Algèbre 03 – Sous-groupes discrets de $\mathbb{R}^n$. Réseaux.

1. Réseaux et sous-réseaux

Définition. Une partie Γ de $\mathbb{R}^n$ est dite *discrète* si la topologie induite par $\mathbb{R}^n$ sur Γ est la topologie discrète.

Proposition. *Une partie fermée Γ de $\mathbb{R}^n$ est discrète si et seulement si $\Gamma \cap K$ est fini pour tout compact K de $\mathbb{R}^n$.*

Notons qu'un sous-groupe discret de $\mathbb{R}^n$ est fermé.

Proposition. *Si Γ est un sous-groupe discret de $\mathbb{R}^n$ alors il existe $1 \leq p \leq n$ et $e_1, \dots, e_p$ dans $\mathbb{R}^n$ linéairement indépendants sur $\mathbb{R}$ tels que $\Gamma = \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_p$.*

Définition. On dit que Γ est un *sous-réseau* de $\mathbb{R}^n$ s'il existe $1 \leq p \leq n$ et $e_1, \dots, e_p$ linéairement indépendants sur $\mathbb{R}$ tels que $\Gamma = \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_p$. On dit alors que $(e_1, \dots, e_p)$ est une *$\mathbb{Z}$-base* de Γ.

Proposition. *Toutes les $\mathbb{Z}$-bases d'un sous-réseau ont le même cardinal ; on l'appelle le rang du sous-réseau.*

Proposition. *Soit $\mathcal{E}$ une $\mathbb{Z}$-base d'un sous-réseau Γ de rang r et $\mathcal{V}$ une base de $\mathrm{Vect}(\Gamma)$, on note $P \in GL_r(\mathbb{R})$ la matrice de passage de $\mathcal{E}$ à $\mathcal{V}$. Alors $\mathcal{V}$ est une $\mathbb{Z}$-base de Γ si et seulement si $P \in GL_r(\mathbb{Z})$.*

Définition. Un sous-réseau de $\mathbb{R}^n$ de rang n est appelé un *réseau* de $\mathbb{R}^n$.

Exemple. $\mathbb{Z} + \sqrt{2}\mathbb{Z}$ est une partie de $\mathbb{R}$ qui n'est pas un réseau de $\mathbb{R}$.

Exemple. $\mathbb{Z}[i] = \mathbb{Z} + i\mathbb{Z}$ est un réseau de $\mathbb{R}^2$ (que l'on identifie à $\mathbb{C}$).

Proposition. *Si Γ est un sous-groupe de $\mathbb{R}^n$ alors les assertions suivantes sont équivalentes :*

- *(i) Γ est un réseau de $\mathbb{R}^n$*
- *(ii) Γ est discret et $\mathbb{R}^n/\Gamma$ est compact*
- *(iii) Γ est discret et de rang n*
- *(iv) Γ est discret et engendre $\mathbb{R}^n$*

Exemple. $\mathbb{Z}^2$ est un réseau de $\mathbb{R}^2$ donc $\mathbb{R}^2/\mathbb{Z}^2$ est compact.

Application. Soit $\theta_1, \dots, \theta_n$ des réels dont au moins un est irrationnel et soit $\varepsilon > 0$. Alors il existe $p_1, \dots, p_n \in \mathbb{Z}$ et $q \geq 1$ tels que $\left|\theta_i - \frac{p_i}{q}\right| \leq \frac{\varepsilon}{q}$.

Théorème de la base adaptée. *Soit Γ un réseau de $\mathbb{R}^n$ et Λ un sous-réseau de Γ de rang $m \leq n$. Alors il existe $e_1, \dots, e_n$ tels que $\Gamma = \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_n$ et il existe des entiers non nuls $d_1, \dots, d_n$ tels que d_j divise d_{j+1} et vérifiant*

$$\Lambda = \mathbb{Z}d_1e_1 \oplus \cdots \oplus \mathbb{Z}d_me_m.$$

Application. Si G est un groupe abélien de type fini alors il existe un entier $r \geq 0$ et des entiers $a_1, \dots, a_m \geq 1$ tels que a_j divise a_{j+1} est vérifiant $G = \mathbb{Z}^r \oplus \mathbb{Z}/a_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/a_m\mathbb{Z}$.

Corollaire. *Si Γ est un sous-réseau de $\mathbb{R}^n$ et Λ un sous-réseau de Γ alors Γ/Λ est fini si et seulement si Γ et Λ ont même rang. Le cardinal de Γ/Λ est alors $d_1 \cdots d_m$.*

2. Domaine fondamental d'un réseau

On considère, dans $\mathbb{R}^n$ muni de la mesure de Lebesgue λ, un réseau Γ de $\mathbb{Z}$-base $(e_1, \dots, e_n)$.
Définition. On dit qu'une partie mesurable $\mathcal{D}$ de $\mathbb{R}^n$ est un *domaine fondamental* pour Γ si, pour tout $x \in \mathbb{R}^n$, il existe un unique $y \in \mathcal{D}$ tel que $x - y \in \Gamma$.

Exemple. Le *parallélogramme fondamental*

$$\{\alpha_1e_1 + \cdots + \alpha_ne_n \ ; \ 0 \leq \alpha_i < 1\}$$

est un domaine fondamental pour Γ ; il en est de même de

$$\{\alpha_1e_1 + \cdots + \alpha_ne_n \ ; \ -1 \leq \alpha_i < 0\}.$$

Conséquence. Tout réseau a un domaine fondamental.

Proposition. *Si $\mathcal{D}$ et $\mathcal{D}'$ sont deux domaines fondamentaux pour Γ alors $\lambda(\mathcal{D}) = \lambda(\mathcal{D}')$ et cette quantité ne dépend pas de la $\mathbb{Z}$-base choisie.*

Définition. La mesure d'un domaine fondamental s'appelle le *volume* de Γ, on le note $v(\Gamma)$.

Exemple. Le volume du réseau $\mathbb{Z}^2$ de $\mathbb{R}^2$ est 1.

Proposition. *Si $\Lambda \subset \Gamma$ est un autre réseau alors $|\Gamma/\Lambda|$ est fini et on a $v(\Lambda) = v(\Gamma)\,|\Gamma/\Lambda|$.*

Lemme de Minkowski. *Soit Γ un réseau de $\mathbb{R}^n$ et S une partie mesurable de $\mathbb{R}^n$ telle que $\lambda(S) > v(\Gamma)$. Alors il existe $x, y \in S$ distincs tels que $x - y \in \Gamma$.*

Corollaire. *Soit Γ un réseau de $\mathbb{R}^n$ et S une partie mesurable, convexe et symétrique par rapport à 0 de $\mathbb{R}^n$. Si l'une des conditions suivantes est vérifiée*
– $\lambda(S) > 2^nv(\Gamma)$
– $\lambda(S) \geq 2^nv(\Gamma)$ et S compacte
alors $S \cap \Gamma$ contient un point autre que 0.

Contre-exemple. Si $(e_1, \dots, e_n)$ est une base de Γ et $S = \{\lambda_1e_1 + \cdots + \lambda_ne_n \ ; \ -1 < \lambda_i < 1\}$ alors $S \cap \Gamma$ ne contient que 0 donc les inégalités dans les conditions sont optimales.

Application (théorème des deux carrés)**.** Un nombre premier de la forme $4k + 1$ est somme de deux carrés.

Application (théorème des quatre carrés)**.** Tout entier naturel est somme de quatre carrés.

3. Réseaux du plan

3.1. **Fonctions elliptiques.** Soit ω_1 et ω_2 deux nombres complexes non nuls tels que $\frac{\omega_1}{\omega_2} \notin \mathbb{R}$ et f une fonction méromorphe sur $\mathbb{C}$ admettant ω_1 et ω_2 pour période.

Définition. On dit que f est une *fonction elliptique pour le réseau $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$.*

Exemple. La fonction $\wp$ de Weierstrass définie ci-dessous est elliptique :

$$\wp = \frac{1}{z^2} + \sum_{\omega\in\Lambda-\{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

Proposition. *Soit f est une fonction elliptique pour un réseau Λ de domaine fondamental $\mathcal{D}$.*

(*i*) *Le nombre de zéros de f dans $\mathcal{D}$ est fini et égal au nombre p de pôles de f.*

(*ii*) *Les valeurs de f sont atteintes exactement p fois.*

(*iii*) *On note z_α les pôles de f et m_α leur multiplicité alors $\sum m_\alpha z_\alpha \in \Lambda$.*

(*iv*) *Si f n'est pas constante alors $p \geq 2$.*

3.2. **Action du groupe modulaire sur le demi-plan de Poincaré.** On identifie le plan $\mathbb{R}^2$ à $\mathbb{C}$, on note $\mathcal{P}$ le demi-plan $\{z \in \mathbb{C}; \mathrm{Im}\ z > 0\}$ et on considère le *groupe modulaire* $PSL_2(\mathbb{Z}) \simeq SL_2(\mathbb{Z})/\{\pm \mathrm{I}_2\}$.

Proposition. *$SL_2(\mathbb{Z})$ est engendré par les matrices*

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ et } T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Proposition. *L'action de $PSL_2(\mathbb{Z})$ sur $\mathcal{P}$ définie par*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az+b}{cz+d}$$

admet pour transversale le domaine $\mathcal{D}_0$ défini par
– *soit* $-\frac{1}{2} \leq \mathrm{Re}\ z < \frac{1}{2}$ *et* $|z| > 1$,
– *soit* $-\frac{1}{2} \leq \mathrm{Re}\ z \leq 0$ *et* $|z| = 1$.

Proposition. *À $\mathbb{C}^*$-homothétie près, les réseaux du plan sont en bijection avec $\mathcal{D}_0$.*

3.3. **Anneaux d'entiers quadratiques.**

Définition. Un *corps quadratique* est une sous-corps K de $\mathbb{C}$ de la forme $K = \mathbb{Q}(\sqrt{d})$ (où $d \in \mathbb{Z}$ est sans facteur carré) ; si $d > 0$, c'est un corps quadratique *réel* ; si $d < 0$, c'est un corps quadratique *imaginaire*.

Exemple. $\mathbb{Q}(\sqrt{-3})$ et $\mathbb{Q}(\sqrt{3})$ sont respectivement deux corps quadratiques imaginaire et réel ; en revanche $\mathbb{Q}(e^{2i\pi/n})$ n'est pas un corps quadratique pour $n \geq 3$.

Un élément z d'un corps de nombre K est dit *entier* s'il existe un polynôme $P \in \mathbb{Z}[X]$ unitaire tel que $P(z) = 0$.

Proposition. *L'ensemble O_K des éléments entiers d'un corps quadratique $K = \mathbb{Q}(\sqrt{d})$ est un anneau et*

(*i*) $O_K = \mathbb{Z}[\sqrt{d}]$ *si* $d \equiv 2, 3 \pmod 4$

(*ii*) $O_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ *si* $d \equiv 1 \pmod 4$

Exemple. L'anneau des entiers de $\mathbb{Q}(\sqrt{-3})$ est $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ et l'anneau des entiers de $\mathbb{Q}(\sqrt{3})$ est $\mathbb{Z}[\sqrt{3}]$.

Corollaire. *Soit O_K l'anneau des entiers d'un corps quadratique $K = \mathbb{Q}(\sqrt{d})$.*

(*i*) *Si $d > 0$ alors O_K est un sous-groupe dense de $\mathbb{R}$.*

(*ii*) *Si $d < 0$ et $d \equiv 2, 3 \pmod 4$ alors O_K est un réseau du plan de $\mathbb{Z}$-base $(1, \sqrt{d})$.*

(*iii*) *Si $d < 0$ et $d \equiv 1 \pmod 4$ alors O_K est un réseau du plan de $\mathbb{Z}$-base $(1, \frac{1+\sqrt{d}}{2})$.*

Proposition. *Soit O_K l'anneau des entiers d'un corps quadratique réel $K = \mathbb{Q}(\sqrt{d})$.*

(*i*) *Le groupe des éléments inversibles de O_K admet un plus petit élément ω strictement supérieur à 1.*

(*ii*) *Ce groupe est égal à $\{\pm\omega^n\ ;\ n \in \mathbb{Z}\}$.*

Exemple. Les éléments inversibles de $\mathbb{Z}[\sqrt{3}]$ sont les nombres de la forme $\pm(2+\sqrt{3})^n$ où $n \in \mathbb{Z}$.

Développements

Théorème de la base adaptée. [3]

Action de $PSL_2(\mathbb{Z})$ sur le demi-plan de Poincaré.

Références

[1] M. Alessandri, *Thèmes de géométrie. Groupes en situation géométrique*, Dunod, 1999.

[2] A. Chambert-Loir et S. Fermigier, *Exercices d'analyse 2*, Dunod, 1999.

[3] R. Goblot, *Algèbre commutative*, Masson, 1996.

[4] P. Samuel, *Théorie algébrique des nombres*, Hermann, 1997.

[5] P. Tauvel, *Mathématiques générales pour l'agrégation*, Masson, 1997.