I.K Théorème de Minkowski (127) (149) (181) (191)

J'ai appris ce développement dans mon cours de théorie des nombres de M1 assuré par Florent Ivorra. La proposition et l'application provienne de son cours et je n'ai pas d'autres référence pour ces deux résultat. Le reste se trouve dans le livre de Pierre Samuel [14].

Pour la 149 je fais la proposition mais pas l'application, pour les autres (127,181,191) je fais l'application mais pas la proposition.

On suppose que E est un $\mathbf{R}$-espace vectoriel euclidien.

Pour $e = (e_1, \dots, e_n)$ une $\mathbb{Z}$-base d'un réseau H, on désigne par P_e le parallélogramme $P_e = \{\sum_{j=1}^{n} a_{i,j} e_j \quad / \quad \forall i \ 0 \leqslant a_i < 1\}$

Lemme 20:

lem :covolume Le volume $\mu(P_e)$ de P_e (avec μ la mesure de Lebesgue sur $\mathbb{R}^n$ est indépendante de la base e choisie pour H.
On l'appelle covolume de H et on note Covol(H).

Démonstration. Si $f = (f_1, \dots, f_n)$ est une autre $\mathbb{Z}$-base de H alors comme $f_i \in H$ pour tout i, on a :

$$f_= \sum_{j=1}^{n} \alpha_{i,j} e_j \qquad \text{avec} \quad \alpha_{i,j} \in \mathbb{Z}.$$

Soit u l'endomorphisme $\mathbb{R}$-linéaire de $\mathbb{R}^n$ tel que $u(e) = f$. La matrice de u dans la base e est inversible et à coefficients dans $\mathbb{Z}$, c'est $(\alpha_{i,j})_{1 \leqslant i,j \leqslant n}$. Son déterminant est donc inversible dans $\mathbb{Z}$ donc égal à ± 1.

Soit b une base orthonormée de $\mathbb{R}^n$. Alors :

$$\mu(P_f) = |\det_b(f)| = |\det_b(u(e))| = |\det(u)||\det_b(e)| = |\pm 1|\mu(P_e) = \mu(P_e).$$

Il y a aussi indépendance vis-à-vis de la base orthonormée choisie (multplication par une matrice orthonale donc de déterminant ± 1). ■

La proposition suivante permet d'exprimer le covolume d'un réseau sans faire usage d'une base orthonormée de l'espace euclidien.

Proposition 21

Soit H un réseau d'un $\mathbb{R}$-espace euclidien E. Alors, pour toute $\mathbf{Z}$-base $(e_1, \dots, e_n)$ de H

$$\text{Covol}(H) = \begin{vmatrix} \langle e_1 \mid e_1 \rangle & \cdots & \langle e_1 \mid e_n \rangle \\ \vdots & & \vdots \\ \langle e_n \mid e_1 \rangle & \cdots & \langle e_n \mid e_n \rangle \end{vmatrix}.$$

Démonstration. Soient $\mathscr{B} = (b_1, \dots, b_n)$ une base orthonormale. On écrit $e_i = \sum_{j=1}^{n} \langle e_i \mid b_j \rangle b_j$. Soit

$$A = \begin{pmatrix} \langle e_1 \mid b_1 \rangle & \cdots & \langle e_n \mid b_1 \rangle \\ \vdots & & \vdots \\ \langle e_1 \mid b_n \rangle & \cdots & \langle e_n \mid b_n \rangle \end{pmatrix} \mathscr{M}_n(\mathbb{R})$$

Par définition Covol$(H) = |\det(A)|$. Ainsi a-t-on

$$\text{covol}(H)^2 = \det(A)^2 = \det\left({}^tA\right)\det(A) = \det\left({}^tAA\right).$$

Or ${}^tAA[i,j] = \sum_{k=1}^{n} \langle e_i \mid b_k\rangle\langle e_j \mid b_k\rangle = \left\langle e_i \ , \ \sum_{k=1}^{n} \langle e_j \mid b_k\rangle b_k \right\rangle = \langle e_i \mid e_j\rangle$

On obtient donc

$$\operatorname{covol}(L)^2 = \begin{pmatrix} \langle e_1 \mid e_1\rangle & \cdots & \langle e_1 \mid e_n\rangle \\ \vdots & & \vdots \\ \langle e_n \mid e_1\rangle & \cdots & \langle e_n \mid e_n\rangle \end{pmatrix}$$

On trouve ainsi la formule annoncée reliant le covolume du réseau au déterminant de Gram de l'une de ses $\mathbb{Z}$-bases. ■

Lemme 22:

Soit H un réseau de $\mathbb{R}^n$. Soit S une partie mesurable de E telle que $\mu(A) > \operatorname{covol}(L)$. Alors il existe alors des éléments $x, y \in S$ distincts tels que $x - y \in H$.

Démonstration. Soit $e = (e_1, \ldots, e_n)$ une **Z**-base de H et soit P_e le domaine fondamental associé. Alors $S = \coprod_{h\in H} [(h + P_e) \cap S)]$. On a donc :

$$\mu(S) = \sum_{h\in H} \mu(S \cap (h + P_e))$$

Mais la mesure de Lebesgue est invariante par translation, donc on a

$$\mu(S \cap (h + P_e)) = \mu\left((-h + S) \cap P_e\right).$$

Ceci impose dès lors que les ensembles $(-h + S) \cap P_e$ ne sont pas disjoints deux à deux car sinon

$$\mu(S) = \sum_{h\in H} \mu\left((-h + S) \cap P_e\right) \leqslant \mu(P_e)$$

ce qui est exclus. On peut donc trouver h et $\tilde{h}$ dans H distincts tels que

$$((-h + S) \cap P_e) \cap ((-\tilde{h} + S) \cap P_e) \neq \varnothing.$$

De là on tire qu'il existe $x, y \in S$ tels que $-h + x = -\tilde{h} + y$. c'est-à-dire $x - y = h - \tilde{h} \in H$ (structure de groupe de H) et comme $h \neq \tilde{h}$, on a aussi $x \neq y$. ■

Théorème 23: Minkowski

Soit H un réseau de $\mathbb{R}^n$ et soit S une partie mesurable de $\mathbb{R}^n$ telle que

1. S est convexe ;
2. S est symétrique par rapport à l'origine ;
3. la mesure de $\mu(S) > 2^n \operatorname{covol}(H)$

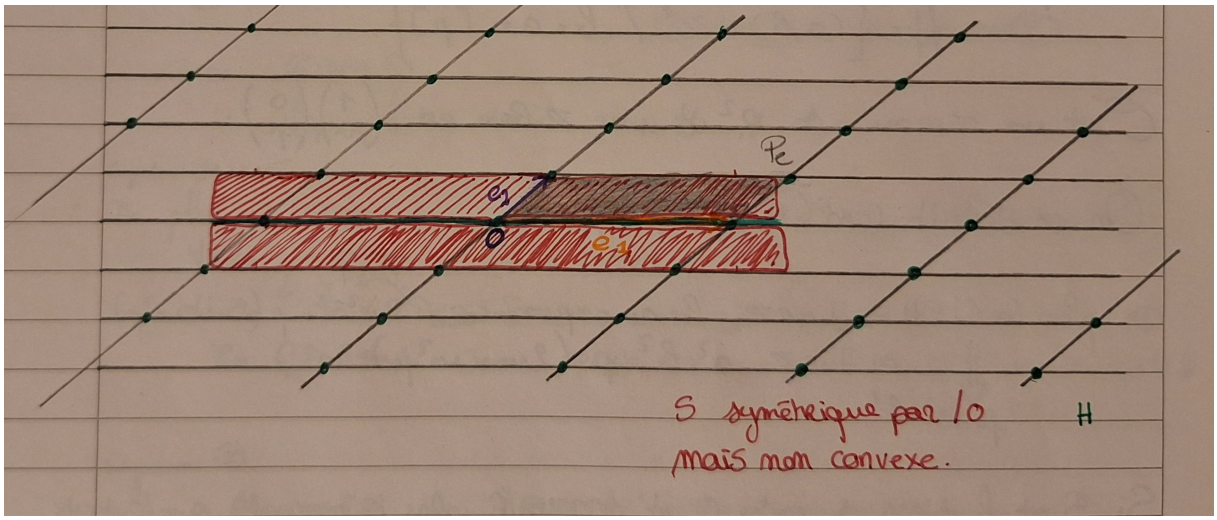
Alors S contient un élément de H non nul.

Le dessin suivant aide à comprendre pourquoi l'hypothèse de convexité est nécessaire. La surface rouge est constitué de deux bandes ouvert situées dans les demis plans $y > 0$ et $y < 0$.

Démonstration. L'ensemble $2H = \{2x \quad / \quad x \in H\}$ est un réseau et si $(e_1, \ldots, e_n)$ est une **Z**-base du réseau H alors $(2e_1, \ldots, 2e_n)$ est une **Z**-base de $2H$. Par multilinéarité du déterminant il vient alors :

$$\operatorname{covol}(2H) = 2^n \operatorname{covol}(H).$$

Ainsi la condition (3) se réécrit en $\mu(S) > \operatorname{covol}(2H)$. Le lemme précédent assure l'existence de $x, y \in S$ distincts tels que $x - y \in 2H$. Puis $\frac{x-y}{2} \in H$. Mais comme S est symétrique $-y \in S$ et comme S est convexe $\frac{x-y}{2} =\in S$. ■



Application 24: le théorème des deux carrés

Soit p un nombre premier impair. Alors p est la somme de deux carrés d'entiers si et seulement si $p \equiv 1 \mod 4$.

Démonstration. On va utiliser de manière cruciale la première loi complémentaire de la loi de réciprocité quadratique.

* Supposons $p = a^2 + b^2$. Alors $p \nmid a$ ou $p \nmid b$ car sinon si $p \mid a$ et $p \mid b$, alors $p^2 \mid a^2$ et $p^2 \mid b^2$ donc divise $p \mid a^2 + b^2 = p$ et donc $p \mid p$, ce qui est absurde.
  Par symétrie des rôles de a et b on peut supposer $p \nmid b$. On a alors $-1 = (a/b)^2$ dans $\mathbf{F}_p$. C'est-à-dire que -1 est un carré modulo p et donc $p \equiv 1 \mod 4$ par la première loi complémentaire de la loi de réciprocité quadratique.
* Réciproquement on suppose $p \equiv 1 \mod 4$. La première loi complémentaire de la loi de réciprocité quadratique assure que -1 est un carré modulo p. On dispose donc de $u \in \mathbb{Z}$ tel que $u^2 \equiv -1 \mod p$. On pose :

$$H = \{(a, b) \in \mathbf{Z}^2 \quad / \quad b \equiv ua \mod p\}.$$

  C'est un réseau de $\mathbb{R}^2$ dont une $\mathbb{Z}$-base est $\begin{pmatrix} 1 \\ u \end{pmatrix}, \begin{pmatrix} 0 \\ p \end{pmatrix}$.

  On en déduit $\mathrm{Covol}(H) = p$.

  De plus si $(a, b) \in H$, alors il existe $n \in \mathbf{Z}$ tel que $b = ua + np$. On a donc

$$b^2 = u^2a^2 + 2uanp + n^2p^2 \equiv -a^2 \mod p,$$

  ce qui donne que p divise $a^2 + b^2$.
  Soit S le disque $D(0, R)$ de centre 0 et de rayon R. Alors S est mesurable, convexe, symétrique par rapport à l'origine et

$$\mu(SA) = \pi R^2.$$

  On prend $R > \sqrt{\frac{4p}{\pi}}$, et l'on obtient $\mu(S) = \pi R^2 > 4\,\mathrm{Covol}(L) = 4p$.

  Alors le théorème de Minkowski fournit $(a, b) \in H \cap S$ non nuls. Comme $\frac{3}{2} > \frac{4}{\pi}$, en prenant $R = \sqrt{\frac{3p}{2}}$ on a :

$$0 < a^2 + b^2 < \frac{3p}{2},$$

  or $p \mid a^2 + b^2$. D'où finalement $p \mid a^2 + b^2 = p$.

■