Théorèmes de Minkowski et applications

Dans cette feuille, on démontre le premier et le second théorème de Minkowski, suivis de quelques applications.

On se placera sauf mention contraire dans $\mathbb{R}^n$ muni de sa structure euclidienne (la norme associée étant notée $\|\cdot\|$) et Λ est un réseau de $\mathbb{R}^n$.

On pose alors

$$\lambda_1(\Lambda) = \min\{\|v\|,\, v \in \Lambda, v \neq 0\}.$$

Plus généralement, pour tout $k \in \{1, \cdots, n\}$, on pose $\lambda_k(\Lambda)$ le plus petit réel r tel qu'il existe k vecteurs $\mathbb{R}$-linéairement indépendants dans Λ de norme au plus r.

Tout réseau Λ de $\mathbb{R}^n$ a un volume naturel (qui est le volume de n'importe lequel de ses domaines fondamentaux), noté $\mathrm{vol}(\Lambda)$.

Les théorèmes de Minkowski sont alors les suivants :

Théorème 1 (Premier théorème de Minkowski)**.** *Pour tout $n \in \mathbb{N}^*$, il existe une constante $C_n > 0$ telle que pour tout réseau Λ de $\mathbb{R}^n$, on a*

$$\lambda_1(\Lambda) \leq C_n \det(\Lambda)^{1/n}.$$

En fait, on peut prendre cette constante égale à $C_n = (2/\sqrt{\pi})\Gamma(n/2+1)^{1/n}$. On appelle constante de Hermite-Minkowski le carré de la constante optimale possible pour cette inégalité, notée γ_n (en particulier, $\gamma_n \leq C_n$).

Théorème 2 (Second théorème de Minkowski)**.** *Pour tout $n \in \mathbb{N}^*$ et tout réseau Λ de $\mathbb{R}^n$,*

$$\sqrt[n]{\lambda_1 \cdots \lambda_n(\Lambda)} \leq \sqrt{\gamma_n} \det(\Lambda)^{1/n}.$$

Le but des exercices est de démontrer ces théorèmes.

Exercice 1. [Théorème du corps convexe de Minkowski]

Soit Λ un réseau de $\mathbb{R}^n$.

(a) *(Théorème de Blichfeldt)* Si S est une partie mesurable de $\mathbb{R}^n$ telle que $\mathrm{vol}(S) > \mathrm{vol}(\Lambda)$, il existe deux points distincts $s_1, s_2 \in S$ tels que $s_1 - s_2 \in \Lambda$.

(b) En déduire que si S est une partie convexe symétrique de $\mathbb{R}^n$ (c'est-à-dire $-S = S$) telle que $\mathrm{vol}(S) > 2^n \mathrm{vol}(\Lambda)$, il existe $s \in \Lambda \cap S$ non nul.

(c) Montrer que l'inégalité peut être large si S est de plus supposé compacte.

Exercice 2. [Calcul du volume de la boule unité]

On note pour tout $n \in \mathbb{N}^*$, V_n le volume de la boule unité dans $\mathbb{R}^n$.

(a) Montrer après changement de variables que

$$V_n = V_{n-1} \cdot \int_0^1 \frac{(1-t)^{(n-1)/2}}{\sqrt{t}} dt.$$

(b) On définit comme d'habitude les fonctions beta et gamma (pour des valeurs positives) par les intégrales

$$B(x,y) = \int_0^1 u^{x-1}(1-u)^{y-1} du, \quad \Gamma(x) = \int_0^{+\infty} t^{x-1}e^{-t} dt.$$

Montrer par un changement de variables que pour tous $x, y > 0$, on a

$$B(x,y) = \frac{\Gamma(x)\Gamma(y)}{\Gamma(x+y)}.$$

En déduire que $V_n = V_{n-1}\Gamma((n+1)/2)\Gamma(1/2)/\Gamma(n/2+1)$.

(*c*) Montrer que $\Gamma(1/2) = \sqrt{\pi}$, et obtenir finalement

$$V_n = \frac{(\sqrt{\pi})^n}{\Gamma(n/2+1)}.$$

(*d*) Retrouver les valeurs habituelles pour $n = 1, 2, 3$.

(*e*) Appliquer l'exercice précédent pour obtenir le premier théorème de Minkowski avec la constante indiquée.

(*f*) A-t-on la valeur optimale pour γ_2 ?

Exercice 3. [Preuve du second théorème de Minkowski]

Soit Λ un réseau de $\mathbb{R}^n$.

(*a*) Montrer qu'il existe une famille de vecteurs $\mathbb{R}$-linéairement indépendants $(x_1, \cdots, x_n)$ de Λ tels que $\lambda_i(\Lambda) = \|x_i\|$ pour tout $i \in \{1, \cdots, n\}$.

(*b*) On note $(x_1^*, \cdots, x_n^*)$ l'orthonormalisé de Gram-Schmidt d'une telle famille, et T la transformation linéaire qui envoie x_i sur x_i^* pour tout $i \in \{1, \cdots, n\}$. Montrer que $T(\Lambda)$ est un réseau de volume $\det(\Lambda)/(\lambda_1 \cdots \lambda_n(\Lambda))$.

(*c*) Soit $w \in \Lambda$ non nul et $v = T(w)$. Prenons k le plus grand indice tel que $\lambda_k(\Lambda) \leq \|w\|$. Montrer que $(x_1, \cdots, x_k, w)$ est liée.

(*d*) En déduire que $\|v\|^2 \geq 1$, donc que $\lambda_1(T(\lambda)) \geq 1$. Conclure.

Exercice 4. [Applications des théorèmes]

(*a*) Soit p un nombre premier congru à 1 modulo 4. Montrer qu'il existe $k \in \mathbb{Z}$ tel que $k^2 = -1 \mod p$, et en considérant le réseau de $\mathbb{R}^2$ de base $(1, k), (0, p)$, montrer qu'il existe $a, b \in \mathbb{Z}$ tels que $a^2 + b^2 = p$.

(*b*) *(Théorème de Pick pour les triangles)* Montrer qu'un triangle T à sommets dans $\mathbb{Z}^2$ et ne contenant pas d'autres points entiers est d'aire 1/2, en considérant un domaine convexe symétrique formé par des copies de T.

(*c*) Soient $L_1, \cdots, L_n$ des formes linéaires sur $\mathbb{R}^n$ et $c_1, \cdots c_n > 0$. Si $c_1 \cdots c_n > \det(M)$, montrer qu'il existe une solution dans $\mathbb{Z}^n$ non nulle du système d'équations

$$|L_i(x)| < c_i, \quad i \in \{1, \cdots, n\}.$$

(*d*) Soit q une forme quadratique définie positive sur $\mathbb{R}^n$, de matrice associée M dans la base canonique. Montrer qu'il existe un vecteur entier non nul $x \in \mathbb{Z}^n$ tel que $q(x) < \gamma_n \det(M)^{1/n}$.