

V

La géométrie des nombres et le groupe des classes

1. La finitude du groupe des classes

Soit K une extension de degré d de $\mathbf{Q}$. Soit L une extension normale (et donc galoisienne) de $\mathbf{Q}$ qui contient K et qui est contenue dans $\mathbf{C}$.

Soient $\sigma_1, \dots, \sigma_d$ des représentants de $\text{Gal}(L/\mathbf{Q})/\text{Gal}(L/K)$. Ce sont des plongements de K dans $\mathbf{C}$. Considérons ceux d'entre eux dont l'image est contenue dans $\mathbf{R}$ (les *places réelles* de K). Numérotons-les $\sigma_1, \dots, \sigma_{r_1}$. Les autres (les *places complexes non réelles* de K) sont intervertis deux-à-deux par la conjugaison complexe. Écrivons-les sous la forme $\sigma_{r_1+1}, \dots, \sigma_{r_1+r_2}, \sigma_{r_1+r_2+1} = \bar{\sigma}_{r_1+1}, \dots, \sigma_d = \bar{\sigma}_{r_1+r_2}$. Les entiers r_1 et r_2 ne dépendent pas du choix de L . On a

$$d = r_1 + 2r_2.$$

Notons $\mathcal{O}_K$ l'anneau des entiers de K . Notons $\mathcal{Cl}(K)$ le *groupe des classes* de K , c'est-à-dire le groupe obtenu en considérant le quotient du groupe des idéaux fractionnaires de K par le sous-groupe des idéaux fractionnaires principaux.

THÉORÈME 1. — *Le groupe $\mathcal{Cl}(K)$ est fini.*

Le théorème 1 est dû à Dirichlet. On va voir qu'il résulte du théorème de Minkowski, qui a été démontré postérieurement. Il n'est pas valide si K est remplacé par le corps des fractions d'un anneau de Dedekind quelconque.

PROPOSITION 1. — *Soit M un nombre entier > 0 . Il n'existe qu'un nombre fini d'idéaux I de $\mathcal{O}_K$ norme absolue $< M$.*

Démonstration. — Notons N_I la norme d'un idéal I . Soient I_1 et I_2 deux idéaux premiers entre eux de $\mathcal{O}_K$. On a

$$N_{I_1 I_2} = N_{I_1} N_{I_2}.$$

Soit $\mathcal{P}$ un idéal premier. Le $\mathcal{O}_K/\mathcal{P}$ -espace vectoriel $\mathcal{P}^k/\mathcal{P}^{k+1}$ est de dimension 1. On a donc

$$N_{\mathcal{P}^k} = N_{\mathcal{P}}^k.$$

La fonction $I \mapsto N_I$ est donc multiplicative.

Il suffit donc de prouver qu'il n'existe qu'un nombre fini d'idéaux premiers de $\mathcal{P}$ de norme $< M$. Cela résulte du fait qu'il n'existe qu'un nombre fini de nombres premiers $< M$ et du fait qu'il n'y a nombre fini d'idéaux premiers de $\mathcal{O}_K$ au dessus de ces nombres premiers.

Pour démontrer la finitude du groupe des classes, il suffit donc de démontrer qu'il existe un nombre M_K ne dépendant que de K tel que tout élément de $\mathcal{C}\ell(K)$ possède un représentant dans $\mathcal{O}_K$ de norme $< M_K$. C'est l'objet du théorème de Minkowski.

Remarque . — Lors de la démonstration de la formule du nombre de classes, on comptera le nombre d'idéaux de $\mathcal{O}_K$ dans une classe donnée et de norme absolue bornée.

2. Le théorème de Minkowski

C'est le théorème suivant. Reprenons les notations de la section précédente. Rappelons que $\mathcal{D}_K$ est le discriminant absolu de K .

THÉORÈME 2. — *Tout élément de $\mathcal{C}\ell(K)$ possède un représentant J dans $\mathcal{O}_K$ de norme N_J vérifiant*

$$N_J \leq \frac{d!}{d^d} \left(\frac{\pi}{4}\right)^{-r_2} |\mathcal{D}_K|^{1/2}.$$

La quantité $\frac{d!}{d^d} \left(\frac{\pi}{4}\right)^{r_2} = M(r_1, r_2)$ est la *constante de Minkowski* du corps K . Voici les valeurs approchées de cette constantes pour $d \leq 5$: $M(1, 0) = 1$, $M(0, 1) = 0,63661$, $M(2, 0) = 0,5$, $M(1, 1) = 0,28299$, $M(3, 0) = 0,22222$, $M(0, 2) = 0,15198$, $M(2, 1) = 0,11937$, $M(4, 0) = 0,09375$, $M(1, 2) = 0,06225$, $M(3, 1) = 0,04889$, $M(5, 0) = 0,0384$.

On démontrera le théorème 2 dans les sections suivantes. Indiquons-en quelques conséquences.

COROLLAIRE 1. — *On a l'inégalité :*

$$|\mathcal{D}_K| \geq \left(\frac{\pi}{4}\right)^{2r_2} \frac{d^{2d}}{(d!)^2}.$$

Démonstration. — Cela résulte du théorème 2 en remarquant que la norme d'un idéal quelconque de $\mathcal{O}_K$ est ≥ 1 .

COROLLAIRE 2. — *Il n'y a pas d'extension de corps de $\mathbf{Q}$ non ramifiée autre que $\mathbf{Q}$.*

Démonstration. — Il suffit de remarquer que les quantités

$$|\mathcal{D}_K|^{1/2} \geq \left(\frac{\pi}{4}\right)^{r_2} \frac{d^d}{d!} \geq \left(\frac{\pi}{4}\right)^{d/2} \frac{d^d}{d!},$$

sont > 1 pour $d > 1$. Il existe donc un diviseur premier de $\mathcal{D}_K$. Ce nombre premier est donc ramifié dans l'extension $K/\mathbf{Q}$.

Le corollaire 2 est dû à Hermite. Le corollaire 3 ci-dessous pourrait aussi se déduire de la (difficile) loi de réciprocité d'Artin. Le corps de classe de Hilbert H_K d'un corps de

nombres K est la plus grande extension abélienne $H_K|K$ partout non ramifiée et telle que toutes les places réelles de K se prolongent en des places réelles de H_K . On reviendra par la suite sur ce corps.

COROLLAIRE 3. — *Le corps de classe de Hilbert de $\mathbf{Q}$ est égal à $\mathbf{Q}$.*

Démonstration. — Cela résulte du corollaire 1 puisque le corps de classe de Hilbert est une extension non ramifiée.

COROLLAIRE 4. — *Le discriminant d'un corps tend vers l'infini lorsque le degré tend vers l'infini.*

Démonstration. — Il suffit de vérifier que l'expression $\mathcal{D}_K \geq (\frac{\pi}{4})^{2r_2} \frac{d^{2d}}{(d!)^2}$ tend vers l'infini lorsque d tend vers l'infini.

Remarque . — La “réciproque” du corollaire 3 est fautive : Le discriminant d'un corps quadratique peut être arbitrairement grand (plus précisément, lorsque p est un nombre premier, le discriminant absolu du corps $\mathbf{Q}(\sqrt{p})$ est divisible par p). Le théorème d'Hermite est une version plus forte du corollaire 4.

On va voir que le théorème de Minkowski résulte de la proposition suivante.

PROPOSITION 2. — *Soit I un idéal non nul de $\mathcal{O}_K$. Il existe un élément a non nul de I tel que*

$$N_{K/\mathbf{Q}}(a) \leq \frac{d!}{d^d} \left(\frac{4}{\pi}\right)^{r_2} N_I |\mathcal{D}_K|^{1/2}.$$

Cela entraîne le théorème de Minkowski.

Démonstration. — Soit I' un idéal fractionnaire de K . Soit $b \in I'$ tel que bI'^{-1} soit un idéal de $\mathcal{O}_K$. Appliquons la proposition 2 à $I = bI'^{-1}$: Il existe $a \in bI'^{-1}$ tel que

$$N_{K/\mathbf{Q}}(a) \leq \frac{d!}{d^d} \left(\frac{4}{\pi}\right)^{r_2} N_{bI'^{-1}} |\mathcal{D}_K|^{1/2}.$$

Posons $J = (a/b)I'$. C'est un idéal fractionnaire de même classe que I' . Il est contenu dans $\mathcal{O}_K$ car $a \in bI'^{-1}$. On a

$$N_J = N_{I'b^{-1}} N_{K/\mathbf{Q}}(a) = N_{K/\mathbf{Q}}(a) / N_{I'^{-1}b}$$

On a donc

$$N_{K/\mathbf{Q}}(a) \leq \frac{d!}{d^d} \left(\frac{4}{\pi}\right)^{r_2} N_J^{-1} N_{K/\mathbf{Q}}(a) |\mathcal{D}_K|^{1/2}.$$

et donc

$$N_J \leq \frac{d!}{d^d} \left(\frac{\pi}{4}\right)^{-r_2} |\mathcal{D}_K|^{1/2}.$$

On a donc prouvé que tout idéal fractionnaire de K est dans même classe qu'un idéal entier de $\mathcal{O}_K$ de norme absolue vérifiant l'inégalité demandée.

3. Ingrédients disparates

Rappelons qu'un *réseau* de $\mathbf{R}^d$ est un sous-groupe discret de $\mathbf{R}^d$ isomorphe à $\mathbf{Z}^d$. Il revient au même de dire que c'est un sous-groupe abélien engendré sur $\mathbf{Z}$ par une base sur $\mathbf{R}$ de $\mathbf{R}^d$. Rappelons que le *volume* $\text{vol}(E)$ d'un ensemble mesurable E est sa mesure de Lebesgue. Le volume d'un réseau L est par abus de notation le volume de $\mathbf{R}^d/L$.

PROPOSITION 3. — *Soit L un réseau de $\mathbf{R}^d$. Soit X un sous-ensemble de $\mathbf{R}^d$ borné, convexe et symétrique par rapport à l'origine (i.e. stable par $x \mapsto -x$). Supposons de plus qu'on ait*

$$\text{vol}(X) > 2^d \text{vol}(L).$$

Alors l'ensemble $X \cap (L - \{0\})$ est non vide.

Démonstration. —

Le volume de L est le volume d'un parallépipède fondamental de L (rappelons qu'un *parallépipède fondamental* est un parallépipède P ouvert de $\mathbf{R}^d$ tel que deux éléments distincts de P définissent deux classes distinctes de $\mathbf{R}^d/L$ et tel que tout élément de $\mathbf{R}^d/L$ ait un représentant dans l'adhérence de P).

Lemme 2. — *Soit A un sous-ensemble borné de $\mathbf{R}^d$, tel que deux éléments distincts de A définissent deux éléments distincts de $\mathbf{R}^d/L$. Alors on a $\text{vol}(A) \leq \text{vol}(L)$.*

Démonstration. — Puisque A est borné il est contenu dans l'adhérence d'un nombre fini de parallépipèdes fondamentaux. Rappelons que la translation préserve le volume. Quitte à décomposer A en un nombre fini de sous-ensemble que l'on translate par des éléments de L , on peut supposer que A est contenu dans l'adhérence $\bar{P}$ d'un parallépipède fondamental. On a donc $\text{vol}(A) \leq \text{vol}(\bar{P}) = \text{vol}(P)$. La dernière égalité provient du fait que P est ouvert.

Déduisons la proposition 3 du lemme 2. Considérons l'ensemble

$$\frac{1}{2}X = \left\{ \frac{1}{2}x \mid x \in X \right\}.$$

Son volume est égal à $2^{-d} \text{vol}(X) > \text{vol}(L)$. D'après le lemme 1, il existe deux éléments distincts x et y de $\frac{1}{2}X$ qui sont congrus modulo L . On a donc $x - y \in L$. Comme $2x$ et $2y$ sont éléments de X et comme X est convexe et symétrique, on a $\frac{2x-2y}{2} = x - y \in X$. On a donc un élément non nul de $X \cap L$.

Considérons l'application $v_K : K \mapsto \mathbf{R}^d \simeq \mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$ qui à $x \in K$ associe $(\sigma_1(x), \dots, \sigma_{r_1}(x), \sigma_{r_1+1}(x), \dots, \sigma_{r_1+r_2}(x))$. C'est un homomorphisme de groupes. Précisons que l'identification entre $\mathbf{C}$ et $\mathbf{R}^2$ est donnée par l'application qui à un nombre complexe associe le couple formé par sa partie réelle et sa partie imaginaire. On en déduit l'identification $\mathbf{R}^{r_1} \times \mathbf{C}^{r_2} \simeq \mathbf{R}^d$.

PROPOSITION 4. — *Soit I un idéal de $\mathcal{O}_K$. L'image de I par v_K est un réseau de volume $2^{-r_2} N_I |\mathcal{D}_K|^{1/2}$.*

Démonstration. — C'est essentiellement le lemme suivant.

Lemme 2. — Soit M un sous- $\mathbf{Z}$ -module libre de rang d de K de base $(x_i)_{i=1,\dots,d}$. Alors $v_K(M)$ est un réseau de $\mathbf{R}^d$ dont le volume est donné par la formule :

$$\text{vol}(v_K(M)) = 2^{-r_2} |\det(\sigma_j(x_i))|.$$

Démonstration. — L'image de $v_K(M)$ dans $\mathbf{R}^d$ est engendrée comme $\mathbf{Z}$ -module par les $U_i = (\sigma_1(x_i), \dots, \sigma_{r_1}(x_i), \text{Re}(\sigma_{r_1+1}(x_i)), \text{Im}(\sigma_{r_1+1}(x_i)), \dots, \text{Re}(\sigma_{r_1+r_2}(x_i)), \text{Im}(\sigma_{r_1+r_2}(x_i)))$. Remarquons qu'on a $|\det(U, \bar{U})| = 2|\det(\text{Re}(U), \text{Im}(U))|$, $U \in \mathbf{C}^2$. On en déduit $|D| = |\det(U_1, \dots, U_d)| = 2^{-r_2} |\det(\sigma_j(x_i))|$. Ce dernier déterminant est non nul (voir la leçon sur les discriminants). Les $v_K(x_i)$ forment bien une base de $\mathbf{R}^d$ et on a bien un réseau de $\mathbf{R}^d$.

On a $\text{vol}(v_K(M)) = |D|$ puisque les vecteurs U_i définissent un parallépipède fondamental de $v_K(M)$.

Venons-en maintenant à la démonstration de la formule du volume. Appliquons d'abord le lemme 2 à $M = \mathcal{O}_K$ qui est un $\mathbf{Z}$ -module libre de rang d . On obtient

$$\text{vol}(v_K(\mathcal{O}_K)) = 2^{-r_2} |\det(\sigma_j(x_i))| = 2^{-r_2} |\mathcal{D}_K|^{1/2},$$

où les x_i forment une base de $\mathcal{O}_K$ sur $\mathbf{Z}$. Un idéal I de $\mathcal{O}_K$ est un $\mathbf{Z}$ -module libre de rang d , puisqu'il est d'indice fini N_I dans $\mathcal{O}_K$. Son volume est égal au volume de $\mathcal{O}_K$ multiplié par cet indice. Cela se voit par exemple en remarquant qu'un parallépipède fondamental de $v_K(I)$ se décompose en N_I parallépipèdes fondamentaux de $v(\mathcal{O}_K)$.

Soit t un nombre réel > 0 . Posons

$$X_t = \{(x_1, \dots, x_{r_1}, z_{r_1+1}, \dots, z_{r_1+r_2}) \in \mathbf{R}^{r_1} \times \mathbf{C}^{r_2} /$$

$$|x_1| + \dots + |x_{r_1}| + 2|z_{r_1+1}| + \dots + 2|z_{r_1+r_2}| < t\}.$$

PROPOSITION 5. — Le volume de X_t est donné par la formule

$$\text{vol}(X_t) = 2^{r_1-r_2} \pi^{r_2} t^d / d!.$$

Démonstration. — On établit cette formule de volume par une double récurrence sur r_1 et r_2 . Notons $V(r_1, r_2, t)$ le volume de X_t . On vérifie la formule pour $r_1 + r_2 = 1$. On trouve

$$V(0, 1, t) = \frac{\pi t^2}{4}$$

et

$$V(1, 0, t) = 2t$$

Cela initialise la récurrence.

Calculons $V(r_1 + 1, r_2, t)$ en utilisant l'hypothèse de récurrence. On a, en isolant la $(r_1 + 1)$ -ième variable,

$$V(r_1 + 1, r_2, t) = \int_{-t}^t V(r_1, r_2, t - |y|) dy = \int_{-t}^t 2^{r_1 - r_2} \pi^{r_2} \frac{(t - |y|)^d}{d!} dy.$$

Un calcul direct montre que le dernier membre est égal à

$$2^{r_1 + 1 - r_2} \pi^{r_2} \frac{t^{d+1}}{(d+1)!}.$$

C'est le résultat désiré.

Calculons maintenant $V(r_1, r_2 + 1, t)$ de façon analogue. On a

$$V(r_1, r_2 + 1, t) = \int_{|z| \leq \frac{t}{2}, z=x+iy} V(r_1, r_2, t - 2|z|) dx dy.$$

Passons en coordonnées polaires : $z = \rho e^{i\theta}$ et $dx dy = \rho d\rho d\theta$. On obtient

$$V(r_1, r_2 + 1, t) = \int_0^{\frac{t}{2}} \int_0^{2\pi} 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{(t - 2\rho)^d}{d!} \rho d\rho d\theta$$

Le calcul de $\int_0^{\frac{t}{2}} (t - 2\rho)^d \rho d\rho$ donne $\frac{t^{d+2}}{4(d+1)(d+2)}$ (par récurrence sur d et en utilisant une intégration par parties). On obtient :

$$V(r_1, r_2 + 1, t) = 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{2\pi}{d!} \frac{t^{d+2}}{4(d+1)(d+2)} = 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2+1} \frac{t^{d+2}}{(d+2)!}.$$

C'est formule cherchée.

4. Démonstration de la proposition 2

Soit I un idéal de $\mathcal{O}_K$. Soit t un nombre réel > 0 . L'ensemble X_t est un sous-ensemble convexe, borné et symétrique par rapport à l'origine de $\mathbf{R}^d$. En combinant les propositions 3, 4 et 5 (appliquées à $X = X_t$ et $L = v_K(I)$), on obtient qu'il existe un élément $x_t \in X_t \cap (v_K(I) - 0)$ dès lors qu'on a l'inégalité

$$t^d > d! \frac{2^{d-r_1}}{\pi^{r_2}} N_I |\mathcal{D}_K|^{1/2}.$$

Ces éléments forment un ensemble fini (car $v_K(I)$ est discret et X_t est borné) et non vide A_t . La suite des A_t est décroissante quand t décroît. Par conséquent l'ensemble

$$A = \bigcap_{t, t^d > d! \frac{2^{d-r_1}}{\pi^{r_2}} N_I |\mathcal{D}_K|^{1/2}} A_t$$

est non vide. Soit $x \in A$. Posons

$$t_0 = (d! \frac{2^{d-r_1}}{\pi^{r_2}} N_I |\mathcal{D}_K|^{1/2})^{1/d}.$$

On a $A = A_{t_0}$ et donc $x \in X_{t_0} \cap (v_K(I) - 0)$. Posons $x = v_K(a)$. Calculons la valeur absolue de la norme de a . On a

$$|N_{K/\mathbf{Q}}(a)| = \prod_{i=1}^d |\sigma_i(a)| = \prod_{i=1}^{r_1} |\sigma_i(a)| \prod_{i=r_1+1}^{r_2} |\sigma_i(a)|^2.$$

Appliquons l'inégalité (dite de la *moyenne arithmético-géométrique*)

$$(\prod_{i=1}^n |x_i|)^{1/n} \leq \frac{1}{n} \sum_{i=1}^n |x_i|,$$

où les x_i sont des nombres réels. On obtient

$$|N_{K/\mathbf{Q}}(a)| \leq \frac{t_0^d}{d^d},$$

puisque $v_K(a) \in X_{t_0}$. Remplaçons t_0 par sa valeur, on obtient :

$$N_{K/\mathbf{Q}}(a) \leq \frac{d!}{d^d} \left(\frac{4}{\pi}\right)^{r_2} N_I |\mathcal{D}_K|^{1/2}.$$

Cela achève de prouver la proposition 2.