

Borne de Minkowski

L'exposition qui suit est tirée de P. Samuel : *Théorie algébrique des nombres*, pages $67-70$.

I. Résultats préparatoires

On commence par démontrer le résultat suivant, dû à Minkowski.

Théorème 1. *Soit H un réseau (i.e. un sous-groupe discret de rang n) de $\mathbf{R}^n$ et S une partie Lebesgue-mesurable de $\mathbf{R}^n$ tels que $\mu(S) > v(H)$ (ici μ désigne la mesure de Lebesgue et $v(H)$ est la mesure d'un domaine fondamental P_e (défini dans la preuve) de $\mathbf{R}^n$ relativement à H). Alors il existe des éléments distincts $x, y \in S$ tels que $x - y \in H$.*

Preuve. Soit $e = (e_1, \dots e_n)$ une $\mathbf{Z}$-base de H et

$$P_e = \left\{ \sum_{i=1}^{n} \alpha_i e_i \colon 0 \leqslant \alpha_i < 1 \right\} . \tag{1}$$

Tout point de $\mathbf{R}^n$ est congru modulo H à un unique point de P_e i.e. P_e est un domaine fondamental pour $\mathbf{R}^n$ relativement à H. (Vérifier que $v(H) := \mu(P_e)$ est indépendant du choix de la base e.) On déduit que S est réunion disjointe des $S \cap (h + P_e)$, lorsque h parcourt H. En particulier

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

Les ensembles $(-h + S) \cap P_e$ ne peuvent être deux à deux disjoints lorsque h parcourt H : en effet, on aurait sinon $\mu(P_e) \geqslant \sum_{h \in H} \mu\left((-h + S) \cap P_e\right)$. Cela contredirait (1) et l'hypothèse du théorème. On déduit l'existence de $h, h' \in H$ distincts tels que $P_e \cap (-h + S) \cap (-h' + S) \neq \emptyset$. On a donc des éléments $x, y \in S$ tels que $-h + x = -h' + y$. Ainsi $x - y = h - h' \in H$ et $x \neq y$ car $h \neq h'$. □

On déduit le corollaire suivant.

Corollaire 1. *Soit H un réseau de $\mathbf{R}^n$ et S une partie Lebesgue-mesurable de $\mathbf{R}^n$ dont on suppose qu'elle est symétrique par rapport à 0 et convexe. On suppose en outre l'une des deux conditions suivantes vérifiée :*

(a) on a $\mu(S) > 2^n v(H)$,

(b) on a $\mu(S) \geqslant 2^n v(H)$ et S est compacte,

alors $S \cap H$ contient un autre point que 0.

Preuve. Dans le cas (a) on applique le théorème 1 à $S' = \frac{1}{2}S$ qui vérifie :

$$\mu(S') = \frac{1}{2^n}\mu(S) > v(H) .$$

Il existe donc deux points distincts $y, z \in S'$ tels que $y - z \in H$. Alors $x := y - z = (1/2)(2y + (-2z))$ est un point de S (rappelons que S est symétrique par rapport à 0 et convexe) qui répond à la question. Pour (b), on applique le cas (a) à $(1 + \varepsilon)S$, où $\varepsilon > 0$ est fixé, quelconque.

En posant $H' = H \setminus \{0\}$, on voit que $H' \cap (1+\varepsilon)S$ est non vide et est fini car discret et compact. Alors $\cap_{\varepsilon>0} H' \cap (1+\varepsilon)S$ est non vide. Tout élément de cette intersection est en particulier dans $\cap_{\varepsilon>0}(1+\varepsilon)S$ qui est égal à S puisque S est compact.□

On se donne maintenant un corps de nombres $K/\mathbf{Q}$ de degré n. Il existe n plongements $\sigma_i \colon K \hookrightarrow \mathbf{C}$. On note r_1 le nombre d'indices i tels que σ_i est à valeurs réelles. Si σ_j n'est pas à valeurs réelles alors $\overline{\sigma_j}$ est un plongement différent, qui n'est pas non plus à valeurs réelles. Quitte à renuméroter on peut donc supposer σ_i à valeurs réelles pour $1 \leqslant i \leqslant r_1$, et $\overline{\sigma_{r_1+j}} = \sigma_{r_1+r_2+j}$ où $2r_2 = n - r_1$ et $1 \leqslant j \leqslant r_2$. On appelle *plongement canonique* de K dans $\mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$ l'application

$$\sigma \colon x \in K \mapsto (\sigma_1(x), \dots, \sigma_{r_1+r_2}(x)) \,.$$

Avec ces notations, on a :

Proposition 1. *Soit M un sous-$\mathbf{Z}$-module libre de rang n de K et soit (x_i) une $\mathbf{Z}$-base de M. Alors $\sigma(M)$ est un $\mathbf{Z}$-module libre de rang n de $\mathbf{R}^n$. De plus*

$$v\left(\sigma(M)\right) = 2^{-r_2} |\det(\sigma_i(x_j))_{i,j}| \,.$$

Preuve. Pour chaque i, les composantes de $\sigma(x_i)$ dans la base canonique de $\mathbf{R}^n$ sont :

$$\sigma_1(x_i) \dots, \sigma_{r_1}(x_i), \Re(\sigma_{r_1+1}(x_i)), \Im(\sigma_{r_1+1}(x_i)), \dots, \Re(\sigma_{r_1+r_2}(x_i)), \Im(\sigma_{r_1+r_2}(x_i)) \,.$$

Soit D le déterminant de la matrice dont la i-ème colonne est donnée ci-dessus. En utilisant les formules $\Re z = 2^{-1}(z + \bar{z})$ et $\Im z = (2i)^{-1}(z - \bar{z})$ et la linéarité du déterminant par rapport aux lignes, on voit facilement que $D = \pm(2i)^{-r_2} \det(\sigma_i(x_j))_{i,j}$. Comme (x_i) est une $\mathbf{Q}$-base de K, et puisque, comme vu en TD, $(\det(\sigma_i(x_j))_{i,j})^2 = \operatorname{disc}(x_1, \dots, x_n)$, on déduit $D \neq 0$. Cela prouve que $\sigma(M)$ est un $\mathbf{Z}$-module libre de rang n. La formule pour le volume de $v(\sigma(M))$ se déduit du calcul de D et du fait que le volume d'un domaine fondamental de $\mathbf{R}^n$ relativement à $\mathbf{Z}^n$ est 1.□.

Proposition 2. *Soit δ_K le discriminant de K et $\mathcal{O}_K$ son anneau d'entiers. Soit $\mathfrak{a}$ un idéal entier non nul de $\mathcal{O}_K$. Alors $\sigma(\mathcal{O}_K)$ et $\sigma(\mathfrak{a})$ sont des sous-$\mathbf{Z}$-modules libres de rang n de $\mathbf{R}^n$ et on a :*

$$v\left(\sigma(\mathcal{O}_K)\right) = 2^{-r_2}|\delta_K|^{1/2} \,,\ v\left(\sigma(a)\right) = 2^{-r_2}|\delta_K|^{1/2}\mathcal{N}\mathfrak{a} \,.$$

Preuve. D'après le cours on sait que $\mathcal{O}_K$ et $\mathfrak{a}$ sont des $\mathbf{Z}$-modules libres de rang n. On peut donc appliquer la proposition 1. On a vu en TD : si (x_i) est une $\mathbf{Z}$-base de $\mathcal{O}_K$ alors $\delta_K = (\det(\sigma_i(x_j))_{i,j})^2$. Cela démontre la première formule. La seconde formule s'en déduit en remarquant que $\sigma(\mathfrak{a})$ est d'indice $\mathcal{N}\mathfrak{a}$ dans $\sigma(\mathcal{O}_K)$ et qu'on obtient donc un domaine fondamental relativemement à $\sigma(\mathfrak{a})$ en prenant la réunion disjointe de $\mathcal{N}\mathfrak{a}$ domaines fondamentaux relatifs à $\sigma(\mathcal{O}_K)$.□

II. Borne de Minkowski

On commence par relier la norme de tout idéal entier non nul $\mathfrak{a}$ de $\mathcal{O}_K$ à la norme d'un élément de $\mathfrak{a}$.

Proposition 3. *Soit K un corps de nombres de degré n et de discriminant δ_K. On note r_1 (resp. r_2) le nombre de plongements réels (resp. le nombre de plongements complexes 2 à 2 conjugués) de K dans $\mathbf{C}$. Alors tout idéal entier non nul $\mathfrak{a}$ de $\mathcal{O}_K$ contient un élément non nul x tel que*

$$\mathcal{N}_{K/\mathbf{Q}}(x) \leqslant \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |\delta_K|^{1/2} \mathcal{N}\mathfrak{a} \,.$$

Preuve. On note toujours σ le plongement canonique de K. Pour $t > 0$ fixé, on considère

$$B_t = \left\{ (y_1 \dots, y_{r_1}, z_1, \dots, z_{r_2}) \in \mathbf{R}^{r_1} \times \mathbf{C}^{r_2} \colon \sum_{i=1}^{r_1} |y_i| + 2 \sum_{j=1}^{r_2} |z_j| \leqslant t \right\} .$$

L'ensemble B_t est compact, convexe, symétrique par rapport à 0. Dans la section 3 on montre que sa mesure de Lebesgue est

$$\mu(B_t) = 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{t^n}{n!} .$$

Partant de cette formule, on fixe t tel que $\mu(B_t) = 2^n v(\sigma(\mathfrak{a}))$ i.e., d'après la proposition 2,

$$2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{t^n}{n!} = 2^{n-r_2} |\delta_K|^{1/2} \mathcal{N}\mathfrak{a} . \tag{2}$$

D'après le corollaire 1, il existe $x \in \mathfrak{a} \setminus \{0\}$ tel que $\sigma(x) \in B_t$. En conservant la numérotation des σ_i adoptée avant l'énoncé de la proposition 1, on calcule la norme de cet élément (voir la formule démontrée en TD) :

$$|\mathcal{N}_{K/\mathbf{Q}}(x)| = \prod_{i=1}^{r_1} |\sigma_i(x)| \prod_{j=r_1+1}^{r_1+r_2} |\sigma_j(x)|^2 .$$

D'après l'inégalité arithmético-géométrique, on déduit

$$|\mathcal{N}_{K/\mathbf{Q}}(x)| \leqslant \left(\frac{1}{n} \sum_{i=1}^{r_1} |\sigma_i(x)| + \frac{2}{n} \sum_{j=r_1+1}^{r_1+r_2} |\sigma_j(x)| \right)^n \leqslant \frac{t^n}{n^n} ,$$

puisque $\sigma(x) \in B_t$. On conclut en combinant (2) et le fait que $r_1 + 2r_2 = n$. □

On déduit (enfin !) la borne de Minkowski.

Corollaire 2. *On conserve les notations de la proposition* 3. *Toute classe d'idéaux de K contient un idéal entier $\mathfrak{b}$ tel que*

$$\mathcal{N}\mathfrak{b} \leqslant \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |\delta_K|^{1/2} .$$

Preuve. Soit $\mathfrak{a}'$ un idéal de la classe donnée. Il est nécessairement non nul par définition du groupe des classes. Quitte à multiplier par un idéal principal convenable on peut supposer que $\mathfrak{a} := (\mathfrak{a}')^{-1}$ est un idéal entier. Appliquons alors la proposition 3 à l'idéal $\mathfrak{a}$. On obtient un élément $x \in \mathfrak{a}$ tel que $\mathfrak{b} := (x)\mathfrak{a}^{-1}$ appartient à la classe donnée et tel que $\mathcal{N}\mathfrak{b}$ satisfait l'inégalité voulue, par multiplicativité de la norme.

III. Calcul de $\mu(B_t)$

On reprend les notations de la preuve de la proposition 3. On va montrer par double récurrence sur r_1 et r_2 vérifiant $r_1 + r_2 \geqslant 1$ que

$$\mu(B_t) = 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{t^n}{n!} .$$

Pour insister sur la dépendance en r_1, r_2 on note $V(r_1, r_2, t) := \mu(B_t)$. On remarque :

$$\begin{aligned} V(1,0,t) &= 2t \ \text{ (c'est la mesure du segment } [-t,t]) , \\ V(0,1,t) &= \frac{\pi t^2}{4} \ \text{ (c'est la mesure d'un disque de rayon } t/2) . \end{aligned}$$

Montrons que la formule au rang r_1 entraine la formule au rang r_1+1 (à r_2 constant).

L'ensemble $B_t \subset \mathbf{R} \times \mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$, correspondant aux rangs r_1+1 et r_2, est défini, pour $y \in \mathbf{R}$ par

$$|y| + \sum_{i=1}^{r_1} |y_i| + 2\sum_{j=1}^{r_2} |z_j| \leqslant t\,.$$

Ainsi

$$V(r_1+1, r_2, t) = \int_{\mathbf{R}} V(r_1, r_2, t-|y|)dy = \int_{-t}^{t} V(r_1, r_2, t-|y|)dy\,,$$

et, par hypothèse de récurrence,

$$V(r_1+1, r_2, t) = 2\int_0^t 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2} \frac{(t-y)^n}{n!}dy = 2^{r_1+1}\left(\frac{\pi}{2}\right)^{r_2} \frac{t^{n+1}}{(n+1)!}\,.$$

Montrons maintenant que la formule au rang r_2 entraine la formule au rang r_2+1 (à r_1 constant). L'ensemble $B_t \subset \mathbf{R}^{r_1} \times \mathbf{C}^{r_2} \times \mathbf{C}$, correspondant aux rangs r_1 et r_2+1, est défini, pour $z \in \mathbf{C}$ par

$$\sum_{i=1}^{r_1} |y_i| + 2\sum_{j=1}^{r_2} |z_j| + |z| \leqslant t\,.$$

Ainsi

$$V(r_1, r_2+1, t) = \int_{\mathbf{C}} V(r_1, r_2, t-2|z|)dz = \int_{|z|\leqslant t/2} V(r_1, r_2, t-2|z|)dz\,,$$

où dz est la mesure de Lebesgue sur $\mathbf{C}$. On fait le changement de variables $z = \rho e^{i\theta}$, $\rho \in \mathbf{R}^+$, $0 \leqslant \theta \leqslant 2\pi$, de jacobien ρ. Par hypothèse de récurrence, on obtient :

$$\begin{aligned} V(r_1, r_2+1, t) &= \int_{\rho=0}^{t/2}\int_{\theta=0}^{2\pi} 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2} \frac{(t-2\rho)^n}{n!}\rho\, d\rho\, d\theta \\ &= 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2} \frac{2\pi}{n!}\int_0^{t/2} (t-2\rho)^n \rho\, d\rho\,. \end{aligned}$$

Pour calculer l'intégrale restante dans le membre de droite, on pose $2\rho = x$ et l'on intègre par parties. On obtient la valeur suivante pour cette intégrale : $\dfrac{t^{n+2}}{4(n+1)(n+2)}$. Finalement

$$V(r_1, r_2+1, t) = 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2+1} \frac{t^{n+2}}{(n+2)!}\,,$$

c'est bien ce que l'on voulait obtenir car $r_1 + 2(r_2+1) = n+2$.