Réseaux cocompacts dans $\mathrm{SL}_d(\mathbb{R})$

Yohann Mouillet, Yuan Wang, Philémon Varnet
sous la supervision de Gaëtan Chenevier

Avril 2025

1 Introduction

Dans un espace euclidien E, on appelle réseau un sous-groupe $R \subset E$ contenant une $\mathbb{Z}$-base qui est aussi une $\mathbb{R}$-base de E. De manière équivalente, c'est un sous-groupe discret tel que $\mathrm{Vect}_{\mathbb{R}}(R) = E$. Ou encore, un sous-groupe discret et libre de rang $\dim E$. Enfin, c'est aussi un sous-groupe discret tel que E/R soit compact (homéomorphe à $\mathbb{T}^d \simeq (\mathbb{S}^1)^d$, où $d = \dim E$).

Parmi ces jolies (et utiles !) caractérisations, l'une se généralise :

Définition 1. Soit G un groupe localement compact. Un réseau cocompact dans G est un sous-groupe Λ discret tel que G/Λ est compact.

L'étude des réseaux cocompacts dans les groupes de Lie, ou plus généralement dans les groupes localement compacts, constitue encore aujourd'hui un domaine de recherche actif. Il s'agit d'une théorie assez riche. Par exemple, l'existence d'un réseau cocompact dans un groupe localement compact G implique nécessairement que G est unimodulaire, c'est-à-dire que ses mesures de Haar à gauche et à droite coïncident. Il y a également de nombreux résultats connus sous le nom de théorèmes de rigidité, dus à Calabi, Weil, Mostow, Margulis..., qui disent, *grosso modo*, que la structure d'un groupe de Lie est en grande partie déterminée par ses réseaux. Les réseaux cocompacts jouent un rôle important dans d'autres domaines des mathématiques. Dans la théorie géométrique des groupes, les réseaux cocompacts fournissent de beaux exemples de groupes discrets ; en géométrie différentielle, le quotient d'un groupe de Lie par un réseau cocompact est précisément ce que l'on appelle un espace homogène compact (de même dimension que le groupe de Lie) ; ils sont aussi cruciaux dans l'étude des systèmes dynamiques homogènes.

Dans ce mémoire, on cherche des réseaux cocompacts dans $\mathrm{SL}_d(\mathbb{R})$. La question est intéressante car on pourrait penser à $\mathrm{SL}_d(\mathbb{Z})$, qui est bien discret, mais qui se trouve être non cocompact, bien qu'il soit de "covolume fini" (c'est la définition d'un réseau non nécessairement cocompact, mais on ne va pas utiliser cette notion). Il va donc falloir chercher d'autres groupes discrets. Le cas $d = 2$ est particulièrement d'intérêt, car $\mathrm{SL}_2(\mathbb{R})$ (plus correctement, $\mathrm{PSL}_2(\mathbb{R})$) correspond au groupe des isométries du demi-plan hyperbolique de Poincaré $\mathcal{H}$. Donc la classification de ses réseaux cocompacts (sans torsion, pour que le quotient soit lisse) est en effet celle des surfaces hyperboliques compactes (i.e. les surfaces de Riemann compactes) qui possèdent $\mathcal{H}$ comme revêtement universel (i.e. qui ont genre >1). On verra qu'une réponse à cette question est donnée par des algèbres de quaternions sur $\mathbb{Q}$, ce qui est peut-être surprenant : on a une réponse arithmétique à une question qui, à première vue, ne semble vraiment pas liée à la théorie des nombres ! Pour d général, on n'a plus cette connexion avec la géométrie hyperbolique, mais la construction de réseaux cocompacts est similaire : il faut utiliser des méthodes arithmétiques, en cherchant certaines algèbres non commutatives sur $\mathbb{Q}$ de dimension d^2.

Expliquons brièvement la démonstration. Dans la section 2, on montre des préliminaires matriciels et topologiques utiles pour la suite, notamment le critère de Mahler qui peut tester la compacité d'un

sous-ensemble fermé de l'espace des réseaux d'un espace euclidien. La preuve du critère de Mahler est basée sur la décomposition KAN du groupe général linéaire sur $\mathbb{R}$ et les ensembles de Siegel. Cette partie s'appuie sur Borel [2, Chapitre 1] et Benoist [1, Section 2.2-2.3].

Dans la section 3, on construit des sous-groupe discrets de $\mathrm{SL}_d(\mathbb{R})$ en supposant l'existence de certaines constructions arithmétiques et algébriques. On montre que ces sous-groupes sont des réseaux cocompacts en injectant les quotients dans un certain espace des réseaux, ce qui nous permet d'utiliser le critère de Mahler. Pour faire cela, il faut montrer que cette injection réalise un homéomorphisme sur son image. Des outils importants incluent les puissances extérieures et les représentations. Cette partie s'appuie sur Benoist [1, Section 2.5-2.7].

Dans la section 4, on montre comme annoncé l'existence des constructions utilisées dans la section précédente. L'idée est de construire une $\mathbb{Q}$-algèbre D appelée l'algèbre cyclique associée à une extension cyclique L de $\mathbb{Q}$ et un nombre premier p. Un bon choix de L et p nous permet de montrer que cette algèbre satisfait des propriétés souhaitées (à division et telle que $D \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathrm{M}_d(\mathbb{R})$). Les ingrédients cruciaux sont le théorème de Dirichlet de la progression arithmétique et une étude soigneuse de l'arithmétique des extensions cyclotomiques de $\mathbb{Q}$. Cette partie s'appuie sur Benoist [1, Section 2.7] et Molin et Rairat [3, Section 4.2].

2 Préliminaires matriciels et topologiques

2.1 Topologie quotient

On commence par une proposition sur les quotients topologiques des groupes.

Proposition 1. *Soient $\Gamma \subset G \subset \mathrm{GL}_d(\mathbb{R})$ des sous-groupes avec Γ discret dans G. Alors la topologie sur G/Γ est à base dénombrable et $g_n\Gamma \xrightarrow[n\to+\infty]{} g\Gamma$ si et seulement s'il existe une suite $(\gamma_n)_{n\in\mathbb{N}} \in \Gamma^{\mathbb{N}}$ telle que $g_n\gamma_n \xrightarrow[n\to+\infty]{} g$.*

Démonstration. G est à base dénombrable car sa topologie est induite de celle de $M_d(\mathbb{R})$. Ensuite, l'image d'une base dénombrable d'ouverts de G par la projection canonique π (qui est ouverte) est une base dénombrable de G/Γ.

Passons à la caractérisation de la convergence. Pour l'implication réciproque c'est clair car étant donné une telle suite γ_n et un voisinage ouvert V de $g\Gamma$, à partir d'un certain rang $g_n\gamma_n \in \pi^{-1}(V)$, soit donc $\pi(g_n) \in V$.

Pour la réciproque, choisissons un voisinage W de 1 dans G tel que $\Gamma \cap W = \{1\}$ (Γ est discret), puis par continuité de $(x, y) \mapsto x^{-1}y$ en g, un voisinage U de g tel que $U^{-1}U \subset W$. A partir d'un certain rang $g_n\Gamma \in \pi(U)$ donc il existe $\gamma_n \in \Gamma$ avec $g_n\gamma_n \in U$. Pour un voisinage quelconque V de g maintenant, le même raisonnement donne à partir d'un certain rang un γ'_n tel que $g_n\gamma'_n \in V \cap U$. Mais par définition de U, $\gamma_n^{-1}\gamma'_n \in \Gamma \cap W$ et $\gamma_n = \gamma'_n$. La suite γ_n convient donc. □

Remarque. Notons qu'ici l'hypothèse discret n'est pas nécessaire mais simplifie la preuve (évite un procédé d'extraction diagonale), et c'est dans ce cadre seulement que nous en aurons besoin Cela permet d'utiliser les caractérisations séquentielles des notions topologiques.

2.2 Décomposition KAN et ensembles de Siegel

Notation. Dans toute la suite, étant donné $d \geq 1$, on notera $K := O_d(\mathbb{R})$ le groupe orthogonal en dimension d,

$$A := \left\{ \begin{pmatrix} a_1 & & \\ & \ddots & \\ & & a_n \end{pmatrix} \;\middle|\; a_1, \ldots, a_n > 0 \right\}$$

et

$$N := \left\{ \begin{pmatrix} 1 & & * \\ & \ddots & \\ & & 1 \end{pmatrix} \right\}$$

La décomposition suivante, appelée décomposition KAN ou décomposition d'Iwasawa de $\mathrm{GL}_d(\mathbb{R})$, s'avérera très utile dans la suite. Étant classique, on ne la reprouve pas.

Proposition 2. *Avec les notations précédentes, l'application produit*

$$\begin{array}{ccc} K \times A \times N & \longrightarrow & \mathrm{GL}_d(\mathbb{R}) \\ (k, a, n) & \longmapsto & kan \end{array}$$

est un homéomorphisme. Sa restriction à $K^1 \times A^1 \times N$, où $K^1 := K \cap \mathrm{SL}_d(\mathbb{R})$ et $A^1 := A \cap \mathrm{SL}_d(\mathbb{R})$, induit un homéomorphisme sur $\mathrm{SL}_d(\mathbb{R})$.

Définition 2.

— Si $s, u > 0$, on note

$$A_s := \{a \in A \mid a_i \leq s a_{i+1},\ \forall i\}$$

ainsi que

$$N_u := \{u \in N \mid |a_{ij}| \leq u,\ \forall i < j\}\,.$$

— On appelle *ensemble de Siegel* de $\mathrm{GL}_n(\mathbb{R})$ tout ensemble de la forme

$$\mathfrak{S}_{s,u} = K \cdot A_s \cdot N_u$$

où $s, u > 0$.

On définit récursivement la notion de famille admissible, qui nous sera utile dans le cadre de la proposition suivante.

Définition 3. Soit Λ un réseau de $\mathbb{R}^d$. On appelle *admissible* une famille $(f_1, \ldots, f_d) \in \Lambda^d$ telle que :

1. f_1 est de norme minimale dans $\Lambda \setminus \{0\}$;
2. l'image $(\bar{f}_2, \ldots, \bar{f}_d)$ de $(f_2, \ldots, f_d)$ par la projection canonique $\Lambda \xrightarrow{\pi} \Lambda/\mathbb{Z}f_1$ est une famille admissible de $\Lambda/\mathbb{Z}f_1$ vu comme réseau de $\mathbb{R}^d/\mathbb{R}f_1 \simeq \mathbb{R}^{d-1}$;
3. pour tout $i \geq 2$, f_i est de norme minimale parmi les vecteurs de $\bar{f}_i = f_i + \mathbb{Z}f_1$.

Interprétons cette définition dans le cas de la dimension $d = 2$: une famille (f_1, f_2) de Λ est admissible si f_1 est de norme minimale non nulle, $(\bar{f}_2)$ est une famille admissible de $\Lambda/\mathbb{Z}f_1$, et f_2 est de norme minimale dans $f_2 + \mathbb{Z}f_1$. Ceci équivaut à $\|f_1\|$ minimale non nulle et $|\langle f_1, f_2\rangle| \leq \frac{1}{2}\|f_1\|^2$ avec $\|f_2\|$ minimale. En effet, quitte à renormaliser, on peut supposer $\|f_1\| = 1$. Avec u un vecteur unitaire dirigeant $(\mathbb{R}f_1)^\perp$, en écrivant $f_2 = \lambda f_1 + \mu u$, les points 2 et 3 signifient λ et μ vérifient $\lambda^2 + \mu^2 \leq \lambda^2 + (\mu + k)^2$ pour tout $k \in \mathbb{Z}$, ie. $|\mu| = |\langle f_1, f_2\rangle| \leq 1/2$, et $|\lambda|$ minimal.

Lemme 1. *Soit Λ un réseau de $\mathbb{R}^d$. Alors :*

1. *il existe une famille admissible de Λ ;*
2. *Une famille admissible de Λ en est une base ;*
3. *Si $k \in K$ et $(f_1, \ldots, f_d) \in \Lambda^d$ est une famille admissible de Λ, alors $(kf_1, \ldots, kf_d)$ est une famille admissible de $k(\Lambda)$.*

Démonstration. Les deux premiers points découlent immédiatement de la définition récursive du caractère admissible. On procède également par récurrence sur $d \geq 1$ pour le troisième point. Soit donc $k \in K$ et $(f_1, \ldots, f_d)$ une famille admissible de Λ.

— Dans le cas $d = 1$, il n'y a que le point 1 à vérifier, ce qui est immédiat puisque

$$\min_{v \in k(\Lambda)\setminus\{0\}} \|v\| = \min_{v \in \Lambda\setminus\{0\}} \|k\,v\| = \min_{v \in \Lambda\setminus\{0\}} \|v\| = \|f_1\| = \|kf_1\|$$

— On suppose le résultat au rang $d - 1 \geq 1$. Comme précédemment, le point 1 est bien vérifié, et similairement pour le point 3. L'action de k sur $\mathbb{R}^d$ induit une isométrie $\mathbb{R}^d/\mathbb{R}f_1 \xrightarrow{\varphi} \mathbb{R}^d/\mathbb{R}kf_1$ qui envoie $\Lambda/\mathbb{Z}f_1$ sur $k(\Lambda)/\mathbb{Z}kf_1$, de sorte que, par hypothèse de récurrence, $(\overline{kf_2}, \ldots, \overline{kf_d}) = (\varphi(\bar{k}_d), \ldots, \varphi(\bar{k}_d))$ est une famille admissible de $\varphi\left(\Lambda/\mathbb{Z}f_1\right) = k(\Lambda)/\mathbb{Z}kf_1$. Ceci démontre le point 2 et conclut.

□

On dispose maintenant de la décomposition suivante, qui est le résultat principal nécessaire à la démonstration du critère de Mahler.

Proposition 3. *Si* $s \geq \dfrac{2}{\sqrt{3}}$ *et* $u \geq \dfrac{1}{2}$, *on a la décomposition*

$$\mathrm{GL}_d(\mathbb{R}) = \mathfrak{S}_{s,u} \cdot \mathrm{GL}_d(\mathbb{Z}).$$

Démonstration. Pour des raisons d'inclusion, il suffit de traiter le cas où $s = \dfrac{2}{\sqrt{3}}$ et $u = \dfrac{1}{2}$.

On peut faire l'interprétation géométrique suivante à cette décomposition : étant donné un réseau Λ de $\mathbb{R}^d$, Λ possède une base vérifiant certaines inégalités de norme.

Soit $g \in \mathrm{GL}_d(\mathbb{R})$ ainsi que $\Lambda := g(\mathbb{Z}^d)$ le réseau défini par g. On procède par récurrence sur $d \geq 1$. Le cas $d = 1$ est clair. Supposons maintenant le résultat au rang $d - 1 \geq 1$.
Le réseau Λ possède une base admissible $(f_1, \ldots, f_d)$ d'après le Lemme 1. Soit $g = kan$ la décomposition KAN de g, et $\gamma \in \mathrm{GL}_d(\mathbb{Z})$ telle que $\gamma(e_i) = g^{-1}(f_i) \in \mathbb{Z}^d$ pour tout i. Quitte à changer g en $g\gamma$, on suppose que $g(e_i) = f_i$. On va montrer qu'alors $g \in \mathfrak{S}_{\frac{2}{\sqrt{3}},\frac{1}{2}}$. D'après le Lemme 1, il suffit de traiter le cas où $k = I_d$; on aura que $k^{-1}(\Lambda)$ admet $(k^{-1}f_1, \ldots, k^{-1}f_d)$ comme base admissible, que $k^{-1}g(e_i) = k^{-1}f_i$ donc $k^{-1}g \in \mathfrak{S}_{\frac{2}{\sqrt{3}},\frac{1}{2}}$ puis enfin $g \in \mathfrak{S}_{\frac{2}{\sqrt{3}},\frac{1}{2}}$ (qui est stable par multiplication à gauche par tout élément de K, par définition).
On a alors $[f_1 \mid \cdots \mid f_d] = g = an$ où

$$a = \begin{pmatrix} a_1 & & \\ & \ddots & \\ & & a_n \end{pmatrix} \in A \qquad n = \begin{pmatrix} 1 & & * \\ & \ddots & \\ & & 1 \end{pmatrix} \in N$$

Par hypothèse de récurrence, on a $|n_{ij}| \leq \dfrac{1}{2}$ pour tout $2 \leq i < j \leq d$ et $a_i \leq \dfrac{2}{\sqrt{3}} a_{i+1}$ pour tout $2 \leq i \leq d - 1$. Il s'agit d'abord de montrer $|n_{1,j}| \leq \dfrac{1}{2}$ si $j \geq 1$, ou autrement dit que $|(f_j)_1| \leq \dfrac{1}{2}$. Or, on a par définition, $\|f_j\| \leq \|f_j + kf_1\| = \|f_j + ke_1\|$ pour tout $k \in \mathbb{Z}$, ce qui se réécrit, en passant au carré et réduisant, $(f_j)_1^2 \leq ((f_j)_1 + k)^2$ d'où le résultat avec $k = \pm 1$. Il reste ensuite à montrer $a_1 \leq \dfrac{2}{\sqrt{3}} a_2$. Ceci provient du fait que $\|f_1\| \leq \|f_2\|$, ce qui se réécrit

$$a_1^2 \leq a_1^2 n_{12}^2 + a_2^2 \leq a_1^2/4 + a_2^2$$

qui équivaut au résultat souhaité. □

2.3 Le critère de Mahler

Définition 4. Si E est un $\mathbb{R}$-espace vectoriel de dimension finie, on définit $\mathcal{R}(E)$ *l'espace des réseaux* de E. $\mathrm{GL}(E)$ agit naturellement et transitivement sur cet espace, que l'on identifie donc à $\mathrm{GL}(E)/\operatorname{Stab}(\Lambda)$ (où Λ est un réseau quelconque).
On munit $\mathcal{R}(E)$ de la topologie quotient associée (qui ne dépend pas du choix de Λ).

Définition 5. Pour $E = \mathbb{R}^d$ muni de sa structure euclidienne canonique, on définit deux fonctions sur l'espace des réseaux $\mathcal{R}(E)$:

- La systole $\mathrm{s}(\Lambda) = \min\limits_{v\in\Lambda\setminus\{0\}} ||v||$;
- Le covolume $\mathrm{cov}(\Lambda) = |\det(B)|$ où B est une base (quelconque) de Λ.
  Ce covolume est bien indépendant de la base choisie : si B et B' sont deux bases de Λ, la matrice de passage de B à B' est un élément de $\mathrm{GL}_d(\mathbb{Z})$ et a un déterminant égal à ± 1.

Lemme 2. s *et* cov *sont continues.*

Démonstration. Pour le covolume, il suffit de voir que $\begin{array}{ccc}\mathrm{GL}_d(\mathbb{R}) & \longrightarrow & \mathbb{R}_+^* \\ g & \longmapsto & |\det(g)|\end{array}$ est continue et invariante par $\mathrm{GL}_d(\mathbb{Z})$, donc définit bien (par la propriété universelle des quotients) une application continue sur $\mathcal{R}(\mathbb{R}^d)$.

Le cas de la systole est un peu moins évident. Comme il est clair que $\begin{array}{ccc}\mathrm{GL}_d(\mathbb{R}) & \xrightarrow{\mathrm{s}} & \mathbb{R}_+^* \\ g & \longmapsto & \inf\limits_{x\in g\mathbb{Z}^d-0} ||x||\end{array}$ passe au quotient par $\mathrm{GL}_d(\mathbb{Z})$, il suffit de montrer sa continuité.

Constatons tout d'abord qu'un réseau est discret et fermé donc $\forall R > 0, g\mathbb{Z}^d \cap \overline{B}(0,R)$ est fini. C'est pour cette raison que l'on peut écrire un min dans la définition de la systole.

Soit donc $g \in \mathrm{GL}_d(\mathbb{R})$, x_0 tel que $\mathrm{s}(g) = ||x_0||$ et $\varepsilon > 0$.

Par continuité de $h \mapsto ||hx_0||$, il existe un voisinage U de g tel que

$$\forall h \in U, \mathrm{s}(h) \leq ||hx_0|| \leq \mathrm{s}(g) + \varepsilon.$$

Pour l'autre inégalité soit $R = 2\,\mathrm{s}(g)$. Il existe un nombre fini de $x \in \mathbb{Z}^d$ tels que $gx \in \overline{B}(0,R)$. On peut donc choisir U' un autre voisinage de g tel que pour chacun de ces x et $h \in U'$, $||hx|| \geq \mathrm{s}(g) - \varepsilon$.

Enfin par continuité de $h \mapsto ||hg^{-1} - 1||$, il existe U'' dans lequel $||hg^{-1} - 1|| \leq \dfrac{1}{2}$. Mais alors si $h \in U''$ et $||gx|| \geq R$,

$$||hx|| \geq ||gx|| - ||hg^{-1} - 1||||gx|| \geq \frac{1}{2}||gx|| \geq \mathrm{s}(g).$$

On obtient bien que pour $h \in U \cap U' \cap U''$, $|\,\mathrm{s}(g) - \mathrm{s}(h)| \leq \varepsilon$. □

Théorème 1 (Critère de Mahler)**.** *Soit $X \subseteq \mathcal{R}(\mathbb{R}^d)$. Alors X est relativement compacte si et seulement si les deux conditions suivantes sont respectées :*

- $\inf\limits_{\Lambda\in X} s(\Lambda) > 0$ *;*
- $\sup\limits_{\Lambda\in X} \mathrm{cov}(\Lambda) < +\infty$.

En d'autres termes, les covolumes des éléments de X sont uniformément bornés et on dispose d'un voisinage U de 0 dans $\mathbb{R}^d$ tel que $U \cap \Lambda = \{0\}$ pour tout $\Lambda \in X$.

Démonstration.

- Supposons X relativement compacte. Alors le résultat est vrai par la continuité de s et de cov et le théorème des bornes atteintes.

— Supposons les deux conditions respectées. Par la proposition 3, on peut considérer un ensemble de Siegel $\mathfrak{S} = K \cdot A_s \cdot N_u$ tel que $\mathrm{GL}_d(\mathbb{R}) = \mathfrak{S}\mathrm{GL}_d(\mathbb{Z})$. L'application induite de l'action transitive de $\mathrm{GL}_d(\mathbb{R})$ sur $\mathcal{R}(\mathbb{R}^d)$

$$\begin{array}{ccc} \mathrm{GL}_d(\mathbb{R}) & \xrightarrow{\varphi} & \mathcal{R}(\mathbb{R}^d) \\ g & \longmapsto & g(\mathbb{Z}^d) \end{array}$$

qui est continue par définition de la topologie assignée à $\mathcal{R}(\mathbb{R}^d)$, reste donc surjective lorsque restreinte à $\mathfrak{S}$. Puisque $\mathrm{Stab}(\mathbb{Z}^d) = \mathrm{GL}_d(\mathbb{Z})$, on identifie $\mathcal{R}(\mathbb{R}^d) \simeq \mathrm{GL}_d(\mathbb{R})/\mathrm{GL}_d(\mathbb{Z})$.
Soit

$$S := \left\{ g \in \mathfrak{S} \;\middle|\; g \cdot \mathrm{GL}_d(\mathbb{Z}) \in \overline{X} \right\} = \varphi^{-1}\left(\overline{X}\right) \cap \mathfrak{S}.$$

Il suffit de montrer que S est compacte. En effet, on aura alors $\overline{X} = \varphi(S)$ compacte par continuité de φ. Puisque $S \subseteq M_d(\mathbb{R})$, il s'agit de montrer que S est une partie fermée et bornée. La fermeture est claire, par continuité de φ et le caractère fermé de $\overline{X}$ et de $\mathfrak{S}$. Reste à montrer la bornitude. Par hypothèse, on a $\delta > 0$ tel que pour tout $g \in S$, $\min\limits_{x \in \mathbb{Z}^d \setminus \{0\}} \|g(x)\| \geq \delta$ et $C > 0$ tel que $|\det(g)| \leq C$. Écrivons, pour $g \in S$, $g = k \cdot a \cdot n$ où $k \in K, a \in A_s, n \in N_u$. On a donc $a_1 = \|g(e_1)\| \geq \delta$ et $a_1 \cdots a_d \leq C$. On en déduit

$$a_i \leq s a_{i+1} \leq \ldots \leq s^{d-i} a_d \quad \text{et} \quad a_i \geq \frac{1}{s^{i-1}} a_1 \geq \frac{1}{s^{i-1}} \delta$$

puis

$$C \geq a_1 \cdots a_d \geq \delta \frac{1}{s} \delta \cdots \frac{1}{s^{d-2}} \delta \cdot a_d = \delta^{d-1} \frac{1}{s^{(d-1)(d-2)/2}} a_d$$

ce qui montre que les a_i sont bornés indépendamment de g. Comme les élément de N_u sont bornés, que la décomposition KAN est un homéomorphisme, il vient que S est bornée, ce qui conclut.

□

3 Réduction au critère de Mahler

Dans cette section on admet l'existence d'une sous-$\mathbb{Q}$-algèbre D de $\mathrm{M}_d(\mathbb{R})$, avec les deux propriétés suivantes :
(1) D est une algèbre à division,
(2) $D \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathrm{M}_d(\mathbb{R})$, ou de manière équivalente, D admet une $\mathbb{Q}$-base qui est aussi une $\mathbb{R}$-base de $\mathrm{M}_d(\mathbb{R})$.
On dit aussi qu'une sous-$\mathbb{Q}$-algèbre satisfaisant la condition (2) est une $\mathbb{Q}$-structure de $\mathrm{M}_d(\mathbb{R})$.

L'existence d'une telle D est non triviale. Elle est une conséquence de la description du groupe de Brauer de $\mathbb{Q}$ et elle est donc liée avec des résultats profonds de l'algèbre et de la théorie des nombres. On laisse la preuve de son existence à la section suivante. On verra dans cette section comment construire des sous-groupes discrets de $\mathrm{SL}_d(\mathbb{R})$ à partir d'une telle D, et on peut montrer que ces sous-groupes sont cocompacts en utilisant le critère de Mahler.

On admet aussi le fait que D admet un ordre, i.e. un sous-anneau $\mathcal{O}$ de D qui est libre comme $\mathbb{Z}$-module et tel que $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Q} \simeq D$. Encore, c'est équivalent à dire que $\mathcal{O}$ admet une $\mathbb{Z}$-base qui est aussi une $\mathbb{Q}$-base de D. En combinant ceci avec la condition (2) de D, on voit que $\mathcal{O}$ est un réseau du $\mathbb{R}$-espace vectoriel $\mathrm{M}_d(\mathbb{R})$. En effet, toute $\mathbb{Q}$-algèbre à division de dimension finie admet un ordre, cette affirmation sera montrée dans la Section 4 (Proposition 11). Il faut remarquer que ni le choix de D ni le choix de $\mathcal{O}$ ne sont canoniques : il y a plusieurs D et $\mathcal{O}$ que l'on peut choisir, et donc ils correspondent à différents réseaux cocompacts de $\mathrm{SL}_d(\mathbb{R})$.

3.1 Une injection

$\mathrm{M}_d(\mathbb{R})$, en tant que $\mathbb{R}$-algèbre, admet une loi de multiplication $\mathbb{R}$-bilinéaire et associative :

$$\begin{aligned}\mathrm{M}_d(\mathbb{R}) \times \mathrm{M}_d(\mathbb{R}) &\longrightarrow \mathrm{M}_d(\mathbb{R}) \\ (A, B) &\longmapsto AB\end{aligned}$$

qui induit un morphisme de $\mathbb{R}$-algèbres, appelé "la multiplication à gauche" :

$$\begin{aligned}\Phi : \mathrm{M}_d(\mathbb{R}) &\longrightarrow \mathrm{End}(\mathrm{M}_d(\mathbb{R})) \\ A &\longmapsto (B \longmapsto AB)\end{aligned}$$

où $\mathrm{End}(\mathrm{M}_d(\mathbb{R})) = \mathrm{End}_{\mathbb{R}}(\mathrm{M}_d(\mathbb{R}))$ est l'anneau des endomorphismes du $\mathbb{R}$-espace vectoriel $\mathrm{M}_d(\mathbb{R})$. On vérifie aisément que Φ est une injection. Effectivement, si $A \neq 0$, alors il existe $x \in \mathbb{R}^d$ tel que $Ax \neq 0$. Alors $AB \neq 0$ pour B la matrice dont tous les colonnes sont formées par les coordonnées du vecteur x. Si on munit $\mathrm{M}_d(\mathbb{R})$ et $\mathrm{End}(\mathrm{M}_d(\mathbb{R}))$ de la topologie induite par une norme, on voit que Φ est un homéomorphisme sur son image par le théorème d'application ouverte. La restriction de Φ à $\mathrm{GL}_d(\mathbb{R})$ induit une injection de groupes $\mathrm{GL}_d(\mathbb{R}) \hookrightarrow \mathrm{GL}(\mathrm{M}_n(\mathbb{R}))$, car $\Phi(A)$ est inversible si A l'est. Réciproquement, si $\Phi(A)$ est inversible, on a que $\Phi(A)^{-1}(I_d)$ donne l'inverse de A, donc A est inversible. En d'autres termes, $\det(A) \neq 0$ si et seulement si $\det(\Phi(A)) \neq 0$. Ce fait nous suggère la proposition suivante.

Proposition 4. *Soit $A \in \mathrm{M}_d(\mathbb{R})$. On a $\det(\Phi(A)) = \det(A)^d$ et $\mathrm{tr}(\Phi(A)) = d\,\mathrm{tr}(A)$.*

Démonstration. $\mathrm{M}_d(\mathbb{R})$ admet une décomposition en sous-espaces invariants par rapport à $\Phi(A)$: $\mathrm{M}_d(\mathbb{R}) = V_1 \oplus V_2 + ... \oplus V_d$, où V_i représente le sous-espace de la i-ième colonne. On conclut en observant que l'action de $\Phi(A)$ sur chaque V_i est isomorphe à l'action naturelle de A sur $\mathbb{R}^d$. □

Notons G le groupe $\{A \in \mathrm{GL}_d(\mathbb{R}) : \det(\Phi(A)) = 1\}$. C'est un groupe qui ressemble à $\mathrm{SL}_d(\mathbb{R})$, mais qui est plus naturel à considérer lorsque l'on fait usage de l'injection Φ. D'après la proposition précédente, on sait que $G = \mathrm{SL}_d(\mathbb{R})$ si d est impair et $G = \mathrm{GL}_d^{\pm}(\mathbb{R}) = \{A \in \mathrm{GL}_d(\mathbb{R}) : \det(A) = \pm 1\}$ si d est pair.

Revenons à la construction de réseaux cocompacts. Comme on a dit précédemment, il existe un réseau $\mathcal{O}$ de $\mathrm{M}_d(\mathbb{R})$ qui est aussi un sous-anneau. De plus, ses éléments non nuls sont de déterminant non nul, car il est contenu dans l'algèbre à division D. Le fait que $\mathcal{O}$ est un anneau nous donne un résultat plus fort, qui dit que le déterminant de ses éléments est uniformément minoré :

Proposition 5. *Soit $A \in \mathcal{O} \setminus \{0\}$, alors $|\det(A)| \geq 1$.*

Démonstration. Choisissons une $\mathbb{Z}$-base de $\mathcal{O}$ (qui est aussi une $\mathbb{R}$-base de $\mathrm{M}_d(\mathbb{R})$ car $\mathcal{O}$ est un réseau). Comme $\mathcal{O}$ est stable sous multiplication matricielle, la matrice de $\Phi(A)$ par rapport à cette base est dans $\mathrm{GL}_{d^2}(\mathbb{Z})$. Donc $\det(\Phi(A)) \in \mathbb{Z}$. On conclut par la Proposition 4 et le fait que $\det(A) \neq 0$. □

Rappelons que le groupe $\mathrm{GL}(\mathrm{M}_d(\mathbb{R}))$ agit transitivement sur l'espaces des réseaux $\mathcal{R}(\mathrm{M}_d(\mathbb{R}))$. Comme $\mathcal{O}$ est un élément de $\mathcal{R}(\mathrm{M}_d(\mathbb{R}))$, on peut identifier $\mathcal{R}(\mathrm{M}_d(\mathbb{R}))$ à l'espace quotient $\mathrm{GL}(\mathrm{M}_d(\mathbb{R}))/\mathrm{Stab}(\mathcal{O})$, où $\mathrm{Stab}(\mathcal{O}) = \{u \in \mathrm{GL}(\mathrm{M}_d(\mathbb{R})) : u \cdot \mathcal{O} = \mathcal{O}\}$. L'image réciproque de $\mathrm{Stab}(\mathcal{O})$ par $\Phi\big|_G$ est $G \cap \mathcal{O}$. Effectivement, si $\Phi(A) \cdot \mathcal{O} = \mathcal{O}$, on a particulièrement $A = \Phi(A)(I_d) \in \mathcal{O}$. Donc Φ induit une application injective $\tilde{\Phi} : G/G \cap \mathcal{O} \to \mathrm{GL}(\mathrm{M}_d(\mathbb{R}))/\mathrm{Stab}(\mathcal{O})$. Cette application est continue car Φ l'est et par la propriété universelle de la topologie quotient.

$\tilde{\Phi}(G/G \cap \mathcal{O})$ est un sous-ensemble de $\mathrm{GL}(\mathrm{M}_d(\mathbb{R}))/\mathrm{Stab}(\mathcal{O}) \simeq \mathcal{R}(\mathrm{M}_d(\mathbb{R}))$, donc on peut tester sa compacité par le critère de Mahler. Comme $\Phi(G) \subseteq \mathrm{SL}(\mathrm{M}_d(\mathbb{R}))$, $\mathrm{cov}(\Phi(A) \cdot \mathcal{O}) = \mathrm{cov}(\mathcal{O})$ pour tout $A \in G$, donc le covolume des éléments dans $\tilde{\Phi}(G/G \cap \mathcal{O})$ est uniformément borné. Supposons par l'absurde que l'on a $\inf_{A \in G} \mathrm{s}(\Phi(A) \cdot \mathcal{O}) = 0$. Alors on peut trouver deux suites $(A_n)_n \in G$, $(O_n)_n \in \mathcal{O} \setminus \{0\}$ telles que $A_n O_n \to 0$. Or on sait que $|\det(A_n O_n)| = |\det(O_n)| \geq 1$ grâce aux Propositions 4 et 5. C'est une contradiction, donc $\inf_{A \in G} \mathrm{s}(\Phi(A) \cdot \mathcal{O}) > 0$. Donc $\tilde{\Phi}(G/G \cap \mathcal{O})$ a réussi les deux tests du critère de Mahler. Ainsi on a montré :

Proposition 6. *$\tilde{\Phi}(G/G\cap\mathcal{O})$ est relativement compact.*

Notre but est de montrer que $G\cap\mathcal{O}$ est un réseau cocompact, mais la Proposition 6 n'est pas suffisante. Il faut encore montrer deux choses : (1) $\tilde{\Phi}(G/G\cap\mathcal{O})$ est fermé, et (2) $\tilde{\Phi}$ est un homéomorphisme sur son image. C'est ce qu'on va faire dans les deux sous-sections suivantes.

3.2 Puissances extérieures et représentations

Rappelons quelques faits sur les puissances extérieures. Pour un espace vectoriel V défini sur un corps quelconque, on peut définir son algèbre extérieure $(\Lambda V, +, \wedge)$ comme le quotient de l'algèbre tensorielle $(TV, +, \otimes)$ par l'idéal homogène engendré par les éléments de la forme $v \otimes v$, $\forall v \in V$. C'est une algèbre graduée : $\Lambda V = \oplus_{k\in\mathbb{N}}\Lambda^k V$, où $\Lambda^k V$ (appelé la k-ième puissance extérieure de V) et engendré par les éléments de la forme $v_1 \wedge ... \wedge v_k$, où $v_1, ..., v_k \in V$. Si V est de dimension finie n, on a $\Lambda^k V = 0$ pour $k > n$ et $\dim \Lambda^k V = \binom{n}{k}$ pour $k \leq n$. Dans ce dernier cas, toute base $e_1, ..., e_n$ de V donne une base $\{e_{i_1} \wedge ... \wedge e_{i_k} : 1 \leq i_1 < ... < i_k \leq n\}$ de $\Lambda^k V$. Les Λ^k sont des foncteurs en le sens que si $f : V \to W$ est une application linéaire, on peut définir $\Lambda^k f : \Lambda^k V \to \Lambda^k W$ comme l'unique application linéaire telle que $\Lambda^k f(v_1 \wedge ... \wedge v_k) = f(v_1) \wedge ... \wedge f(v_k)$. Lorsque f est injective on a que $\Lambda^k f$ l'est aussi, car f injective implique l'existence d'une rétraction $g : W \to V$ telle que $g \circ f = \mathrm{Id}_V$, alors $\Lambda^k g \circ \Lambda^k f = \mathrm{Id}_{\Lambda^k V}$ par fonctorialité. On peut donc identifier $\Lambda^k V$ comme un sous-espace de $\Lambda^k W$. Si f est un endomorphisme sur un espace vectoriel V de dimension finie n, alors $\Lambda^n f$ est égale à la multiplication par $\det(f)$ sur la droite $\Lambda^n V$. Ceci fournit une interprétation (remarquablement, sans utilisation d'une base) du déterminant.

Proposition 7. *Soient V un espace vectoriel, W un sous-espace vectoriel de dimension finie n. Soit $g \in \mathrm{GL}(V)$. Alors W est un sous-espace invariant de g si et seulement si $\Lambda^n W$ est un sous-espace invariant de $\Lambda^n g$.*

Démonstration. Une implication est claire. On montre l'implication qui est plus difficile. Supposons que $\Lambda^n W$ est un sous-espace invariant de $\Lambda^n g$. Par l'absurde, on suppose qu'il existe $w \in W$ tel que $g(w) \notin W$. Étendons w en une base $e_1 = w, e_2, ..., e_n$ de W. Comme $e_1 \wedge ... \wedge e_n$ engendre la droite $\Lambda^n(W)$, on peut écrire $\Lambda^n(g)(e_1 \wedge ... \wedge e_n) = ke_1 \wedge ... \wedge e_n$ pour k une constante. On sait que $g(w) \wedge e_1 \wedge ... \wedge e_n \neq 0$ car $g(w) \notin W$. Alors

$$kg(w) \wedge e_1 \wedge ... \wedge e_n = g(w) \wedge \Lambda^n g(e_1 \wedge ... \wedge e_n) = \Lambda^{n+1} g(w \wedge w \wedge e_2 ... \wedge e_n) = 0.$$

Ceci implique que $k = 0$. Mais c'est impossible car

$$0 \neq e_1 \wedge ... \wedge e_n = \Lambda^n g^{-1}(\Lambda^n g(e_1 \wedge ... \wedge e_n)) = k\Lambda^n g^{-1}(e_1 \wedge ... \wedge e_n).$$

Ainsi on a une contradiction. □

Une façon puissante d'étudier un groupe est d'étudier ses représentations. Dans notre cas, on veut étudier la relation entre $\mathrm{GL}(\mathrm{M}_d(\mathbb{R}))$ et ses sous-groupes $\Phi(G)$ et $\mathrm{Stab}(\mathcal{O})$.

Lemme 3. *Il existe une $\mathbb{R}$-représentation de dimension finie V de $\mathrm{GL}(\mathrm{M}_d(\mathbb{R}))$ et un vecteur $v \in V$ avec les propriétés suivantes :*

(1) $\mathrm{Stab}(v) = \Phi(G)$,

(2) $\mathrm{Stab}(\mathcal{O}).v$ *est fermé discret dans V.*

Démonstration. $\mathrm{GL}(\mathrm{M}_d(\mathbb{R}))$ agit sur $\mathrm{End}(\mathrm{M}_d(\mathbb{R}))$ par multiplication (i.e. composition) à gauche. Cette action fait $\mathrm{End}(\mathrm{M}_d(\mathbb{R}))$ une $\mathbb{R}$-représentation de dimension d^4 de $\mathrm{GL}(\mathrm{M}_d(\mathbb{R}))$. Remarquons que $\Phi(\mathrm{M}_d(\mathbb{R})) \subseteq \mathrm{End}(\mathrm{M}_d(\mathbb{R}))$ est un sous-espace vectoriel de dimension d^2. Les éléments de $\mathrm{GL}(\mathrm{M}_d(\mathbb{R}))$ qui laissent le sous-espace $\Phi(\mathrm{M}_d(\mathbb{R}))$ invariant sont ceux de $\Phi(\mathrm{GL}_d(\mathbb{R}))$. Effectivement, si $u \in \mathrm{GL}(\mathrm{M}_d(\mathbb{R}))$

satisfait $u.\Phi(\mathrm{M}_d(\mathbb{R})) = \Phi(\mathrm{M}_d(\mathbb{R}))$, alors particulièrement on a $u = u \circ \mathrm{Id} = u.\Phi(I_d) \in \Phi(\mathrm{M}_d(\mathbb{R}))$. Donc $u \in \mathrm{GL}(\mathrm{M}_d(\mathbb{R})) \cap \Phi(\mathrm{M}_d(\mathbb{R})) = \Phi(\mathrm{GL}_d(\mathbb{R}))$.

On peut alors appliquer la Proposition 7. Considérons la représentation $\Lambda^{d^2}\mathrm{End}(\mathrm{M}_d(\mathbb{R}))$. Par la Proposition 7, les éléments de $\mathrm{GL}(\mathrm{M}_d(\mathbb{R}))$ qui laissent la droite $\Lambda^{d^2}\Phi(\mathrm{M}_d(\mathbb{R}))$ invariante sont encore ceux de $\Phi(\mathrm{GL}_d(\mathbb{R}))$. On voit aussi que l'action de $\Phi(A)$ pour un $A \in \mathrm{GL}_d(\mathbb{R})$ sur $\Lambda^{d^2}\Phi(\mathrm{M}_d(\mathbb{R}))$ est égale à la multiplication par le déterminant du action de $\Phi(A)$ sur $\Phi(\mathrm{M}_d(\mathbb{R}))$, qui est exactement la même chose que $\det(\Phi(A))$. Donc on a que pour tout élément non nul $v \in \Lambda^{d^2}(\Phi(\mathrm{M}_d(\mathbb{R}))$, son stabilisateur $\mathrm{Stab}(v) = \{\Phi(A) : A \in \mathrm{GL}_d(\mathbb{R}), \det(\Phi(A)) = 1\} = \Phi(G)$.

Choisissons une $\mathbb{Z}$-base $E_1, ..., E_{d^2}$ de $\mathcal{O}$. C'est aussi une $\mathbb{R}$-base de $\mathrm{M}_d(\mathbb{R})$. On prend $V = \Lambda^{d^2}\mathrm{End}(\mathrm{M}_d(\mathbb{R}))$ et $v = \Phi(E_1) \wedge ... \wedge \Phi(E_{d^2}) \in \Lambda^{d^2}\Phi(\mathrm{M}_d(\mathbb{R}))$. Ce qui précède montre la propriété (1), il reste à montrer la propriété (2). Soit $u \in \mathrm{Stab}(\mathcal{O})$. Pour $1 \leq i, j \leq d^2$, on a $u.\Phi(E_i)(E_j) = u \circ \Phi(E_i)(E_j) = u(E_iE_j) \in \mathcal{O} = \oplus_{k=1}^{d^2}\mathbb{Z}E_k$ car $E_iE_j \in \mathcal{O}$ et $u \in \mathrm{Stab}(\mathcal{O})$. Donc la matrice de $u.\Phi(E_i)$ par rapport à la base $E_1, ..., E_{d^2}$ est de coefficients dans $\mathbb{Z}$. De manière équivalente, $u.\Phi(E_i) \in \oplus_{1 \leq j,k \leq d^2}\mathbb{Z}E_j^* \otimes E_k$, ici on a utilisé l'isomorphisme $\mathrm{End}(\mathrm{M}_d(\mathbb{R})) \simeq \mathrm{M}_d(\mathbb{R})^* \otimes \mathrm{M}_d(\mathbb{R})$. Donc,

$$u.v = u.\Phi(E_1) \wedge ... \wedge u.\Phi(E_{d^2}) \in \left(\bigoplus_{1 \leq j,k \leq d^2} \mathbb{Z}E_{jk}\right)^{\wedge d^2} \subseteq \bigoplus_{1 \leq j_1, k_1, ..., j_{d^2}, k_{d^2} \leq d^2} \mathbb{Z}E_{j_1k_1} \wedge ... \wedge E_{j_{d^2}k_{d^2}}$$

(on utilise E_{jk} pour noter $E_j^* \otimes E_k$). Alors le dernier terme ci-dessus est bien sûr un réseau dans V, et donc son sous-ensemble $\mathrm{Stab}(\mathcal{O}).v$ est fermé discret dans V. □

3.3 Fin de la preuve

Proposition 8. *$\tilde{\Phi}$ est un homéomorphisme sur une partie fermée de $\mathrm{GL}(\mathrm{M}_d(\mathbb{R}))/\mathrm{Stab}(\mathcal{O})$.*

Démonstration. On sait déjà que $\tilde{\Phi}$ est une application continue injective. Il reste à montrer que $\tilde{\Phi}$ est fermée. $G/G\cap\mathcal{O}$ et $\mathrm{GL}(\mathrm{M}_d(\mathbb{R}))/\mathrm{Stab}(\mathcal{O})$ sont à base dénombrable par la Proposition 1. En particulier, ils sont des espaces séquentiels, i.e., leur topologie est déterminée par les suites convergentes. Soit F un fermé de $G/G \cap \mathcal{O}$ et $(\overline{u_n})_n$ une suite dans $\tilde{\Phi}(F)$ qui converge vers $\bar{h} \in \mathrm{GL}(\mathrm{M}_d(\mathbb{R}))/\mathrm{Stab}(\mathcal{O})$. On peut écrire $u_n = \tilde{\Phi}(\overline{g_n}) = \overline{\Phi(g_n)}$ pour $g_n \in G$. D'après la Proposition 1, la convergence implique qu'il existe $\gamma_n \in \mathrm{Stab}(\mathcal{O})$ tels que $\Phi(g_n)\gamma_n \to h$. On prend l'inverse et on agit sur $v \in V$ comme dans le Lemme 3. On obtient

$$\gamma_n^{-1}.v = \gamma_n^{-1}\Phi(g_n^{-1}).v \to h^{-1}.v.$$

Or les $\gamma_n^{-1}.v$ sont contenus dans une partie fermé discret de V, ce qui force $\gamma_n^{-1}.v = h^{-1}.v$ pour n assez grand. Donc on a (toujours pour n assez grand)

$$\gamma_n h^{-1} \in \mathrm{Stab}(v) \cap \mathrm{Stab}(\mathcal{O})h^{-1} = \Phi(G) \cap \mathrm{Stab}(\mathcal{O})h^{-1}.$$

Ceci implique que

$$(\gamma_n h^{-1})(\gamma_m h^{-1})^{-1} \in \Phi(G) \cap \mathrm{Stab}(\mathcal{O}) = \Phi(G \cap \mathcal{O}).$$

Donc on peut écrire $\gamma_n h^{-1} = \Phi(k_n g^{-1})$ avec $k_n \in G \cap \mathcal{O}$ et $g \in G$ (on peut prendre par exemple g tel que $\Phi(g^{-1}) = \gamma_m h^{-1}$ pour m assez grand fixé). Alors $\Phi(g_n k_n g^{-1})h = \Phi(g_n)\gamma_n \to h$, i.e. $\Phi(g_n k_n) \to \Phi(g)$. On a donc $g_n k_n \to g$ car Φ est un homéomorphisme sur son image. En projetant sur $G/G\cap\mathcal{O}$, on obtient que $\overline{g_n} = \overline{g_n k_n} \to \bar{g}$. Comme F est fermé, $\bar{g} \in F$ et donc $\bar{h} = \lim_n u_n = \tilde{\Phi}(\bar{g}) \in \tilde{\Phi}(F)$ par la continuité de $\tilde{\Phi}$. Ainsi on a montré que $\tilde{\Phi}(F)$ est fermé et on a fini. □

En combinant les Propositions 6 et 8, on a montré :

Proposition 9. *$G \cap \mathcal{O}$ est un réseau cocompact de G.*

On a presque fini. Si d est impair on sait que $G = \mathrm{SL}_d(\mathbb{R})$ et donc on a bien construit un réseau cocompact de $\mathrm{SL}_d(\mathbb{R})$. Mais si d est pair ce n'est pas le cas. Cela ne pose pas de problème parce que dans ce cas-là $\mathrm{SL}_d(\mathbb{R})$ n'est qu'un sous-groupe ouvert d'indice 2 de $G = \mathrm{GL}_d^{\pm}(\mathbb{R})$.

Théorème 2. *Soit $d \in \mathbb{N}$. Si $\Gamma \subseteq \mathrm{GL}_d^{\pm}(\mathbb{R})$ est un réseau cocompact, alors $\Gamma \cap \mathrm{SL}_d(\mathbb{R})$ est un réseau cocompact de $\mathrm{SL}_d(\mathbb{R})$. En particulier, $\mathrm{SL}_d(\mathbb{R}) \cap \mathcal{O}$ est un réseau cocompact de $\mathrm{SL}_d(\mathbb{R})$.*

Démonstration. $\Gamma \cap \mathrm{SL}_d(\mathbb{R}) \subseteq \mathrm{SL}_d(\mathbb{R})$ est clairement un sous-groupe discret, donc il suffit de montrer que $\mathrm{SL}_d(\mathbb{R})/\Gamma \cap \mathrm{SL}_d(\mathbb{R})$ est compact. $\mathrm{SL}_d(\mathbb{R})$ est un sous-groupe ouvert de $\mathrm{GL}_d^{\pm}(\mathbb{R})$ donc l'application naturelle $\mathrm{SL}_d(\mathbb{R}) \to \mathrm{GL}_d^{\pm}(\mathbb{R})/\Gamma$ est ouverte. En passant au quotient, on obtient une application ouverte et injective $\mathrm{SL}_d(\mathbb{R})/\Gamma \cap \mathrm{SL}_d(\mathbb{R}) \to \mathrm{GL}_d^{\pm}(\mathbb{R})/\Gamma$. Donc $\mathrm{SL}_d(\mathbb{R})/\Gamma \cap \mathrm{SL}_d(\mathbb{R})$ est homéomorphe à son image $\mathrm{SL}_d(\mathbb{R})\Gamma/\Gamma$. Or on sait que son image est fermé car $\mathrm{SL}_d(\mathbb{R})$ est un sous-groupe d'index 2, donc distingué, donc $\mathrm{SL}_d(\mathbb{R})\Gamma = \mathrm{SL}_d(\mathbb{R})$ ou $\mathrm{GL}_d^{\pm}(\mathbb{R})$, qui est dans les deux cas bien fermé dans $\mathrm{GL}_d^{\pm}(\mathbb{R})$. La dernière partie du théorème découle de ce qui précède et de la Proposition 9. □

4 Constructions algébriques et arithmétiques

Il s'agit maintenant de démontrer le résultat admis dans la partie précédente pour arriver à une preuve complète :

Proposition 10. *Il existe $\mathcal{O} \subset \mathrm{M}_d(\mathbb{R})$ vérifiant les 3 propriétés suivantes :*
- $\mathcal{O}$ est un sous-anneau.
- $\mathcal{O}$ admet une $\mathbb{Z}$-base qui est aussi une $\mathbb{R}$-base de $\mathrm{M}_d(\mathbb{R})$ ($\mathcal{O}$ est un réseau de $\mathrm{M}_d(\mathbb{R})$).
- Tout élément non nul de $\mathcal{O}$ est inversible (dans $\mathrm{M}_d(\mathbb{R})$).

Pour démontrer cela, nous passerons par l'intermédiaire de $\mathbb{Q}$. En revanche nous n'utiliserons pas du tout les outils de la théorie du groupe de Brauer et adoptons une méthode plus élémentaire.

Mais commençons par donner une définition générale.

4.1 Ordres

Dans cette partie, sauf mention explicite du contraire toutes les algèbres seront de dimension finie.

Définition 6. Soient $A \subset K$, A anneau et K corps, et B_K une K-algèbre. On dit que $B_A \subset B_K$ est une A-structure de B_K si :

— B_A est une sous-A-algèbre.

— B_A admet une A-base qui est aussi une K-base de B_K.

Si $A = \mathbb{Z}$, une $\mathbb{Z}$-structure est appelée un ordre.

Il est à noter qu'alors toute A-base de B_A est aussi une K-base de B_K.

Exemple. $\mathrm{M}_d(\mathbb{Z})$ est un ordre dans $\mathrm{M}_d(\mathbb{Q})$.

Avant de reformuler notre proposition en termes d'ordre, remarquons que l'on dispose de la proposition suivante :

Proposition 11. *Toute $\mathbb{Q}$-algèbre de dimension finie admet un ordre.*

Démonstration. Soit D une $\mathbb{Q}$-algèbre de dimension finie n, avec e_1,...,e_n une $\mathbb{Q}$-base, et $e_1 = 1_D$. Par finitude il existe $N \in \mathbb{N}_{>0}$ tel que $e_i e_j \in \bigoplus_{k=1}^{n} \frac{1}{N}\mathbb{Z}e_k$, $\forall 1 \leq i, j \leq n$. Alors $\mathcal{O} = \bigoplus_{k=1}^{n} N\mathbb{Z}e_k$ admet une $\mathbb{Z}$-base Ne_1,...,Ne_n qui est aussi une $\mathbb{Q}$-base de D et on a de plus

$$Ne_i \cdot Ne_j = N^2 e_i e_j \in N^2 \bigoplus_{k=1}^{n} \frac{1}{N}\mathbb{Z}e_k = \mathcal{O}$$

pour tout $1 \leq i, j \leq n$, ce qui montre par bilinéarité la stabilité de $\mathcal{O}$ sous multiplication. $\mathbb{Z}1_D + \mathcal{O}$ forme alors un ordre de D. □

Autrement dit, pour prouver l'existence de notre ordre dont tous les éléments sont inversibles (dans $\mathrm{M}_d(\mathbb{R})$)), il suffit de montrer l'existence d'une $\mathbb{Q}$-structure à division de $\mathrm{M}_d(\mathbb{R})$. Il sera plus agréable par la suite de travailler avec un corps au lieu d'un anneau, pour avoir des arguments de théorie de Galois, etc.

Définition 7. Si A est une k-algèbre et $x \in A$, on note $m_x \in L_k(A)$ la multiplication à gauche par x. On définit alors $\mathrm{Tr}_A(x) = \mathrm{tr}(m_x)$ et $N_A(x) = \det(m_x)$.

Exemple. Si $x \in k$, alors $\mathrm{Tr}_A(x) = \dim_k(A)x$ et $N_A(x) = x^{\dim_k(A)}$.

Proposition 12. *Soit $k \subset K$ des corps, B_k une k-structure de B_K et $x \in B_k$. Alors $\mathrm{Tr}_{B_k}(x) = \mathrm{Tr}_{B_K}(x)$ et $N_{B_k}(x) = N_{B_K}(x)$.*

Démonstration. Il suffit de constater que les matrices de $m_x \in L_k(B_k)$ et $m_x \in L_K(B_K)$ dans une k-base de B_k qui est aussi une K-base de B_K sont identiques. □

Dans toute la suite, on s'intéresse à présent plus particulièrement au cas où $K = \mathbb{R}$ et $B_K = M_d(\mathbb{R})$. $k \subset \mathbb{R}$ est un sous-corps quelconque.

Proposition 13. *Pour $x \in \mathrm{M}_d(\mathbb{R})$, $\mathrm{Tr}_{M_d(\mathbb{R})}(x) = d\,\mathrm{tr}(x)$ et $N_{\mathrm{M}_d(\mathbb{R})}(x) = \det(x)^d$.*

Démonstration. C'est une simple reformulation de la proposition 4 que l'on rappelle ici. □

Proposition 14. *Soit A est une k-structure de $\mathrm{M}_d(\mathbb{R})$ et $x \in A$, alors le polynôme caractéristique de x est à coefficients dans k.*

Démonstration. D'après les propositions précédentes, pour $a \in$, $\mathrm{tr}(a) = \dfrac{1}{d}\mathrm{Tr}_{\mathrm{M}_d(\mathbb{R})}(a) = \dfrac{1}{d}\mathrm{Tr}_A(a) \in k$. Par les relations de Newton les coefficients de χ_x s'expriment comme polynômes à coefficients entiers en les $\mathrm{tr}(x^k)$, donc sont dans k. □

Corollaire 1. *Avec les même notations, si x est inversible dans $\mathrm{M}_d(\mathbb{R})$, son inverse est dans A.*

4.2 Les quaternions "généralisés"

Dans toute cette partie on prend $a, b \in \mathbb{Q}^*$ que l'on ajustera plus tard. L'idée est de construire l'algèbre à division requise dans le cas $d = 2$. Pour cela, nous généralisons la notion de quaternions. Les quaternions de Hamilton sont usuellement définis par $\mathbb{H} = \{\begin{pmatrix} u & -v \\ \overline{v} & \overline{u} \end{pmatrix}, u, v \in \mathbb{C}\}$. Via la base $\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \mathbf{I} = \begin{pmatrix} i & 0 \\ 0 & -1 \end{pmatrix}, \mathbf{J} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \mathbf{K} = \mathbf{IJ} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$, on vérifie qu'ils forment une $\mathbb{R}$-structure à division de $\mathrm{M}_2(\mathbb{C})$. Mais ici on veut une $\mathbb{Q}$-structure à division de $\mathrm{M}_2(\mathbb{R})$, il va falloir ajuster les choses.

Définition 8. On définit $(\dfrac{a,b}{\mathbb{Q}}) = \{\begin{pmatrix} u & bv \\ \overline{v} & \overline{u} \end{pmatrix}, u, v \in \mathbb{Q}(\sqrt{a})\} = \mathrm{Vect}_{\mathbb{Q}}(\mathbf{1}, \mathbf{I}, \mathbf{J}, \mathbf{K})$, où la conjugaison est cette fois ci l'automorphisme de $\mathbb{Q}(\sqrt{a})$ et $\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \mathbf{I} = \begin{pmatrix} \sqrt{a} & 0 \\ 0 & -\sqrt{a} \end{pmatrix}, \mathbf{J} = \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix}, \mathbf{K} = \mathbf{IJ} = \begin{pmatrix} 0 & b\sqrt{a} \\ -\sqrt{a} & 0 \end{pmatrix}$.

Si $a > 0$, on a bien une inclusion $\left(\frac{a,b}{\mathbb{Q}}\right) \subset \mathrm{M}_2(\mathbb{R})$. Comme il est clair que $\mathbf{1}, \mathbf{I}, \mathbf{J}, \mathbf{K}$ sont $\mathbb{R}$-libres, $\left(\frac{a,b}{\mathbb{Q}}\right)$ est bien une $\mathbb{Q}$-structure de $M_2(\mathbb{R})$. Si de plus a et b sont entiers $\mathrm{Vect}_{\mathbb{Z}}(\mathbf{1}, \mathbf{I}, \mathbf{J}, \mathbf{K})$ forme un ordre.

Il reste maintenant à ajuster a et b afin d'obtenir une algèbre à division. Pour cela, observons que le déterminant se calcule comme suit :

$$\det(x\mathbf{1} + y\mathbf{I} + z\mathbf{J} + t\mathbf{K}) = x^2 - ay^2 - bz^2 + abt^2.$$

Il s'agit donc de trouver a et b tels que ce déterminant soit non nul dès que $(x, y, z, t) \neq (0, 0, 0, 0)$, ce qui montrera que $\left(\frac{a,b}{\mathbb{Q}}\right)$ est à division d'après le corollaire 1. Or on dispose de la proposition suivante :

Proposition 15. *Si a est premier impair et b n'est pas un carré modulo a, la forme bilinéaire $(x, y, z, t) \mapsto \det(x\mathbf{1} + y\mathbf{I} + z\mathbf{J} + t\mathbf{K}) = x^2 - ay^2 - bz^2 + abt^2$ n'admet pas de zéros rationnels non triviaux.*

Démonstration. Supposons $x^2 - ay^2 - bz^2 + abt^2 = 0$, $(x, y, z, t) \neq 0$. Quitte à multiplier par le produit des dénominateurs on peut supposer que x, y, z, t sont entiers. Quitte à diviser par leur pgcd on peut les prendre premiers entre eux.

- Si $(x, z) \neq (0, 0) \mod a$, on obtient une solution non triviale à l'équation $u^2 - bv^2 = 0$ dans $\mathbb{Z}/a\mathbb{Z}$. C'est absurde car b est non carré modulo a.
- Si $(x, z) = (0, 0) \mod a$, $(z, t) \neq (0, 0) \mod a$ car les x, y, z, t sont premiers entre eux. Diviser par a l'égalité $x^2 - ay^2 - bz^2 + abt^2 = 0$ et la réduire modulo a : (z, t) donne aussi une solution non triviale à l'équation $u^2 - bv^2 = 0$ dans $\mathbb{Z}/a\mathbb{Z}$ et on obtient la même contradiction.

□

Des exemples de $\mathbb{Q}$-structure à division de $\mathrm{M}_2(\mathbb{R})$ existent donc. On peut par exemple imaginer que l'on a choisi $D = \left(\frac{3,2}{\mathbb{Q}}\right)$.

4.3 Outils en théorie des nombres

On veut à présent généraliser l'exemple des quaternions à une dimension d quelconque. Pour ce faire, certains outils supplémentaires vont être nécessaires, à commencer par

Théorème 3 (Dirichlet)**.** *Soit $a, n \in \mathbb{Z}$ premiers entre eux. Il existe (une infinité) de premiers $p \equiv a \mod n$.*

Démonstration. Admis ici. □

Nous utiliserons aussi des notions générales sur l'arithmétique des corps de nombres et leur anneau d'entiers.

Si K est un corps de nombres, on définit $\mathcal{O}_K$ son anneau d'entiers algébrique. On sait que c'est un anneau, mais il va en falloir un peu plus pour le comprendre. En particulier on veut montrer :

Théorème 4. *$\mathcal{O}_K$ est un groupe libre de rang $n = [K : \mathbb{Q}]$.*

Avant de le démontrer, faisons quelques observations.

Proposition 16. *Si $x \in K$, il existe $d \in \mathbb{Z}^*$ tel que $dx \in \mathcal{O}_K$.*

Démonstration. K étant un corps de nombre, x est algébrique d'où l'existence de $a_0, ..., a_{n-1} \in \mathbb{Q}$ tels que $x^n + a_{n-1}x^{n-1} + ... + a_0 = 0$, et il suffit de choisir d tel que $da_i \in \mathbb{Z}$, $\forall i$. □

En particulier, si on prend $e_1, ..., e_n$ une $\mathbb{Q}$-base de K, quitte à les multiplier par un entier on obtient le

Corollaire 2. *il existe une $\mathbb{Q}$-base de K constituée d'éléments de $\mathcal{O}_K$.*

Le dernier ingrédient utile pour démontrer le théorème est la trace Tr_K. Comme K admet une base dans $\mathcal{O}_K$, on en déduit que pour $x \in \mathcal{O}_K$, $\mathrm{Tr}_K(x) \in \mathbb{Z}$. De plus la forme bilinéaire sur $(x, y) \mapsto \mathrm{Tr}_K(xy)$ est symétrique et non dégénérée car si $x \in K$ vérifie $\mathrm{Tr}_K(xy) = 0 \forall y \in K$,en posant $X^r + a_{r-1}X^{r-1} + ... + a_0$ son polynôme minimal, $-na_0 = \mathrm{Tr}_K(x(x^{r-1} + a_{r-1}x^{r-2} + ... + a_1)) = 0$ et $x = 0$.

Démonstration. (du théorème)

Soit $e_1, ..., e_n$ une $\mathbb{Q}$-base de K dans $\mathcal{O}_K$. Soit $e_1^*, ..., e_n^*$ la base duale définie par $\mathrm{Tr}_K(e_i e_j^*) = \delta_{ij}$. On a alors l'encadrement

$$\mathrm{Vect}_{\mathbb{Z}}(e_1, ..., e_n) \subset \mathcal{O}_K \subset \frac{1}{n} \mathrm{Vect}_{\mathbb{Z}}(e_1^*, ..., e_n^*).$$

La première inclusion est évidente, et la deuxième vient du fait que si $x \in \mathcal{O}_K$ s'écrit $\sum_i \lambda_i e_i^*$ dans la base duale, en multipliant par e_j et prenant la trace : $n\lambda_j = \mathrm{Tr}_K(e_j x) \in \mathbb{Z}$.

$\mathcal{O}_K$ est donc coincé entre deux groupes libres de rang n : c'est une groupe libre de rang n. □

Remarquons que dans cette preuve, la difficulté n'est pas de sortir un sous-groupe libre de rang n de $\mathcal{O}_K$, mais plutôt de montrer pourquoi $\mathcal{O}_K$ est libre de rang $\leq n$. En fait, même le fait qu'il soit de type fini n'est pas évident.

Donnons une preuve alternative de ce résultat, reposant justement sur la notion de réseau et dont l'approche sera utile par la suite.

Soit r le nombre plongements réels $K \to \mathbb{R}$ et s le nombre de paires de plongements complexes conjugués $K \to \mathbb{C}$, avec donc $n = r + 2s$. Soit $\Phi : \begin{array}{ccc} K & \longrightarrow & \mathbb{R}^n \cong \mathbb{R}^r \times \mathbb{C}^s \\ x & \longmapsto & (\sigma_i(x))_i \end{array}$, où on ne compte qu'une seule fois chaque paire de morphismes complexes. Φ est donc un morphisme de groupes $\mathbb{Q}$-linéaire, injectif.

Ainsi, $\mathcal{O}_K \cong \Phi(\mathcal{O}_K)$ en tant que groupes. Or, nous allons voir que $\Phi(\mathcal{O}_K)$ est un sous-groupe discret de $\mathbb{R}^n$, soit donc un sous-réseau qui sera donc libre de rang $\leq n$.

Proposition 17. *$\Phi(\mathcal{O}_K)$ est un sous-groupe discret de $\mathbb{R}^n$.*

Démonstration. Montrons que l'intersection de $\Phi(\mathcal{O}_K)$ avec une boule $\overline{B}(0, R)$ est finie. Mais en effet si $x \in \mathcal{O}_K$ vérifie $|\sigma(x)| \leq R$ pour tout morphisme $\sigma : K \to \mathbb{C}$, alors son polynôme minimal μ, qui est de degré $\leq n$, admet pour racine seulement des $\sigma(x)$. D'après les relations racines-coefficients, on peut borner les coefficients de μ par une constante ne dépendant que de R.

Or, μ est à coefficients entier car $x \in \mathcal{O}_K$. Il n'existe donc qu'un nombre fini de polynômes minimaux possible pour x, donc un nombre fini de x vérifiant les conditions. Cela permet bien de conclure que $\Phi(\mathcal{O}_K)$ est discret. □

Remarque. $\mathcal{O}_K$ est donc un ordre dans K : mieux, c'est l'ordre maximal, dans le sens où tout ordre $\mathcal{O}$ est inclus dans $\mathcal{O}_K$.

Enfin, un dernier résultat nous sera utile sur le comportement des nombres premiers dans les extensions cyclotomiques :

Proposition 18. *Soit L_n la n-ième extension cyclotomique et p un premier dont la classe dans $\mathbb{Z}/n\mathbb{Z}$ génère $(\mathbb{Z}/n\mathbb{Z})^\times$. Alors $p\mathcal{O}_{L_n}$ est un idéal premier de $\mathcal{O}_{L_n}$.*

Démonstration. Soit $\mathfrak{m}$ un idéal maximal de $\mathcal{O}_{L_n}$ contenant $p\mathcal{O}_{L_n}$. L'objectif est de montrer que $p\mathcal{O}_{L_n} = \mathfrak{m}$. A cette fin il suffit de montrer l'égalité des indices $|\mathcal{O}_{L_n}/\mathfrak{m}|$ et $|\mathcal{O}_{L_n}/p\mathcal{O}_{L_n}|$. En effet, ce dernier est bien fini et vaut p^m, où $m = [L_n : \mathbb{Q}] = \phi(n)$ car $\mathcal{O}_{L_n}$ libre de rang d.

Quand à $\mathcal{O}_{L_n}/\mathfrak{m}$, c'est un corps fini de caractéristique p, c'est donc un extension de $\mathbb{F}_p$ de degré $f \leq m$. Supposons par l'absurde que $f < m$. Alors $\forall x \in \mathcal{O}_{L_n}/\mathfrak{m}, x^{p^f} - x = 0$. En particulier pour ω racine primitive n-ième de l'unité, $\omega \in \mathcal{O}_{L_n}^{\times}$ donc $\omega^{p^f-1} - 1 \equiv 0 \mod \mathfrak{m}$. Mais par hypothèse sur p, $p^f \neq 1 \mod n$ donc ω^{p^f-1} est une racine de l'unité différente de 1. Or, en dérivant le polynôme $X^n - 1$ puis l'évaluant en 0 on obtient la formule

$$\prod_{i=1}^{n-1}(1-\omega^i) = n.$$

On a donc $n \equiv 0 \mod \mathfrak{m}$, mais $\mathfrak{m} \cap \mathbb{Z}$ est un idéal strict de $\mathbb{Z}$ contenant $p\mathbb{Z}$: c'est $p\mathbb{Z}$. Comme p est premier à n par hypothèse, c'est absurde. □

Remarque. En observant cette preuve, on remarque que l'on utilise de l'égalité $[L_n : \mathbb{Q}] = \phi(n)$ seulement l'inégalité triviale $[L_n : \mathbb{Q}] \leq \phi(n)$: on n'utilise donc pas irréductibilité des polynômes cyclotomiques (ce qui n'est pas si important car on utilise le calcul de $Gal(L_n/\mathbb{Q})$ dans la partie suivante, mais mérite d'être noté).

4.4 Construction d'une algèbre à division sur $\mathbb{Q}$

Place maintenant à la construction générale de la proposition 10.

Etape 1 : On commence par choisir une extension cyclique L de $\mathbb{Q}$, réelle et de degré d.

Pour construire une telle extension, commençons par choisir $q \equiv 1 \mod 2d$ premier avec le théorème de Dirichlet. Soit $\zeta = \exp(\frac{2i\pi}{q})$ et $L_q = \mathbb{Q}(\zeta)$ la q-ième extension cyclotomique. L_q est galoisienne de groupe de Galois $(\mathbb{Z}/q\mathbb{Z})^{\times} \cong \mathbb{Z}/(q-1)\mathbb{Z}$ (car q est premier).

La conjugaison complexe τ est un morphisme d'ordre 2 de L_q, donc par correspondance de Galois, L_q^{τ} est une extension de $\mathbb{Q}$ galoisienne de groupe de Galois $G = \dfrac{\mathbb{Z}/(q-1)\mathbb{Z}}{\langle\tau\rangle}$ cyclique (car quotient d'un groupe cyclique), et réelle par définition.

Par construction de q, $d||G|$ on peut donc prendre H le sous-groupe de G d'indice d. Il correspond donc à une sous extension $L = (L_q^{\tau})^H$, réelle, de degré d et de groupe de Galois G/H, donc cyclique. Dans la suite on fixe σ un générateur de son groupe de Galois.

Etape 2 : On construit à présent un surcorps non commutatif de dimension d sur L.

A cette fin, considérons les "polynômes non commutatifs" sur L : $L^*[T]$ définis par la loi de multiplication $\forall l \in L, Tl = \sigma(l)T$. On en déduit que $T^d l = \sigma^d(l)T^d = lT$, donc pour $p \in \mathbb{Q}$ (que nous choisirons plus tard), $T^d - p$ est dans le centre de $L^*[T]$, donc l'idéal engendré est un idéal bilatère.

On prend alors $D = L^*[T]/(T^d - p)$, qui est (en tant qu'ev) de dimension d sur L avec comme base naturelle $\mathcal{B} = (1, T, ..., T^{d-1})$ (on note encore T la classe de T dans le quotient). C'est donc bien une algèbre de dimension d^2 sur $\mathbb{Q}$, et de centre $\mathbb{Q}$. Avec la proposition 11, on sait qu'on peut choisir un ordre dans D. Mais si $p \in \mathbb{Z}$, on peut en choisir un disingué : $\mathcal{O} = \mathrm{Vect}_{\mathcal{O}_K}(1, ..., T^{d-1})$.

Remarque. Dans cette construction, L est appelée une "algèbre cyclique".

Etape 3 : On dispose donc de cette algèbre de la bonne dimension, mais on veut la voir comme une algèbre de matrice. Or, faire agir D par multiplication à gauche sur elle même donne un plongement dans $\mathrm{M}_{d^2}(\mathbb{Q})$, et ce n'est pas ce que l'on veut. La multiplication à gauche n'est pas L-linéaire (à cause du défaut de commutativité) et de permet donc pas d'avoir un plongement dans $\mathrm{M}_d(L)$. En

revanche la multiplication à droite par un élément de D est bien L-linéaire et donne une inclusion $\begin{array}{ccc} D & \xrightarrow{i} & \mathrm{M}_d(L) \\ d & \longmapsto & (x \mapsto xd) \end{array}$. (via la base $\mathcal{B}$). Mais le produit se fait à l'envers : $i(xy) = i(y)i(x)$. Pour résoudre ce souci on peut composer i avec la transposition, ce qui revient à faire agir D non pas sur lui-même mais sur son dual $L_L(D, L)$. On obtient, en faisant le calcul, le plongement

$$\Theta : \begin{array}{ccc} D & \longrightarrow & \mathrm{M}_d(L) \\ l_0 + ... + l_{d-1}T^{d-1} & \longmapsto & \begin{pmatrix} l_0 & l_1 & l_2 & ... & l_{d-1} \\ p\sigma l_{d-1} & \sigma l_0 & \sigma l_1 & ... & \sigma l_{d-2} \\ p\sigma^2 l_{d-2} & p\sigma^2 l_{d-1} & \sigma^2 l_0 & ... & \sigma^2 l_{d-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ p\sigma^{d-1} l_1 & p\sigma^{d-1} l_2 & p\sigma^{d-1} l_3 & ... & \sigma^{d-1} l_0 \end{pmatrix} \end{array}$$

Ainsi $\Theta(\mathcal{O})$ est un groupe libre de rang d^2, qui s'avère être discret dans $\mathrm{M}_d(\mathbb{R})$ pour la même raison que $\Phi(\mathcal{O}_K)$ dans la Proposition 17, qui montre que $\mathcal{O}_K$ est un ordre dans K. $\Theta(\mathcal{O})$ est donc bien un ordre de $\mathrm{M}_d(\mathbb{R})$, et donc $\Theta(D)$ en est bien une $\mathbb{Q}$-structure.

Remarque. On aurait pu travailler aussi directement avec i au lieu de Θ car toutes les propriétés de D qui nous intéressent sont stables par renversement de la multiplication.

Etape 4 : On cherche à présent à ajuster le paramètre p, que l'on suppose à présent premier, pour obtenir une algèbre à division. Il suffit pour cela, d'après le corollaire 1, de montrer que le déterminant $\det \Phi(d)$ est non nul dès que $d \neq 0$. Ecrivons $d = l_0 + ... + l_{d-1}T^{d-1}$, et supposons pour l'instant que

1. $d \in \mathcal{O}$,
2. $l_0 \notin p\mathcal{O}_L$.

Alors $\det \Phi(d) \equiv l_0\sigma(l_0)...\sigma^{d-1}(l_0) \mod p\mathcal{O}_L$. Si p reste premier dans $\mathcal{O}_L$, ce déterminant est non nul mod p donc est bien non nul. Pour cela il suffit, comme $L \subset L_q$, que p reste premier dans $\mathcal{O}_{L_q}$. D'après la proposition 18, il faut que p génère $(\mathbb{Z}/q\mathbb{Z})^\times$, mais $(\mathbb{Z}/q\mathbb{Z})^\times$ est bien cyclique (on rappelle que q est premier) et le théorème de Dirichlet permet bien de choisir un tel p.

Montrons que quitte à multiplier d par un inversible, on peut supposer que nos conditions sont remplies.

1. La première est facile : par la proposition 16 on peut multiplier d par un entier suffisamment grand et tous les $l_i \in \mathcal{O}_L$.
2. Pour la deuxième, remarquons que $\mathcal{O}_L$ étant libre sur $\mathbb{Z}$, un élément non nul de $\mathcal{O}_L$ ne peut pas être divisible par des puissances arbitrairement grandes de p. Quitte à diviser d par la bonne puissance de p, on peut supposer que $d \in \mathcal{O}$ mais que l'un des $l_i \notin p\mathcal{O}_L$. Si l'on note i le plus petit tel indice, $\frac{1}{T^i}d$ vérifie bien la condition requise.

D est donc bien une algèbre à division.

Remarque. Comme on le voit bien dans la version matricielle de D, l'algèbre $\left(\frac{a,b}{\mathbb{Q}}\right)$ est un cas particulier d'algèbre cyclique de dimension 2^2, avec $L = \mathbb{Q}(\sqrt{a})$ (réelle, cyclique de degré 2), puis T correspond à $\mathbf{J}$ et p correspond à b.

5 Conclusion

On a montré l'existence des réseaux cocompacts dans $\mathrm{SL}_d(\mathbb{R})$. On voit que les méthodes utilisées proviennent de domaines mathématiques divers — topologie, géométrie, algèbre et arithmétique — et illustrent une fois encore combien les mathématiques constituent un ensemble profondément unifié.

Une question naturelle est la suivante : est-ce que tous les réseaux cocompacts de $\mathrm{SL}_d(\mathbb{R})$ peuvent être construits via cette méthode ? La réponse est positive pour $d \geq 2$. Un théorème célèbre de Margulis, beaucoup plus difficile, affirme que pour la plupart des groupes de Lie, leurs réseaux cocompacts peuvent tous être construits par la méthode arithmétique décrite dans ce mémoire. Ce théorème révèle un lien plus profond entre les groupes de Lie et la théorie des nombres. Il a pour corollaire les théorèmes de rigidité mentionnés dans l'introduction.

Références

[1] Yves Benoist. Five lectures on lattices in semisimple Lie groups. In *Géométries à courbure négative ou nulle, groupes discrets et rigidités*, volume 18 of *Sémin. Congr.*, pages 117–176. Soc. Math. France, Paris, 2009.

[2] Armand Borel. *Introduction aux groupes arithmétiques*, volume No. 1341 of *Publications de l'Institut de Mathématique de l'Université de Strasbourg, XV. Actualités Scientifiques et Industrielles*. Hermann, Paris, 1969.

[3] Pascal Molin et Sylvain Rairat. Le théorème de Kronecker-Weber. 2004.