⑧ Le théorème de Minkowski

Proposition. Soient $\|\cdot\|$ une norme sur $\mathbb{R}^n$ et V le volume de la boule unité B. Soit r un entier naturel. Si $V \geq r\,2^n$, il existe

$$\pm u_1, \dots, \pm u_r \in \mathbb{Z}^n$$

de normes ≤ 1 et deux à deux distincts.

Démonstration : On traite d'abord le cas où $V > r\,2^n$. Soit $f = \mathbb{1}_{B(0,1/2)}$ la fonction indicatrice de la boule $B(0, \frac{1}{2})$ pour la norme $\|\cdot\|$. Posons

$$F(x) = \sum_{u \in \mathbb{Z}^n} f(x-u) = \sum_{\substack{u \in \mathbb{Z}^n \\ \|x-u\| < \frac{1}{2}}} 1$$

Somme finie !

Calculons

$$\int_{[0,1]^n} F(x)\,dx = \sum_{u \in \mathbb{Z}^n} \int_{[0,1]^n} f(x-u)\,dx$$

$$= \sum_{u \in \mathbb{Z}^n} \int_{u+[0,1]^n} f(x)\,dx$$

$$= \int_{\mathbb{R}^n} f(x)\,dx$$

$$= \mathrm{vol}\left(B\left(0, \tfrac{1}{2}\right)\right) = \frac{V}{2^n} > 2$$

Comme $\mathrm{vol}([0,1]^n) = 1$, il existe $x \in [0,1]^n$ tel que $F(x) > 2$, d'où $F(x) \geq 2+1$ car F est à valeurs entières. Il existe donc 3 éléments distincts $u_0, \dots, u_2 \in \mathbb{Z}^2$ tels que $f(x-u_i) \geq 1$, c'est-à-dire $\|x-u_i\| < \frac{1}{2}$.

Quitte à les renommer, on peut supposer que $u_0 \leq u_1 \leq u_2 \leq \dots$ pour l'ordre lexicographique sur $\mathbb{Z}^n$. Pour tout $i \in \{1, \dots, 2\}$,

$$\|u_i - u_0\| \leq \|x-u_i\| + \|x-u_0\| < \frac{1}{2} + \frac{1}{2} = 1$$

Les vecteurs de $\mathbb{Z}^n$ sont entiers et donc à deux distincts. De plus,

$$u_i - u_0 = -(u_j - u_0)$$

impliquant $u_0 = \dfrac{u_i + u_j}{2}$, en contradiction avec le fait que u_0 est le minimum pour l'ordre lexicographique. En effet, si

$$u_0 = (u_0^1, \dots, u_0^n)$$
$$u_i = (u_i^1, \dots u_i^n)$$
$$u_j = (u_j^1, \dots u_j^n)$$

$$u_0^1 \leq u_i^1 \leq u_j^1$$
$$\text{et } u_0^1 = \frac{u_i^1 + u_j^1}{2}$$
$$\Rightarrow u_0^1 = u_i^1 = u_j^1$$

et ainsi de suite. Les $2n$ vecteurs $\pm(u_i - u_0) \in \mathbb{Z}^n$ sont donc non nuls, deux à deux distincts et de normes ≤ 1.

Supposons maintenant $V = 2^n$. Considérons les normes $\alpha\|\cdot\|$ avec $\alpha > 1$ réel. Comme la boule de la boule unité pour cette norme est $\alpha^n V > 2^n$, il existe $2n$ vecteurs $\pm v_{1,\alpha}, \dots, \pm v_{n,\alpha} \in \mathbb{Z}^n$ non nuls, deux à deux distincts tels que $\|v_{i,\alpha}\| \leq \alpha$ pour tout i. Comme $B(0,\alpha)$ est compact, il existe une suite $(\alpha_n)_n$ telle que $\alpha_n \to 1$ et $v_{i,\alpha_n} \longrightarrow v_i$. On a alors $\|v_i\| \leq 1$. Comme les vecteurs v_{i,α_n} sont à coordonnées entières, on a finalement $v_{i,\alpha_n} = v_i$ pour n assez grand. En particulier, les $2n$ vecteurs $\pm v_1, \dots, \pm v_n$ sont non nuls, deux à deux distincts, de normes ≤ 1 □

Théorème (Minkowski) Soient G un réseau de rang n de $\mathbb{R}^n$ et $\|\cdot\|$ une norme sur $\mathbb{R}^n$ de boule unité B. Il existe $u \in G$ non nul tel que

$$\|u\| \leq 2 \left(\frac{V(G)}{\mathrm{vol}(B)} \right)^{1/n}$$

où $V(G) = |\det(u_1, \dots, u_n)|$ pour une base

$(u_1, \dots, u_n)$ de G.

Démonstration : Soit A la matrice de la base $(u_1, \dots, u_n)$ de G. Considérons la norme $\|\cdot\|'$ sur $\mathbb{R}^n$ donnée par

$$\|x\|' = \alpha \|Ax\|$$

où $\alpha = \frac{1}{2}\left(\frac{\mathrm{vol}(B)}{V(G)}\right)^{1/n}$. La boule unité B' pour cette norme est égale à $\alpha^{-1} A^{-1} B$ et a donc volume

$$\frac{\mathrm{vol}(B)}{\alpha^n |\det A|} = \frac{2^n V(G)}{|\det A|} = 2^n$$

D'après la proposition, il existe $x \in \mathbb{Z}^n$ non nul (puisque x et $-x$ sont distincts) tel que $\|x\|' \leq 1$. Alors le vecteur

$$u = x_1 u_1 + \dots + x_n u_n \in G$$

satisfait à

$$\|u\| = \|Ax\| = \frac{\|x'\|}{\alpha} \leq 2\left(\frac{V(G)}{\mathrm{vol}(B)}\right)^{1/n},$$

ce qu'il fallait démontrer □

Pour appliquer le théorème de Minkowski, il est utile de se rappeler que la boule unité B de $\mathbb{R}^n$ pour la norme euclidienne a volume

$$\mathrm{vol}(B) = \frac{\pi^{n/2}}{\Gamma(1+\frac{n}{2})}$$

où $\Gamma(s) = \int_0^\infty e^{-x} x^{s-1} dx$ désigne la fonction gamma d'Euler.

Application : somme de 4 carrés

Lemme : Soient $l_1, \dots, l_2 : \mathbb{Z}^n \to \mathbb{Z}$ des formes linéaires et $d_1, \dots d_2 \geq 1$ des entiers. L'ensemble

$$G = \{ x \in \mathbb{Z}^n \mid l_i(x) \equiv 0 \bmod d_i \}$$

est un réseau de rang n de $\mathbb{R}^n$ tel que

$$V(G) \leq d_1 \dots d_2 .$$

Preuve : Il suffit de montrer que $\mathbb{Z}^n/G$ est un groupe fini de cardinal $\leq d_1 \dots d_2$. (En effet, $G \subset \mathbb{Z}^n$ est discret dans $\mathbb{R}^n$, donc c'est le groupe abélien libre engendré

par une famille libre $(u_1, \dots, u_r)$ de $\mathbb{R}^n$. Si le quotient $\mathbb{Z}^n/G$ est fini, alors $r = n$, c'est-à-dire G est un réseau de rang n de $\mathbb{R}^n$. Par le théorème de la base adaptée, appliqué à $G \subset \mathbb{Z}^n$, il existe une base $w_1, \dots w_n$ de $\mathbb{Z}^n$ et des entiers $c_1, \dots, c_n$ tels que $(c_1 w_1, \dots, c_n w_n)$ soit une base de G. Alors

$$\left|\mathbb{Z}^n/G\right| = c_1 \dots c_n = \frac{V(G)}{V(\mathbb{Z}^n)} = V(G).$$

Considérons l'application

$$\begin{aligned} L : \mathbb{Z}^n &\longrightarrow \prod_{i=1}^{n} \mathbb{Z}/d_i\mathbb{Z} \\ X &\longmapsto (l_i(x) \bmod d_i) \end{aligned}$$

qui est un morphisme de groupes de noyau G.

Alors $\mathbb{Z}^n/G \simeq \operatorname{Im} L \subset \prod_{i=1}^{n} \mathbb{Z}/d_i\mathbb{Z}$

est fini de cardinal un diviseur de $d_1 \dots d_n$ □

<u>Lemme</u> : Pour tout p premier, il existe des entiers a, b tels que

$$p \mid a^2 + b^2 + 1.$$

Preuve : Il y a $1 + \frac{p-1}{2} = \frac{p+1}{2}$ éléments de $\mathbb{Z}/p\mathbb{Z}$ de la forme a^2, et de même pour $-1-b^2$. Comme $\frac{p+1}{2} + \frac{p+1}{2} > p$, il existe $a, b \in \mathbb{Z}/p\mathbb{Z}$ tels que $a^2 = -1-b^2$, c'est-à-dire $a^2 + b^2 + 1 = 0$. □

Théorème (Lagrange) Pour tout entier $n \geq 0$, il existe des entiers x, y, z, t tels que

$$n = x^2 + y^2 + z^2 + t^2$$

Preuve : On peut supposer n sans facteur carré ; car si $n = x^2 + y^2 + z^2 + t^2$, alors

$$nr^2 = (xr)^2 + (yr)^2 + (zr)^2 + (tr)^2.$$

Soit p un facteur premier de n. Soient $a_p, b_p \in \mathbb{Z}$ tels que $p \mid a_p^2 + b_p^2 + 1$. Alors

$$G = \left\{ (x,y,z,t) \in \mathbb{Z}^4 \;\middle|\; \begin{array}{l} x \equiv a_p z + b_p t \\ y \equiv b_p z - a_p t \end{array} \mod p \right\}$$

est un réseau de rang 4 de $\mathbb{R}^4$ tel que $V(G) \leq n^2$ par le lemme précédent, appliqué aux formes linéaires

$$x - a_p z - b_p t, \quad y - b_p z - a_p t$$

pour tous les facteurs premiers p de n.
D'après le théorème de Minkowski, il existe
$(x,y,z,t) \in G$ non nul tel que

$$\sqrt{x^2+y^2+z^2+t^2} \leq 2\left(\frac{n^2}{\pi^{4/2}/\Gamma(1+\frac{4}{2})}\right)^{1/4}$$

$$= 2\left(\frac{2n^2}{\pi^2}\right)^{1/4}$$

$$\Rightarrow \quad x^2+y^2+z^2+t^2 \leq \frac{4\sqrt{2}}{\pi} n < 2n$$

Posons $N = x^2+y^2+z^2+t^2$ et démontrons que $N = n$. Pour chaque $p \mid n$,

$$N = x^2+y^2+z^2+t^2$$
$$\equiv (a_p z + b_p t)^2 + (b_p z - a_p t)^2 + z^2 + t^2$$
$$\equiv (a_p^2 + b_p^2 + 1) z^2 + (b_p^2 + a_p^2 + 1) t^2$$
$$\equiv 0 \mod p,$$

donc $p \mid N$. Il s'ensuit que $n \mid N$. Mais $0 < N < 2n$, donc nécessairement $N = n$ et

$$n = x^2+y^2+z^2+t^2$$

□