Séminaire des doctorants : Géométrie des nombres

Antoine BOIVIN

22 juin 2024

Résumé

La géométrie des nombres est une branche de l'arithmétique, fondée à la fin du XIXème siècle par Hermann Minkovski, dans laquelle on interprète les énoncés en termes de réseaux pour utiliser leurs propriétés géométriques. Le point de départ est le théorème, dû à Minkovski, énonçant qu'un convexe de $\mathbb{R}^n$ (symétrique par rapport à l'origine)« suffisamment volumineux » contient au moins un point entier (qui n'est pas l'origine).

Dans cet exposé, nous allons donner un énoncé précis de ce théorème et voir comment l'appliquer à différents problèmes arithmétiques : l'approximation diophantienne simultanée, l'écriture d'entier comme sommes de 4 carrés et, si le temps le permet, l'étude des classes d'idéaux d'un corps de nombres.

Table des matières

1 Théorème de Minkowski

Définition 1.0.1. Soit V un $\mathbb{R}$-espace vectoriel de dimension finie. Un réseau est un sous-groupe additif discret de V qui engendre V comme $\mathbb{R}$-espace vectoriel.

Exemple 1.0.2. $\mathbb{Z}^n \subset \mathbb{R}^n$

Proposition 1.0.3. *Soit V un $\mathbb{R}$-espace vectoriel de dimension finie. Une partie L est un réseau de V si, et seulement si, il existe une base $(e_1, \dots, e_{\dim(V)})$ de V tel que*

$$L = \mathbb{Z}e_1 \oplus \dots \oplus \mathbb{Z}e_{\dim(V)}$$

On dira que $(e_1, \dots, e_n)$ est une base de L.

Démonstration. voir [Bou07] □

Dans la suite, on considérera $V = \mathbb{R}^n$.

Théorème 1.0.4. *Soient L un réseau de $\mathbb{R}^n$, $\mathcal{B} = (e_1, \dots, e_n)$, $\mathcal{B}' = (f_1, \dots, f_n)$ deux bases de E. Alors il existe $M \in \mathrm{GL}_n(\mathbb{Z})$ telle que*

$$Me_i = f_i$$

Démonstration. Les bases $\mathcal{B}$ et $\mathcal{B}'$ induisent des automorphismes de $\mathbb{R}^n$ qui induisent des isomorphismes $\varphi_{\mathcal{B}}, \varphi_{\mathcal{B}'} : \mathbb{Z}^n \to L$. Le morphisme $M = \varphi_{\mathcal{B}'}^{-1}\varphi_{\mathcal{B}}$ est donc un isomorphisme de $\mathbb{Z}^n$ i.e. un élément de $\mathrm{GL}_n(\mathbb{Z})$. □

Définition 1.0.5. Soit L un réseau de $\mathbb{R}^n$. Soit $\mathcal{B}$ une base de L. Le déterminant de L est

$$\det(L) \coloneqq |\det_{\mathcal{B}^{can}}(\mathcal{B})|$$

où $\mathcal{B}^{can}$ est la base canonique de $\mathbb{R}^n$.

Lemme 1.0.6. *Le réel $\det(L)$ ne dépend pas du choix de la base.*

Exemple 1.0.7. $\det(\mathbb{Z}^n) = 1$

Lemme 1.0.8. *Soient $(X, \mathcal{A}, \mu)$ un espace mesuré et (N_α) une famille au plus dénombrable de parties mesurables de X. Si $\sum_\alpha \mu(N_\alpha) > k\mu\left(\bigcup_\alpha N_\alpha\right)$ alors il existe un point de X qui est dans au moins $k+1$ parties.*

Démonstration. On a l'inégalité :

$$\int_{\bigcup_\beta N_\beta} \sum_\alpha 1_{N_\alpha} = \sum_\alpha \int_{\bigcup_\beta N_\beta} 1_{N_\alpha} = \sum_\alpha \mu(N_\alpha) > k\mu\left(\bigcup_\alpha N_\alpha\right) = \int_{\bigcup_\beta N_\beta} k$$

On en déduit qu'il existe $x \in X$ tel que

$$\sum_\alpha 1_{N_\alpha}(x) > k.$$

□

Théorème 1.0.9 (Blichfeldt)**.** *Soit* $k > 0$ *et* M *une partie mesurable de* $\mathbb{R}^n$ *de volume* $> k$*. Il existe* $k+1$ *points dont les différences sont à coordonnées entières.*

Démonstration. L'espace $\mathbb{R}^n$ s'écrit comme une décomposition

$$\mathbb{R}^n = \coprod_{k\in\mathbb{Z}^n} k + [0,1[^n$$

Par conséquent, on a une décomposition de M :

$$M = \coprod_{k\in\mathbb{Z}^n} (k + [0,1[^n) \cap M$$

On en déduit donc l'inégalité

$$\begin{aligned}\sum_{k\in\mathbb{Z}^n} \lambda([0,1[^n \cap (M-k)) &= \sum_{k\in\mathbb{Z}^n} \lambda(k + [0,1[^n \cap (M)) \\ &= \lambda(\coprod_{k\in\mathbb{Z}^n} (k + [0,1[^n) \cap M) = \lambda(M) \\ &> k = k\lambda([0,1[^n) \geqslant k\lambda\left(\bigcup_{k\in\mathbb{Z}^n} [0,1[^n \cap (M-k)\right)\end{aligned}$$

Il existe donc $z \in [0,1[^n$ et $\alpha_0, \ldots, \alpha_k \in \mathbb{Z}^n$ tel que $m_i \coloneqq z + \alpha_i \in M$. De plus,

$$m_i - m_j = \alpha_i - \alpha_j \in \mathbb{Z}^n$$

□

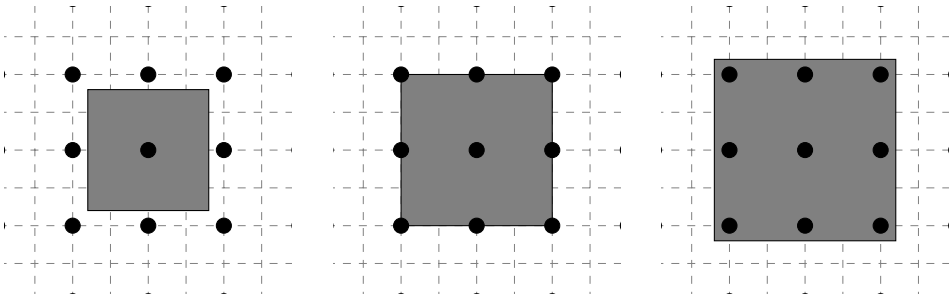

FIGURE 1 – C_t pour $t < 1$, $t = 1$ et $t > 1$

Lemme 1.0.10. *Soit* C *un convexe symétrique par rapport à l'origine (*$x \in C \Rightarrow -x \in C$*). Notons* $C_{1/2}$ *l'image de* C *par l'homothétie de rapport* $1/2$*. Si* $C_{1/2}$ *rencontre un translaté* $\beta + C_{1/2}$ *alors* C *contient* β*.*

Démonstration. Soit $x = \beta + y$ un point d'intersection de $C_{1/2} \cap (\beta + C_{1/2})$. Alors $2x, 2y \in C$ et donc $2x, -2y$ aussi (par symétrie par rapport à l'origine). Par convexité, $\frac{2x-2y}{2} = x - y = \beta$ aussi. □

Théorème 1.0.11 (Minkowski I)**.** *Soit* C *un convexe de* $\mathbb{R}^n$ *symétrique par rapport à l'origine Alors*

- *Si* $\mathrm{Vol}(C) > 2^n$ *alors* C *contient au moins 2 points à coordonnées entières (en dehors de l'origine) ;*
- *Si* $\mathrm{Vol}(C) = 2^n$ *alors* $\overline{C}$ *contient au moins 2 points à coordonnées entières (en dehors de l'origine) ;*

Démonstration. Comme $\mathrm{Vol}(C_{1/2}) = 2^{-n}\mathrm{Vol}(C) > 1$ alors il existe deux points dont la différence β est à coordonnées entières. Autrement dit, $C_{1/2} \cap (C_{1/2} + \beta)$ est non vide. Grâce au lemme précédent, cela veut dire que $\beta \in C$. □

Exemple 1.0.12. $C_t =]-t, t[^2$, $\mathrm{Vol}(C_t) = 4t^2$.

- Si $t < 1$ alors C_t a un seul point entier : l'origine ;
- Si $t = 1$ alors $\overline{C_t}$ a 9 points entiers mais C_t n'en n'a qu'un, l'origine ;
- Si $t > 1$ alors C_t a, au moins, 9 points.

Exemple 1.0.13. Conv((-0.12,-0.12),(0.92,7.8),(0.92,-0.12)) a qu'un seul point entier 0 mais a une aire de 4.1>4.

Théorème 1.0.14 (Minkowski II). *Soit* C *un convexe de* $\mathbb{R}^n$ *symétrique par rapport à l'origine (*$x \in C \Rightarrow -x \in C$*) et* L *un réseau de* $\mathbb{R}^n$ *de déterminant* Δ*. Alors*

- *Si* $\mathrm{Vol}(C) > 2^n\Delta$ *alors* C *contient au moins 2 points à coordonnées entières (en dehors de l'origine) ;*
- *Si* $\mathrm{Vol}(C) = 2^n\Delta$ *alors* $\overline{C}$ *contient au moins 2 points à coordonnées entières (en dehors de l'origine) ;*

Démonstration. Soit H un isomorphisme $\mathbb{Z}^n \to L$. Alors

$$\mathrm{Vol}(H^{-1}C) = \int_{H^{-1}C} 1 = \int_C \mathrm{Jac}(H^{-1}) = \det(H^{-1})\lambda(C) > 2^n$$

On est alors ramené au premier théorème de Minkowski. □

2 Applications

2.1 Approximation diophantienne simultanée

Théorème 2.1.1. *Soient* $\alpha_1, \ldots, \alpha_n \in \mathbb{R}$*. Il existe* $p \geqslant 1$*,* $p_1, \ldots, p_n \in \mathbb{Z}$ *tel que*

$$\begin{cases} \left|\alpha_1 - \frac{p_1}{p}\right| < \frac{1}{p^{1+1/n}} \\ \quad\vdots \\ \left|\alpha_n - \frac{p_n}{p}\right| < \frac{1}{p^{1+1/n}} \end{cases}$$

Démonstration. Soit $s < 1$. Posons

$$K_s \coloneqq \{(y, x_1, \ldots, x_n) \in \mathbb{R}^{n+1} \mid |x - \alpha_i y| \leqslant s, |y| \leqslant s^{-n}\}$$

Exemple 2.1.2. $n = 1$ et $K_s \subset \mathbb{R}^2$. Alors

$$K_s = \mathrm{Conv}((\alpha s^{-1} - s, s^{-1}), (\alpha s^{-1} + s, s^{-1}), (-\alpha s^{-1} - s, -s^{-1}), (s - \alpha s^{-1}, -s^{-1}))$$

Le volume de K_s est

$$\begin{aligned}\mathrm{Vol}(K_s) &= \mathtt{Base} \times \mathtt{hauteur} = \mathrm{Vol}(K_s \cap \{y = -s^{-n}\}) \times 2s^{-n} \\ &= \mathrm{Vol}(n-\text{cube de côté } 2s) \times 2s^{-n} = (2s)^n 2s^{-n} = 2^{n+1} = 2^{\dim(\mathbb{R}^{n+1})}\end{aligned}$$

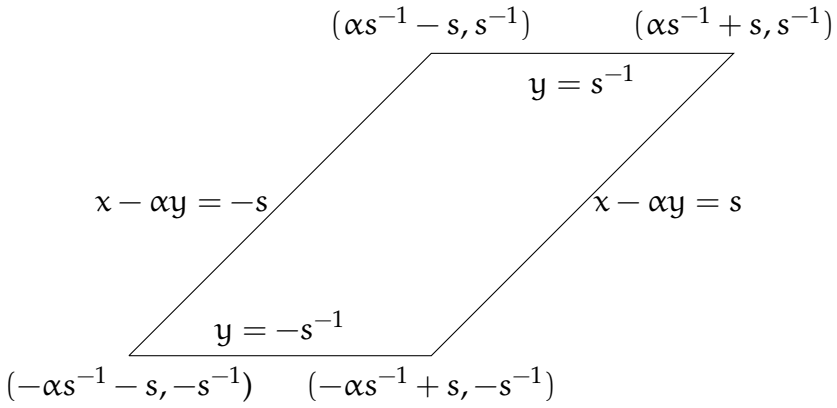

FIGURE 2 – Le convexe K_s

et ne dépend donc pas de s.
Par le théorème de Minkowski, $K \cap \mathbb{Z}^{n+1} = \overline{K} \cap \mathbb{Z}^{n+1} \neq \emptyset$. Soit $(p, p_1, \ldots, p_n)$ un élément de leur intersection. Alors

$$\begin{cases} |p_i - \alpha p| \leqslant s \\ |p| \leqslant s^{-n} \end{cases}$$

On en déduit donc

$$\begin{cases} |\alpha - p_i/p| \leqslant \frac{1}{|p|} s = \frac{1}{|p|^{1+1/n}} \\ s \leqslant p^{1/n} \end{cases}$$

□

2.2 Somme des 4 carrés

Théorème 2.2.1. *Tout nombre entier s'écrit comme la somme de quatre carrés.*

Lemme 2.2.2 (Identité des 4 carrés d'Euler)**.** *Si* p *et* q *s'écrivent comme somme de quatre carrés alors* pq *aussi.*

Démonstration.

$$\begin{aligned}(x_1^2+y_1^2+z_1^2+t_1^2)(x_2^2+y_2^2+z_2^2+t_2^2) =&(x_1x_2+y_1y_2+z_1z_2+t_1t_2)^2\\ &+(x_1y_2-y_1x_2+t_1z_2-z_1t_2)^2\\ &+(x_1z_2-z_1x_2+y_1t_2-t_1y_2)^2\\ &+(x_1t_2-t_1x_2+z_1y_2-y_1z_2)^2.\end{aligned}$$

□

Proposition 2.2.3. *Soit* p *un nombre premier. Il existe* $a, b \in \mathbb{N}$ *tel que* p *divise* a^2+b^2+1

Démonstration. Pour démontrer ce résultat, on va utiliser le lemme suivant :

Lemme 2.2.4. *Un entier* a *est un carré modulo* p *si, et seulement si,* $\left(\frac{a}{p}\right)=1$ *i.e. si, et seulement si,* $a^{\frac{p-1}{2}} \equiv 1[p]$

Grâce à ce lemme, on voit que -1 est un carré modulo p si, et seulement si, $p \equiv 1[4]$. Dans ce cas là, le lemme est démontré (en prenant $b=0$).

Supposons donc $p \equiv 3[4]$.
On va considérer les couples $(k, p-k-1)$ de résidus quadratiques. Grâce à l'égalité suivante

$$\left(\frac{p-k-1}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{k+1-p}{p}\right)=-\left(\frac{k+1}{p}\right),$$

cela revient à calculer le cardinal de l'ensemble suivant :

$$A_{01}=\left\{k\in\{1,\dots,p-1\} \mid \left(\frac{k}{p}\right)=1, \left(\frac{k+1}{p}\right)=-1\right\}$$

qui vaut $\frac{p+1}{4}$ pour $p \equiv 3[4]$ (voir [Lem00]).

□

Démonstration du théorème 2.2.1. Soient $a, b \in \mathbb{Z}$ tel que a^2+b^2+1 est divisible par p. Soit L le réseau de $\mathbb{R}^4$ dont les générateurs sont :

$$\begin{pmatrix}p\\0\\0\\0\end{pmatrix}, \begin{pmatrix}0\\p\\0\\0\end{pmatrix}, \begin{pmatrix}a\\b\\1\\0\end{pmatrix}, \begin{pmatrix}b\\-a\\0\\1\end{pmatrix}$$

i.e.

$$L = \{(x, y, z, t) \in \mathbb{R}^4 \mid z \equiv ax + by[p], t \equiv bx - ay[p]\}$$

Le déterminant de L est p^2.
On va ensuite considérer le convexe (symétrique par rapport à l'origine)

$$C \coloneqq \mathbb{B}^3_{\sqrt{2p}} = \{(x, y, z, t) \in \mathbb{R}^4 \mid x^2 + y^2 + z^2 + t^2 < 2p\}$$

qui est de volume

$$\mathrm{Vol}(C) = \frac{\pi^2}{2}(\sqrt{2p})^4 = (2\pi^2)p^2 > 8\det(L)$$

Par le théorème de Minkowski, il existe $(x, y, z, t) \in L$ tel que

$$0 < x^2 + y^2 + z^2 + t^2 < 2p$$

Par définition de L, il existe des entiers q_1, q_2, q_3, q_4 tels que

$$0 < (q_1 p + a q_3 + b q_4)^2 + (q_2 p + b q_3 - a q_4)^2 + q_3^2 + q_4^2 < 2p \qquad (1)$$

En développant, on obtient

$$\begin{aligned}
&(q_1 p + a q_3 + b q_4)^2 + (q_2 p + b q_3 - a q_4)^2 + q_3^2 + q_4^2 \\
&= q_1 p(-) + a^2 q_3^2 + 2ab q_3 q_4 + b^2 q_4 + q_2 p(-) + b^2 q_3^2 - 2ab q_3 q_4 + a^2 q_4 + q_3 + q_4 \\
&= p(-) + (a^2 + b^2 + 1)(q_3 + q_4)
\end{aligned}$$

Comme $a^2 + b^2 + 1$ est divisible par p alors $(q_1 p + a q_3 + b q_4)^2 + (q_2 p + b q_3 - a q_4)^2 + q_3^2 + q_4^2$ est un entier divisible par p. Grâce à l'égalité (1), on en déduit que

$$(q_1 p + a q_3 + b q_4)^2 + (q_2 p + b q_3 - a q_4)^2 + q_3^2 + q_4^2 = p$$

□

Références

[Bou07] N. Bourbaki. *Topologie générale : Chapitres 5 à 10*. Bourbaki, Nicolas. Springer Berlin Heidelberg, 2007.

[Lem00] Franz Lemmermeyer. *Reciprocity laws : from Euler to Eisenstein*. Springer Monographs in Mathematics. Springer, 1 edition, 2000.