ÉNS Lyon, Préparation à l'agrégation 2010

Théorème de Minkowski et applications

Le théorème de Minkowski affirme qu'étant donné un réseau de $\mathbf{R}^n$, toute partie convexe de $\mathbf{R}^n$, symétrique par rapport à l'origine et "suffisamment grosse" contient un point non nul du réseau. Plus précisément :

Théorème (Minkowski)**.** *Soit Λ un réseau de $\mathbf{R}^n$, et C une partie convexe de $\mathbf{R}^n$, symétrique par rapport à l'origine, borélienne et telle que $\mu(C) > 2^n\mu(\mathbf{R}^n/\Lambda)$, où μ est la mesure de Lebesgue sur $\mathbf{R}^n$. Alors l'ensemble $C \cap (\Lambda - \{0\})$ est non vide.*

Dans ce problème, on donne une démonstration de ce théorème (voir P. Samuel, *Théorie algébrique des nombres*, Hermann, 2003, Chapitre 4, §4.1). On donne ensuite une application au théorème des quatre carrés de Lagrange (voir P. Tauvel, *Géométrie*, 2ème édition, Dunod, 2005, Théorème 5.5.4), et une application aux formes quadratiques.

Soit Λ un réseau de $\mathbf{R}^n$. Un parallélotope fondamental pour Λ est une partie de la forme

$$P = \Big\{\sum_{i=1}^{n} a_i e_i ; a_1, \dots, a_n \in [0,1[\Big\},$$

où $(e_1, \dots, e_n)$ est une base de Λ comme $\mathbf{Z}$-module.

1. Montrer que la mesure $\mu(P)$ ne dépend pas du choix du parallélotope fondamental P. On l'appelle *covolume* du réseau Λ. On la notera $\mu(\mathbf{R}^n/\Lambda)$.
2. Soit A une partie de $\mathbf{R}^n$. Montrer que A est la réunion disjointe des $A \cap (\lambda + P)$ lorsque λ parcourt Λ.
3. On suppose que A est μ-mesurable et que $\mu(A) > \mu(\mathbf{R}^n/\Lambda)$. Montrer que les ensembles $A_\lambda := (A - \lambda) \cap P$ $(\lambda \in \Lambda)$ ne peuvent être deux à deux disjoints.
4. En déduire qu'il existe $x, y \in A$ distincts tels que $x - y \in \Lambda$.
5. Montrer le théorème de Minkowski (utiliser le résultat précédent avec $A = \frac{1}{2}C$).
6. Démontrer la variante suivante : si C est une partie convexe compacte de $\mathbf{R}^n$, symétrique par rapport à l'origine et telle que $\mu(C) \geq 2^n\mu(\mathbf{R}^n/\Lambda)$, alors $C \cap (\Lambda - \{0\})$ est non vide.
7. Pour chacune des versions du théorème de Minkowski, montrer que l'hypothèse sur la mesure de C ne peut être affaiblie.

Application 1 : le théorème des quatre carrés

Théorème (Lagrange)**.** *Tout entier naturel est somme de quatre carrés.*

1. Montrer que l'ensemble des sommes de 4 carrés dans $\mathbf{Z}$ est stable par multiplication (on pourra utiliser l'algèbre $\mathbf{H}$ des quaternions).

Soit p un nombre premier.

2. Montrer qu'il existe $r, s \in \mathbf{Z}$ tels que $r^2 + s^2 + 1 \equiv 0 \pmod{p}$.

3. Calculer le covolume du réseau $\Lambda = M\mathbf{Z}^4$ défini par la matrice

$$M = \begin{pmatrix} p & 0 & r & s \\ 0 & p & s & -r \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

4. Pour tout $\lambda \in \Lambda$, montrer que $\|\lambda\|^2 \equiv 0 \pmod{p}$, où $\|\cdot\|$ désigne la norme euclidienne usuelle sur $\mathbf{R}^4$.
5. En appliquant le théorème de Minkowski à une boule euclidienne convenable, montrer que p est somme de 4 carrés et conclure.

Application 2 : un résultat sur les formes quadratiques

Soit q une forme quadratique sur $\mathbf{R}^n$, et Λ un réseau de $\mathbf{R}^n$. On suppose que $q|_\Lambda \geq 0$ et que pour tout $C \in \mathbf{R}$, l'ensemble $\{x \in \Lambda; q(x) < C\}$ est fini. Le but de l'exercice est de montrer que q est définie positive.

1. Montrer que q est une forme quadratique positive.
2. Montrer que pour tout $\lambda \in \Lambda - \{0\}$, on a $q(\lambda) > 0$.
3. Montrer que q atteint un minimum $m > 0$ sur $\Lambda - \{0\}$.
4. On suppose par l'absurde que q n'est pas définie positive. Montrer que la partie $C = \{x \in \mathbf{R}^n; q(x) \leq \frac{m}{2}\}$ est de mesure infinie.
5. Conclure en utilisant le théorème de Minkowski.
6. Trouver une forme quadratique q sur $\mathbf{R}^2$ telle que $q(\lambda) > 0$ pour tout $\lambda \in \mathbf{Z}^2 - \{0\}$, mais qui n'est pas définie positive.

Remarque. Une application classique du théorème de Minkowski concerne la théorie des nombres (mais cela dépasse le niveau de l'agrégation) : si K est une extension finie de $\mathbf{Q}$, et si A est un sous-anneau de K formés d'entiers algébriques (par exemple $A = \mathbf{Z}[i]$ ou $A = \mathbf{Z}[\sqrt{2}]$), alors le groupe abélien A^* des inversibles de A est de type fini, et les "classes d'idéaux" de A sont en nombre fini (voir le livre de Samuel cité ci-dessus).