TD 7 : Géométrie des nombres

Exercice 1. [Autour du théorème de Minkowski]

(a) Donner un contre-exemple au théorème de Minkowski lorsque le volume du convexe est exactement 2^n fois le volume du réseau.

(b) Soient $L_1, \cdots, L_n$ des formes linéaires sur $\mathbb{R}^n$ définies par

$$L_i(x_1, \cdots, x_n) = \sum_{j=1}^{n} a_{ij} x_j, \qquad 1 \leq i \leq n,$$

et $M = (a_{ij})_{1 \leq i,j \leq n}$. Pour des réels positifs $c_1, \cdots, c_n$ tel que $c_1 \cdots c_n > |\det(M)|$, montrer qu'il existe un élément m de $\mathbb{Z}^n$ non nul tel que

$$|L_i(m)| < c_i, \qquad 1 \leq i \leq n.$$

(c) (*Petites normes d'éléments d'un réseau*). On note V_n le volume de la boule unité euclidienne dans $\mathbb{R}^n$. Montrer que pour tout réseau Λ, il existe un vecteur non nul de Λ de norme plus petite que

$$\frac{2}{V_n^{1/n}} \operatorname{vol}(\Lambda).$$

Ce résultat est-il optimal ? Tester pour $n = 1$ et 2.

(d) (*Petites valeurs de formes quadratiques*) 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

$$q(x) \leq \frac{\det(M)^{1/n}}{V_n^{1/n}}.$$

(e) Combiner les deux estimations précédentes, c'est-à-dire pour q et Λ à la fois.

Exercice 2. [Formule de Pick]

La formule de Pick est la suivante : étant donné un polygone convexe P de $\mathbb{R}^2$ dont les sommets sont à coordonnées entières, on a

$$\text{Aire}(P) = I + \frac{B}{2} - 1,$$

où I est le nombre de points de $\mathbb{Z}^2$ dans l'intérieur de P, et B le nombre de points sur le bord de P (incluant les sommets). Le but de l'exercice est de prouver ette formule.

On appelle triangle élémentaire un triangle de $\mathbb{R}^2$ un triangle de $\mathbb{R}^2$ à sommets dans $\mathbb{Z}^2$ n'ayant aucun autre point de $\mathbb{Z}^2$ ni sur ses arêtes ni dans son intérieur.

(a) Montrer qu'un triangle élémentaire a une aire au moins égale à $1/2$.

(b) Montrer que l'image d'un triangle élémentaire par une translation par $\mathbb{Z}^2$, ou une rotation d'angle π est encore un triangle élémentaire.

(c) Etant donné un triangle élémentaire T dont l'un des sommets est 0, fabriquer un convexe ne contenant pas de points entiers à part 0 et sur son bord d'aire exactement 8 fois celle de T.

(d) En déduire que l'aire d'un triangle élémentaire est exactement $1/2$ avec le théorème de Minkowski.

(*La suite n'utilise plus de géométrie des nombres, mais est pour les curieux de la preuve générales à partir du cas des triangles*).

(e) Étant donné un polygone P de $\mathbb{R}^2$ à sommets entiers, montrer qu'il peut s'écrire comme union de triangles deux à deux soit disjoints soit avec exactement une arête commune et à sommets entiers.

(f) Montrer qu'on peut même imposer que ces triangles soient élémentaires, et en déduire la formule de Pick générale.

Exercice 3. [Géométrie des nombres et formes quadratiques]

(a) Soit p un nombre premier congru à 1 modulo 4. Montrer qu'il existe $k \in \mathbb{Z}$ tel que $k^2 = -1 \mod p$. 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 $0 < a^2 + b^2 \leq (4/\pi)p$. Montrer que de plus p divise $a^2 + b^2$ ici, et en déduire que $a^2 + b^2 = p$.

La suite de l'exercice est consacrée à un théorème de Legendre : étant donné une forme quadratique indéfinie

$$q(x,y,z) = ax^2 + by^2 + cz^2 \quad (a,b,c \in \mathbb{Z}, abc \neq 0),$$

montrer qu'il existe une solution non nulle entière de $q(x,y,z) = 0$ si et seulement si il en existe une modulo p pour tout nombre premier p.

(b) Expliquer pourquoi il faut que q soit indéfinie, et qu'on peut se ramener à $a, b > 0$ et $c < 0$.

(c) Expliquer pourquoi on peut supposer que a, b, c sont globalement premiers entre eux, et sans facteur carré.

(d) Par changement de variables, montrer qu'on peut finalement se ramener à a, b et c premiers entre eux deux à deux, ce qu'on fera pour la suite.

(e) Soit p un éventuel diviseur premier impair de c et (x_p, y_p) une solution non nulle modulo p de $ax^2+by^2 = 0 \mod p$ par hypothèse. Construire à partir de (x_p, y_p) des formes linéaires L_p et L'_p à coefficients entiers telles que modulo p

$$ax^2 + by^2 = L_p(x,y,z) \cdot L'_p(x,y,z) \mod p$$

.

(f) En faisant de même avec les diviseurs premiers impairs de a ou b, et en étudiant le cas $p = 2$, construire deux formes linéaires L et L' à coefficients entiers telles que

$$ax^2 + by^2 - cz^2 = L(x,y,z) \cdot L'(x,y,z) \mod abc.$$

(g) Par le théorème de Minkowski appliqué au corps convexe C de $\mathbb{R}^3$ égal à $[-\sqrt{bc}, \sqrt{bc}] \times [-\sqrt{ac}, \sqrt{ac}] \times [-\sqrt{ab}, \sqrt{ab}]$ de $\mathbb{R}^3$, montrer qu'il existe une solution entière $(x, y, z) \in C \backslash \{0\}$ de $L(x, y, z) = 0 \mod abc$. En déduire que pour ce triplet,

$$q(x, y, z) = 0 \text{ ou } abc.$$

(h) Dans le cas où $q(x, y, z) = abc$, montrer que

$$q(xz + by, yz - ax, z^2 + ab) = 0.$$

Conclure.

Culture : Ce résultat est un cas particulier du théorème de Hasse-Minkowski : une n-forme quadratique à coefficients rationnels a un vecteur isotrope dans $\mathbb{Q}^n$ si et seulement si elle en a dans tous les $\mathbb{Q}_p$ et dans $\mathbb{R}$.