

Feuille d'exercices 4

Réseaux

Exercice 1. Dans la suite K est l'un des corps $\mathbb{Q}$ ou $\mathbb{R}$ et V est un K -espace vectoriel de dimension finie $n > 0$. Une partie Γ de V est un sous-réseau s'il existe une famille libre $\mathbf{e} = (e_1, \dots, e_r)$ de V telle que $\Gamma = \mathbb{Z}e_1 + \dots + \mathbb{Z}e_r$. On dit que $\mathbf{e}$ est une $\mathbb{Z}$ -base de Γ et r est son rang. On dit que Γ est un réseau si $r = n$.

- $\mathbb{Z} + \sqrt{2}\mathbb{Z}$ est-il un sous-réseau de $\mathbb{R}$?
- Soit Γ un réseau de V , $\mathbf{e}$ une $\mathbb{Z}$ -base de Γ et $\mathbf{v}$ une base de V . Montrez que $\mathbf{v}$ est une $\mathbb{Z}$ -base de Γ si et seulement si la matrice de passage de $\mathbf{e}$ à $\mathbf{v}$ appartient à $GL_n(\mathbb{Z})$.
- Soient Γ un réseau de V et $\Lambda \subset \Gamma$ un sous-groupe. Montrez que Λ est un sous-réseau de V et qu'il existe une $\mathbb{Z}$ -base $(e_1, \dots, e_n)$ de Γ , $1 \leq s \leq n$ et $a_1, \dots, a_s \in \mathbb{Z}^\times$ vérifiant :
 - $(a_1e_1, \dots, a_se_s)$ est une $\mathbb{Z}$ -base de Λ ,
 - pour $1 \leq i < s$, a_i divise a_{i+1}

En déduire une CNS pour que Γ/Λ soit fini et calculez son cardinal en fonction des a_i .

- On suppose ici $K = \mathbb{Q}$. Soient Γ, Λ des réseaux de V . Montrez que
 - il existe $d \in \mathbb{N} \setminus \{0\}$ tel que $d\Gamma \subset \Lambda$,
 - $\Gamma + \Lambda$ et $\Gamma \cap \Lambda$ sont des réseaux de V .
- On suppose ici $K = \mathbb{R}$ et on munit V de sa topologie canonique. Montrez que tout sous-groupe discret¹ Γ de V en est un sous-réseau.

Indication: soit $(e_1, \dots, e_r)$ une famille libre maximale de Γ et $\mathcal{K} = \{\lambda_1e_1 + \dots + \lambda_re_r; \lambda_i \in [0, 1]\}$. En utilisant le fait que $\mathcal{K} \cap \Gamma$ est fini et en considérant pour $j \in \mathbb{Z}$ et $x = \lambda_1e_1 + \dots + \lambda_re_r \in \Gamma$, les $x_j = jx - ([j\lambda_1]e_1 + \dots + [j\lambda_r]e_r)^2$, montrez que $\lambda_i \in \mathbb{Q}$ et concluez.

A quelles conditions est-ce un réseau?

Preuve: (i) $\sqrt{2}$ n'appartenant pas à $\mathbb{Q}$, $G = \mathbb{Z} + \sqrt{2}\mathbb{Z}$ est dense dans $\mathbb{R}$; si G était un réseau on aurait $G = \alpha\mathbb{Z}$ et serait discret, ce qui n'est pas.

(ii) Si $\mathbf{v}$ est une $\mathbb{Z}$ -base de Γ , la matrice de passage de $\mathbf{e}$ à $\mathbf{v}$ et celle de $\mathbf{v}$ à $\mathbf{e}$ sont à coefficients dans $\mathbb{Z}$ et sont inverses l'une de l'autre, d'où le résultat. Réciproquement soit P (resp. P^{-1}) la matrice de passage de $\mathbf{e}$ à $\mathbf{v}$ (reps. de $\mathbf{v}$ à $\mathbf{e}$). Comme P est à coefficients dans $\mathbb{Z}$, le réseau engendré par $\mathbf{e}$ est inclus dans celui engendré par $\mathbf{v}$; l'inclusion inverse découle de même du fait que P^{-1} est à coefficients dans $\mathbb{Z}$.

(iii) C'est le théorème (??) du cours, i.e. le théorème de la base adaptée, sur les modules de type fini sur un anneau principal. Le quotient Γ/Λ est fini si et seulement si les deux réseaux ont le même rang et alors le cardinal est égal à la valeur absolue du produit des a_i , $1 \leq i \leq n$.

¹i.e. tel que pour tout compact $\mathcal{K}$ de V , $\mathcal{K} \cap \Gamma$ est fini

² $[\lambda]$ désigne la partie entière de λ

(iv) - Soient $\mathbf{e}$ et $\mathbf{f}$ des $\mathbb{Z}$ -bases de respectivement Γ et Λ . On note $P = (p_{i,j})_{1 \leq i,j \leq n} \in GL_n(\mathbb{Q})$ la matrice de passage de $\mathbf{f}$ à $\mathbf{e}$ et soit d le ppcm des dénominateurs des $p_{i,j}$, $1 \leq i, j \leq n$, écrits sous formes irréductibles. Il est alors clair que l'on a $d\Gamma \subset \Lambda$.

- Soit d comme ci-dessus. On a alors

$$d\Gamma \subset \Gamma \cap \Lambda \subset \Gamma$$

$$\Gamma \subset \Gamma + \Lambda \subset d^{-1}\Lambda$$

L'inclusion $\Gamma \cap \Lambda \subset \Gamma$ (resp. $\Gamma + \Lambda \subset d^{-1}\Lambda$) prouve d'après (iii) que $\Gamma \cap \Lambda$ (resp. $\Gamma + \Lambda$) est un sous-réseau de Γ (resp. $d^{-1}\Lambda$). Les autres inclusions montrent que $\Gamma + \Lambda$ et $\Gamma \cap \Lambda$ sont de rang n .

(v) On procède comme suggéré dans l'indication; $\mathcal{K}$ étant compact, $\mathcal{K} \cap \Gamma$ est fini; on note $y_1, \dots, y_s$ ses éléments. Soit $x = \sum_{i=1}^r \lambda_i e_i \in \Gamma$, $\lambda_i \in \mathbb{R}$. On considère pour $j \in \mathbb{Z}$, $x_j = jx - \sum_{i=1}^r [j\lambda_i]e_i$; $x_j \in \Gamma \cap \mathcal{K}$ de sorte qu'il existe $j \neq k$ tels que $x_j = x_k$, soit $(j-k)\lambda_i = [j\lambda_i] - [k\lambda_i]$ pour $1 \leq i \leq r$ et donc $\lambda_i \in \mathbb{Q}$. Pour $1 \leq i \leq s$, on écrit $y_i = \sum_{k=1}^r \lambda_k^i e_k$ avec $\lambda_k^i \in \mathbb{Q}$ et soit d le ppcm des dénominateurs des λ_k^i écrits sous forme irréductible. De l'égalité $x = x_1 + \sum_{i=1}^r [\lambda_i]e_i$, on en déduit $dx \in \mathbb{Z}e_1 + \dots + \mathbb{Z}e_r$ soit $d\Gamma \subset \mathbb{Z}e_1 + \dots + \mathbb{Z}e_r$, soit $\Gamma \subset \mathbb{Z}d^{-1}e_1 + \dots + \mathbb{Z}d^{-1}e_r = \Lambda$ et ainsi Γ est un sous-groupe du sous-réseau Λ de V et donc Γ est un sous-réseau de V . En outre Γ est un réseau de V si et seulement si Γ est discret et V/Γ est compact. □

Exercice 2. On reprend les notations de l'exercice précédent avec $K = \mathbb{R}$. On note μ la mesure de Lebesgue de $\mathbb{R}^n$, $(\epsilon_1, \dots, \epsilon_n)$ sa base canonique et $(\cdot|\cdot)$ le produit scalaire associé $(\epsilon_i|\epsilon_j) = \delta_{i,j}$. Pour Γ un réseau de $\mathbb{R}^n$ et $\mathbf{e} = (e_1, \dots, e_n)$ une $\mathbb{Z}$ -base de Γ , on pose

$$- P_{\mathbf{e},\Gamma} = \left\{ \sum_{i=1}^n \lambda_i e_i; \lambda_1, \dots, \lambda_n \in [0, 1] \right\},$$

$$- D_{\mathbf{e},\Gamma} = \left\{ \sum_{i=1}^n \lambda_i e_i; \lambda_1, \dots, \lambda_n \in [0, 1[\right\},$$

On note $S_{\mathbf{e},\Gamma}$ (resp. $T_{\mathbf{e},\Gamma}$) la matrice de terme général $(e_i|e_j)$ (resp. $(\epsilon_i|\epsilon_j)$).

(a) Montrez que $S_{\mathbf{e},\Gamma} = {}^t T_{\mathbf{e},\Gamma} T_{\mathbf{e},\Gamma}$. En utilisant la formule du jacobien pour le changement de variables dans les intégrales multiples, en déduire l'égalité $\mu(P_{\mathbf{e},\Gamma}) = \sqrt{\det S_{\mathbf{e},\Gamma}}$. Montrez ensuite que $\mu(P_{\mathbf{e},\Gamma})$ ne dépend que de Γ et non de $\mathbf{e}$; on dit que c'est la mesure du réseau et on la note $\mu(\mathbb{R}^n/\Gamma)$.

(b) Une partie $\mathcal{D}$ de $\mathbb{R}^n$ est un domaine fondamental de Γ , si $\mathcal{D}$ est μ -mesurable et si ses translatés par les vecteurs de Γ forment une partition de $\mathbb{R}^n$. Montrez que $D_{\mathbf{e},\Gamma}$ est un domaine fondamental et que $\mu(\mathcal{D}) = \mu(\mathbb{R}^n/\Gamma)$ pour tout domaine fondamental $\mathcal{D}$ de Γ .

(c) En utilisant le théorème de la base adaptée, montrez que si $\Lambda \subset \Gamma$ sont des réseaux alors Γ/Λ est fini et

$$\mu(\mathbb{R}^n/\Lambda) = \text{card}(\Gamma/\Lambda) \mu(\mathbb{R}^n/\Gamma)$$

(d) (i) Soit $\varphi : \mathbb{R}^n \longrightarrow \mathbb{R}^n/\Gamma$ la surjection canonique associée au réseau Γ et soit F une partie de $\mathbb{R}^n$, μ -mesurable vérifiant $\mu(F) > \mu(\mathbb{R}^n/\Gamma)$. Montrez que la restriction de φ à F n'est pas injective.

- (ii) Dédurre de (i), le théorème de Minkowski: soient Γ un réseau de $\mathbb{R}^n$ et A une partie μ -mesurable, convexe, symétrique par rapport à O et vérifiant $\mu(A) > 2^n \mu(\mathbb{R}^n/\Gamma)$, alors $A \cap \Gamma \neq \{O\}$.
- (iii) Montrez que si C est un convexe compact de $\mathbb{R}^n$, symétrique par rapport à O tel que $\mu(C) \geq 2^n \mu(\mathbb{R}^n/\Gamma)$ alors $C \cap \Gamma \neq \{O\}$.
- (iv) Soit v_n le volume de la boule unité fermée de $\mathbb{R}^n$. Montrez qu'il existe $\gamma \in \Gamma$ différent de O et de norme inférieure ou égale à deux fois la racine n -ième de $v_n^{-1} \mu(\mathbb{R}^n/\Gamma)$.

Preuve: (a) L'égalité $S_{\mathbf{e},\Gamma} = {}^t T_{\mathbf{e},\Gamma} T_{\mathbf{e},\Gamma}$ découle directement des formules classiques du cours d'algèbre bilinéaire en remarquant par exemple que $T_{\mathbf{e},\Gamma}$ est la matrice de passage de la base $\mathbf{e}$ à la base canonique; ainsi on a $\det S_{\mathbf{e},\Gamma} = (\det T_{\mathbf{e},\Gamma})^2 \geq 0$. En outre, par la formule du changement de variable dans une intégrale multiple via le jacobien, on a $\mu(P_{\mathbf{e},\Gamma}) = \int_{P_{\mathbf{e},\Gamma}} d\mu = \int_0^1 \cdots \int_0^1 |\det T_{\mathbf{e},\Gamma}| dx_1 \cdots dx_n$, soit $\mu(P_{\mathbf{e},\Gamma}) = \sqrt{\det S_{\mathbf{e},\Gamma}}$.

Si $\mathbf{f}$ est une autre $\mathbb{Z}$ -base de Γ , on note Q la matrice de passage de $\mathbf{e}$ à $\mathbf{f}$; $Q \in GL_n(\mathbb{Z})$ et $S_{\mathbf{f},\Gamma} = {}^t Q S_{\mathbf{e},\Gamma} Q$, soit $\det S_{\mathbf{f},\Gamma} = \det S_{\mathbf{e},\Gamma} (\det Q)^2$; or comme $Q \in GL_n(\mathbb{Z})$, on a $\det Q \in \mathbb{Z}^\times$, soit $\det Q = \pm 1$, d'où le résultat.

(b) $D_{\mathbf{e},\Gamma}$ est évidemment un domaine fondamental. Soient alors $\mathcal{D}_1$ et $\mathcal{D}_2$ des domaines fondamentaux quelconques. En considérant $\mathcal{D}_2$ comme un domaine fondamental, on écrit

$$\mathcal{D}_1 = \coprod_{v \in \Gamma} \mathcal{D}_1 \cap (v + \mathcal{D}_2),$$

Γ étant dénombrable et μ étant invariante par translation, on a

$$\begin{aligned} \mu(\mathcal{D}_1) &= \sum_{v \in \Gamma} \mu(\mathcal{D}_1 \cap (v + \mathcal{D}_2)) \\ &= \sum_{v \in \Gamma} \mu((-v + \mathcal{D}_1) \cap \mathcal{D}_2) \end{aligned}$$

Or comme $-\Gamma = \Gamma$, on en déduit $\mu(\mathcal{D}_1) = \sum_{v \in \Gamma} \mu(\mathcal{D}_2 \cap (v + \mathcal{D}_1)) = \mu(\mathcal{D}_2)$, la dernière égalité découlant du fait que $\mathcal{D}_1$ est un domaine fondamental.

(c) D'après le théorème de la base adaptée, il existe une $\mathbb{Z}$ -base $\mathbf{v} = (v_1, \dots, v_n)$ de Γ et des entiers $a_1 | a_2 | \cdots | a_n$ tels que $\mathbf{w} = (a_1 v_1, \dots, a_n v_n)$ est une $\mathbb{Z}$ -base de Λ . Ainsi on obtient $\text{card}(\Gamma/\Lambda) = \prod_{i=1}^n a_i$ et $S_{\mathbf{w},\Lambda} = {}^t D S_{\mathbf{v},\Gamma} D$ avec $D = \text{diag}(a_1, \dots, a_n)$, d'où le résultat.

(d) (i) Soit $\mathcal{D}$ un domaine fondamental:

$$\mu(F) = \sum_{\gamma \in \Gamma} \mu(F \cap (\gamma + \mathcal{D})) = \sum_{\gamma \in \Gamma} \mu((F - \gamma) \cap \mathcal{D}) > \mu(D)$$

d'où il en résulte que les $(F - \gamma) \cap \mathcal{D}$ pour $\gamma \in \Gamma$ ne sont pas deux à deux disjoints. Soient donc $x, y \in F$ et $\alpha \neq \beta \in \Gamma$ vérifiant $x - \alpha = y - \beta$ soit $x - y = \alpha - \beta \in \Gamma \setminus \{O\}$ et donc φ non injective.

(ii) Soit $F = \frac{1}{2}A$; on a donc $\mu(F) > \mu(\mathbb{R}^n/\Gamma)$. D'après la question précédente, il existe donc $x, y \in F$ tels que $x - y \in \Gamma \setminus \{O\}$. En outre $2x$ et $-2y$ appartiennent à A d'après la propriété de symétrie de A par rapport à O , et donc $x - y = \frac{(2x-2y)}{2}$ appartient à A d'après la propriété de convexité de A , d'où le résultat.

(iii) Soit $C_r = (1+1/r)C$ pour $r \geq 1$; $C = \bigcap_{r \geq 1} C_r$ et $\mu(C_r) > 2^n \mu(\mathbb{R}^n/\Gamma)$. D'après la question précédente, soit $x_r \in C_r \cap (\Gamma \setminus \{O\}) \subset K := 2C \cap (\Gamma \setminus \{O\})$; K étant fini, on peut extraire de la suite $(x_r)_{r \geq 1}$ une sous-suite convergente, donc stationnaire, d'où le résultat.

(iv) Une boule $\overline{B}(O, r)$ vérifie $\overline{B}(O, r) \cap (\Gamma \setminus \{O\}) \neq \emptyset$ dès que $v_n r^n \geq \mu(\mathbb{R}^n/\Gamma)$, d'où le résultat. $\square$

Exercice 3. *Quelques applications arithmétiques:*

- (a) Soient $\epsilon > 0$ et $(\alpha_1, \dots, \alpha_n) \in \mathbb{R}^n \setminus \mathbb{Q}^n$; montrez qu'il existe $p_1, \dots, p_n \in \mathbb{Z}$ et $q \in \mathbb{N}$ non nul tels que pour tout $1 \leq i \leq n$, on ait $|\alpha_i - \frac{p_i}{q}| < \frac{\epsilon}{q}$.

Indication: considérez le groupe Γ engendré par les vecteurs de la base canonique et le vecteur $(\alpha_1, \dots, \alpha_n)$ et remarquez que Γ n'est pas un réseau et n'est donc pas discret.

- (b) Montrez que si $p \equiv 1 \pmod{4}$, p premier, alors p est somme de deux carrés.

Indication: (-1) étant un carré modulo p , soit $u \in \mathbb{Z}$ tel que $u^2 + 1 \equiv 0 \pmod{p}$ et soit $\Gamma = \{(a, b) \in \mathbb{Z}^2 \mid a \equiv ub \pmod{p}\}$. Soit $\psi : \mathbb{Z}^2 \rightarrow \mathbb{Z}/p\mathbb{Z}$ défini par $\psi(a, b) = \overline{a - ub}$. Montrez que Γ est un réseau de mesure p et utilisez le point (d) (iv) de l'exercice précédent.

- (c) Montrez que tout nombre premier p est somme de quatre carrés.

Indication: montrez l'existence d'un couple $(u, v) \in \mathbb{Z}^2$ tel que $u^2 + v^2 + 1 \equiv 0 \pmod{p}$. On fixe un tel couple et soit $\Gamma = \{(a, b, c, d) \in \mathbb{Z}^4 \mid ua + vb \equiv c \pmod{p} \text{ et } ub - va \equiv d \pmod{p}\}$. Soit $\psi : \mathbb{Z}^4 \rightarrow (\mathbb{Z}/p\mathbb{Z})^2$ défini par $\psi(a, b, c, d) = (\overline{c - ua - vb}, \overline{d + va - ub})$. Montrez que Γ est un réseau de $\mathbb{R}^4$ de mesure p^2 et utilisez le point (d) (iv) de l'exercice précédent.

Preuve: (a) Soit Γ le groupe engendré par $(e_1, \dots, e_n, e_0)$ où $e_1, \dots, e_n$ sont les vecteurs de la base canonique de $\mathbb{R}^n$ et $e_0 = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$. Si Γ était discret, il serait un réseau; soit $\mathbf{f}$ une

$\mathbb{Z}$ -base de Γ et P la matrice de passage de $(e_1, \dots, e_n)$ à $\mathbf{f}$, $P \in M_n(\mathbb{Z})$ et $P^{-1} \in M_n(\mathbb{Q})$ de sorte que e_0 est une combinaison linéaire à coefficients dans $\mathbb{Q}$ des e_i , ce qui n'est pas. Ainsi Γ n'est pas discret et admet un point d'accumulation P . Soit alors $\epsilon > 0$ avec $\overline{B}(O, \epsilon) \cap \Lambda = \{O\}$, où Λ est le réseau $\mathbb{Z}e_1 + \dots + \mathbb{Z}e_n$; il existe alors des entiers comme dans l'énoncé tels que $(qe_0 + p_1e_1 + \dots + p_ne_n) - (q'e_0 + p'_1e_1 + \dots + p'_ne_n)$ soit de norme inférieure à ϵ avec $q - q' \neq 0$, d'où le résultat.

car $\gamma \notin \Lambda$, d'où le résultat.

(b) Soit x un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$; on a $x^{p-1} = 1$ et $u = x^{p-1/4}$ est d'ordre 4, soit u^2 d'ordre 2; or dans un corps commutatif de caractéristique différent de 2, il y a exactement un élément d'ordre 2, i.e. -1 ; en effet l'équation $X^2 - 1$ y a au plus deux solutions. Soit alors $\Gamma = \{(a, b) \in \mathbb{Z}^2 \mid a \equiv ub \pmod{p}\}$ et $\psi : \mathbb{Z}^2 \rightarrow \mathbb{Z}/p\mathbb{Z}$ défini par $\psi(a, b) = \overline{a - ub}$; ψ est clairement surjective et son noyau est Γ de sorte que ψ induit un isomorphisme $\mathbb{Z}^2/\Gamma \simeq \mathbb{Z}/p\mathbb{Z}$. On en déduit donc que Γ est un réseau de mesure p car $\mu(\mathbb{R}^2/\mathbb{Z}^2) = 1$. D'après l'exercice précédent question (d) (iv), il existe donc $\gamma = ae_1 + be_2 \neq O \in \Gamma$ de module inférieur ou égal à $2\sqrt{\frac{p}{\pi}}$, soit $0 < a^2 + b^2 \leq 4p/\pi < 2p$; or comme $\gamma \in \Gamma$, on a $a^2 + b^2 \equiv b^2(u^2 + 1) \equiv 0 \pmod{p}$, d'où $a^2 + b^2 = p$.

(c) Le cas $p = 2 = 1^2 + 1^2 + 0^2 + 0^2$ est vite traité, soit donc $p \geq 3$ premier. Soit $\phi : (\mathbb{Z}/p\mathbb{Z})^\times \rightarrow (\mathbb{Z}/p\mathbb{Z})^\times$ défini par $\phi(x) = x^2$; $\mathbb{Z}/p\mathbb{Z}$ étant un corps, $\text{Ker } \phi = \{1, -1\}$ de sorte que $\mathbb{I}\phi$ est de cardinal $(p-1)/2$. En remarquant que 0 est un carré, on en déduit que $\{u^2 \mid u \in \mathbb{Z}/p\mathbb{Z}\}$ est de cardinal $(p+1)/2$ et qu'il en est de même pour $\{1 - v^2 \mid v \in \mathbb{Z}/p\mathbb{Z}\}$; comme $2(p+1)/2 > p$ on en déduit que $\{u^2 \mid u \in \mathbb{Z}/p\mathbb{Z}\} \cap \{1 - v^2 \mid v \in \mathbb{Z}/p\mathbb{Z}\}$ est non vide, et on fixe u, v tels que $u^2 + v^2 + 1 \equiv 0 \pmod{p}$. Avec les notations de l'énoncé, ψ est clairement surjective et son noyau est le groupe Γ ; ψ induit donc un isomorphisme $\mathbb{Z}^4/\Gamma \simeq (\mathbb{Z}/p\mathbb{Z})^2$. On en déduit donc que Γ est un réseau de mesure p^2 . D'après le point (d) (iv) de l'exercice précédent, soit

$\gamma = (a, b, c, d) \in \Gamma \setminus \{O\}$ de norme au carré inférieure ou égale à $4\sqrt{2}p/\pi < 2p$. Or comme $\gamma \in \Gamma$, on a $a^2 + b^2 + c^2 + d^2 \equiv (a^2 + b^2)(u^2 + v^2 + 1) \equiv 0 \pmod{p}$, soit $p = a^2 + b^2 + c^2 + d^2$.

Remarque: En utilisant l'identité remarquable³

$$\begin{aligned} (a^2 + b^2 + c^2 + d^2)(\alpha^2 + \beta^2 + \gamma^2 + \delta^2) &= (a\alpha - b\beta - c\gamma - d\delta)^2 + (a\beta + b\alpha + c\delta - d\gamma)^2 + \\ &\quad + (a\gamma + c\alpha + d\beta - b\delta)^2 + (a\delta + b\gamma + d\alpha - c\beta)^2 \end{aligned}$$

on en déduit que tout entier est somme de quatre carrés.

□

³cf. le corps des quaternions