_+^*$ est continue.

Question 3. L'application $||.|| : \mathbf{GL}_n(\mathbb{R}) \to \mathbb{R}_+^*$, $M \mapsto ||M||$ est continue par définition. Donc, puisque U est compacte, l'image de U par $||.||$ est un compact de $\mathbb{R}_+^*$. En particulier, il existe $c > 0$ tel que $||M|| \geqslant c$ pour tout $M \in U$. Cela implique l'inégalité demandée.

Question 4. Notons

$$\begin{array}{rccc} m_n : & \mathbf{GL}_n(\mathbb{R}) & \longrightarrow & \mathbb{R}_+^* \\ & M & \longmapsto & \inf\limits_{\substack{a\in\mathbb{Z}_n \\ a\neq 0}} ||M(a)||. \end{array}$$

On a alors $m_n = m \circ \tau_n$. Pour montrer que m est continue il suffit, par le même argument qu'à la question **IV.2** (utilisant le lemme E), de montrer que m_n est continue. Pour cela, il suffit de montrer que la restriction de m_n à toute partie compacte de $\mathbf{GL}_n(\mathbb{R})$ est continue. Soit donc U une partie compacte de $\mathbf{GL}_n(\mathbb{R})$. Notons c une constante strictement positive vérifiant la conclusion de la question **IV.3**. Soit $d = \max\limits_{M\in U} ||M(e)||$ (d est bien défini car U

est compact et l'application $U \to \mathbb{R}_+^*$, $M \mapsto ||M(e)||$ est continue). On a alors, pour tout $M \in U$,

$$m_n(M) = \inf_{a \in \mathbb{Z}^n \cap \overline{B}(0,d/c)} ||M(a)||.$$

Posons $E = \mathbb{Z}^n \cap \overline{B}(0, d/c)$. C'est un ensemble fini d'après la question **III.6**. Comme chaque fonction $U \to \mathbb{R}_+^*$, $M \mapsto ||M(a)||$ est continue (pour $a \in E$), la fonction m_n est continue comme minimum d'un nombre fini de fonctions continues.

On vient de montrer que m est continue. On a montré dans la question **IV.2** que ν est continue. Donc γ est continue comme composée de produits et de quotients de fonctions continues.

Question 5. Supposons pour commencer $\mathcal{Y}$ compacte. L'application $d_1 : \mathbf{GL}_n(\mathbb{R}) \to \mathbb{R}_+^*$, $M \mapsto ||M(e)|| = d_1(M)$ est continue (l'égalité $||M(e)|| = d_1(M)$ a été démontrée dans la question **III.8**). Donc $d_1(\mathcal{Y})$ est un compact de $\mathbb{R}_+^*$ donc il existe α et β' deux constantes positives telles que $d_1(\mathcal{Y}) \subset [\alpha, \beta']$.

D'autre part, notons $f = (0, \ldots, 0, 1)$. Alors

$$(\#) \qquad ||M(f)|| = ||DT(f)|| \geqslant d_n(M)$$

car $d_n(M)$ est le dernier coefficient de $DT(f)$. Puisque $\mathcal{Y}$ est compacte et puisque l'application $\mathbf{GL}_n(\mathbb{R}) \to \mathbb{R}_+^*$, $M \mapsto ||M(f)||$ est continue, il existe une constante $\beta > 0$ tel que $||M(f)|| \leqslant \beta$ pour tout $M \in \mathcal{Y}$. En particulier, d'après (#), on a $d_n(M) \leqslant \beta$ pour tout $M \in \mathcal{Y}$.

Réciproquement, soit $\mathcal{Y}$ une partie fermée de $\mathcal{S}_n$ telle que $d_1(M) \geqslant \alpha$ et $d_n(M) \leqslant \beta$ pour tout $M \in \mathcal{Y}$. Compte tenu des inégalités entre les $d_i(M)$ lorsque $M \in \mathcal{S}_n$, il existe a et b dans $\mathbb{R}_+^*$ tels que $d_i(M) \in [a, b]$ pour tout i et pour tout $M \in \mathcal{Y}$. Notons E l'ensemble des triplets (K, D, T) où K est une matrice orthogonale, D est une matrice diagonale à coefficients dans $[a, b]$ et T est une matrice triangulaire dont les coefficients non diagonaux sont de valeur absolue $\leqslant 1/2$. Alors E est compact (car le groupe orthogonal est compact) et $\mathcal{Y}$ est contenue dans l'image de l'application continue $E \to \mathbf{GL}_n(\mathbb{R})$, $(K, D, T) \mapsto KDT$. Cette image est donc compacte et, $\mathcal{Y}$ étant fermée, $\mathcal{Y}$ est compacte.

Question 6. Soit $\mathcal{P}$ une partie compacte de $\mathcal{R}_n$. L'application ν étant continue, $\nu(\mathcal{P})$ est une partie majorée de $\mathbb{R}$: cela montre (i). D'autre part, l'application m étant continue, il existe $r > 0$ tel que $m(\Gamma) \geqslant r$ pour tout $\Gamma \in \mathcal{P}$. En particulier, $\Gamma \cap B(0, r) = \{0\}$ pour tout $\Gamma \in \mathcal{P}$: cela montre (ii).

Réciproquement, soit $\mathcal{P}$ une partie fermée de $\mathcal{R}_n$ vérifiant les propriétés (i) et (ii). On note $\mathcal{Y}$ l'image inverse de $\mathcal{P}$ par l'application continue $\tau_n' : \mathcal{S}_n \to \mathcal{R}_n$. Puisque τ_n' est surjective d'après la question **III.14**, on a $\tau_n'(\mathcal{Y}) = \mathcal{P}$. Il suffit donc de montrer que $\mathcal{Y}$ est compacte.

Puisque $\mathcal{P}$ est fermée et τ_n' est continue, $\mathcal{Y}$ est fermée. Soit maintenant r et s dans $\mathbb{R}_+^*$ tels que $\nu(\mathcal{P}) \subset [0, s]$ et $\Gamma \cap B(0, r) = \{0\}$ pour tout $\Gamma \in \mathcal{P}$. On a donc, pour tout $M \in \mathcal{Y}$, $|\det(M)| \leqslant s$ et $||M(e)|| = d_1(M) \geqslant r$. On a donc $d_1(M) \ldots d_n(M) \leqslant s$ et donc

$$s \geqslant \left(\frac{\sqrt{3}}{2}\right)^{(n-1)(n-2)/2} d_1(M)^{n-1} d_n(M) \geqslant \left(\frac{\sqrt{3}}{2}\right)^{(n-1)(n-2)/2} r^{n-1} d_n(M)$$

pour tout $M \in \mathcal{Y}$. En particulier, $d_n(\mathcal{Y})$ est une partie majorée de $\mathbb{R}_+^*$. D'après la question **IV.5**, $\mathcal{Y}$ est compacte. D'où le résultat.

Question 7. Soit $\Gamma \in \mathcal{R}_n$ et soit $l = \nu(\Gamma)$. Alors $\Gamma' = \dfrac{1}{\sqrt[n]{l}}\Gamma \in \mathcal{R}'_n$ et $\gamma(\Gamma) = \gamma'(\Gamma')$, ce qui montre le résultat.

Question 8. On a $\gamma' : \mathcal{R}'_n \to \mathbb{R}_+^*$, $\Gamma \mapsto m(\Gamma)^2$. Soit K un compact de $]0, +\infty[$. Alors $\mathcal{P}' = \gamma'^{-1}(K)$ est un fermé de $\mathcal{R}'_n$ car γ' est continue. Il suffit donc, d'après la question **IV.6**, de montrer que $\mathcal{P}'$ satisfait aux assertions (i) et (ii) de cette question. Soient a et b dans $\mathbb{R}_+^*$ tels que $K \subset [a, b]$. Soit donc $\Gamma \in \mathcal{P}'$. Puisque $m(\Gamma)^2 \geqslant a$, on a $\Gamma \cap B(0, \sqrt{a}) = \{0\}$, ce qui montre (ii). D'autre part, puisque $\nu(\Gamma) = 1$, (i) est trivialement vérifié. D'où le résultat.

Question 9. L'application $\gamma' : \mathcal{R}'_n \to \mathbb{R}$ est majorée (voir la question **III.12**). D'après la question **IV.7**, il suffit de voir qu'elle atteint sa borne supérieure (que nous notons r). Fixons $\Gamma_0 \in \mathcal{R}'_n$ et posons $r_0 = \gamma'(\Gamma_0)$ et $\mathcal{P}' = \gamma'^{-1}([r_0, r])$. D'après la question **IV.8**, $\mathcal{P}'$ est une partie compacte de $\mathcal{R}'_n$. D'autre part, la borne supérieure de γ' sur $\mathcal{R}'_n$ est égale à la borne supérieure de γ' sur $\mathcal{P}'$ par construction. Puisque $\mathcal{P}'$ est compact et non vide, et puisque γ' est continue, cette borne supérieure est atteinte.

Partie V. Étude de l'ensemble des points d'un réseau de norme minimale

Question 1. La forme bilinéaire symétrique

$$\begin{array}{ccc} \mathbb{R}^n \times \mathbb{R}^n & \longrightarrow & \mathbb{R} \\ (x, y) & \longmapsto & \dfrac{\langle x, y\rangle}{m(\Gamma)^2} \end{array}$$

appartient à B_Γ.

Question 2. Posons

$$c(\Gamma) = \inf_{a \in \Gamma - S(\Gamma)} \frac{||a||}{m(\Gamma)}.$$

Soit $a_0 \in \Gamma - S(\Gamma)$ et $r_0 = ||a_0||$. Alors $\Gamma \cap \overline{B}(0, r_0)$ est fini (voir question **III.6**). Par conséquent, $E = (\Gamma - S(\Gamma)) \cap \overline{B}(0, r_0)$ est lui aussi fini. Il est aussi non vide (car $a_0 \in E$). Donc

$$c(\Gamma) = \inf_{a \in E} \frac{||a||}{m(\Gamma)} > 1.$$

Soit maintenant $y \in \Gamma - S(\Gamma)$. Alors

$$||M^{-1}|| \cdot ||M(y)|| \geqslant ||M^{-1}(M(y))|| = ||y|| \geqslant c(\Gamma) m(\Gamma),$$

ce qui est le résultat demandé.

Question 3. Soit U un voisinage de la matrice identité dans $\mathbf{GL}_n(\mathbb{R})$ tel que

$$||M^{-1}|| < \sqrt{c(\Gamma)} \quad \text{et} \quad ||M|| < \sqrt{c(\Gamma)}$$

pour tout $M \in U$. Soit $M \in U$ et soit $a \in S(M(\Gamma))$. Il existe alors $b \in \Gamma$ tel que $a = M(b)$. Nous voulons montrer que $b \in S(\Gamma)$. Pour cela, remarquons tout d'abord que, si $b' \in S(\Gamma)$, alors

$$||M(b')|| \leqslant ||M|| \cdot ||b'|| < \sqrt{c(\Gamma)} m(\Gamma).$$

Donc
$$m(M(\Gamma)) < \sqrt{c(\Gamma)}m(\Gamma).$$
Supposons maintenant $b \notin S(\Gamma)$. Alors, d'après la question **V.2**, on a
$$||M(b)|| \geqslant \sqrt{c(\Gamma)}m(\Gamma),$$
donc $a = M(b) \notin S(M(\Gamma))$.

Question 4. D'après la question **V.3**, il existe $\varepsilon > 0$ tel que, si $|\alpha| < \varepsilon$, alors
$$S(M_\alpha(\Gamma)) \subset M_\alpha(S(\Gamma)) \quad \text{et} \quad M_\alpha^2 = I_n + \alpha M.$$
Donc
$$m(M_\alpha(\Gamma)) = ||M_\alpha(a)||,$$
où a est un élément de $S(\Gamma)$. Soit donc α tel que $|\alpha| < \varepsilon$. On a alors
$$\begin{aligned} ||M_\alpha(\Gamma)||^2 &= \langle M_\alpha(a), M_\alpha(a)\rangle \\ &= \langle M_\alpha^2(a), a\rangle \\ &= \langle a, a\rangle + \alpha\langle M(a), a\rangle \\ &= m(\Gamma)^2 + \alpha(B(a,a) - B'(a,a)) \\ &= m(\Gamma)^2, \end{aligned}$$
la deuxième égalité découlant du fait que M_α est symétrique.

Question 5. La matrice M étant symétrique, elle est diagonalisable : notons $\lambda_1, \ldots, \lambda_n$ ses valeurs propres (avec multiplicité) : elles sont réelles. Posons
$$t = \sum_{i=}^{n} \lambda_i = \mathrm{Tr}(M) \quad \text{et} \quad u = \sum_{i=1}^{n} \lambda_i^2 = \mathrm{Tr}(M^2).$$
On a alors
$$t^2 - u = \sum_{1 \leqslant i<j \leqslant n} \lambda_i \lambda_j.$$
Par conséquent,
$$\det(M_\alpha) = \prod_{i=1}^{n}(1 + \alpha\lambda_i) = 1 + t\alpha + (t^2 - u)\alpha^2 + o(\alpha^3).$$

Si on suppose de plus que $\gamma(\Gamma)$ est maximum on a alors, lorsque $|\alpha|$ est assez petit, $\gamma(M_\alpha(\Gamma)) \leqslant \gamma(\Gamma)$ et $m(M_\alpha(\Gamma)) = m(\Gamma)$ d'après la question **V.4**. On peut aussi supposer que $\det(M_\alpha) > 0$. Par conséquent, lorsque $|\alpha|$ est assez petit, on a $\det(M_\alpha) \geqslant 1$ ce qui implique, d'après le développement limité ci-dessus, que $t = 0$ et $t^2 - u \geqslant 0$. Donc $u \leqslant 0$, ce qui implique que $\lambda_1 = \cdots = \lambda_n = 0$. Donc $M = 0$, c'est-à-dire $B = B'$. Donc B_Γ a un seul élément.

Question 6. (a) Pour $a \in S(\Gamma)$, écrivons $a = \sum_{b \in \mathcal{B}} \lambda_b b$ et notons (E_a) l'équation linéaire dont les inconnues sont les $(X_{b,b'})_{b,b' \in \mathcal{B}}$ définie par
$$\sum_{b,b' \in \mathcal{B}} \lambda_b \lambda_{b'} X_{b,b'} = 1.$$
Il est alors clair que $B \in B_\Gamma$ si et seulement si la famille $(B(b,b'))_{b,b' \in \mathcal{B}}$ est solution du système d'équations linéaires $(E_a)_{a \in S(\Gamma)}$. C'est donc un système de $|S(\Gamma)|$ équations

linéaires mais, comme les équations (E_a) et (E_{-a}) sont équivalentes $(a \in S(\Gamma))$ ce système est équivalent à un système linéaire de $|S(\Gamma)|/2$ équations linéaires.

(b) La forme bilinéaire B étant déterminée par la donnée des $B(b, b')$, b, $b' \in \mathcal{B}$, et la condition de symétrie étant déduite des équations $B(b, b') = B(b', b)$ pour $b \neq b' \in \mathcal{B}$, on en déduit que $B \in B_\Gamma$ si et seulement si la famille $(B(b, b'))_{b,b' \in \mathcal{B}}$ satisfait un système de $\big(n(n-1) + |S(\Gamma)|\big)/2$ équations linéaires. Puisque ce système à n^2 inconnues admet une seule solution, cela implique que $\big(n(n-1) + |S(\Gamma)|\big)/2 \geqslant n^2$, c'est-à-dire que

$$|S(\Gamma)| \geqslant n(n+1).$$

(c) Notons M la matrice de $\mathbf{GL}_n(\mathbb{R})$ telle que $\mathcal{B} = M(\mathcal{B}_{\mathrm{can}})$. On a alors

$$(\langle b, b' \rangle)_{b,b' \in \mathcal{B}} = {}^t M M$$

donc
$$\det(\langle b, b' \rangle)_{b,b' \in \mathcal{B}} = \det(M)^2 = \nu(\Gamma)^2.$$

(d) Les coefficients λ_b définis dans le **(a)** sont entiers donc l'unique solution du système d'équations linéaires est à coefficients rationnels. Or, d'après la question **V.1**, cette unique solution est $\big(\langle b, b' \rangle / m(\Gamma)^2\big)_{b,b' \in \mathcal{B}}$. On déduit donc de **(c)** que $\nu(\Gamma)^2 / m(\Gamma)^{2n}$ est rationnel, c'est-à-dire que $\gamma(\Gamma)^n$ est rationnel.