ENS de Lyon 2018-2019
M1 Introduction à la théorie des nombres

Introduction à la théorie des nombres

Version du 8 avril 2019

Introduction

Ce cours est une introduction à la théorie algébrique des nombres, c'est-à-dire essentiellement l'extension de l'arithmétique élémentaire aux extensions finies du corps $\mathbf{Q}$. Deux des principaux moteurs du développement historique de ce pan des mathématiques sont d'une part l'étude des équations diophantiennes, d'autre part celle du comportement des réductions des polynômes à coefficients entiers modulo différents nombres premiers.

0.1 Équations diophantiennes

Il s'agit de la recherche et de l'étude des solutions entières et/ou rationnelles des équations polynomiales à coefficients entiers. L'exemple paradigmatique est l'équation de Fermat $X^n + Y^n = Z^n$.

Exemple 1 (Triplets pythagoriciens) — Étude de l'équation $X^2 + Y^2 = Z^2$.

(*Première méthode*) Soit $(x, y, z) \in \mathbf{Z}^3$ une solution *non triviale* de cette équation, c'est-à-dire telle que $xyz \neq 0$. Si $d = \mathrm{pgcd}(x, y, z)$, alors on peut écrire $x = \pm dx', y = \pm dy'$ et $z = \pm dz'$, avec $(x', y', z') \in \mathbf{N}^3$ solution de cette même équation et $\mathrm{pgcd}(x', y', z') = 1$; il est donc suffisant de déterminer toutes les solutions *positives* et *premières entre elles*, solutions que l'on qualifiera de *primitives*.

Supposons donc $x, y, z \geqslant 0$ et $\mathrm{pgcd}(x, y, z) = 1$. L'un des deux nombres x, y est pair car

$$x^2 + y^2 = z^2 \equiv 0, 1 \pmod 4,$$

et de fait un seul l'est puisque x, y et z sont premiers entre eux. Quitte à permuter x et y, nous pouvons donc supposer $2|x, 2 \nmid y$ et $2 \nmid z$ puis écrire

$$\left(\frac{y}{2}\right)^2 = \frac{z^2 - x^2}{4} = \frac{x + z}{2} \cdot \frac{x - z}{2} \qquad (*)$$

dans $\mathbf{Z}$. Tout diviseur commun de $\frac{x+z}{2}$ et $\frac{x-z}{2}$ divise x, z ainsi que $y^2 = z^2 - x^2$; les entiers $\frac{x+z}{2}$ et $\frac{z-x}{2}$ sont donc premiers entre eux. En observant que ces deux nombres entiers sont positifs, on déduit alors de l'identité $(*)$ que ce sont des carrés : il existe $a, b \in \mathbf{Z}$ tels que

$$\frac{x + z}{2} = a^2 \quad \text{et} \quad \frac{z - x}{2} = b^2 \quad \text{avec} \quad 0 < b < a \quad \text{et} \quad \mathrm{pgcd}(a, b) = 1.$$

Au final, nous obtenons la paramétrisation usuelle des solutions primitives de l'équation de Pythagore : à permutation près de x et y,

$$x = a^2 - b^2, \quad y = 2ab \quad \text{et} \quad z = a^2 + b^2, \quad \text{avec } 0 < b < a \quad \text{et} \quad \mathrm{pgcd}(a, b) = 1.$$

(*Seconde méthode*) Nous pouvons modifier la démonstration précédente en remplaçant l'anneau $\mathbf{Z}$ par l'anneau $\mathbf{Z}[i] = \mathbf{Z} \oplus \mathbf{Z}i \subset \mathbf{C}$ des *entiers de Gauss*. Cet anneau étant également *euclidien*, les raisonnements arithmétiques usuels y ont cours.

Soit $(x, y, z) \in \mathbf{Z}^3$ une solution primitive de l'équation de Pythagore et écrivons

$$z^2 = x^2 + y^2 = (x + iy)(x - iy). \qquad (*')$$

Si $\lambda \in \mathbf{Z}[i]$ divise simultanément $x + iy$ et $x - iy$, alors λ divise $\mathrm{pgcd}(2x, 2y) = 2$, puis $\lambda | \mathrm{pgcd}(2, z^2) = 1$ car z est impair ; ainsi, $x + iy$ et $x - iy$ sont premiers entre eux dans $\mathbf{Z}[i]$. On déduit alors de l'identité $(*')$ que $x + iy$ est un carré dans $\mathbf{Z}[i]$, à une unité près : il existe $a + ib \in \mathbf{Z}$ tels que

$$x + iy = \varepsilon(a + ib)^2 = \varepsilon(a^2 - b^2 + 2iab) \quad \text{avec} \quad \varepsilon \in \mathbf{Z}[i]^\times = \{\pm 1, \pm i\}.$$

En tenant compte des conditions $x, y, z > 0$ et $2|y$, nous obtenons finalement $x = a^2 - b^2$ et $y = 2ab$ avec $0 < b < a$, puis $z = a^2 + b^2$.

Remarque. Le point-clef de ces deux démonstrations est le fait suivant : si A est un anneau euclidien et $a, b \in A$ sont deux éléments premiers entre eux tels que ab soit une puissance n-ième, alors a et b sont des puissances n-ième à une unité près.

Exercice. Démontrer que l'équation $X^4 + Y^4 = Z^2$ n'admet pas de solution non triviale dans $\mathbf{Z}^3$. (On pourra raisonner par l'absurde en considérant une solution entière non triviale telle que $|z|$ soit minimal et utiliser ce qui précède pour écrire $x^2 = a^2 - b^2$ puis $x = u^2 - v^2$ avec $0 < b < a$, $0 < u < v$ et $\mathrm{pgcd}(a, b) = \mathrm{pgcd}(u, v) = 1$. Observer alors que $uv(u^2 + v^2)$ est un carré, puis en déduire l'existence d'entiers positifs c, d, e tels que $u = c^2, v = d^2$ et $u^2 + v^2 = e^2$. Il reste à voir que la nouvelle solution entière (c, d, e) de l'équation $X^4 + Y^4 = Z^2$ viole l'hypothèse initiale de minimalité.)

Exemple 2 (Bachet, Mordell) — Étude de l'équation $Y^2 = X^3 - 1$.

Soit $(x, y) \in \mathbf{Z}^2$ une solution de cette équation. Écrivons

$$x^3 = (y + i)(y - i) \qquad (*'')$$

dans l'anneau euclidien $\mathbf{Z}[i]$ et observons que

$$\mathrm{pgcd}(y + i, y - i) | \mathrm{pgcd}(2y, 2i, x^3) = \mathrm{pgcd}(2, x^3).$$

Puisque $x^3 = y^2 + 1 \equiv 1, 2 \pmod 4$, le nombre entier x est nécessairement impair et donc $\mathrm{pgcd}(y + i, y - i) = 1$. Il découle alors de l'identité $(*'')$ que $y + i$ est un cube dans $\mathbf{Z}[i]$ à une unité près, et même est précisément un cube car toutes les unités $\pm 1, \pm i$ de $\mathbf{Z}[i]$ sont elles-mêmes des cubes. Il existe donc $(a, b) \in \mathbf{Z}^2$ tels que

$$y + i = (a + ib)^3, \quad \text{c'est-à-dire} \begin{cases} y = & a^3 - 2a^2 b \\ 1 = & 3a^2 b - b^3 \quad = b(3a^2 - b^2) \end{cases}$$

On en déduit de la seconde équation $b = \pm 1$ et $3a^2 - 1 = b$, donc $b = -1$ et $a = 0$, puis finalement $y = 0$ et $x = 1$.

L'équation $Y^2 = X^3 - 1$ admet donc une unique solution entière, le couple $(1, 0)$.

Exemple 3 (Bachet, Mordell (bis)) — Étude de l'équation $Y^2 = X^3 - 19$.

Soit $(x, y) \in \mathbf{Z}^2$ une solution de cette équation. En introduisant le sous-anneau

$$\mathbf{Z}[\sqrt{-19}] = \mathbf{Z} \oplus \mathbf{Z} i\sqrt{19}$$

de $\mathbf{C}$, nous pouvons écrire

$$x^3 = (y + i\sqrt{19})(y - i\sqrt{19}).$$

Si $\delta \in \mathbf{Z}[\sqrt{-19}]$ est un élément divisant simultanément $y + i\sqrt{19}$ et $y - i\sqrt{19}$, alors δ divise $2 \cdot 19$ et $\delta | x^3$, donc δ divise $\mathrm{pgcd}(x^3, 2 \cdot 19)$. Or $2 \nmid x$ — sinon $y^2 \equiv 5 \pmod 8$, or les carrés modulo 8 sont $0, 1$ et 4 — et $19 \nmid x$ — sinon $19|y$, puis $19^2 | x^3 - y^2 = 19$. Par conséquent,

$$\mathrm{pgcd}(x^3, 2 \cdot 19) = 1 \quad \text{et} \quad \delta \in \mathbf{Z}[\sqrt{-19}]^\times.$$

Les éléments $u + iv\sqrt{19}$ de $\mathbf{Z}[\sqrt{-19}]$ sont tels que $u^2 + 19v^2 = 1$, donc $\mathbf{Z}[\sqrt{-19}] = \{\pm 1\}$.

Si l'anneau $\mathbf{Z}[\sqrt{-19}]$ est *factoriel*, nous pouvons à ce stade affirmer que $y + i\sqrt{19}$ est un cube et donc obtenir $a, b \in \mathbf{Z}$ tels que

$$y + i\sqrt{19} = (u + iv\sqrt{19})^3, \quad \text{c'est-à-dire} \quad \begin{cases} y = & a^3 - 3 \cdot 19ab^2 \\ 1 = & -19b^3 + 3a^2 b = \quad b(3a^2 - 19b^2) \end{cases}$$

Il vient alors ($b = 1$ et $3a^2 - 19 = 1$) ou ($b = -1$ et $3a^2 - 19 = -1$), d'où l'on déduit que l'équation $X^3 = Y^2 + 19$ n'a pas de solution entière.

Cependant,

$$7^3 = 343 = 324 + 19 = 18^2 + 19...$$

Nous devons donc conclure de tout ceci que l'anneau $\mathbf{Z}[\sqrt{-19}]$ *n'est pas factoriel* !

Remarque. La non-factorialité de cet anneau peut s'obtenir plus directement à partir de l'identité

$$35 = 5 \cdot 7 = (4 + \sqrt{-19})(4 - \sqrt{-19}).$$

Il s'agit de *deux factorisations différentes de* 35 *dans* $\mathbf{Z}[\sqrt{-19}]$ *en produits d'éléments irréductibles non associés.*

On le vérifie aisément à l'aide de la *norme*

$$N : \mathbf{Z}[\sqrt{-19}] \to \mathbf{Z}, \quad a + b\sqrt{-19} \mapsto a^2 + 19b^2$$

qui est une fonction multiplicative (calcul immédiat). Si $\lambda = a + b\sqrt{-19}$ est un diviseur de 5 dans $\mathbf{Z}[\sqrt{-19}]$, alors $N(\lambda) = a^2 + 19b^2 | N(5) = 25$; or 25 n'admet manifestement pas de diviseur non trivial de cette forme, donc $\lambda \in \{\pm 1, \pm 5\}$ et 5 est un élément irréductible de $\mathbf{Z}[\sqrt{-19}]$. En raisonnant de la même manière, on vérifie que 7 et $4 \pm \sqrt{-19}$ sont également irréductibles. Enfin, tous ces éléments irréductibles sont deux à deux non associés puisque $\mathbf{Z}[\sqrt{-19}]^\times = \{\pm 1\}$.

0.2 Lois de réciprocité

Soit $f \in \mathbf{Z}[T]$ un polynôme unitaire et irréductible. Peut-on déterminer les nombres premiers p tels que la réduction de f modulo p soit scindée à racines distinctes (i.e. séparable) ?

Exemple 4 (Fermat) — Le polynôme $T^2 + 1$ est scindé à racines simples modulo p si et seulement si $p \equiv 1 \pmod 4$.

Démonstration. Ce polynôme est séparable modulo p si et seulement si $p \neq 2$ et il est scindé modulo p si et seulement si le groupe $\mathbf{F}_p^\times$ contient un élément d'ordre 4. Comme $\mathbf{F}_p^\times$ est cyclique, c'est le cas si et seulement si $4 | p - 1$. □

Le résultat suivant généralise cette observation.

Théorème (Loi de réciprocité quadratique, Gauss) — *Soit $f = T^2 + bT + c \in \mathbf{Z}[T]$ un polynôme irréductible et soit $D = b^2 - 4ac$ son discriminant. Pour tout nombre premier p ne divisant pas D, la factorisation de f modulo p ne dépend que de la classe de p modulo D.*

Autrement dit, tous les nombres premiers p ne divisant pas D tels que f soit irréductible (resp. scindé) modulo p sont dans une même classe de congruence modulo D ! Ce phénomène

n'est certainement pas évident de prime abord et ses généralisations en degré supérieur sont encore mystérieuses...

Chapitre 1

Les corps de nombres et leurs anneaux d'entiers

1.1 Nombres algébriques, entiers algébriques

Soit K un corps contenant $\mathbf{Q}$ et soit $\alpha \in K$. Considérons le morphisme

$$\varphi_\alpha : \mathbf{Q}[T] \to K, \quad P \mapsto P(\alpha).$$

Si Ker $\varphi_\alpha = (0)$, alors $\mathbf{Q}[\alpha] = \text{Im } \varphi_\alpha$ est un $\mathbf{Q}$-espace vectoriel de dimension infinie. Si Ker $\varphi_\alpha \neq (0)$, alors Ker $\varphi_\alpha = (f)$ avec $f \in \mathbf{Q}[T]$ non nul et φ_α induit un morphisme injectif

$$\mathbf{Q}[T]/(f) \hookrightarrow K.$$

On en déduit que $\mathbf{Q}[\alpha] = \text{Im } \varphi_\alpha$ est une $\mathbf{Q}$-algèbre de dimension finie intègre, donc un corps (et f est irréductible).

Définition 1.1 — *Un élément α de K est dit* algébrique *(sur $\mathbf{Q}$) s'il existe $P \in \mathbf{Q}[T]$ non nul tel que $P(\alpha) = 0$. On dit que α est* entier *(sur $\mathbf{Z}$) s'il existe $P \in \mathbf{Z}[T]$ unitaire (donc non nul) tel que $P(\alpha) = 0$.*

Exemple. Le nombre réel $\frac{1+\sqrt{5}}{2}$ est entier sur $\mathbf{Z}$ car est annulé par $T^2 - T - 1$.

Si $\alpha \in K$ est algébrique, son *polynôme minimal*, noté $f_{\alpha,\min}$, est le générateur unitaire de Ker φ_α. Le *degré* de α est le degré de $f_{\alpha,\min}$; on le note $\deg(\alpha)$.

On peut toujours écrire α sous la forme $\alpha = \frac{\beta}{m}$, avec $m \in \mathbf{Z}_{>0}$ et β entier sur $\mathbf{Z}$. En effet, si $m \in \mathbf{Z}_{>0}$ est un dénominateur commun des coefficients de $f_{\alpha,\min}$, alors $m^d f_{\alpha,\min}(T) = g(mT)$ avec $g \in \mathbf{Z}[T]$ unitaire, donc $m\alpha$ est entier sur $\mathbf{Z}$. Le plus petit entier $n \geqslant 1$ tel que $n\alpha$ soit entier sur $\mathbf{Z}$ est le *dénominateur* du nombre algébrique α.

Exemple. Le dénominateur des racines de $4T^2 + 2T + 1$ est 2.

Proposition 1.2 — *Soit $\alpha \in K$ algébrique sur $\mathbf{Q}$. Pour que α soit entier sur $\mathbf{Z}$, il faut et il suffit que son polynôme minimal $f_{\alpha,\min}$ appartienne à $\mathbf{Z}[T]$.*

Démonstration. La condition est évidemment suffisante. Pour voir qu'elle est nécessaire, il suffit d'observer que si $f_{\alpha,\min}$ divise $P \in \mathbf{Z}[T]$ unitaire, alors $f_{\alpha,\min} \in \mathbf{Z}[T]$ (utiliser la multiplicativité du contenu d'un polynôme). □

Exemples. (i) Un nombre rationnel a est entier sur $\mathbf{Z}$ si et seulement si $a \in \mathbf{Z}$.

(ii) Soit $d \in \mathbf{Z}$ et $\alpha = \frac{1+\sqrt{d}}{2}$. Puisque $f_{\alpha,\min} = T^2 - T + \frac{1-d}{4}$, le nombre algébrique α est entier sur $\mathbf{Z}$ si et seulement si $d \equiv 1 \pmod 4$.

Lemme 1.3 — *Soit $\alpha \in K$. Les conditions suivantes sont équivalentes :*

(i) *α est entier sur $\mathbf{Z}$;*
(ii) *le sous-anneau $\mathbf{Z}[\alpha]$ est un $\mathbf{Z}$-module de type fini ;*
(iii) *il existe un $\mathbf{Z}$-module de type fini non nul $M \subset K$ tel que $\alpha M \subset M$.*

Démonstration. (i) $\Rightarrow$ (ii). Si $P(\alpha) = 0$ avec $P \in \mathbf{Z}[T]$ unitaire de degré d, alors

$$\mathbf{Z}[\alpha] = \sum_{i=0}^{d-1} \mathbf{Z}\alpha^i.$$

L'implication (ii) $\Rightarrow$ (iii) est triviale.

(iii) $\Rightarrow$ (i). Soit $\pi : \mathbf{Z}^n \to M \subset K$ un épimorphisme. Il existe une matrice $A \in \mathrm{M}_n(\mathbf{Z})$ telle que $\pi(Ax) = \alpha\pi(x)$ pour tout $x \in \mathbf{Z}^n$. Le polynôme $P = \det(T\mathrm{I}_n - A) \in \mathbf{Z}[T]$ est unitaire et $P(\alpha)M = 0$ en vertu du théorème de Cayley-Hamilton, donc $P(\alpha) = 0$. □

Proposition 1.4 — *L'ensemble des éléments de K algébriques sur $\mathbf{Q}$ est un sous-corps. L'ensemble des éléments de K entiers sur $\mathbf{Z}$ est un sous-anneau.*

Démonstration. Considérons $\alpha, \beta \in K$ entiers sur $\mathbf{Z}$, de degrés respectifs d, d'. Les sous-anneau $\mathbf{Z}[\alpha, \beta]$ de K est un $\mathbf{Z}$-module de type fini, engendré par la famille des $\alpha^i\beta^j$ avec $0 \leqslant i < d$ et $0 \leqslant j < d'$. Comme $(\alpha+\beta)\mathbf{Z}[\alpha,\beta] \subset \mathbf{Z}[\alpha,\beta]$ et $\alpha\beta\mathbf{Z}[\alpha,\beta] \subset \mathbf{Z}[\alpha,\beta]$, $\alpha+\beta$ et $\alpha\beta$ sont entiers sur $\mathbf{Z}$. On en déduit que la somme et le produit de deux entiers algébriques est un entier algébrique, puis, en introduisant des dénominateurs, que la somme et le produit de deux nombres algébriques est algébrique. Enfin, si $\alpha \in K$ est algébrique et non nul, alors α^{-1} est algébrique, de polynôme minimal

$$f_{\alpha^{-1},\min} = f_{\alpha,\min}(0)^{-1} T^{\deg(\alpha)} f_{\alpha,\min}(T^{-1}).$$

□

Lorsque $K = \mathbf{C}$, le sous-corps des nombres (complexes) algébriques est noté $\overline{\mathbf{Q}}$. Ceux qui sont entiers sur $\mathbf{Z}$ sont appelés *entiers algébriques* ; ils forment un sous-anneau noté $\overline{\mathbf{Z}}$.

Remarque. Le corps $\overline{\mathbf{Q}}$ est dénombrable.

1.2 Corps de nombres

Définition 1.5 — *Un* corps de nombres *est un corps K qui est une extension finie de $\mathbf{Q}$. Son* degré *est la dimension de K comme $\mathbf{Q}$-espace vectoriel ; on le note $[K : \mathbf{Q}]$.*

Tout élément α de K est algébrique (sur $\mathbf{Q}$), de degré divisant $[K : \mathbf{Q}]$ car $\mathbf{Q}(\alpha)$ est une sous-extension de K.

Exemples. $\mathbf{Q}$ (degré 1), $\mathbf{Q}(i)$ (degré 2), $\mathbf{Q}[T]/(T^3 - 2)$ (degré 3), $\mathbf{Q}(\sqrt{5}, \sqrt[3]{2})$ (degré 6), $\mathbf{Q}(e^{\frac{2i\pi}{n}})$ (degré $\varphi(n)$).

Théorème 1.6 (Élément primitif) — *Pour tout corps de nombres K, il existe $\alpha \in K$ tel que $K = \mathbf{Q}(\alpha)$.*

Démonstration. En raisonnant par récurrence sur le nombre de générateurs de K en tant que $\mathbf{Q}$-algèbre, on peut supposer $K = \mathbf{Q}(\alpha, \beta)$. Nous allons prouver $K = \mathbf{Q}(\vartheta)$, où ϑ est une combinaison linéaire convenable de α et β.

Soit L/K une extension scindant les polynômes minimaux de α et β. On note $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ et $\beta = \beta_1, \beta_2, \ldots, \beta_m$ les racines de $f_{\alpha,\min}$ et $f_{\beta,\min}$ dans L. Ces polynômes sont séparables, car irréductibles sur $\mathbf{Q}$ de caractéristique nulle. Puisque $\mathbf{Q}$ est infini, il existe $\lambda \in \mathbf{Q}$ tel que $\lambda \neq \frac{\alpha_i - \alpha}{\beta - \beta_j}$ pour $1 \leqslant i \leqslant n$, $2 \leqslant j \leqslant m$, i.e. tel que $\vartheta = \alpha + \lambda\beta \neq \alpha_i + \lambda\beta_j$ si $(i,j) \neq (1,1)$. Par construction, $\mathrm{pgcd}(f_{\alpha,\min}(\vartheta - \lambda T), f_{\beta,\min}) = T - \beta$ dans $L[T]$, donc $\beta \in \mathbf{Q}(\vartheta)$ puis $\mathbf{Q}(\vartheta) = \mathbf{Q}(\alpha,\beta)$. □

Corollaire 1.7 — *Un corps de nombres K admet exactement $[K : \mathbf{Q}]$ plongements distincts dans $\mathbf{C}$.*

Démonstration. Écrivons $K = \mathbf{Q}(\alpha) \simeq \mathbf{Q}[T]/(f)$, où $f = f_{\alpha,\min}$. On a

$$\mathrm{Hom}_{\mathbf{Corps}}(K, \mathbf{C}) \xrightarrow{\sim} \mathrm{Hom}_{\mathbf{Anneaux}}(\mathbf{Q}[T]/(f), \mathbf{C}) \xrightarrow{\sim} \{z \in \mathbf{C} \mid f(z) = 0\}$$

$$\varphi \longmapsto \varphi(\overline{T})$$

(tout morphisme d'anneaux de $\mathbf{Q}$ dans $\mathbf{C}$ est l'identité sur $\mathbf{Q}$). Comme f est séparable,

$$\mathrm{Card}\ \mathrm{Hom}_{\mathbf{Corps}}(K, \mathbf{C}) = \deg(f) = [K : \mathbf{Q}].$$

□

Un plongement $\sigma : K \to \mathbf{C}$ est dit *réel* si $\sigma(K) \subset \mathbf{R}$. On note classiquement r_1 le nombre de plongements réels de K dans $\mathbf{C}$. Les autres plongements se regroupent en paires $\{\sigma, \overline{\sigma}\}$ de plongements conjugués qui sont (abusivement) dit *complexes* ; il y en a $2r_2$, et alors

$$[K : \mathbf{Q}] = r_1 + 2r_2.$$

Remarque. Si $K \simeq \mathbf{Q}[T]/(f)$, alors r_1 est le nombre de racines réelles de f dans $\mathbf{C}$. Connaissant f, ce nombre est effectivement calculable (voir l'exemple suivant la proposition 1.9).

Soit Σ_r l'ensemble des plongements réels de K et soit Σ'_c un ensemble de représentants de plongements complexes de K modulo conjugaison. L'application naturelle

$$\Phi : K \to \mathbf{R}^{\Sigma_r} \oplus \mathbf{C}^{\Sigma'_c}, \quad x \mapsto \left((\sigma(x)\right)_{\sigma \in \Sigma_r \cup \Sigma'_c}$$

induit un isomorphisme de $\mathbf{R}$-algèbres

$$\Phi_{\mathbf{R}} : K \otimes_{\mathbf{Q}} \mathbf{R} \simeq \mathbf{R}^{\Sigma_r} \oplus \mathbf{C}^{\Sigma'_c}.$$

Pour le vérifier, choisissons un élément primitif $\alpha \in K$ de polynôme minimal f et utilisons l'isomorphisme de $\mathbf{R}$-algèbres $\mathbf{R}[T]/(f) \simeq K \otimes_{\mathbf{Q}} \mathbf{R}$ identifiant $\overline{T}$ et $\alpha \otimes 1$ pour transformer $\Phi_{\mathbf{R}}$ en le morphisme

$$\mathbf{R}[T]/(f) \to \mathbf{R}^{\Sigma_r} \oplus \mathbf{C}^{\Sigma'_c}, \quad \overline{T} \mapsto \left(\sigma(\alpha)\right)_{\sigma \in \Sigma_r \cup \Sigma'_c}.$$

En posant

$$f_\sigma = \begin{cases} T - \sigma(\alpha), & \text{si } \sigma \in \Sigma_r \\ (T - \sigma(\alpha))(T - \overline{\sigma}(\alpha)), & \text{si } \sigma \in \Sigma'_c \end{cases}$$

le membre de droite s'identifie à

$$\prod_{\sigma \in \Sigma_r \cup \Sigma'_c} \mathbf{R}[T]/(f_\sigma)$$

et l'on retrouve alors l'énoncé du théorème chinois des restes.

Exemple. $K = \mathbf{Q}(\alpha)$, $f_{\alpha,\min} = T^4 - 2 = (T - \sqrt[4]{2})(T + \sqrt[4]{2})(T - i\sqrt[4]{2})(T + i\sqrt[4]{2})$. Le corps K admet deux plongements réels :

$$\sigma_1 : K \hookrightarrow \mathbf{C}, \quad \alpha \mapsto \sqrt[4]{2} \quad \text{et} \quad \sigma_2 : K \hookrightarrow \mathbf{C}, \quad \alpha \mapsto -\sqrt[4]{2}$$

et deux plongements complexes non réels conjugués :

$$\sigma_3 : K \hookrightarrow \mathbf{C}, \quad \alpha \mapsto i\sqrt[4]{2} \quad \text{et} \quad \sigma_4 : K \hookrightarrow \mathbf{C}, \quad \alpha \mapsto -i\sqrt[4]{2}.$$

1.3 Traces, normes, discriminants

Soit K_0 un corps et soit A une K_0-algèbre finie (c'est-à-dire de dimension finie en tant qu'espace vectoriel sur K_0). Tout élément α de A donne naissance à un K_0-endomorphisme $m_{\alpha,A/K_0}$ de A défini par

$$\forall x \in A, \qquad m_{\alpha,A/K_0}(x) = \alpha x.$$

On introduit :

(i) la *trace* de α, notée $\mathrm{Tr}_{A/K_0}(\alpha) = \mathrm{tr}\left(m_{\alpha,A/K_0}\right) \in K_0$;

(ii) la *norme* de α, notée $\mathrm{N}_{A/K_0}(\alpha) = \det\left(m_{\alpha,A/K_0}\right) \in K_0$

(iii) le *polynôme caractéristique* de α, noté $f_{\alpha,A/K_0}(T) = \det\left(T\mathrm{id}_K - m_{\alpha,A/K_0}\right) \in K_0[T]$.

Il est utile d'observer l'identité

$$f_{\alpha,A/K_0} = T^n - \mathrm{Tr}_{A/K_0}(\alpha)T^{n-1} + \ldots + (-1)^n \mathrm{N}_{A/K_0}(\alpha),$$

où $n = \dim_{K_0}(A)$.

Pour tous $\alpha, \beta \in A$,

$$\mathrm{Tr}_{A/K_0}(\alpha + \beta) = \mathrm{Tr}_{A/K_0}(\alpha) + \mathrm{Tr}_{A/K_0}(\beta) \quad \text{et} \quad \mathrm{N}_{A/K_0}(\alpha\beta) = \mathrm{N}_{A/K_0}(\alpha)\mathrm{N}_{A/K_0}(\beta).$$

Il convient également d'observer que ces constructions sont compatibles aux isomorphismes de K_0-algèbres : si $\varphi : A \to B$ est un isomorphisme entre deux K_0-algèbres finies, alors

$$f_{\varphi(\alpha),B/K_0} = f_{\alpha,A/K_0}, \quad \textit{donc} \quad \mathrm{Tr}_{B/K_0}(\varphi(\alpha)) = \mathrm{Tr}_{A/K_0}(\alpha), \quad \text{et} \quad \mathrm{N}_{B/K_0}(\varphi(\alpha)) = \mathrm{N}_{A/K_0}(\alpha).$$

Exemple. $K_0 = \mathbf{Q}$, $A = K = \mathbf{Q}(\sqrt[4]{2})$, $\alpha = \sqrt{2} = (\sqrt[4]{2})^2$.

Dans la base $\left(1, \sqrt[4]{2}, \sqrt{2}, (\sqrt[4]{2})^3\right)$ de K sur $\mathbf{Q}$, la matrice de $m_{\alpha,K}$ est

$$\begin{pmatrix} 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

et

$$f_{\alpha,K/\mathbf{Q}} = T^4 - 4T^2 + 4, \quad \mathrm{Tr}_{K/\mathbf{Q}}(\alpha) = 0 \text{ et } \mathrm{N}_{K/\mathbf{Q}}(\alpha) = 4.$$

Si, par contre, on voit α dans le sous-corps $F = \mathbf{Q}(\sqrt{2})$, alors

$$f_{\alpha,F/\mathbf{Q}} = T^2 - 2, \quad \mathrm{Tr}_{F/\mathbf{Q}}(\alpha) = 0 \text{ et } \mathrm{N}_{F/\mathbf{Q}}(\alpha) = 2.$$

Remarque. L'exemple précédent illustre que les notions de trace, de norme et de polynôme caractéristique ne dépendent pas seulement de α, mais aussi de l'extension K/K_0.

Proposition 1.8 — *Soit K un corps de nombres.*

(i) *Pour tout* $\alpha \in K$,

$$f_{\alpha,K/\mathbf{Q}} = \prod_{\sigma:K\hookrightarrow\mathbf{C}} (T-\sigma(\alpha)), \quad \mathrm{Tr}_{\alpha,K/\mathbf{Q}}(\alpha) = \sum_{\sigma:K\hookrightarrow\mathbf{C}} \sigma(\alpha) \quad \text{et} \quad \mathrm{N}_{\alpha,K/\mathbf{Q}}(\alpha) = \prod_{\sigma:K\hookrightarrow\mathbf{C}} \sigma(\alpha).$$

(ii) *Si* L *est une extension finie de* K *et* $\alpha \in K$*, alors*

$$f_{\alpha,L/\mathbf{Q}} = f_{\alpha,K/\mathbf{Q}}^{[L:K]}, \quad \mathrm{Tr}_{K/\mathbf{Q}}(\alpha) = [L:K]\ \mathrm{Tr}_{K/\mathbf{Q}}(\alpha) \quad \text{et} \quad \mathrm{N}_{L/\mathbf{Q}}(\alpha) = \mathrm{N}_{K/\mathbf{Q}}(\alpha)^{[L:K]}.$$

Démonstration. (i) L'isomorphisme de $\mathbf{R}$-algèbres

$$\Phi : K \otimes_{\mathbf{Q}} \mathbf{R} \to \mathbf{R}^{\Sigma_r} \oplus \mathbf{C}^{\Sigma_c'}$$

introduit à la fin de la section 1.1 permet d'identitifer $f_{\alpha,K/\mathbf{Q}}$ au polynôme caractéristique de la multiplication par $\Phi(\alpha)$ dans $\mathbf{R}^{\Sigma_r} \oplus \mathbf{C}^{\Sigma_c'}$. Dans la base canonique de cet espace vectoriel réel, la matrice de la multiplication par $\Phi(\alpha)$ est diagonalisable par blocs, avec des blocs

$$M_\sigma = (\sigma(\alpha))$$

pour $\sigma \in \Sigma_r$ et

$$M_\sigma = \begin{pmatrix} \mathrm{Re}\ \sigma(\alpha) & -\mathrm{Im}\ \sigma(\alpha) \\ \mathrm{Im}\ \sigma(\alpha) & \mathrm{Re}\ \sigma(\alpha) \end{pmatrix}$$

pour $\sigma \in \Sigma_c'$. On en déduit

$$f_{\alpha,K/\mathbf{Q}} = \prod_{\sigma\in\Sigma_r} (T-\sigma(\alpha)) \prod_{\sigma\in\Sigma_c'} (T-\sigma(\alpha))(T-\overline{\sigma}(\alpha)) = \prod_{\sigma:K\hookrightarrow\mathbf{C}} (T-\sigma(\alpha)),$$

puis

$$\mathrm{Tr}_{K/\mathbf{Q}}(\alpha) = \sum_{\sigma:K\hookrightarrow\mathbf{C}} \sigma(\alpha) \ \text{ et } \ \mathrm{N}_{K/\mathbf{Q}}(\alpha) = \prod_{\sigma:K\hookrightarrow\mathbf{C}} \sigma(\alpha).$$

(ii) Si $\mathcal{B} = (e_1, \ldots, e_n)$ est une $\mathbf{Q}$-base de K et $(f_1, \ldots, f_m)$ est une K-base de L, alors $\mathcal{B}' = (e_1 f_1, \ldots, e_n f_1, \ldots, e_1 f_m, \ldots, e_n f_m)$ est une $\mathbf{Q}$-base de L telle que $\mathrm{Mat}_{\mathcal{B}'}(m_{\alpha,L/\mathbf{Q}}) = \mathrm{diag}(M, \ldots, M)$, où $M = \mathrm{Mat}_{\mathcal{B}}(m_{\alpha,K/\mathbf{Q}})$. Les identités souhaitées s'en déduisent immédiatement. □

Remarques. 1. En particulier, pour tout corps de nombres K et tout $\alpha \in K$,

$$f_{\alpha,K/\mathbf{Q}} = f_{\alpha,\min}^{[K:\mathbf{Q}(\alpha)]}.$$

2. De façon générale, pour toute tour d'extensions $L/K/K_0$,

$$\mathrm{Tr}_{L/K_0} = \mathrm{Tr}_{K/K_0} \circ \mathrm{Tr}_{L/K} \quad \text{et} \quad \mathrm{N}_{L/K_0} = \mathrm{N}_{K/K_0} \circ \mathrm{N}_{L/K}$$

(exercice).

Proposition 1.9 — *Soit* K *un corps de nombres. L'application*

$$K \times K \to \mathbf{Q}, \quad (x,y) \mapsto \mathrm{Tr}_{K/\mathbf{Q}}(xy)$$

est une forme bilinéaire non dégénérée.

Démonstration. Étendons les scalaires à $\mathbf{R}$ et identifions $K \otimes_{\mathbf{Q}} \mathbf{R}$ à la $\mathbf{R}$-algèbre $A = \mathbf{R}^{\Sigma_r} \oplus \mathbf{C}^{\Sigma_c'}$ comme précédemment. La forme bilinéaire considérée est induite par la forme bilinéaire

$$A \times A \to \mathbf{R}, \quad (x,y) \mapsto \mathrm{Tr}_{A/\mathbf{R}}(xy),$$

laquelle est la somme directe orthogonale des formes bilinéaires $(x,y) \mapsto \mathrm{Tr}_{\mathbf{R}/\mathbf{R}}(xy) = xy$ (sur $\mathbf{R}$) et $(x,y) \mapsto \mathrm{Tr}_{\mathbf{C}/\mathbf{R}}(xy)$ (sur $\mathbf{C}$), de signatures respectives 1 et $(1,1)$. Cette forme bilinéaire est donc non dégénérée. □

Remarque. La signature de la forme bilinéaire $(x,y) \mapsto \mathrm{Tr}_{A/\mathbf{R}}(xy)$ est $(r_1 + r_2, r_2)$, ce qui fournit donc une manière *effective* de calculer les entiers r_1 et r_2.

Exemple. Soit $K = \mathbf{Q}(\alpha)$ avec $\alpha^3 - \alpha^2 - 2\alpha - 8 = 0$. Le polynôme $f = f_{\alpha,\min} = T^3 - T^2 - 2T - 8$ est irréductible sur $\mathbf{Q}$; sinon, il possèderait une racine dans $\mathbf{Q}$, donc dans $\mathbf{Z}$, et celle-ci devrait diviser 8 ; on vérifie que ceci est impossible.

On a $\mathrm{Tr}_{K/\mathbf{Q}}(\alpha) = 1$ et $\mathrm{Tr}_{K/\mathbf{Q}}(\alpha^2) = 1^2 - 2 \cdot (-2) = 5$ (via les formules de Newton), puis

$$\mathrm{Tr}_{K/\mathbf{Q}}(\alpha^3) = \mathrm{Tr}_{K/\mathbf{Q}}(\alpha^2 + 2\alpha + 8) = 5 + 2 + 24 = 31$$

et

$$\mathrm{Tr}_{K/\mathbf{Q}}(\alpha^4) = \mathrm{Tr}_{K/\mathbf{Q}}(\alpha^3 + 2\alpha^2 + 8\alpha) = 31 + 10 + 8 = 49,$$

donc

$$\mathrm{Mat}_{(1,\alpha,\alpha^2)}\left(m_{\alpha,K/\mathbf{Q}}\right) = \begin{pmatrix} 3 & 1 & 5 \\ 1 & 5 & 31 \\ 5 & 31 & 49 \end{pmatrix}.$$

La signature de cette matrice symétrique réelle est $(2,1)$, donc

$$r_1 = r_2 = 1.$$

Définition 1.10 — *Soit K un corps de nombres de degré n. Le* discriminant *d'un n-uplet $(\omega_1, \ldots, \omega_n) \in K^n$ est le nombre rationnel*

$$\Delta(\omega_1, \ldots, \omega_n) = \det\left(\mathrm{Tr}_{K/\mathbf{Q}}(\omega_i\omega_j)\right)_{1 \leqslant i,j \leqslant n}.$$

Proposition 1.11 — *Soit K un corps de nombres et soit $(\omega_1, \ldots, \omega_n) \in K^n$.*

(i)

$$\Delta(\omega_1, \ldots, \omega_n) = \det\left(\sigma(\omega_i)\right)_{\substack{1 \leqslant i \leqslant n \\ \sigma : K \hookrightarrow \mathbf{C}}}^2$$

(ii) *Si $\omega'_i = \sum_{j=1}^n a_{ij}\omega_j$ avec $a_{ij} \in \mathbf{Q}$ et $1 \leqslant i \leqslant n$, alors*

$$\Delta(\omega'_1, \ldots, \omega'_n) = \Delta(\omega_1, \ldots, \omega_n) \cdot \det(a_{ij})^2.$$

(iii) *$\Delta(\omega_1, \ldots, \omega_n) \neq 0$ si et seulement si $(\omega_1, \ldots, \omega_n)$ est une $\mathbf{Q}$-base de K.*

Démonstration. (i) $\mathrm{Tr}_{K/\mathbf{Q}}(\omega_i\omega_j) = \sum_\sigma \sigma(\omega_i)\sigma(\omega_j)$ (produit matriciel).

(ii) Il suffit d'écrire

$$\left(\mathrm{Tr}_{K/\mathbf{Q}}(\omega'_i\omega'_j)\right) = {}^t(a_{ij}) \cdot \left(\mathrm{Tr}_{K/\mathbf{Q}}(\omega_i\omega_j)\right) \cdot (a_{ij})$$

et de prendre les déterminants.

(iii) Cela découle immédiatement du caractère non dégénéré de la forme bilinéaire $(x,y) \mapsto \mathrm{Tr}_{K/\mathbf{Q}}(xy)$. □

Soit K un corps de nombres de degré n et soit $\alpha \in K$ tel que $K = \mathbf{Q}(\alpha)$, de telle sorte que $(1, \alpha, \ldots, \alpha^{n-1})$ soit une $\mathbf{Q}$-base de K. On a :

$$\Delta(1, \alpha, \ldots, \alpha^{n-1}) = \det\left(\sigma(\alpha^i)\right)^2 = (-1)^{\frac{n(n-1)}{2}} \prod_{\sigma \neq \tau} (\sigma(\alpha) - \tau(\alpha))$$

en vertu de la formule de Vandermonde. Cette quantité est le *discriminant* du polynôme $f_{\alpha, K/\mathbf{Q}} = \prod_\sigma (T - \sigma(\alpha))$, noté $\mathrm{disc}\,(f_{\alpha,\min})$. On peut le calculer comme un résultant, ou comme une norme :

$$\Delta(1, \alpha, \ldots, \alpha^{n-1}) = \mathrm{disc}\,(f_{\alpha,\min}) = (-1)^{\frac{n(n-1)}{2}} \mathrm{Res}\left(f_{\alpha,\min}, f'_{\alpha,\min}\right) = (-1)^{\frac{n(n-1)}{2}} \mathrm{N}_{K/\mathbf{Q}}\left(f'_{\alpha,\min}(\alpha)\right).$$

Exemples. 1. Pour $d \in \mathbf{Z}$ non carré,

$$\Delta(1, \sqrt{d}) = \begin{vmatrix} 2 & 0 \\ 0 & 2d \end{vmatrix} = 4d.$$

2. Considérons $f = T^n + aT + b \in \mathbf{Q}[T]$ supposé irréductible. Notons β une racine de f et posons

$$\gamma = f'(\beta) = n\beta^{n-1} + a = -(n-1)a - nb\beta^{-1},$$

d'où

$$\beta = \frac{-nb}{(n-1)a + \gamma}.$$

Comme $\mathbf{Q}(\beta) = \mathbf{Q}(\gamma)$, le polynôme minimal de γ est de degré n. On a

$$f\left(\frac{-nb}{(n-1)a + T}\right) = \frac{(-nb)^n + (-nba)((n-1)a + T)^{n-1} + b((n-1)a + T)^n}{(T + (n-1)a)^n},$$

donc le polynôme minimal de γ est

$$(T + (n-1)a)^n - na(T + (n-1)a)^{n-1} + (-n)^n b^{n-1}$$

et

$$\mathrm{N}_{\mathbf{Q}(\beta)/\mathbf{Q}}(\gamma) = n^n b^{n-1} + (-1)^{n-1}(n-1)^{n-1} a^n,$$

d'où

$$\mathrm{disc}(f) = (-1)^{\frac{n(n-1)}{2}} \left(n^n b^{n-1} + (-1)^{n-1}(n-1)^{n-1} a^n\right).$$

1.4 Anneaux d'entiers

Soit K un corps de nombres. Les éléments de K entiers sur $\mathbf{Z}$ forment un sous-anneau de K, noté $\mathcal{O}_K$ (prop. 1.4) et tel que $K = \mathrm{Frac}(\mathcal{O}_K)$.

Pour tout $\alpha \in K$,

$$\alpha \in \mathcal{O}_K \iff f_{\alpha,\min} \in \mathbf{Z}[T] \iff f_{\alpha, K/\mathbf{Q}} \in \mathbf{Z}[T].$$

Exemple. Si $[K : \mathbf{Q}] = 2$, alors il existe un unique $d \in \mathbf{Z}$ sans facteur carré tel que $K = \mathbf{Q}(\sqrt{d})$ et

$$\mathcal{O}_K = \begin{cases} \mathbf{Z}[\sqrt{d}] & \text{si } d \equiv 2, 3 \pmod 4 \\ \mathbf{Z}\left[\frac{1+\sqrt{d}}{2}\right] & \text{si } \pmod 4. \end{cases}$$

Proposition 1.12 — *Soit K un corps de nombres. L'anneau des entiers $\mathcal{O}_K$ est un $\mathbf{Z}$-module libre de rang $[K : \mathbf{Q}]$.*

Démonstration. Nous allons donner deux démonstrations.

(*Première démonstration*) Considérons une $\mathbf{Q}$-base $(\omega_1, \ldots, \omega_n)$ de K formée d'éléments de $\mathcal{O}_K$. Soit $(\omega_1^*, \ldots, \omega_n^*)$ sa base duale relativement à la forme bilinéaire non dégénérée $(x, y) \mapsto \mathrm{Tr}_{K/\mathbf{Q}}(xy)$. Pour tout $\alpha \in K$,

$$\alpha = \sum_{i=1}^{n} \mathrm{Tr}_{K/\mathbf{Q}}(\alpha\omega_i)\omega_i^*$$

et $\mathrm{Tr}_{K/\mathbf{Q}}(\alpha\omega_i) \in \mathbf{Z}$ si $\alpha \in \mathcal{O}_K$, donc

$$\bigoplus_{i=1}^{n} \mathbf{Z}\omega_i \subset \mathcal{O}_K \subset \bigoplus_{i=1}^{n} \mathbf{Z}\omega_i^*$$

et $\mathcal{O}_K$ est par conséquent un $\mathbf{Z}$-module libre de rang $n = [K : \mathbf{Q}]$. Observons également que l'on a

$$\omega_i^* \in \frac{1}{\Delta} \bigoplus_{j=1}^{n} \mathbf{Z}\omega_j,$$

où $\Delta = \Delta(\omega_1, \ldots, \omega_n)$.

(*Seconde démonstration*) Si $(\omega_1, \ldots, \omega_n)$ est une $\mathbf{Q}$-base de K formée d'éléments de $\mathcal{O}_K$, alors $|\Delta(\omega_1, \ldots, \omega_n)|$ est un nombre entier strictement positif. Choisissons maintenant $(\omega_1, \ldots, \omega_n)$ minimisant $|\Delta(\omega_1, \ldots, \omega_n)|$. Si l'inclusion de $\bigoplus_{i=1}^n \mathbf{Z}\omega_i$ dans $\mathcal{O}_K$ est stricte, alors il existe un élément $x = \sum_{i=1}^n a_i\omega_i$ de $\mathcal{O}_K$ tel que $a_{i_0} \in \mathbf{Q} \setminus \mathbf{Z}$ pour un certain $i_0 \in \{1, \ldots, n\}$. En remplaçant x par $x - [a_{i_0}]\omega_i$, on peut supposer $0 < a_{i_0} < 1$. Posons alors $\omega_i' = \omega_i$ si $i \neq i_0$ et $\omega_{i_0}' = x$; on a

$$\Delta(\omega_1, \ldots, \omega_n') = a_{i_0}^2 \Delta(\omega_1, \ldots, \omega_n)$$

et ceci contredit la minimalité de $|\Delta(\omega_1, \ldots, \omega_n)|$. □

Définition 1.13 — *Soit K un corps de nombres de degré n. Le* discriminant *de K est le discriminant $\Delta(\omega_1, \ldots, \omega_n)$ de n'importe quelle base de $\mathcal{O}_K$. C'est un nombre entier naturel, noté D_K.*

Noter que bien-fondé de cette définition découle du point (ii) de la proposition 1.11 puisque $\det(A) = \pm 1$ pour toute matrice $A \in \mathrm{GL}_n(\mathbf{Z})$.

Exemple. Si $K = \mathbf{Q}(\sqrt{d})$ avec $d \in \mathbf{Z}$ sans facteur carré, alors

$$D_K = \begin{cases} \Delta(1, \sqrt{d}) = \begin{vmatrix} 2 & 0 \\ 0 & 2d \end{vmatrix} = 4d, & \text{si } d \equiv 2, 3 \pmod 4 \\ \Delta\left(1, \frac{1+\sqrt{d}}{2}\right) = \begin{vmatrix} 2 & 1 \\ 1 & \frac{1+d}{2} \end{vmatrix} = d & \text{si } d \equiv 1 \pmod 4. \end{cases}$$

Remarques. 1. On peut démontrer que le discriminant D_K d'un corps de nombres K est nécessairement congru à 0 ou 1 modulo 4 (critère de Stickelberger).

2. Le signe de D_K est $(-1)^{r_2}$ puisque la signature de la forme bilinéaire $(x, y) \mapsto \mathrm{Tr}_{K \otimes_{\mathbf{Q}} \mathbf{R}/\mathbf{Q}}(xy)$ est $(r_1 + r_2, r_2)$ (voire remarque suivant la proposition 1.9).

Déterminer l'anneau des entiers d'un corps de nombres et son discriminant est un problème difficile en général. Prenons l'exemple simple d'un corps quadratique $K = \mathbf{Q}(\sqrt{m})$, où m est

un nombre entier positif. Si l'on écrit m sous la forme $m = m_0^2 d$ avec $m_0 \in \mathbf{N}$ et $d \in \mathbf{N}$ sans facteur carré, alors $K = \mathbf{Q}(\sqrt{d})$ et $\mathcal{O}_K = \mathbf{Z}[\delta]$ avec $\delta = \sqrt{d}$ ou $\delta = \frac{1+\sqrt{d}}{2}$ selon la congruence de d modulo 4. Cependant, il est en pratique très difficile de déterminer le plus grand diviseur sans facteur carré d d'un nombre entier m donné dès que ce dernier est assez grand [1].

Le résultat suivant est souvent utile.

Proposition 1.14 — *Soit K un corps de nombres de degré n et soit $(\omega_1, \ldots, \omega_n)$ une $\mathbf{Q}$-base de K formée d'éléments de $\mathcal{O}_K$. Si l'on désigne par M le sous-groupe de $\mathcal{O}_K$ engendré par les ω_i, alors*

$$\Delta(\omega_1, \ldots, \omega_n) = (\mathcal{O}_K : M)^2 D_K$$

où $(\mathcal{O}_K : M) = \mathrm{Card}(\mathcal{O}_K/M)$ est l'indice de M dans $\mathcal{O}_K$.

Démonstration. Soit $(e_1, \ldots, e_n)$ une $\mathbf{Z}$-base de $\mathcal{O}_K$. Écrivons $\omega_i = \sum_{j=1}^n a_{ij} e_j$ $(1 \leqslant i \leqslant n)$ avec $A = (a_{ij}) \in \mathrm{M}_n(\mathbf{Z})$, ce qui fournit l'identité

$$\Delta(\omega_1, \ldots, \omega_n) = (\det\ A)^2 \Delta(e_1, \ldots, e_n) = (\det\ A)^2 D_K.$$

Nous avons par ailleurs un isomorphisme $\mathbf{Z}^n/\mathrm{Im}\ A \simeq \mathcal{O}_K/M$ en vertu du diagramme commutatif

$$\begin{array}{ccc} \mathbf{Z}^n & \xrightarrow{\sim} & M \\ {\scriptstyle A}\downarrow & & \downarrow \\ \mathbf{Z}^n & \xrightarrow{\sim} & \mathcal{O}_K \end{array}$$

donc

$$(\mathcal{O}_K : M) = (\mathbf{Z}^n : \mathrm{Im}\ A) = |\det\ A|$$

par application du théorème des diviseurs élémentaires. □

Corollaire 1.15 — *Soit K un corps de nombres de degré n.*

(i) *Si $\omega_1, \ldots, \omega_n$ sont des éléments de $\mathcal{O}_K$ tels que $\Delta(\omega_1, \ldots \omega_n)$ soit sans facteur carré, alors $\mathcal{O}_K = \bigoplus_{i=1}^n \mathbf{Z}\omega_i$.*

(ii) *S'il existe $\alpha \in \mathcal{O}_K$ tel que $\deg(\alpha) = n$ et $\mathrm{disc}\,(f_{\alpha,\min})$ soit sans facteur carré, alors $\mathcal{O}_K = \mathbf{Z}[\alpha]$.*

Démonstration. (i) On déduit immédiatement de la proposition précédente que l'indice de $\bigoplus_{i=1}^n \mathbf{Z}\omega_i$ dans $\mathcal{O}_K$ est égal à 1.

(ii) Il suffit d'appliquer (i) avec $\omega_i = \alpha^{i-1}$ pour $1 \leqslant i \leqslant n$. □

Exemples. 1. Le polynôme $f = \mathrm{T}^3 - T - 1$ est irréductible sur $\mathbf{Q}$ (il aurait sinon une racine dans $\mathbf{Q}$ qui serait alors un élément de $\mathbf{Z}$ divisant 1, donc ± 1, or $f(\pm 1) \neq 0$). Posons $K = \mathbf{Q}(\alpha)$ avec $f(\alpha) = 0$.

En utilisant les formules de Newton, il vient

$$\mathrm{Tr}_{K/\mathbf{Q}}(\alpha) = 0, \quad \mathrm{Tr}_{K/\mathbf{Q}}(\alpha^2) = 2, \quad \mathrm{Tr}_{K/\mathbf{Q}}(\alpha^3) = 3 \quad \text{et} \quad \mathrm{Tr}_{K/\mathbf{Q}}(\alpha^4) = 2,$$

donc

$$\Delta(1, \alpha, \alpha^2) = \begin{vmatrix} 3 & 0 & 2 \\ 0 & 2 & 3 \\ 2 & 3 & 2 \end{vmatrix} = -23.$$

Nous obtenons ainsi

$$\mathcal{O}_K = \mathbf{Z}[\alpha] \quad \text{et} \quad D_K = -23.$$

1. D'un point de vue théorique, on ne sait pas si ce problème est plus simple que celui de factoriser complètement m.

2. Reprenons l'exemple suivant la proposition 1.9. Soit $K = \mathbf{Q}(\alpha)$ avec $\alpha^3 - \alpha^2 - 2\alpha - 8 = 0$ et $f = f_{\alpha,\min} = T^3 - T^2 - 2T - 8$. On a

$$\Delta(1, \alpha, \alpha^2) = \begin{vmatrix} 3 & 1 & 5 \\ 1 & 5 & 31 \\ 5 & 31 & 49 \end{vmatrix} = -4 \cdot 503$$

donc

$$\mathbf{Z}[\alpha] \subset \mathcal{O}_K \subset \frac{1}{2}\mathbf{Z}[\alpha].$$

Posons $\beta = \frac{\alpha+\alpha^2}{2}$. Il s'agit d'un élément de $\mathcal{O}_K$ car $\beta^3 - 3\beta^2 - 10\beta - 8 = 0$. Comme

$$\Delta(1, \alpha, \beta) = \frac{1}{4}\Delta(1, \alpha, \alpha^2) = -503$$

est sans facteur carré, nous obtenons

$$\mathcal{O}_K = \mathbf{Z}[\alpha, \beta] = \mathbf{Z} \oplus \mathbf{Z}\alpha \oplus \mathbf{Z}\beta = \mathbf{Z} \oplus \mathbf{Z}\alpha \oplus \mathbf{Z}\frac{\alpha + \alpha^2}{2}.$$

Considérons maintenant $x \in \mathcal{O}_K$, écrit sous la forme

$$x = c + a\alpha + b\beta, \quad a, b, c \in \mathbf{Z}.$$

Il vient

$$x^2 = (c^2 + 6b^2 + 8ab) + (-a^2 + 2b^2 + 2ac)\alpha + (2a^2 + 3b^2 + 2bc + 4ab)\beta,$$

donc

$$\Delta(1, x, x^2) = \begin{vmatrix} 1 & c & C \\ 0 & a & A \\ 0 & b & B \end{vmatrix} \Delta(1, \alpha, \beta) = -503(aB - bA)^2$$

où l'on a posé $A = (-a^2 + 2b^2 + 2ac)$, $B = (2a^2 + 3b^2 + 2bc + 4ab)$ et $C = (c^2 + 6b^2 + 8ab)$. Comme

$$aB - bA \equiv ab^2 + a^2b \equiv ab(a + b) \equiv 0 \pmod 2,$$

nous en déduisons que l'entier $\Delta(1, x, x^2)$ est toujours pair et donc que l'anneau $\mathcal{O}_K$ n'est pas monogène.

1.5 Corps cyclotomiques

Soit $n \geqslant 1$ un nombre entier et soit K un corps. Une racine n-ième de l'unité x dans K est dite *primitive* si x est d'ordre n, donc si $x^d \neq 1$ pour tout diviseur strict d de n.

Posons

$$\boldsymbol{\mu}_n(K) = \{x \in K \mid x^n - 1 = 0\} \quad \text{et} \quad \boldsymbol{\mu}'_n(K) = \{x \in K \mid x^n - 1 = 0 \text{ et } \mathrm{ord}(x) = n\}.$$

Le sous-groupe $\boldsymbol{\mu}_n(K)$ de $K^\times$ est cyclique et, si $\boldsymbol{\mu}'_n(K) \neq \varnothing$, alors $\boldsymbol{\mu}'_n(K)$ est l'ensemble de ses générateurs.

Proposition 1.16. — (i) *Il existe une unique suite* $(\Phi_n)_{n\geqslant 1}$ *dans* $\mathbf{Z}[T]$ *telle que*

$$\forall n \in \mathbf{Z}_{\geqslant 1}, \quad T^n - 1 = \prod_{d|n} \Phi_d.$$

Tous les Φ_n sont des polynômes unitaires.

(ii) *Pour tout corps K de caractéristique première à p, les racines de Φ_n dans K sont les racines primitives n-ième de l'unité dans K :*

$$\{x \in K \mid \Phi_n(x) = 0\} = \boldsymbol{\mu}'_n(K).$$

Démonstration. (ii) Soit K un corps de caractéristique première à p. Via l'homomorphisme canonique de $\mathbf{Z}$ dans K, nous pouvons identifier Φ_n à un polynôme à coefficients dans K. Pour tout $x \in K$,

$$\begin{aligned} x \in \boldsymbol{\mu}'_n(K) &\iff \Big(x^n - 1 = 0 \text{ et } x^d - 1 \neq 0 \text{ pour tout diviseur strict } d \text{ de } n\Big) \\ &\iff (x^n - 1 = 0 \text{ et } \Phi_d(x) \neq 0 \text{ pour tout diviseur strict } d \text{ de } n) \end{aligned}$$

en vertu de l'identité

$$T^d - 1 = \prod_{d'|d} \Phi_{d'},$$

donc

$$\boldsymbol{\mu}'_n(K) = \{x \in K \mid \Phi_n(x) = 0 \text{ et } \Phi_d(x) \neq 0 \text{ pour tout diviseur strict } d \text{ de } n\}.$$

Le polynôme $T^n - 1$ est séparable puisque $\operatorname{pgcd}(T^n - 1, nT^{n-1}) = 1$, donc il résulte de l'identité

$$T^n - 1 = \prod_{d|n} \Phi_d$$

que les polynômes Φ_d associés aux diviseurs d de n sont premiers entre eux ; dès lors,

$$\boldsymbol{\mu}'_n(K) = \{x \in K \mid \Phi_n(x) = 0 \,\text{et}\, \Phi_d(x) \neq 0 \,\text{pour tout diviseur srict } d \text{ de } n\} = \{x \in K \mid \Phi_n(x) = 0\}.$$

(i) Munissons $\mathbf{N} \setminus \{0\}$ de la relation d'ordre partiel définie par la divisibilité, pour laquelle toute partie finie non vide admet un plus petit élément (le pgcd). On raisonne par récurrence sur $n \geqslant 1$.

Le cas $n = 1$ est trivial et $\Phi_1 = T - 1$. Considérons maintenant $n \geqslant 2$ et supposons que l'on dispose de polynômes unitaires $\Phi_d \in \mathbf{Z}[T]$ indexés par les diviseurs stricts d de n et tels que

$$T^d - 1 = \prod_{d'|d} \Phi_{d'}.$$

Il découle de cette dernière identité que les racines de Φ_d dans $\mathbf{C}$ sont les racines primitives d-ièmes de l'unité, donc

$$\operatorname{pgcd}(\Phi_d, \Phi'_d) = 1 \quad \text{si } d' \neq d.$$

Puisque $T^d - 1$ divise $T^n - 1$ dans $\mathbf{Z}[T]$, le polynôme Φ_d divise $T^n - 1$ dans $\mathbf{Z}[T]$ et donc

$$\prod_{d|n, d\neq n} \Phi_d \big| T^n - 1$$

dans $\mathbf{Q}[T]$ par factorialité. Le polynôme de gauche est unitaire et à coefficients entiers, donc il en est de même du quotient

$$\Phi_n = \frac{T^n - 1}{\prod_{d|n, d\neq n} \Phi_d}.$$

□

Lemme 1.17. — (i) *Pour tout* $n \in \mathbf{Z}_{\geqslant 1}$,

$$\Phi_n = \prod_{d|n} (T^d - 1)^{\mu(n/d)}$$

où μ *désigne la fonction de Möbius.*

(ii) *Pour tout nombre premier* p *et tout* $n \in \mathbf{Z}_{\geqslant 1}$,

$$\Phi_{np}(T) = \begin{cases} \Phi_n(T^p) & \text{si } p|n \\ \frac{\Phi_n(T^p)}{\Phi_n(T)} & \text{si } p \nmid n. \end{cases}$$

Démonstration. (i) Rappelons que la fonction de Möbius $\mu : \mathbf{Z}_{\geqslant 1} \to \{0, -1, 1\}$ est définie par

$$\mu(m) = \begin{cases} 1 & \text{si } m = 1 \\ (-1)^r & \text{si } m \text{ est le produit de } r \text{ nombres premiers distincts} \\ 0 & \text{si } m \text{ a un facteur carré.} \end{cases}$$

L'égalité souhaitée se déduit immédiatement de de l'identité

$$\sum_{\delta|m} \mu(\delta) = \sum_{i=0}^{r} \binom{r}{i} (-1)^i = 0$$

pour tout entier $m \geqslant 2$, où r désigne le nombre de diviseurs premiers distincts de m. Il suffit en effet d'écrire

$$\prod_{d|n} (T^d - 1)^{\mu(n/d)} = \prod_{d'|d|n} \Phi_{d'}^{\mu(n/d)} = \prod_{d'|n} \Phi_{d'}^{\sum_{\delta|\frac{n}{d'}} \mu(\delta)} = \Phi_n.$$

(ii) Les racines du polynôme $\Phi_n(T^p)$ dans $\mathbf{C}$ sont les nombres complexes z tels que $\mathrm{ord}(z^p) = n$. Comme

$$\mathrm{ord}(z^p) = \begin{cases} \mathrm{ord}(z) & \text{si} p \nmid \mathrm{ord}(z); \\ \frac{\mathrm{ord}(z)}{p} & \text{si } p|\mathrm{ord}(z) \end{cases}$$

ce sont précisément les nombres complexes z tels que

$$(\mathrm{ord}(z) = n \text{ et } p \nmid n) \quad \text{ou} \quad \mathrm{ord}(z) = np.$$

On en déduit

$$\Phi_n(T^p) = \begin{cases} \Phi_{np}(T)\Phi_n(T) & \text{si } p \nmid n \\ \Phi_{np}(T) & \text{si } p|n. \end{cases}$$

□

Proposition 1.18. — *Le polynôme* Φ_n *est irréductible sur* $\mathbf{Q}$.

Démonstration. Soit $g \in \mathbf{Q}[T]$ un polynôme unitaire irréductible divisant Φ_n. Comme Φ_n est unitaire et à coefficients entiers, il vient $g \in \mathbf{Z}[T]$ et $\Phi_n = gh$ avec $h \in \mathbf{Z}[T]$ unitaire. Soit p un nombre premier ne divisant pas n. En observant que $\Phi_n(T)|\Phi_n(T^p)$ en vertu du lemme ? ? ?, nous obtenons $g(T)|g(T^p)$ ou $g(T)|h(T^p)$.

Si $g(T)|h(T^p)$, alors la réduction modulo p conduit à

$$\overline{g}(T)|\overline{h(T)^p} = \overline{h}(T)^p$$

et donc les deux polynômes $\overline{g}$ et $\overline{h}$ ont un facteur irréductible commun dans $\mathbf{F}_p[T]$. Il s'ensuit que $\overline{\Phi_n} = \overline{g}\overline{h}$ possède un facteur carré, ce qui est impossible puisque les conditions $\overline{\Phi}_n | T^n - 1$ et $p \nmid n$ impliquent la séparabilité de $\overline{\Phi_n}$.

Nous obtenons ainsi $g(T)|g(T^p)$ dans $\mathbf{Z}[T]$, d'où l'on déduit $g(\alpha^p) = 0$ pour toute racine complexe α de g ; l'ensemble des racines complexes de g est donc stable par élévation à la puissance p. Puisque ceci vaut pour tout nombre premier p ne divisant pas n, il en découle que g s'annule identiquement sur $\mu_n'(\mathbf{C})$ et donc $g = \Phi_n$. □

Il découle de la proposition précédente que $\mathbf{Q}[T]/(\Phi_n)$ est un corps de nombres de degré $\varphi(n)$. C'est le *n-ième corps cyclotomique*, que l'on note $\mathbf{Q}(\boldsymbol{\mu}_n)$ ou $\mathbf{Q}(\zeta_n)$ (auquel cas ζ_n désigne une racine primitive n-ième de l'unité).

Proposition 1.19. — *Pour tout nombre entier $n \geqslant 3$,*

$$\operatorname{disc}(\Phi_n) = (-1)^{\frac{\phi(n)}{2}} \frac{n^{\varphi(n)}}{\prod_{p|n} p^{\frac{\varphi(n)}{p-1}}}.$$

Démonstration[2]. Soit ζ_n une racine primitive n-ième de l'unité dans $\mathbf{C}$. Le corps $\mathbf{Q}(\zeta_n)$ est totalement imaginaire, donc $\varphi(n) = 2r_2$ et le signe de $\operatorname{disc}(\Phi_n) = \Delta(1, \zeta_n, \ldots, \zeta_n^{\varphi(n)-1})$ est $(-1)^{\frac{\varphi(n)}{2}}$.

Calculons

$$|\Delta(1, \zeta_n, \ldots, \zeta_n^{\varphi(n)-1})| = \left|\mathrm{N}_{\mathbf{Q}(\zeta_n)}\left(\Phi_n'(\zeta_n)\right)\right|.$$

D'après le point (i) du lemme 1.17,

$$\Phi_n = (T^n - 1) \prod_{\substack{d|n \\ d \neq n}} (T^d - 1)^{\mu(n/d)}$$

donc

$$\Phi_n'(\zeta_n) = n\zeta_n^{n-1} \prod_{\substack{d|n \\ d \neq n}} (\zeta_n^d - 1)^{\mu(n/d)}$$

et

$$\mathrm{N}_{\mathbf{Q}(\zeta_n)/\mathbf{Q}}\left(\Phi_n'(\zeta_n)\right) = \pm n^{\varphi(n)} \prod_{\substack{d|n \\ d \neq n}} \mathrm{N}_{\mathbf{Q}(\zeta_n)/\mathbf{Q}}\left(\zeta_n^d - 1\right)^{\mu(n/d)}$$

car $\mathrm{N}_{\mathbf{Q}(\zeta_n)/\mathbf{Q}}(\zeta_n) = \pm\Phi_n(0) = \pm 1$.

Calculons maintenant $\left|\mathrm{N}_{\mathbf{Q}(\zeta_n)/\mathbf{Q}}\left(\zeta_n^d - 1\right)\right|$. Comme ζ_n^d est une racine primitive $\frac{n}{d}$-ième de l'unité, son polynôme minimal est $\Phi_{n/d}$; celui de $\zeta_n^d - 1$ est donc $\Phi_{n/d}(T+1)$ et

$$\mathrm{N}(\zeta_n^d - 1) = \left(\pm\Phi_{n/d}(1)\right)^{\varphi(n)/\varphi(n/d)}.$$

Le point (ii) du lemme 1.17 permet de calculer $\Phi_m(1)$ pour tout $m \geqslant 1$: si $m = p_1^{a_1} \cdots p_r^{a_r}$, alors

$$\Phi_m(1) = \Phi_{p_1 \cdots p_r}(1) = \begin{cases} \Phi_{p_1}(1) = p_1 & \text{si } r = 1 \\ 1 & \text{si } r \geqslant 2. \end{cases}$$

2. Ce calcul est tiré du livre *Polynomials*, de Victor Prasolov, Springer, p.94.)

Seuls les diviseurs d de n tels que n/d soit primaire vont donc compter. Comme $\mu(n/d) = 0$ si n/d a un facteur carré, on en déduit :

$$\left|N\left(\Phi_n'(\zeta_n)\right)\right| = n^{\varphi(n)} \prod_{p|n} \Phi_p(1)^{-\varphi(n)/\varphi(p)} = n^{\varphi(n)} \prod_{p|n} p^{\frac{-\varphi(n)}{p-1}}.$$

□

Cas particulier :

$$\operatorname{disc}\left(\Phi_{p^m}\right) = p^{(m(p-1)-1)p^{m-1}}$$

pour tout $m \geqslant 1$.

Nous allons terminer cette section par la détermination des anneaux des entiers des corps cyclotomiques. Le cas des corps $\mathbf{Q}(\boldsymbol{\mu}_{p^m})$ avec p premier est relativement aisé car les Φ_{p^m} sont des *polynômes d'Eisenstein*, notion dont l'étude fait l'objet du complément A à la fin de ce chapitre. Le cas général s'en déduit via la décomposition d'un nombre entier en produit de facteurs primaires, en recourant à un résultat général sur les extensions *linéairement disjointes* de corps de nombres dont la démonstration fait l'objet du complément B.

Proposition 1.20. — *Soit p un nombre premier et $r \geqslant 1$. L'anneau des entiers du corps cyclotomique $K = \mathbf{Q}(\boldsymbol{\mu}_{p^r})$ est*

$$\mathcal{O}_K = \mathbf{Z}[\zeta_{p^r}],$$

où ζ_{p^r} désigne une racine primitive p^r-ième de l'unité, et

$$D_K = \pm p^{p^{r-1}((p-1)r-1)}.$$

Démonstration. Posons $\zeta = \zeta_{p^r}$. En vertu de la proposition précédente,

$$\Delta(1, \zeta, \ldots, \zeta^{\varphi(p^r)-1}) = \operatorname{disc}(\Phi_{p^r}) = \pm \frac{p^{r\varphi(p^r)}}{p^{\frac{\varphi(p^r)}{p-1}}} = \pm p^{r(p-1)p^{r-1} - p^{r-1}} = \pm p^{p^{r-1}(p(r-1)-1)}.$$

Comme D_K divise $\Delta(1, \zeta, \ldots, \zeta^{\varphi(p^r)})$ (proposition 1.14), nous en déduisons que D_K est une puissance de p.

Par ailleurs,

$$\Phi_{p^r}(T+1) = \frac{(T+1)^{p^r} - 1}{(T+1)^{p^{r-1}} - 1} \equiv \frac{T^{p^r}}{T^{p^{r-1}}} \equiv T^{\varphi(p^r)} \pmod{p}$$

et

$$\Phi_{p^r}(1) = p$$

donc $\Phi_{p^r}(T+1)$ est un polynôme d'Eisenstein en p (Définition A1). Il en découle que D_K et $\Delta(1, \zeta, \ldots, \zeta^{\varphi(p^r)})$ ont la même valuation p-adique (corollaire A3), puis que ces deux nombres entiers sont égaux puisque tous deux sont des puissances de p de même signe. Au final, nous obtenons donc (proposition 1.14)

$$\mathcal{O}_K = \mathbf{Z}[\zeta] \quad \text{et} \quad D_K = \Delta(1, \zeta, \ldots, \zeta^{\varphi(p^r)}) = \pm p^{p^{r-1}(r(p-1)-1)}.$$

□

Proposition 1.21. — *Soit $n \geqslant 3$ et soit ζ_n une racine primitive n-ième de l'unité. L'anneau des entiers du corps de nombres $K = \mathbf{Q}(\mu_n) = \mathbf{Q}(\zeta_n)$ est*

$$\mathcal{O}_K = \mathbf{Z}[\zeta_n]$$

et

$$D_K = \mathrm{disc}(\Phi_n) = (-1)^{\frac{\varphi(n)}{2}} \frac{n^{\varphi(n)}}{\prod_{p|n} p^{\frac{\varphi(n)}{p-1}}}.$$

Démonstration. Pour tout nombre premier p divisant n,

$$\xi_p = \zeta_n^{np^{-v_p(n)}}$$

est une racine primitive $p^{v_p(n)}$-ième de l'unité dans K. Désignons par K_p le sous-corps $\mathbf{Q}(\xi_p)$.

L'application canonique

$$\lambda : \bigotimes_{p|n} K_p \to \mathbf{Q}(\zeta_n), \quad \otimes_{p|n} x_p \mapsto \prod_{p|n} x_p$$

est un isomorphisme de $\mathbf{Q}$-algèbres. Il s'agit en effet d'un morphisme de $\mathbf{Q}$-algèbres qui est surjectif puisque $\zeta_n = \prod_{p|n} \xi_p$ et

$$\dim_{\mathbf{Q}} \left(\bigotimes_{p|n} K_p \right) = \prod_{p|n} [K_p : \mathbf{Q}] = \prod_{p|n} \varphi(p^{v_p(n)}) = \varphi(n) = [K : \mathbf{Q}].$$

Ceci prouve que les extensions $K_p/\mathbf{Q}$ sont linéairement disjointes. En vertu de la proposition B.2, nous en déduisons

$$\mathcal{O}_K = \lambda \left(\bigotimes_{p|n} \mathcal{O}_{K_p} \right) \quad \text{et} \quad D_K = \prod_{p|n} D_{K_p}^{\frac{[K:\mathbf{Q}]}{[K_p:\mathbf{Q}]}} = \prod_{p|n} D_{K_p}^{\frac{\varphi(n)}{\varphi(p^r)}}.$$

Puisque

$$\mathcal{O}_{K_p} = \mathbf{Z}[\xi_p] = \mathbf{Z}[\zeta_n^{np^{-r}}] \quad \text{et} \quad D_{K_p} = \pm p^{p^{r-1}(r(p-1)-1)}$$

avec $r = v_p(n)$, nous avons donc obtenu

$$\mathcal{O}_K = \mathbf{Z}[\zeta_n] \ \text{ et } \ D_K = \pm \prod_{p|n} p^{\frac{\varphi(n)}{\varphi(p^r)} p^{r-1}(r(p-1)-1)} = \pm \prod_{p|n} p^{r\varphi(n)} \prod_{p|n} p^{-\frac{\varphi(n)}{\varphi(p^r)} p^{r-1}} = \pm n^{\varphi(n)} \prod_{p|n} p^{-\frac{\varphi(n)}{p-1}}.$$

Enfin, l'hypothèse $n \geqslant 3$ garantit que tous les plongements complexes de K sont non réels, donc $r_2 = \frac{1}{2}\varphi(n)$ et

$$D_K = (-1)^{r_2} |D_K| = (-1)^{\frac{\varphi(n)}{2}} |D_K|$$

en vertu de la seconde remarque suivant la définition 1.13. □

Complément A. Polynômes d'Eisenstein

Soit p un nombre premier.

On note $v_p : \mathbf{Q}^\times \to \mathbf{Z}$ la *valuation p-adique*. C'est l'unique application de $\mathbf{Q}^\times$ dans $\mathbf{Z}$ satisfaisant aux trois conditions suivantes :

(i) $v_p(xy) = v_p(x) + v_p(y)$

(ii) $v_p(x+y) \geqslant \min\{v_p(x), v_p(y)\}$

(iii) $v_p(1) = 0$ et $v_p(p) = 1$.

On vérifie aisément que l'on a

$$v_p(a) = \max\{m \in \mathbf{N} \mid p^m | a\}$$

pour tout $a \in \mathbf{Z} \setminus \{0\}$.

Exercice. Établir cette identité. (On pourra d'abord prouver que l'application v_p est positive sur $\mathbf{Z}$, puis qu'elle est nulle sur $\mathbf{Z} \setminus p\mathbf{Z}$.)

Définition A.1 — *On dit que $f \in \mathbf{Z}[T]$ unitaire est un* polynôme d'Eisenstein en p *si $f = T^n + a_{n-1}T^{n-1} + \ldots + a_0$ avec $p | a_i$ et $p^2 \nmid a_0$.*

Proposition A.2 — *Soit p un nombre premier et soit $f \in \mathbf{Z}[T]$ unitaire un polynôme d'Eisenstein en p.*

(i) *f est irréductible sur $\mathbf{Q}$.*

(ii) *Si $K = \mathbf{Q}(\alpha)$ avec $f(\alpha) = 0$, alors*

$$p \nmid (\mathcal{O}_K : \mathbf{Z}[\alpha]).$$

Démonstration. (i) Si $f = gh$ avec $g, h \in \mathbf{Q}[T]$ unitaires, alors $g, h \in \mathbf{Z}[T]$, puis $\overline{g} = X^a$ et $\overline{h} = X^b$ dans $\mathbf{F}_p[T]$ avec $a + b = n$ puisque $\overline{g}\,\overline{h} = \overline{f} = X^n$. Si $a, b \geqslant 1$, alors $p | g(0)$ et $p | h(0)$, donc $p^2 | f(0) = g(0)h(0)$, ce qui est exclu.

(ii) Raisonnons par l'absurde en supposant $p | (\mathcal{O}_K : \mathbf{Z}[\alpha])$. Il existe alors $x \in \mathcal{O}_K \setminus \mathbf{Z}[\alpha]$ tel que $px \in \mathbf{Z}[\alpha]$. Écrivons alors

$$x = \frac{1}{p}(u_0 + u_1\alpha + \ldots + u_{n-1}\alpha^{n-1}), \quad u_i \in \mathbf{Z}.$$

Par hypothèse, p ne divise pas tous les u_i ; soit i_0 le plus petit indice i tel que $p \nmid u_i$. Alors

$$y = \frac{1}{p}u_{i_0}\alpha^{i_0} + \sum_{i>i_0} \frac{1}{p}u_i\alpha^i = x - \sum_{i<i_0} \frac{u_i}{p}\alpha^i \in \mathcal{O}_K$$

puis

$$\frac{1}{p}u_{i_0}\alpha^{n-1} = \alpha^{n-i_0-1}y - \frac{\alpha^n}{p}\sum_{i>i_0} u_i\alpha^{i-i_0-1} \in \mathcal{O}_K$$

car $\frac{\alpha^n}{p} = -\sum_{i=0}^{n-1} \frac{a_i}{p}\alpha^i \in \mathbf{Z}[\alpha]$ par hypothèse. En prenant la norme, on en déduit

$$\frac{u_{i_0}^n a_0^{n-1}}{p^n} = \mathrm{N}_{K/\mathbf{Q}}\left(\frac{u_{i_0}}{p}\alpha^{n-1}\right) \in \mathbf{Z},$$

puis $p | u_{i_0}$ puisque $p^2 \nmid a_0$. Ceci contredit le choix de i_0, donc

$$p \nmid (\mathcal{O}_K : \mathbf{Z}[\alpha]).$$

□

Corollaire A.3 — *Soit $K = \mathbf{Q}(\alpha)$ un corps de nombres de degré n et soit p un nombre premier. Si $f_{\alpha,\min}$ est un polynôme d'Eisenstein en p, alors*

$$v_p(D_K) = v_p(\Delta(1, \alpha, \ldots, \alpha^{n-1})).$$

Démonstration. Il s'agit d'une conséquence immédiate de la proposition précédente puisque

$$\Delta(1, \alpha, \ldots, \alpha^{n-1}) = (\mathcal{O}_K : \mathbf{Z}[\alpha])D_K.$$

□

Exemples.

1. Soit $K = \mathbf{Q}(\alpha)$ avec $\alpha = \sqrt[4]{2}$), auquel cas $\Delta(1, \alpha, \alpha^2, \alpha^3) = -2^{11}$; on en déduit que D_K est de la forme -2^m avec $0 \leqslant m \leqslant 11$ et $m \equiv 11 \pmod 2$. Comme $f_{\alpha,\min} = T^4 - 2$ est un polynôme d'Eisenstein en 2,

   $$v_2(D_K) = v_2(\Delta(1, \alpha, \alpha^2, \alpha^3)) = 11.$$

   On en déduit

   $$D_K = -2^{11} \quad \text{et} \quad \mathcal{O}_K = \mathbf{Z}[\sqrt[4]{2}].$$

2. Soit $K = \mathbf{Q}(\alpha)$ avec $\alpha = \sqrt[3]{2}$, auquel cas

   $$\Delta(1, \alpha, \alpha^2) = -\mathrm{N}_{K/\mathbf{Q}}(3\alpha^2) = -\mathrm{N}_{K/\mathbf{Q}}(6\alpha^{-1}) = -6^3\mathrm{N}_{K/\mathbf{Q}}(\alpha)^{-1} = -2^2 3^3.$$

   Le polynôme $f_{\alpha,\min} = T^3 - 2$ étant d'Eisenstein en 2,

   $$v_2(D_K) = v_2(\Delta(1, \alpha, \alpha^2)) = 2.$$

   Si l'on pose $\beta = \alpha + 1$, alors $K = \mathbf{Q}(\beta)$ et $f_{\beta,\min} = (T-1)^3 - 2 = T^3 - 3T^2 + 3T - 3$ est un polynôme d'Eisenstein en 3, donc

   $$v_3(D_K) = v_3(\Delta(1, \beta, \beta^2)) = v_3(\Delta(1, \alpha, \alpha^2)) = 3.$$

   On en déduit

   $$D_K = -108 \quad \text{et} \quad \mathcal{O}_K = \mathbf{Z}[\alpha].$$

Complément B. Extensions linéairement disjointes

Lemme B.1 — *Soit F/K une extension finie de corps et soit L, L' deux sous-corps de F contenant K. Supposons que l'on ait $F = LL'$. Les deux conditions suivantes sont alors équivalentes :*

(i) $[F : K] = [L : K][L' : K]$

(ii) $L \otimes_K L'$ *est un corps.*

Démonstration. Considérons l'application canonique $\varphi : L \otimes_K L' \to F$ qui envoie $x \otimes y$ sur xy. Il s'agit d'un morphisme de K-algèbres, et l'hypothèse $F = LL'$ signifie que φ est une surjection. Puisque $\dim_K (L \otimes_K L') = [L : K][L' : K]$, il découle de la condition (i) que φ est un isomorphisme, et donc que $L \otimes_K L'$ est un corps. Réciproquement, si $L \otimes_K L'$ est un corps, alors φ est automatiquement une injection, donc un isomorphisme, et alors $[F : K] = \dim_K (L \otimes_K L') = [L : K][L' : K]$. □

Lorsque les deux conditions équivalentes du lemme sont réalisées, les extensions L/K et L'/K sont dites *linéairement disjointes.*

Proposition B.2 — *Soit F un corps de nombres. Supposons que L et L' soient deux sous-corps de F tels que*

(i) $F = LL'$ *;*

(ii) les extensions $L/\mathbf{Q}$ et $L'/\mathbf{Q}$ sont linéairement disjointes ;

(iii) $\mathrm{pgcd}(D_L, D'_L) = 1$.

Alors

$$\mathcal{O}_F = \mathcal{O}_L \mathcal{O}_{L'} \quad \text{et} \quad D_F = D_L^{[L':\mathbf{Q}]} D_{L'}^{[L:\mathbf{Q}]}.$$

Démonstration. Considérons une $\mathbf{Z}$-base $(\omega_1, \ldots, \omega_m)$ de $\mathcal{O}_L$ et désignons par $(\omega_1^*, \ldots, \omega_m^*)$ sa base duale relativement à la forme $\mathbf{Q}$-bilinéaire non dégénérée

$$b : L \times L \to \mathbf{Q}, \quad (x, y) \mapsto b(x, y) = \mathrm{Tr}_{L/\mathbf{Q}}(xy).$$

Rappelons que chaque ω_i^* appartient au sous-$\mathbf{Z}$-module de L engendré par $D_L^{-1}\omega_1, \ldots, D_L^{-1}\omega_m$ (voir la première démonstration de la proposition 1.12). Les conditions (i) et (ii) se traduisent en disant que (ω_i) est une L'-base de F, ce qui permet d'écrire

$$F = \bigoplus_{1 \leqslant i \leqslant m} L'\omega_i = \bigoplus_{1 \leqslant i \leqslant m 1 \leqslant j \leqslant n} \mathbf{Q}\omega_i\omega'_j.$$

La démonstration repose sur deux observations préliminaires.

(a) La forme L'-bilinéaire $b_{L'}$ sur F déduite de b par extension des scalaires de $\mathbf{Q}$ à L' coïncide avec la forme L'-bilinéaire $(x, y) \mapsto \mathrm{Tr}_{F/L'}(xy)$.

Il suffit de le vérifier sur une L'-base de$F$. Pour tout $a \in L$,

$$\mathrm{Tr}_{F/L'}(a) = \mathrm{Tr}_{L/\mathbf{Q}}(a)$$

car les endomorphismes $m_{a,F/L'} \in \mathrm{End}_{L'}(F)$ et $m_{a,L/\mathbf{Q}} \in \mathrm{End}_{\mathbf{Q}}(L)$ induits par la multiplication par a ont la même matrice dans la base (ω_i). On en déduit :

$$\mathrm{Tr}_{F/L'}(\omega_i\omega_j) = \mathrm{Tr}_{L/\mathbf{Q}}(\omega_i\omega_j) = b_{L'}(\omega_i, \omega_j)$$

pour tous $i, j \in \{1, \ldots, m\}$.

(b) Si $a \in \mathcal{O}_F$, alors $\mathrm{Tr}_{F/L'}(a) \in \mathcal{O}_{L'}$.

Considérons $a \in \mathcal{O}_F$ et rappelons que l'on désigne par $m_{a,F/L'}$ le L'-endomorphisme de F défini par la multiplication par a. Le polynôme minimal de $m_{a,F/L'}$ divise le polynôme minimal $f = f_{a,\min}$ de a sur $\mathbf{Q}$; ce dernier étant par hypothèse à coefficients entiers, ses racines (dans un corps de nombres scindant f) sont toutes des entiers algébriques. Les valeurs propres de $m_{a,F/L'}$ sont donc des entiers algébriques, et il en est en particulier de même pour sa trace

$$\mathrm{tr}(m_{a,F/L'}) = \mathrm{Tr}_{F/L'}(a).$$

Venons-en à la démonstration de notre théorème. Considérons un élément x de $\mathcal{O}_F$ et écrivons-le

$$x = \sum_{i,j} a_{ij}\omega_i\omega'_j = \sum_i \left(\sum_j a_{ij}\omega'_j \right) \omega_i, \qquad a_{ij} \in \mathbf{Q}.$$

En vertu des deux observations (a) et (b), nous pouvons écrire

$$x = \sum_{1 \leqslant i \leqslant m} \mathrm{Tr}_{F/L'}(x\omega_i)\omega_i^* \in \frac{1}{D_L} \bigoplus_{1 \leqslant i \leqslant m} \mathcal{O}_{L'}\omega_i,$$

donc

$$\sum_j a_{ij}\omega'_j \in \frac{1}{D_L}\mathcal{O}_{L'}$$

pour tout $i \in \{1, \ldots, m\}$, puis

$$D_L a_{ij} \in \mathbf{Z} \quad (1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant n)$$

puisque $\mathcal{O}_{L'} = \bigoplus_j \mathbf{Z}\omega'_j$.

Par symétrie, on a également $D_{L'}a_{ij} \in \mathbf{Z}$ pour tous i, j. On déduit alors de la condition (iii) que les a_{ij} sont des entiers relatifs, d'où $\mathcal{O}_F = \mathcal{O}_L\mathcal{O}_{L'}$.

Achevons la démonstration en calculant le discriminant de F. Par transitivité de la trace,

$$\mathrm{Tr}_{F/\mathbf{Q}}(\omega_i\omega'_j) = \mathrm{Tr}_{L'/\mathbf{Q}}\left(\mathrm{Tr}_{F/L'}(\omega_i\omega'_j)\right) = \mathrm{Tr}_{L'/\mathbf{Q}}\left(\mathrm{Tr}_{F/L'}(\omega_i)\omega'_j\right)$$

pour tous $i \in \{1, \ldots, m\},\ j \in \{1, \ldots, n\}$. Puisque $\mathrm{Tr}_{F/L'}(\omega_i) = \mathrm{Tr}_{L/\mathbf{Q}}(\omega_i)$ en vertu du fait (a), nous en déduisons

$$\mathrm{Tr}_{F/\mathbf{Q}}(\omega_i\omega'_j) = \mathrm{Tr}_{L'/\mathbf{Q}}\left(\omega'_j\mathrm{Tr}_{L/\mathbf{Q}}(\omega_i)\right) = \mathrm{Tr}_{L/\mathbf{Q}}(\omega_i)\mathrm{Tr}_{L'/\mathbf{Q}}(\omega'_j).$$

Si l'on pose $A = (\mathrm{Tr}_{L/\mathbf{Q}}(\omega_i\omega_k)) \in \mathrm{M}_m(\mathbf{Z})$ et $B = (\mathrm{Tr}_{L'/\mathbf{Q}}(\omega'_j\omega'_\ell)) \in \mathrm{M}_n(\mathbf{Z})$, alors, en ordonnant lexicographiquement les couples (i, j) dans $\{1, \ldots, m\} \times \{1, \ldots, n\}$,

$$C = \left(\mathrm{Tr}_{F/\mathbf{Q}}(\omega_i\omega'_j\omega_k\omega'_\ell)\right)_{(i,j),(k,\ell)} = \begin{pmatrix} Ab_{11} & \ldots & Ab_{1n} \\ \vdots & & \vdots \\ Ab_{n1} & \ldots & Ab_{nn} \end{pmatrix} \in \mathrm{M}_{mn}(\mathbf{Z})$$

donc

$$\det(C) = \det(A)^n \det(B)^m$$

(pour le voir, utiliser des opérations élémentaires sur les lignes de A, puis sur celles de B, pour trigonaliser C) et, finalement,

$$D_F = D_L^{[L':\mathbf{Q}]} D_{L'}^{[L:\mathbf{Q}]}.$$

□

Exemple. Soit d et d' deux entiers premiers entre eux et congrus à 1 modulo 4. Si l'on pose $L = \mathbf{Q}(\sqrt{d})$ et $L' = \mathbf{Q}(\sqrt{d'})$, alors on sait que

$$\mathcal{O}_L = \mathbf{Z}\left[\frac{1+\sqrt{d}}{2}\right],\ D_L = d \ \text{ et } \ \mathcal{O}_{L'} = \mathbf{Z}\left[\frac{1+\sqrt{d'}}{2}\right],\ D_{L'} = d'.$$

Par ailleurs, le polynôme $T^2 - d'$ est irréductible sur L ; sinon, il serait scindé sur L et alors $L = L'$, ce qui est exclu vu les discriminants de ces deux corps. On en déduit que $L \otimes_{\mathbf{Q}} L' \simeq L[T]/(T^2 - d')$ est un corps, donc L et L' sont deux extensions linéairement disjointes de $\mathbf{Q}$. Nous pouvons ainsi appliquer la proposition précédente et conclure : si $F = \mathbf{Q}(\sqrt{d}, \sqrt{d'}) = LL'$, alors

$$\mathcal{O}_F = \mathcal{O}_L \mathcal{O}_{L'} = \mathbf{Z}\left[\frac{1+\sqrt{d}}{2}, \frac{1+\sqrt{d'}}{2}, \frac{(1+\sqrt{d})(1+\sqrt{d'})}{4}\right] \ \text{ et } \ D_F = (dd')^2.$$

Chapitre 2

Factorisation idéale des nombres algébriques

En guise de motivation, considérons le corps de nombres $K = \mathbf{Q}(\sqrt{-5})$ et son anneau des entiers $\mathcal{O}_K = \mathbf{Z}[\sqrt{-5}]$, dans lequel nous pouvons écrire

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

L'anneau $\mathcal{O}_K$ ne contient pas d'élément de norme 2 ou 3 car $N_{K/\mathbf{Q}}(x + y\sqrt{-5}) = x^2 + 5y^2 \neq 2, 3$ pour tous $x, y \in \mathbf{Z}$. Comme

$$\mathrm{N}_{K/\mathbf{Q}}(2) = 4, \quad \mathrm{N}_{K/\mathbf{Q}}(3) = 9 \ \text{ et } \ \mathrm{N}_{K/\mathbf{Q}}(1 \pm \sqrt{-5}) = 6$$

il en découle que $2, 3$ et $1 \pm \sqrt{-5}$ sont des éléments irréductibles deux à deux non associés dans $\mathcal{O}_K$. Nous avons ainsi mis en évidence deux factorisations distinctes de 6 en produits d'éléments irréductibles dans $\mathcal{O}_K$, ce qui prouve que cet anneau n'est *pas* factoriel.

Une autre façon de voir les choses est d'utiliser le fait qu'un anneau noethérien est factoriel si et seulement si tout élément irréductible engendre un idéal *premier*[1]. Puisqu'ici l'anneau

$$\mathcal{O}_K/2\mathcal{O}_K \simeq \mathbf{Z}[T]/(2, T^2 + 5) \simeq \mathbf{F}_2[T]/(T^2 + 1) \simeq \mathbf{F}_2[T]/(T^2)$$

n'est pas intègre, l'idéal $2\mathcal{O}_K$ n'est pas premier et l'anneau $\mathcal{O}_K$ n'est donc pas factoriel.

Nous allons voir que l'on peut remédier au défaut de factorialité de $\mathcal{O}_K$ en utilisant des « diviseurs idéaux » qui ne sont autre que les *idéaux* (non nuls) de cet anneau. Cet exemple est repris de ce point de vue à la suite de la démonstration du théorème 2.4.

Convention. Dans ce qui suit, tous les anneaux considérés sont unitaires et commutatifs.

2.1 Anneaux de Dedekind

Soit A un anneau et B une A-algèbre. Un élément b de B est dit *entier* sur A s'il est racine d'un polynôme *unitaire* $f \in A[T]$; il revient au même de demander que la multiplication par b stabilise un sous-A-module de type fini contenant 1 dans B.

Si A est un anneau intègre de corps des fractions K, les éléments de K entiers sur A constituent un sous-anneau $\overline{A}$ de K appelé *clôture intégrale* de A dans K. On dit que A est *intégralement clos* si $\overline{A} = A$.

1. Dans tout anneau intègre, un élément a tel que l'idéal (a) soit premier est irréductible. Requérir que les idéaux principaux engendrés par les éléments irréductibles soient premiers revient à demander que le *lemme d'Euclide* soit valable dans cet anneau : si a est irréductible et $a|bc$, alors $a|b$ ou $a|c$.

Définition 2.1 — *Un anneau A est dit* de Dedekind *si*
(i) *A est intégralement clos (donc en particulier intègre) ;*
(ii) *A est noethérien ;*
(iii) *tout idéal premier non nul est maximal.*

Proposition 2.2 — (i) *Tout anneau principal est de Dedekind.*
(ii) *Si K est un corps de nombres, l'anneau $\mathcal{O}_K$ des entiers de K est un anneau de Dedekind.*

Démonstration. (i) Un anneau principal est évidemment noethérien et intégralement clos (exercice). Tout idéal premier non nul est de la forme (p) avec $p \in A$ irréductible ; si $(p) \subset (a)$, alors $p = ab$ puis $(p) = (a)$ ou $(a) = A$, donc l'idéal (p) est maximal.

(ii) Pour établir la noethérianité de l'anneau $\mathcal{O}_K$, il suffit d'observer qu'il est de type fini en tant que $\mathbf{Z}$-module (Proposition 1.12) et que ses idéaux sont des sous-$\mathbf{Z}$-modules. Vérifions maintenant que $\mathcal{O}_K$ est intégralement clos. Si $x \in K$ est entier sur $\mathcal{O}_K$, alors la multiplication par x stabilise un sous-$\mathcal{O}_K$-module non nul M dans K qui est de type fini sur $\mathcal{O}_K$, donc sur $\mathbf{Z}$ puisque $\mathcal{O}_K$ est un $\mathbf{Z}$-module de type fini ; on en déduit que x appartient à $\mathcal{O}_K$. Considérons enfin un idéal premier non nul $\mathfrak{p} \subset \mathcal{O}_K$ et un élément non nul a dans $\mathfrak{p}$. Il découle des inclusions

$$a\mathcal{O}_K \subset \mathfrak{p} \subset \mathcal{O}_K$$

que $\mathfrak{p}$ est un $\mathbf{Z}$-module libre de rang $[K : \mathbf{Q}]$, puis que $\mathcal{O}_K/\mathfrak{p}$ est un anneau fini et intègre (car $\mathfrak{p}$ est premier), donc un corps ; l'idéal $\mathfrak{p}$ est par conséquent maximal. □

Remarques. 1. La condition (iii) peut se traduire en disant que la *dimension de Krull* de l'anneau A est au plus égale à 1 : les chaînes d'idéaux premiers $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \ldots \subsetneq \mathfrak{p}_d$ sont de longueur (=nombre d'inclusions) au plus 1.

2. La géométrie algébrique fournit une autre source fondamentale d'anneaux de Dedekind. Si k est un corps algébriquement clos et $f \in k[X, Y]$ est un polynôme irréductible, alors $A = k[X, Y]/(f)$ est l'anneau des coordonnées de la courbe affine C d'équation $f = 0$. On peut démontrer que l'anneau A est de Dedekind si et seulement si les conditions équivalentes suivantes sont vérifiées [2] :
(i) $A = \overline{A}$;
(ii) $f, \frac{\partial f}{\partial X}$ et $\frac{\partial f}{\partial Y}$ engendrent l'idéal $k[X, Y]$;
(iii) la courbe C est non singulière.
En général, la clôture intégrale de A dans son corps des fractions est un anneau de Dedekind. Cette opération est le pendant algébrique de la *résolution des singularités* de C.

Définition 2.3 — *Soit A un anneau intègre de corps des fractions K. Un* idéal fractionnaire *est un sous-A-module* non nul $\mathfrak{a}$ *de K tel qu'il existe $d \in A - \{0\}$ avec $d\mathfrak{a} \subset A$. De manière équivalente, il s'agit d'une partie de K de la forme $\frac{1}{d}\mathfrak{a}$, où $\mathfrak{a} \subset A$ est un idéal non nul et $d \in A - \{0\}$.*

Remarques. 1. Tout sous-A-module de type fini $\mathfrak{a}$ de K est un idéal fractionnaire : il suffit en effet de considérer un dénominateur commun d des éléments d'une famille génératrice de $\mathfrak{a}$ pour avoir $d\mathfrak{a} \subset A$.

2. Réciproquement, si l'anneau A est noethérien, alors tout idéal fractionnaire de A est un sous-A-module de type fini de K (immédiat).

3. Si $A = \mathbf{Z}$, les idéaux fractionnaires sont les parties de $\mathbf{Q}$ de la forme $\mathbf{Z}r$ avec $r \in \mathbf{Q}^\times$.

2. Voir par exemple le livre *Undergraduate algebraic geometry* de Miles Reid, London Mathematical Society

L'ensemble $I(A)$ des idéaux fractionnaires de A est muni d'une structure de monoïde associatif, commutatif et unitaire en posant

$$\mathfrak{a} \cdot \mathfrak{b} = \{\sum_{i \in I} a_i b_i \mid I \text{ fini}, \quad a_i \in \mathfrak{a},\ b_i \in \mathfrak{b}\}.$$

L'élément neutre est l'idéal trivial A et l'application

$$K^\times \to I(A), \quad x \mapsto Ax$$

est un morphisme de monoïdes. Le sous-ensemble $I^+(A)$ formé des idéaux de A est un sous-monoïde de $I(A)$.

On vérifie immédiatement cette multiplication est compatible avec l'inclusion : pour tous idéaux fractionnaires $\mathfrak{a}, \mathfrak{b}$ et $\mathfrak{c}$ de A,

$$\mathfrak{a} \subset \mathfrak{b} \Longrightarrow \mathfrak{a} \cdot \mathfrak{c} \subset \mathfrak{b} \cdot \mathfrak{c}.$$

Théorème 2.4 — *Soit A un anneau de Dedekind et soit P l'ensemble des ses idéaux premiers non nuls.*

(i) *Le monoïde $I(A)$ est un groupe : tout idéal fractionnaire possède un inverse.*

(ii) *L'application*

$$\mathbf{Z}^{(P)} \to I(A), \quad m \mapsto \prod_{\mathfrak{p} \in P} \mathfrak{p}^{m(\mathfrak{p})}$$

est un isomorphisme de groupes envoyant $\mathbf{N}^{(P)}$ sur $I^+(A)$.

La démonstration de ce théorème requiert trois lemmes préliminaires.

Lemme 2.5 — *Soit A un anneau et $\mathfrak{p}, \mathfrak{a}, \mathfrak{b}$ des idéaux. Si $\mathfrak{p}$ est premier et $\mathfrak{a} \cdot \mathfrak{b} \subset \mathfrak{p}$, alors $\mathfrak{a} \subset \mathfrak{p}$ ou $\mathfrak{b} \subset \mathfrak{p}$.*

Démonstration. La contraposée est immédiate : s'il existe $a \in \mathfrak{a}$ et $b \in \mathfrak{b}$ n'appartenant pas à $\mathfrak{p}$, alors ab est un élément de $\mathfrak{a} \cdot \mathfrak{b}$ n'appartenant pas à $\mathfrak{p}$. □

Lemme 2.6 — *Soit A un anneau noethérien. Tout idéal non nul de A contient un produit fini d'idéaux premiers non nuls.*

Démonstration. On raisonne par l'absurde en supposant que l'ensemble des idéaux non nuls de A ne contenant aucun produit fini d'idéaux premiers non nuls est non vide. Par noethérianité de A, cet ensemble admet un élément maximal pour l'inclusion ; notons-le $\mathfrak{a}$. Bien évidemment, l'idéal $\mathfrak{a}$ n'est pas premier donc il existe $a, b \in A - \mathfrak{p}$ tels que $ab \in \mathfrak{a}$. Par maximalité de $\mathfrak{a}$, il existe alors des idéaux premiers $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ et $\mathfrak{q}_1, \ldots, \mathfrak{q}_m$ tels que

$$\mathfrak{p}_1 \cdots \mathfrak{p}_n \subset \mathfrak{a} + Aa \quad \text{et} \quad \mathfrak{q}_1 \cdots \mathfrak{q}_m \subset \mathfrak{a} + Ab.$$

On en déduit

$$\mathfrak{p}_1 \cdots \mathfrak{p}_n \cdot \mathfrak{q}_1 \cdots \mathfrak{q}_m \subset (\mathfrak{a} + Aa) \cdot (\mathfrak{a} + Ab) \subset \mathfrak{a} + Aab = \mathfrak{a},$$

ce qui contredit la définition de $\mathfrak{a}$. □

Remarque. Cette démonstration est parfaitement analogue à celle établissant que tout élément non nul d'un anneau noethérien peut s'écrire comme le produit d'un nombre fini d'éléments irréductibles.

Dans ce qui suit, A est un anneau de Dedekind de corps des fractions K. Pour tout idéal fractionnaire $\mathfrak{a}$ de A, posons

$$\tilde{\mathfrak{a}} = \{x \in K \mid x\mathfrak{a} \subset A\}.$$

Il s'agit d'un idéal fractionnaire de A : en effet, c'est clairement un sous-A-module de K et, si a est un élément non nul de $\mathfrak{a}$, alors $a\tilde{\mathfrak{a}} \subset A$.

Lemme 2.7 — *Pour tout idéal premier non nul $\mathfrak{p}$ de A,*

(i) $A \subsetneq \tilde{\mathfrak{p}}$

(ii) $\mathfrak{p} \cdot \tilde{\mathfrak{p}} = A$

Démonstration. (i) Soit x un élément non nul de $\mathfrak{p}$. Considérons des idéaux premiers non nuls $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ tels que

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \subset (x)$$

(Lemme 2.6) et choisissons-les tels que r soit minimal. Par maximalité de $\mathfrak{p}$, l'inclusion

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \subset \mathfrak{p}$$

implique l'existence d'un indice i tel que $\mathfrak{p}_i \subset \mathfrak{p}$ (Lemme 2.5) et donc $\mathfrak{p}_i = \mathfrak{p}$. On peut supposer $i = 1$. La minimalité de r fournit un élément y de $\mathfrak{p}_2 \cdots \mathfrak{p}_r$ n'appartenant pas à Ax (si $r = 1$, on peut prendre $y = 1$). L'élément $\frac{y}{x}$ de K n'appartient pas à A et vérifie

$$\frac{y}{x}\mathfrak{p} \subset \frac{1}{x}\mathfrak{p} \cdot \mathfrak{p}_2 \cdots \mathfrak{p}_r \subset \frac{1}{x}Ax = A,$$

donc $\frac{y}{x}$ appartient à $\tilde{\mathfrak{p}}$.

(ii) On a

$$\mathfrak{p} \subset \mathfrak{p} \cdot \tilde{\mathfrak{p}} \subset A$$

par définition de $\mathfrak{p}$, donc $\mathfrak{p} \cdot \tilde{\mathfrak{p}} = \mathfrak{p}$ ou $\mathfrak{p} \cdot \tilde{\mathfrak{p}} = A$ par maximalité de $\mathfrak{p}$. Le premier cas est exclu : il implique en effet que les éléments de $\tilde{\mathfrak{p}}$ sont tous entiers sur A, donc appartiennent à A, et ceci contredit (i). □

Démonstration du théorème 2.4. Considérons le morphisme de monoïdes

$$\varphi : \mathbf{Z}^{(P)} \to I(A), \quad m \mapsto \prod_{\mathfrak{p} \in P} \mathfrak{p}^{m(\mathfrak{p})}$$

où l'on a posé $\mathfrak{p}^{-1} = \tilde{\mathfrak{p}}$.

Nous allons tout d'abord établir la surjectivité de φ en raisonnant par l'absurde. Soit $\mathfrak{a} \subset A$ un idéal non nul. Supposons que $\mathfrak{a}$ ne soit pas dans l'image de φ et soit maximal pour cette propriété. Cet idéal n'est ni trivial ni premier, donc il existe $\mathfrak{p} \in P$ tel que $\mathfrak{a} \subsetneq \mathfrak{p}$. On en déduit les inclusions

$$\mathfrak{a} \subset \tilde{\mathfrak{p}} \cdot \mathfrak{a} \subset \tilde{\mathfrak{p}} \cdot \mathfrak{p} = A.$$

La première est stricte car sinon $\tilde{\mathfrak{p}} \subset A$ puisque A est intégralement clos, donc $\tilde{\mathfrak{p}} \cdot \mathfrak{a}$ appartient à l'image de φ. On en déduit alors que

$$\mathfrak{a} = \mathfrak{p} \cdot (\tilde{\mathfrak{p}} \cdot \mathfrak{a})$$

appartient également à l'image de φ ; contradiction !

Le monoïde $I(A)$ est engendré par les éléments inversibles $\mathfrak{p} \in P$, donc tout élément de $I(A)$ est inversible et $I(A)$ est un groupe. Vérifions que l'inverse d'un idéal fractionnaire non nul $\mathfrak{a}$ est bien l'idéal fractionnaire $\tilde{\mathfrak{a}}$. L'inclusion $\mathfrak{a}^{-1} \subset \tilde{\mathfrak{a}}$ découle immédiatement de l'identité

$$\mathfrak{a}^{-1} \cdot \mathfrak{a} = A$$

tandis que l'inclusion réciproque se déduit de

$$\mathfrak{a} \cdot \tilde{\mathfrak{a}} \subset A$$

en multipliant de part et d'autre par $\mathfrak{a}^{-1}$.

Il reste à démontrer que l'application φ est injective. Un élément du noyau de φ fournit une identité

$$\prod_{\mathfrak{p}} \mathfrak{p}^{m(\mathfrak{p})} = \prod_{\mathfrak{p}} \mathfrak{p}^{n(\mathfrak{p})}$$

avec $m(\mathfrak{p}), n(\mathfrak{p}) \geqslant 0$ pour tout $\mathfrak{p}$. En multipliant chaque côté par des $\mathfrak{p}^{-1}$, on peut en outre supposer $\max\{m(\mathfrak{p}), n(\mathfrak{p})\} = 0$ pour tout $\mathfrak{p}$. La conclusion découle maintenant du lemme 2.5 : si $\mathfrak{p}_1, \ldots, \mathfrak{p}_m, \mathfrak{q}_1, \ldots, \mathfrak{p}_n$ sont des idéaux premiers non nuls tous distincts tels que

$$\mathfrak{p}_1 \cdots \mathfrak{p}_m = \mathfrak{q}_1 \cdots \mathfrak{q}_n,$$

alors il existe $i \in \{1, \ldots, m\}$ tel que $\mathfrak{p}_i \subset \mathfrak{q}_1$ et donc $\mathfrak{p}_i = \mathfrak{q}_1$ par maximalité de $\mathfrak{p}_i$, ce qui est exclu. □

Tout idéal fractionnaire $\mathfrak{a}$ de A s'écrit donc de manière unique sous la forme

$$\mathfrak{a} = \prod_{\mathfrak{p} \in P} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})}$$

avec $v_{\mathfrak{p}}(\mathfrak{a}) \in \mathbf{Z}$ nul pour presque tout $\mathfrak{p}$. L'application

$$v_{\mathfrak{p}} : \mathrm{I}(A) \to \mathbf{Z}$$

est appelée la *valuation* $\mathfrak{p}$*-adique.*

Proposition 2.8 (Formulaire) — *Soit* $\mathfrak{a}$ *et* $\mathfrak{b}$ *des idéaux fractionnaires de* A*.*

(i) *Pour tout* $\mathfrak{p} \in P$*,*

$$v_{\mathfrak{p}}(\mathfrak{a} \cdot \mathfrak{b}) = v_{\mathfrak{p}}(\mathfrak{a}) + v_{\mathfrak{p}}(\mathfrak{b}).$$

(ii) *On a*

$$\mathfrak{a} \subset \mathfrak{b} \quad \Longrightarrow \quad \forall \mathfrak{p} \in P, \quad v_p(\mathfrak{b}) \leqslant v_{\mathfrak{p}}(\mathfrak{a}).$$

(iii) *Pour tout* $\mathfrak{p} \in P$*,*

$$v_{\mathfrak{p}}(\mathfrak{a} + \mathfrak{b}) = \min\{v_{\mathfrak{p}}(\mathfrak{a}), v_{\mathfrak{p}}(\mathfrak{b})\}.$$

(iv) *Pour tout* $\mathfrak{p} \in P$*,*

$$v_{\mathfrak{p}}(\mathfrak{a} \cap \mathfrak{b}) = \max\{v_{\mathfrak{p}}(\mathfrak{a}), v_{\mathfrak{p}}(\mathfrak{b})\}.$$

Démonstration. (i) C'est immédiat.

(ii) On a

$$\mathfrak{a} \subset \mathfrak{b} \iff \mathfrak{a} \cdot \mathfrak{b}^{-1} \subset A \iff \big(\forall \mathfrak{p} \in P, \quad v_{\mathfrak{p}}(\mathfrak{a} \cdot \mathfrak{b}^{-1}) \geqslant 0\big)$$

et la conclusion découle alors de (i).

(iii) On vérifie immédiatement que $\mathfrak{a} + \mathfrak{b}$ est le plus petit idéal fractionnaire contenant $\mathfrak{a}$ et $\mathfrak{b}$; la conclusion découle alors de (ii).

(iv) On vérifie immédiatement que $\mathfrak{a} \cap \mathfrak{b}$ est le plus grand idéal fractionnaire contenu dans $\mathfrak{a}$ et $\mathfrak{b}$; la conclusion découle alors de (ii). □

Interprétation. On dispose d'une notion parfaite de divisibilité dans $\mathrm{I}^+(A)$.

Étant donné deux idéaux fractionnaires entiers $\mathfrak{a}, \mathfrak{b} \in \mathrm{I}^+(A)$, c'est-à-dire simplement deux idéaux non nuls de A, convenons de dire que $\mathfrak{a}$ *divise* $\mathfrak{b}$ et de noter $\mathfrak{a}|\mathfrak{b}$ s'il existe un idéal fractionnaire $\mathfrak{c}$ tel que

$$\mathfrak{b} = \mathfrak{a} \cdot \mathfrak{c}.$$

Cette condition est équivalente à $\mathfrak{b} \cdot \mathfrak{a}^{-1} \subset A$, donc à $\mathfrak{b} \subset \mathfrak{a}$ d'après le point (ii) ci-dessus. Notons que la motivation derrière cette définition est l'observation suivante : si a, b sont deux éléments de A, alors

$$a|b \iff (b) \subset (a).$$

1. Tout idéal $\mathfrak{a} \in \mathrm{I}^+(A)$ possède un multiple principal : en effet, si a est un élément non nul de $\mathfrak{a}$, alors $(a) \subset \mathfrak{a}$ et donc $\mathfrak{a}|(a)$. Ainsi, nous pouvons penser aux idéaux comme à des « diviseurs idéaux » des éléments de A.

2. Pour tous $\mathfrak{a}, \mathfrak{b} \in \mathrm{I}^+(A)$, on établit immédiatement les identités

$$\mathfrak{a} + \mathfrak{b} = \mathrm{pgcd}(\mathfrak{a}, \mathfrak{b}) \quad \text{et} \quad \mathfrak{a} \cap \mathfrak{b} = \mathrm{ppcm}(\mathfrak{a}, \mathfrak{b}).$$

Notons que la première égalité implique directement

$$\mathfrak{a} = \mathrm{pgcd}\{(x), \quad x \in \mathfrak{a}\}$$

pour tout $\mathfrak{a} \in \mathrm{I}^+(A)$. Par ailleurs, la comparaison des valuations $\mathfrak{p}$-adiques fournit la relation

$$\mathrm{pgcd}(\mathfrak{a}, \mathfrak{b}) \cdot \mathrm{ppcm}(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} \cdot \mathfrak{b}.$$

3. Pour $\mathfrak{a}, \mathfrak{b} \in \mathrm{I}^+(A)$, on dit que $\mathfrak{a}$ et $\mathfrak{b}$ sont *premiers entre eux* si $\mathfrak{a} + \mathfrak{b} = A$. Il en découle aisément que l'application canonique de A dans $A/\mathfrak{a} \oplus A/\mathfrak{b}$ est surjective et que son noyau $\mathfrak{a} \cap \mathfrak{b}$ coïncide avec $\mathfrak{a} \cdot \mathfrak{b}$ (exercice) ; ceci nous permet donc d'énoncer une généralisation du théorème chinois des restes : *si deux idéaux* $\mathfrak{a}, \mathfrak{b} \in \mathrm{I}^+(A)$ *sont premiers entre eux, alors l'application canonique*

$$A/\mathfrak{a} \cdot \mathfrak{b} \to A/\mathfrak{a} \oplus A/\mathfrak{b}$$

est un isomorphisme d'anneaux.

Exemple (retour). Reprenons l'anneau $A = \mathbf{Z}[\sqrt{-5}]$ considéré dans l'introduction à ce chapitre et l'identité

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Puisque $A = \mathcal{O}_{\mathbf{Q}(\sqrt{-5})}$, il s'agit d'un anneau de Dedekind. Posons

$$\mathfrak{p}_2 = \mathrm{pgcd}(2, 1 + \sqrt{-5}) = (2, 1 + \sqrt{-5}) \quad \text{et} \quad \mathfrak{p}_3 = \mathrm{pgcd}(3, 1 + \sqrt{-5}) = (3, 1 + \sqrt{-5}).$$

Il s'agit d'idéaux premiers en vertu des isomorphismes

$$A/\mathfrak{p}_2 \simeq \mathbf{F}_2[T]/(1 + T) \simeq \mathbf{F}_2 \quad \text{et} \quad A/\mathfrak{p}_3 \simeq \mathbf{F}_3[T]/(1 + T) \simeq \mathbf{F}_3$$

et

$$\mathfrak{p}_2 \cdot \mathfrak{p}_3 = (6, 2(1 + \sqrt{-5}), 3(1 + \sqrt{-5}), (1 + \sqrt{-5})^2) = (1 + \sqrt{-5}).$$

De même, les idéaux

$$\mathfrak{p}_2' = \mathrm{pgcd}(2, 1 - \sqrt{-5}) = (2, 1 - \sqrt{-5}) \quad \text{et} \quad \mathfrak{p}_3' = \mathrm{pgcd}(3, 1 - \sqrt{-5}) = (3, 1 - \sqrt{-5})$$

sont premiers et

$$\mathfrak{p}_2' \cdot \mathfrak{p}_3' = (1 - \sqrt{-5}).$$

Notons que l'on a $\mathfrak{p}_2' = \mathfrak{p}_2$. Notre identité initiale fournit la factorisation

$$(6) = \mathfrak{p}_2 \cdot \mathfrak{p}_3 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_3' = \mathfrak{p}_2^2 \cdot \mathfrak{p}_3 \cdot \mathfrak{p}_3$$

et elle s'explique en observant que

$$\mathfrak{p}_2^2 = (4, 2(1+\sqrt{-5}), 2(1-\sqrt{-5}), 6) = (2) \quad \text{et} \quad \mathfrak{p}_3 \cdot \mathfrak{p}_3' = (9, 3(1+\sqrt{-5}), 3(1-\sqrt{-5}), 6) = (3).$$

Considérons toujours un anneau de Dedekind A de corps des fractions K. Le morphisme de groupes

$$K^\times \to \mathrm{I}(A), \quad x \mapsto (x) = Ax$$

a pour noyau le groupe $A^\times$ des éléments inversibles de A et pour image le sous-groupe $\mathrm{P}(A)$ de $\mathrm{I}(A)$ formé des idéaux fractionnaires *principaux*. Le quotient $\mathrm{I}(A)/\mathrm{P}(A)$ est appelé le *groupe des classes d'idéaux* de A et est noté $\mathrm{Cl}(A)$. En utilisant la factorisation des idéaux fractionnaires, nous pouvons écrire une suite exacte :

$$0 \longrightarrow A^\times \longrightarrow K^\times \xrightarrow{v} \mathbf{Z}^{(P)} \longrightarrow \mathrm{Cl}(A) \longrightarrow 0$$

où v est l'application définie par

$$v(x) = (\mathfrak{p} \mapsto v_\mathfrak{p}(x) = v_\mathfrak{p}(Ax))$$

pour tout $x \in K^\times$.

Proposition 2.9. — *Soit A un anneau de Dedekind. Les conditions suivantes sont équivalentes :*

(i) *le groupe* $\mathrm{Cl}(A)$ *est trivial ;*
(ii) *A est principal ;*
(iii) *A est factoriel ;*
(iv) *tout idéal premier non nul de A est principal.*

Démonstration. L'implication (i) $\Rightarrow$ (ii) est immédiate.

L'implication (ii) $\Rightarrow$ (iii) est classique. Un anneau principal étant noethérien, l'existence d'une factorisation en produit d'irréductibles est acquise pour tout élément non inversible de A. Pour obtenir l'unicité, on observe que tout élément irréductible p de A engendre nécessairement un idéal maximal : si $(p) \subset I \subsetneq A$ et $I = (a)$, alors $a|p$ et a n'est pas inversible, donc $p = \varepsilon a$ avec $\varepsilon \in A^\times$ et $I = (a) = (p)$. Il en découle en particulier que l'idéal (p) est premier, ce qui fournit l'analogue du lemme d'Euclide dans A :

$$\forall a, b \in A, \quad p|ab \quad \Rightarrow \quad p|a \ \text{ ou } \ p|b.$$

Prouvons l'implication (iii) $\Rightarrow$ (iv). Soit $\mathfrak{p}$ un idéal premier non nul de A et soit $a \neq 0$ un élément de $\mathfrak{p}$. En écrivant $a = p_1 \cdots p_r$ avec les p_i irréductibles, nous obtenons l'existence d'un i tel que $p_i \in \mathfrak{p}$. S'il existe $b \in \mathfrak{p} \setminus (p_i)$, alors $\mathfrak{p}$ contient de même l'un des facteurs irréductibles q de b et q n'est pas associé à p_i puisque $p_i \nmid b$. On en déduit que $\mathfrak{p}$ contient l'idéal $(p_i) + (q)$, lequel est égal à A par factorialité ; cela contredit le caractère premier de $\mathfrak{p}$. Ainsi, tout idéal premier non nul de A est principal. □

Remarques. 1. Les anneaux factoriels et les anneaux de Dedekind fournissent deux extensions « orthogonales » de la classe des anneaux principaux. Pour mémoire, on rappelle que si un anneau A est factoriel alors il en est de même de l'anneau $A[T]$.

2. Nous verrons au chapitre suivant que si K est un corps de nombres, alors le groupe $\mathrm{Cl}(\mathcal{O}_K)$ est *fini* ; il en découle qu'il existe un entier $h \geqslant 1$ tel que $\mathfrak{a}^h$ soit principal pour tout idéal fractionnaire $\mathfrak{a}$ de $\mathcal{O}_K$.

2.2 Factorisation et ramification

Soit K un corps de nombres. Si $\mathfrak{a} \in \mathrm{I}^+(A)$ est un idéal non nul de $\mathcal{O}_K$, alors $\mathfrak{a}$ est un $\mathbf{Z}$-module libre de rang $[K : \mathbf{Q}]$ (cf. démonstration de la proposition 2.2) et donc $\mathcal{O}_K/\mathfrak{a}$ est un groupe fini. On définit la *norme* de $\mathfrak{a}$, notée $\mathrm{N}(\mathfrak{a})$ par

$$\mathrm{N}(\mathfrak{a}) = \mathrm{Card}\,(\mathcal{O}_K/\mathfrak{a})\,.$$

Proposition 2.10 — *Soit K un corps de nombres.*

(i) *Pour tout $\alpha \in \mathcal{O}_K \setminus \{0\}$,*

$$\mathrm{N}(\alpha\mathcal{O}_K) = |\mathrm{N}_{K/\mathbf{Q}}(\alpha)|.$$

(ii) *Pour tous idéaux non nuls $\mathfrak{a}, \mathfrak{b} \subset \mathcal{O}_K$,*

$$\mathrm{N}(\mathfrak{a} \cdot \mathfrak{b}) = \mathrm{N}(\mathfrak{a})\mathrm{N}(\mathfrak{b}).$$

Démonstration. (i) Posons $n = [K : \mathbf{Q}]$. Le choix d'une base du $\mathbf{Z}$-module libre $\mathcal{O}_K$ permet d'écrire un diagramme commutatif

$$\begin{array}{ccc} \mathbf{Z}^n & \xrightarrow{\sim} & \mathcal{O}_K \\ {\scriptstyle A}\downarrow & & \downarrow{\scriptstyle m_{\alpha,K/\mathbf{Q}}} \\ \mathbf{Z}^n & \xrightarrow{\sim} & \mathcal{O}_K \end{array}$$

dans lequel $A \in \mathrm{M}_n(\mathbf{Z})$ est la matrice de la multiplication par α dans cette base. On en déduit un isomorphisme de $\mathbf{Z}$-modules

$$\mathcal{O}_K/\alpha\mathcal{O}_K \simeq \mathbf{Z}^n/\mathrm{im}(A)$$

et donc

$$\mathrm{N}(\alpha\mathcal{O}_K) = \mathrm{Card}\,(\mathcal{O}_K/\alpha\mathcal{O}_K) = \mathrm{Card}\,(\mathbf{Z}^n/\mathrm{im}(A)) = |\det(A)| = |\mathrm{N}_{K/\mathbf{Q}}(\alpha)|$$

(voir la preuve de la proposition 1.14 pour la justification de l'avant-dernière égalité).

(ii) Par factorisation (Théorème 2.4), il suffit de considérer le cas où $\mathfrak{a}$ et $\mathfrak{b}$ sont premiers.

Si $\mathfrak{a} \neq \mathfrak{b}$, alors $\mathfrak{a}$ et $\mathfrak{b}$ sont premiers entre eux et la conclusion découle directement du théorème chinois des restes :

$$\mathcal{O}_K/\mathfrak{a} \cdot \mathfrak{b} \simeq \mathcal{O}_K/\mathfrak{a} \times \mathcal{O}_K/\mathfrak{b}.$$

Supposons maintenant $\mathfrak{b} = \mathfrak{a}$ et considérons la suite exacte courte de $\mathcal{O}_K$-modules finis

$$0 \longrightarrow \mathfrak{a}/\mathfrak{a}^2 \longrightarrow \mathcal{O}_K/\mathfrak{a}^2 \longrightarrow \mathcal{O}_K/\mathfrak{a} \longrightarrow 0$$

dont on déduit l'égalité

$$\mathrm{N}(\mathfrak{a}^2) = \mathrm{N}(\mathfrak{a}) \cdot \mathrm{Card}\left(\mathfrak{a}/\mathfrak{a}^2\right).$$

Le $\mathcal{O}_K$-module $\mathfrak{a}/\mathfrak{a}^2$ est naturellement muni d'une structure d'espace vectoriel sur le corps fini $\mathcal{O}_K/\mathfrak{a}$ et

$$\mathrm{Card}\left(\mathfrak{a}/\mathfrak{a}^2\right) = \mathrm{Card}\,(\mathcal{O}_K/\mathfrak{a})^{\dim_{\mathcal{O}_K/\mathfrak{a}}\left(\mathfrak{a}/\mathfrak{a}^2\right)}.$$

Soit a un élément de $\mathfrak{a} \setminus \mathfrak{a}^2$. La factorisation de (a) est de la forme

$$(a) = \mathfrak{a}^m \cdot \mathfrak{b}$$

avec $m \geqslant 1$ et $\mathfrak{b} \in \mathrm{I}^+(A)$ non divisible par $\mathfrak{a}$. Les conditions $(a) \subset \mathfrak{a}$ et $(a) \not\subset \mathfrak{a}^2$ impliquent $m = 1$. Les idéaux $\mathfrak{a}$ et $\mathfrak{b}$ sont premiers entre eux donc

$$A = \mathfrak{a} + \mathfrak{b} \quad \text{puis} \quad \mathfrak{a} = \mathfrak{a}^2 + \mathfrak{a} \cdot \mathfrak{b} = \mathfrak{a}^2 + (a)$$

et ainsi a engendre le $\mathcal{O}_K/\mathfrak{a}$-espace vectoriel $\mathfrak{a}/\mathfrak{a}^2$. On en déduit l'inégalité

$$\dim_{\mathcal{O}_K/\mathfrak{a}} \left(\mathfrak{a}/\mathfrak{a}^2\right) \leqslant 1,$$

puis l'égalité puisque $\mathfrak{a}/\mathfrak{a}^2 \neq 0$. □

Les deux propriétés que l'on vient d'établir permettent d'étendre la norme en un morphisme de groupes

$$\mathrm{N} : \mathrm{I}(A) \to \mathbf{Q}_{>0}$$

en posant

$$\mathrm{N}(\mathfrak{a}) = \mathrm{N}(d\mathfrak{a})|\mathrm{N}_{K/\mathbf{Q}}(d)|^{-1}$$

avec $d \in \mathcal{O}_K \setminus \{0\}$ tel $d\mathfrak{a} \subset \mathcal{O}_K$.

Soit K un corps de nombres et soit $\mathfrak{p}$ un idéal premier non nul de $\mathcal{O}_K$. L'anneau quotient

$$\kappa(\mathfrak{p}) = \mathcal{O}_K/\mathfrak{p}$$

est un corps fini et le noyau $\mathfrak{p} \cap \mathbf{Z}$ du morphisme canonique $\mathbf{Z} \to \mathcal{O}_K/\mathfrak{p}$ est un idéal premier non nul de $\mathbf{Z}$; il existe donc un unique nombre premier p tel que $p \in \mathfrak{p}$, c'est-à-dire tel que $\mathfrak{p}|p$. Avec ces notations, il vient

$$\mathrm{N}(\mathfrak{p}) = p^{[\kappa(\mathfrak{p}):\mathbf{F}_p]}.$$

On appelle *degré résiduel* de $\mathfrak{p}$ l'entier

$$f(\mathfrak{p}/p) = [\kappa(\mathfrak{p}) : \mathbf{F}_p].$$

On appelle *indice de ramification* de $\mathfrak{p}$ l'entier

$$e(\mathfrak{p}/p) = v_{\mathfrak{p}}\left(p\mathcal{O}_K\right)$$

c'est-à-dire la plus grande puissance de $\mathfrak{p}$ qui divise p. On dit que p est *ramifié* dans K s'il existe $\mathfrak{p}$ tel que $e(\mathfrak{p}/p) \geqslant 2$.

Proposition 2.11 — *Soit K un corps de nombres.*

(i) *Pour tout nombre premier p,*

$$\sum_{\mathfrak{p}|p} e(\mathfrak{p}/p) f(\mathfrak{p}/p) = [K : \mathbf{Q}].$$

(ii) *Il n'y a qu'un nombre fini d'idéaux de $\mathcal{O}_K$ de norme bornée.*

Démonstration. (i) Écrivons

$$p\mathcal{O}_K = \prod_{\mathfrak{p}|p} \mathfrak{p}^{v_{\mathfrak{p}}(p)} = \prod_{\mathfrak{p}|p} \mathfrak{p}^{e(\mathfrak{p}/p)}.$$

Par multiplicativité de la norme, il vient

$$p^{[K:\mathbf{Q}]} = \mathrm{N}_{K/\mathbf{Q}}(p) = \mathrm{N}(p\mathcal{O}_K) = \prod_{\mathfrak{p}|p} \mathrm{N}(\mathfrak{p})^{e(\mathfrak{p}/p)} = \prod_{\mathfrak{p}|p} p^{f(\mathfrak{p}/p)e(\mathfrak{p}/p)} = p^{\sum_{\mathfrak{p}|p} e(\mathfrak{p}/p)f(\mathfrak{p}/p)}$$

et donc l'égalité annoncée.

(ii) Soit $C > 0$ un nombre réel et soit $\mathfrak{a} \in \mathrm{I}^+(\mathcal{O}_K)$ un idéal tel que $\mathrm{N}(\mathfrak{a}) \leqslant C$. Si $\mathfrak{a} = \mathfrak{p}_1^{m_1} \cdots \mathfrak{p}_r^{m_r}$ est la factorisation de $\mathfrak{a}$ en produit d'idéaux premiers, alors $\mathrm{N}(\mathfrak{a}) = \mathrm{N}(\mathfrak{p}_1)^{m_1} \cdots \mathrm{N}(\mathfrak{p}_r)^{m_r}$ et donc

– chaque $\mathfrak{p}_i$ divise un nombre premier p majoré par C ;
– chaque exposant m_i est majoré par $C/\log 2$.
Il n'y a ainsi qu'un nombre fini de possibilités pour $\mathfrak{a}$. □

Pour presque tout nombre premier p, la factorisation de $p\mathcal{O}_K$ en produit d'idéaux premiers se ramène à la factorisation d'un polynôme dans $\mathbf{F}_p[T]$.

Proposition 2.12. — *Soit K un corps de nombres. Soit $\alpha \in \mathcal{O}_K$ un élément tel que $K = \mathbf{Q}(\alpha)$ et soit $f \in \mathbf{Z}[T]$ son polynôme minimal. Soit p un nombre premier ne divisant pas $(\mathcal{O}_K : \mathbf{Z}[\alpha])$. Supposons que f se factorise dans $\mathbf{F}_p[T]$ sous la forme*

$$f = h_1^{e_1} \cdots h_r^{e_r}$$

avec $h_1, \ldots, h_r \in \mathbf{F}_p[T]$ irréductibles et distincts, et considérons des relèvements unitaires $g_1, \ldots, g_r$ de $h_1, \ldots, h_r$ dans $\mathbf{Z}[T]$.

Dans cette situation,

(i) *les idéaux $\mathfrak{p}_i = (p, g_i(\alpha))$ sont premiers entre eux et distincts ;*
(ii) *$e(\mathfrak{p}_i/p) = e_i$ et $f(\mathfrak{p}_i/p) = \deg h_i$ pour tout $i \in \{1, \ldots, r\}$;*
(iii) *$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$.*

Démonstration. Considérons le diagramme commutatif de $\mathbf{Z}$-modules

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbf{Z}[\alpha] & \longrightarrow & \mathcal{O}_K & \longrightarrow & \mathcal{O}_K/\mathbf{Z}[\alpha] & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle p} & & \downarrow{\scriptstyle p} & & \downarrow{\scriptstyle p} & & \\ 0 & \longrightarrow & \mathbf{Z}[\alpha] & \longrightarrow & \mathcal{O}_K & \longrightarrow & \mathcal{O}_K/\mathbf{Z}[\alpha] & \longrightarrow & 0 \end{array}$$

Les lignes sont exactes, donc on obtient (par le lemme du serpent) une suite exacte longue

$$0 \longrightarrow \ker \varphi \longrightarrow \mathbf{Z}[\alpha]/p\mathbf{Z}[\alpha] \longrightarrow \mathcal{O}_K/p\mathcal{O}_K \longrightarrow \operatorname{coker} \varphi \longrightarrow 0$$

où φ désigne la multiplication par p dans le groupe $\mathcal{O}_K/\mathbf{Z}[\alpha]$. Il s'agit d'un isomorphisme en vertu de l'hypothèse $p \nmid (\mathcal{O}_K : \mathbf{Z}[\alpha])$, donc

$$\mathbf{Z}[\alpha]/p\mathbf{Z}[\alpha] \simeq \mathcal{O}_K/p\mathcal{O}_K.$$

On en déduit des isomorphismes

$$\mathcal{O}_K/(p, g_i(\alpha)) \simeq \mathbf{Z}[\alpha]/(p, g_i(\alpha)) \simeq \mathbf{Z}[T]/(p, g_i) \simeq \mathbf{F}_p[T]/(h_i)$$

et $\mathfrak{p}_i = (p, g_i(\alpha))$ est ainsi un idéal premier de $\mathcal{O}_K$ tel que

$$\mathrm{N}(\mathfrak{p}_i) = p^{\deg\, h_i}.$$

Ces idéaux premiers sont deux à deux distincts puisque les polyômes h_i sont premiers entre eux.

Nous maintenant écrire

$$\prod_i \mathfrak{p}_i^{e_i} = \prod_i (p, g_i(\alpha))^{e_i} \subset \prod_i (p, g_i(\alpha)^{e_i}) \subset p\mathcal{O}_K$$

en vertu de l'identité

$$\prod_i g_i(\alpha)^{e_i} \equiv f(\alpha) \equiv 0 \pmod{p}.$$

Comme

$$\mathrm{N}\left(\prod_i \mathfrak{p}_i^{e_i}\right) = \prod_i \mathrm{N}(\mathfrak{p}_i)^{e_i} = p^{\sum_i e_i \deg\, h_i} = p^{\deg\, f} = p^{[K/\mathbf{Q}]} = \mathrm{N}(p\mathcal{O}_K),$$

l'inclusion précédente est une égalité et donc

$$p\mathcal{O}_K = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i}, \quad e(\mathfrak{p}_i/p) = e_i.$$

□

Exemple. Considérons $K = \mathbf{Q}(\alpha)$ avec $\alpha^3 - \alpha - 1 = 0$ et donc $f = T^3 - T - 1$. Comme $\Delta(1, \alpha, \alpha^2) = -23$, l'anneau $\mathcal{O}_K$ coïncide avec $\mathbf{Z}[\alpha]$. Un nombre premier p se factorise donc dans $\mathcal{O}_K$ de la même manière que f se factorise modulo p.

- On vérifie immédiatement que le polynôme f est irréductible modulo 2, 3 et 7, donc les idéaux $(2), (3)$ et (7) sont premiers dans $\mathcal{O}_K$.
- La factorisation de f dans $\mathbf{F}_5[T]$ est

  $$f = (T-2)(T^2 + 2T + 2)$$

  donc

  $$(5) = \mathfrak{p}_5\mathfrak{p}_{25}, \quad \text{avec } \mathfrak{p}_5 = (5, \alpha - 2) \text{ et } \mathfrak{p}_{25} = (5, \alpha^2 + 2\alpha + 2)$$

  (la norme de chaque idéal premier figure en indice).
- La factorisation de f dans $\mathbf{F}_{23}[T]$ est

  $$f = (T-10)^2(T-3)$$

  donc

  $$(23) = \mathfrak{p}_{23}^2\mathfrak{p}'_{23} \quad \text{avec } \mathfrak{p}_{23} = (23, \alpha - 10) \text{ et } \mathfrak{p}'_{23} = (23, \alpha - 3).$$

  On observe que 23 est ramifié dans K.
- La factorisation de f dans $\mathbf{F}_{59}[T]$ est

  $$f = (T-4)(T-13)(T+17)$$

  donc

  $$(59) = \mathfrak{p}_{59}\mathfrak{p}'_{59}\mathfrak{p}''_{59}, \quad \text{avec } \mathfrak{p}_{59} = (59, \alpha - 4), \quad \mathfrak{p}'_{59} = (59, \alpha - 13) \text{ et } \mathfrak{p}''_{59} = (59, \alpha + 17).$$

Remarque. La proposition précédente a un intérêt algorithmique car on sait factoriser efficacement les polynômes sur les corps finis (algorithmes de Berlekamp et de Cantor-Zassenhaus ; voir par exemple le *Cours d'algèbre* de Michel Demazure).

La situation est particulièrement claire dans le cas d'une extension d'Eisenstein (cf. Complément A au premier chapitre).

Corollaire 2.13. — *Soit $K = \mathbf{Q}(\alpha)$ un corps de nombres avec $\alpha \in \mathcal{O}_K$ de polynôme minimal f. Si p est un nombre premier tel que f soit d'Eisenstein en p, alors*

$$p\mathcal{O}_K = \mathfrak{p}^n \quad \text{avec } n = [K : \mathbf{Q}] \text{ et } \mathfrak{p} = (p, \alpha).$$

Démonstration. La proposition précédente s'applique car p ne divise pas $(\mathcal{O}_K : \mathbf{Z}[\alpha])$ (Proposition A.2). Comme $f \equiv T^n \pmod{p}$, la conclusion est immédiate. □

Exemple. Considérons le corps cyclotomique $K = \mathbf{Q}(\zeta_{p^m})$. Le polynôme $\Phi_{p^m}(1-T)$ est d'Eisenstein en p, donc le nombre premier p est totalement ramifié dans K et

$$p\mathcal{O}_K = \mathfrak{p}^{\varphi(p^m)} \quad \text{avec} \quad \mathfrak{p} = (p, \zeta_{p^m} - 1).$$

Il découle de l'identité

$$\Phi_{p^m}(1-T) = \Phi_p((1-T)^{p^{m-1}}) = (1-T)^{(p-1)p^{m-1}} + (1-T)^{(p-2)p^{m-1}} + \ldots + 1 = (-T)^{\varphi(p^m)} + \ldots + p$$

que $1 - \zeta_{p^m}$ divise p dans $\mathcal{O}_K$, donc

$$\mathfrak{p} = (1 - \zeta_{p^m}).$$

Nous allons achever cette section en donnant une description remarquable des nombres premiers ramifiés dans un corps de nombres.

Théorème 2.14 (Dedekind) — *Soit K un corps de nombres. Un nombre premier p est ramifié dans K si et seulement si p divise le discriminant D_K. En particulier, il n'existe qu'un nombre fini de nombres premiers ramifiés dans K.*

Démonstration. Notons A la $\mathbf{F}_p$-algèbre $\mathcal{O}_K/p\mathcal{O}_K$ et désignons par $x \mapsto \overline{x}$ la projection canonique de $\mathcal{O}_K$ sur A. Pour tout $x \in \mathcal{O}_K$, la multiplication par x dans $\mathcal{O}_K$ induit par réduction modulo p la multiplication par $\overline{x}$ dans A, donc

$$\mathrm{Tr}_{A/\mathbf{F}_p}(\overline{x}) \equiv \mathrm{Tr}_{\mathcal{O}_K/\mathbf{Z}}(x) \pmod{p}.$$

La forme bilinéaire symétrique

$$b : \mathcal{O}_K \times \mathcal{O}_K \to \mathbf{Z}, \quad (x, y) \mapsto \mathrm{Tr}_{\mathcal{O}_K/\mathbf{Z}}(xy)$$

induit par réduction modulo p la forme bilinéaire symétrique

$$\overline{b} : A \times A \to \mathbf{F}_p, \quad (x, y) \mapsto \mathrm{Tr}_{A/\mathbf{F}_p}(xy).$$

En se souvenant que D_K est le déterminant de la matrice B de b dans une $\mathbf{Z}$-base de $\mathcal{O}_K$ (Définition 1.13), on obtient

$$p | D_K \iff p | \det B \iff \det \overline{B} = 0 \iff \overline{b} \text{ est dégénérée.}$$

Écrivons $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ avec $\mathfrak{p}_i \neq \mathfrak{p}_j$ si $i \neq j$, de sorte que

$$A \simeq \mathcal{O}_K/\mathfrak{p}_1^{e_1} \times \ldots \times \mathfrak{O}_K/\mathfrak{p}_r^{e_r}$$

La forme bilinéaire $\overline{b}$ est la somme directe orthogonale des formes bilinéaires symétriques $(x, y) \mapsto \overline{b}_i(x, y) = \mathrm{Tr}_{A_i/\mathbf{F}_p}(xy)$ avec $A_i = \mathcal{O}_K/\mathfrak{p}_i^{e_i}$, donc elle est dégénérée si et seulement si l'une des formes $\overline{b}_i$ l'est. Ceci est le cas si et seulement si l'un des entiers e_i est strictement supérieur à 1 en vertu du lemme suivant. □

Lemme 2.15. — *Soit k un corps et soit A une k-algèbre de dimension finie. Soit b la forme bilinéaire symétrique*

$$A \times A \to k, \quad (x, y) \mapsto \mathrm{Tr}_{A/k}(xy).$$

(i) *Si A est un corps qui est une extension finie séparable de k, alors la forme bilinéaire b est non dégénérée.*

(ii) *Si A contient un élément nilpotent non nul, alors la forme bilinéaire b est dégénérée.*

Démonstration. (i) Pour tout $x \in A$,

$$\mathrm{Tr}_{A/k}(x) = \sum_{\sigma} \sigma(x)$$

où σ parcourt l'enemble des k-plongements de A dans une clôture algébrique de k. Si $\mathrm{Tr}_{A/k}(xy) = 0$ pour tout $y \in A$, alors

$$\sum_{\sigma} \sigma(x)\sigma = 0$$

dans $\mathrm{End}_k(A)$, donc $\sigma(x) = 0$ pour tout σ en vertu du théorème d'indépendance des caractères et $x = 0$.

(ii) Si $x \in A$ est nilpotent et non nul, alors, pour tout $y \in A$, l'endomorphisme de multiplication par xy dans A est nilpotent et donc $\mathrm{Tr}_{A/k}(xy) = 0$. □

Exemple. Le discriminant du corps cyclotomique $\mathbf{Q}(\zeta_n)$ a les mêmes diviseurs premiers que n, donc un nombre premier p est ramifié dans $\mathbf{Q}(\zeta_n)$ si et seulement si $p|n$.

2.3 Factorisation dans une extension galoisienne

Convention. Étant donné un corps de nombres K et un idéal premier non nul $\mathfrak{p}$ de $\mathcal{O}_K$, posons

$$\kappa(\mathfrak{p}) = \mathcal{O}_K/\mathfrak{p}.$$

Soit L/K une extension galoisienne de corps de nombres, de groupe de Galois G. L'action de G sur L préserve $\mathcal{O}_L$ et induit donc une action de G sur l'ensemble P_L des idéaux premiers non nuls de $\mathcal{O}_L$: si $\mathfrak{P} \in P_L$, tout $\sigma \in G$ induit un isomorphisme d'anneaux

$$\mathcal{O}_L/\mathfrak{P} \xrightarrow{\sim} \mathcal{O}_L/\sigma(\mathfrak{P})$$

et donc $\sigma(\mathfrak{P}) \in P_L$.

Si $\mathfrak{p}$ est un idéal premier non nul de $\mathcal{O}_K$, alors la factorisation de l'idéal non nul $\mathfrak{p}\mathcal{O}_L$ s'écrit sous la forme

$$\mathfrak{p}\mathcal{O}_L = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e(\mathfrak{P}/\mathfrak{p})}$$

avec $e(\mathfrak{P}/\mathfrak{p}) \in \mathbf{N}$. On pose par ailleurs

$$f(\mathfrak{P}/\mathfrak{p}) = [\kappa(\mathfrak{P}) : \kappa(\mathfrak{p})].$$

Proposition 2.16 — (i) *Le groupe G opère transitivement sur l'ensemble des diviseurs premiers de $\mathfrak{p}$ dans $\mathcal{O}_L$.*

(ii) *Les entiers $e(\mathfrak{P}/\mathfrak{p})$ et $f(\mathfrak{P}/\mathfrak{p})$ ne dépendent pas du diviseur premier $\mathfrak{P}$ de $\mathfrak{p}$ dans $\mathcal{O}_L$. Notant respectivement e et f leurs valeurs et en désignant par g le nombre de diviseurs premiers distincts de $\mathfrak{p}$ dans $\mathcal{O}_L$, il vient*

$$efg = [L : K].$$

Démonstration. (i) Notons $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ les diviseurs premiers de $\mathfrak{p}$ dans $\mathcal{O}_L$ et choisissons $x \in \mathcal{O}_L$ tel que $x \in \mathfrak{P}_1$ et $x \notin \mathfrak{P}_2 \cdots \mathfrak{P}_g$; ceci est possible car les idéaux $\mathfrak{P}_1$ et $\mathfrak{P}_2 \cdots \mathfrak{P}_g$ sont premiers entre eux. Fixons un entier i entre 1 et g. Comme

$$\prod_{\sigma \in G} \sigma(x) \in \mathfrak{P}_1 \cap \mathcal{O}_K = \mathfrak{p} \subset \mathfrak{P}_i,$$

l'idéal premier $\mathfrak{P}_i$ contient l'un des conjugués $\sigma(x)$ de x. Pour un tel choix de σ, $\sigma(\mathfrak{P}_1) \cap \mathfrak{P}_i \neq 0$ et donc $\mathfrak{P}_i = \sigma(\mathfrak{P}_1)$.

(ii) La première assertion est une conséquence immédiate du point (i) et de l'unicité de la factorisation de l'idéal $\mathfrak{p}\mathcal{O}_L$ en produit d'éléments de P_L. Pour établir la seconde, on utilise l'isomorphisme de $\mathcal{O}_K/\mathfrak{p}$-espaces vectoriels

$$\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \simeq \bigoplus_{i=1}^{g} \mathcal{O}_L/\mathfrak{P}_i^{e_i}$$

donné par le théorème chinois des restes et l'on examine les cardinaux :

$$\mathrm{Card}\,(\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L) = \mathrm{N}_{L/\mathbf{Q}}(\mathfrak{p}\mathcal{O}_L) = \mathrm{N}_{K/\mathbf{Q}}(\mathfrak{p})^{[L:K]} = p^{[\kappa(\mathfrak{p}):\mathbf{F}_p][L:K]}$$

et

$$\mathrm{Card}\left(\bigoplus_{i=1}^{g} \mathcal{O}_L/\mathfrak{P}_i^{e_i}\right) = \prod_{i=1}^{g} \mathrm{N}_{L/\mathbf{Q}}(\mathfrak{P}_i)^{e_i} = p^{[\kappa(\mathfrak{P}_i):\mathbf{F}_p]e_i} = \prod_{i=1}^{g} p^{e_i f_i [\kappa(\mathfrak{p}):\mathbf{F}_p]} = p^{efg[\kappa(\mathfrak{p}):\mathbf{F}_p]}$$

donc

$$[L:K] = efg.$$

□

Soit $\mathfrak{P} \in P_L$ et $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$. Le sous-groupe

$$D(\mathfrak{P}/\mathfrak{p}) = \{\sigma \in G \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}$$

est appelé le *groupe de décomposition* de $\mathfrak{P}$. D'après la proposition précédente, les groupes de décomposition des différents diviseurs premiers divisant un même $\mathfrak{p} \in P_K$ sont tous conjugués. Tout élément σ de $D(\mathfrak{P}/\mathfrak{p})$ induit un automorphisme du corps $\kappa(\mathfrak{P})$ fixant le sous-corps $\kappa(\mathfrak{p})$; nous obtenons-donc un morphisme de groupes

$$\varphi_{\mathfrak{P}} : D(\mathfrak{P}/\mathfrak{p}) \to \mathrm{Gal}(\kappa(\mathfrak{P})|\kappa(\mathfrak{p})).$$

Son noyau

$$I(\mathfrak{P}/\mathfrak{p}) = \{\sigma \in G \mid \sigma(x) \equiv x \pmod{\mathfrak{P}} \text{ pour tout } x \in \mathcal{O}_L\}$$

est appelé le *sous-groupe d'inertie* de $\mathfrak{P}$.

Proposition 2.17 — (i) *Le morphisme $\varphi_{\mathfrak{P}}$ est surjectif.*

(ii) *On a*

$$\mathrm{Card}\ D(\mathfrak{P}/\mathfrak{p}) = e(\mathfrak{P}/\mathfrak{p})f(\mathfrak{P}/\mathfrak{p}) \quad \text{et} \quad \mathrm{Card}\ I(\mathfrak{P}/\mathfrak{p}) = e(\mathfrak{P}/\mathfrak{p}).$$

Démonstration. (i) Soit $a \in \kappa(\mathfrak{P})$ un élément primitif sur $\kappa(\mathfrak{p})$, de polynôme minimal $g \in \kappa(\mathfrak{p})[T]$. L'isomorphisme d'anneaux

$$\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \simeq \bigoplus_{\mathfrak{Q}|\mathfrak{p}} \mathcal{O}_L/\mathfrak{Q}^e$$

donné par le théorème chinois des restes nous permet de choisir un élément α de $\mathcal{O}_L$ tel que

$$\alpha \equiv a \pmod{\mathfrak{P}} \quad \text{et} \quad \alpha \in \prod_{\substack{\mathfrak{Q}|\mathfrak{p} \\ \mathfrak{Q} \neq \mathfrak{P}}} \mathfrak{Q}.$$

Si $f \in \mathcal{O}_K[T]$ est le polynôme minimal de α sur K, alors g divise f dans $\kappa(\mathfrak{p})[T]$. Considérons maintenant un élément τ de $\mathrm{Gal}(\kappa(\mathfrak{P})|\kappa(\mathfrak{p}))$. L'image de a est une racine de g, donc il existe une racine β de f dans $\mathcal{O}_L$ telle que $\beta \equiv \tau(a) \pmod{\mathfrak{P}}$ [3]. Le groupe G agit transitivement sur les racines de f dans L, donc il existe $\sigma \in G$ tel que $\beta = \sigma(\alpha)$. Notons que β n'appartient pas à $\mathfrak{P}$ puisque $\tau(a) \neq 0$. Par construction, $\sigma(\mathfrak{P})$ est l'unique idéal premier de $\mathcal{O}_L$ divisant $\mathfrak{p}$ et ne contenant pas $\sigma(\alpha)$, donc $\sigma(\mathfrak{P}) = \mathfrak{P}$. Au final, nous avons exhibé un élément σ de G tel que $\sigma \in D(\mathfrak{P}/\mathfrak{p})$ et $\varphi_{\mathfrak{P}}(\sigma) = \tau$.

(ii) Il s'agit d'une conséquence immédiate de (i) puisque

$$\mathrm{Card}\ \mathrm{Gal}(\kappa(\mathfrak{P})|\kappa(\mathfrak{p})) = [\kappa(\mathfrak{P}) : \kappa(\mathfrak{p})] = f(\mathfrak{P}/\mathfrak{p}).$$

□

Considérons maintenant un sous-corps K' de L contenant K. Chaque $\mathfrak{P} \in P_L$ détermine un idéal premier non nul $\mathfrak{P}_{K'} = \mathfrak{P} \cap \mathcal{O}_{K'}$ de $\mathcal{O}_{K'}$ et, en posant $\mathfrak{p} = \mathfrak{P}_K$, nous avons

$$\begin{cases} e(\mathfrak{P}/\mathfrak{p}) = e(\mathfrak{P}/\mathfrak{P}_{K'}) \cdot e(\mathfrak{P}_{K'}/\mathfrak{p}) \\ f(\mathfrak{P}/\mathfrak{p}) = f(\mathfrak{P}/\mathfrak{P}_{K'}) \cdot f(\mathfrak{P}_{K'}/\mathfrak{p}) \end{cases}$$

ainsi que

$$\begin{cases} D(\mathfrak{P}/\mathfrak{P}_{K'}) = D(\mathfrak{P}/\mathfrak{p}) \cap \mathrm{Gal}(L|K') \\ I(\mathfrak{P}/\mathfrak{P}_{K'}) = I(\mathfrak{P}/\mathfrak{p}) \cap \mathrm{Gal}(L|K') \end{cases}$$

Proposition 2.18 — *Avec les notations ci-dessus,*

(i) $\mathfrak{p}$ *est non ramifié en* $\mathfrak{P}_{K'} \iff I(\mathfrak{P}/\mathfrak{p}) \subset \mathrm{Gal}(L|K')$

(ii) $\mathfrak{p}$ *est décomposé en* $\mathfrak{P}_{K'} \iff D(\mathfrak{P}/\mathfrak{p}) \subset \mathrm{Gal}(L|K')$.

Démonstration. (i) $\mathfrak{p}$ est non ramifié en $\mathfrak{P}_{K'}$ si et seulement si

$$\begin{aligned} e(\mathfrak{P}_{K'}/\mathfrak{p}) = 1 &\iff e(\mathfrak{P}/\mathfrak{p}) = e(\mathfrak{P}/\mathfrak{P}_{K'}) \\ &\iff I(\mathfrak{P}/\mathfrak{p}) = I(\mathfrak{P}/\mathfrak{P}_{K'}) \\ &\iff I(\mathfrak{P}/\mathfrak{p}) \subset \mathrm{Gal}(L/K') \end{aligned}$$

(ii) $\mathfrak{p}$ est décomposé en $\mathfrak{P}_{K'}$ si et seulement si

$$\begin{aligned} e(\mathfrak{P}_{K'}/\mathfrak{p})f(\mathfrak{P}_{K'}/\mathfrak{p}) = 1 &\iff e(\mathfrak{P}/\mathfrak{p})f(\mathfrak{P}/\mathfrak{P}_{K'}) = e(\mathfrak{P}/\mathfrak{P}_{K'})f(\mathfrak{P}/\mathfrak{P}_{K'}) \\ &\iff D(\mathfrak{P}/\mathfrak{p}) = D(\mathfrak{P}/\mathfrak{P}_{K'}) \\ &\iff D(\mathfrak{P}/\mathfrak{p}) \subset \mathrm{Gal}(L/K') \end{aligned}$$

□

Corollaire 2.19 — *Soit F un corps de nombres et soient K_1, K_2 deux sous-corps tels que $F = K_1K_2$. Soit p un nombre premier.*

(i) *p est non ramifié dans F si et seulement si p est non ramifié dans K_1 et dans K_2.*

3. Observer que f est scindé sur L puisque l'extension L/K est galoisienne

(ii) *p est totalement décomposé dans F si et seulement si p est totalement décomposé dans K_1 et dans K_2.*

Démonstration. Il s'agit d'une conséquence immédiate de la proposition précédente en considérant une extension galoisienne $L/\mathbf{Q}$ contenant F et en utilisant l'identité

$$\mathrm{Gal}(L/F) = \mathrm{Gal}(L/K_1) \cap \mathrm{Gal}(L/K_2).$$

□

Soit L/K une extension finie galoisienne de corps de nombres de soit $\mathfrak{p} \in P_K$ non ramifié dans $\mathcal{O}_L$. Pour chaque $\mathfrak{P} \in P_L$ divisant $\mathfrak{p}$, il découle de la proposition 2.17 que l'application canonique

$$\mathrm{D}(\mathfrak{P}/\mathfrak{p}) \to \mathrm{Gal}(\kappa(\mathfrak{P})|\kappa(\mathfrak{p}))$$

est un isomorphisme. Le groupe de droite étant cyclique, engendré par l'automorphisme de Frobenius

$$\mathrm{Frob}_p^{N(\mathfrak{p})} : \kappa(\mathfrak{P}) \to \kappa(\mathfrak{P}), \quad x \mapsto x^{N(\mathfrak{p})},$$

il existe donc un unique élément σ dans $\mathrm{D}(\mathfrak{P}/\mathfrak{p})$ tel que

$$\sigma(x) \equiv x^{N(\mathfrak{p})} \pmod{\mathfrak{P}}$$

pour tout $x \in \mathcal{O}_L$; on le note $(\mathfrak{P}, L/K)$ et on l'appelle l'*élément de Frobenius* en $\mathfrak{P}$.

Pour tout $\tau \in \mathrm{Gal}(L/K)$,

$$(\tau(\mathfrak{P}, L/K) = \tau(\mathfrak{P}, L/K)\tau^{-1}$$

donc les éléments de Frobenius associés aux différents diviseurs premiers de $\mathfrak{p}$ dans $\mathcal{O}_L$ constituent une classe de conjugaison dans $\mathrm{Gal}(L|K)$. Si ce groupe est *abélien*, alors tous les éléments de Frobenius associés à $\mathfrak{p}$ sont égaux et notés $(\mathfrak{p}, L/K)$.

Proposition 2.20 — *Soit $n \geqslant 1$ un nombre entier et soit*

$$\chi : \mathrm{Gal}(\mathbf{Q}(\zeta_n)|\mathbf{Q}) \xrightarrow{\sim} (\mathbf{Z}/n\mathbf{Z})^\times$$

l'isomorphisme défini par l'identité $\sigma(\zeta_n) = \zeta_n^{\chi(\sigma)}$ pour tout $\sigma \in \mathrm{Gal}(\mathbf{Q}(\zeta_n)|\mathbf{Q})$. Considérons un nombre premier p et écrivons $n = p^a m$ avec $a = v_p(n)$ et $p \nmid m$.

(i) *Si $p|n$, alors p est ramifié dans $\mathbf{Q}(\zeta_n)$. Chaque diviseur premier de p a pour indice de ramification $e = p^{a-1}(p-1)$ et pour degré résiduel l'ordre de p dans $(\mathbf{Z}/m\mathbf{Z})^\times$.*

(ii) Si $p \nmid n$, alors p est non ramifié dans $\mathbf{Q}(\zeta_n)$ et

$$\chi\left((p, \mathbf{Q}(\zeta_n)/\mathbf{Q})\right) = p.$$

(iii) *Si $p \nmid n$, alors $p\mathcal{O}_{\mathbf{Q}(\zeta_n)} = \mathfrak{P}_1 \cdots \mathfrak{P}_g$ avec*

$$f(\mathfrak{P}_i/p) = \text{ordre de } p \text{ dans } (\mathbf{Z}/n\mathbf{Z})^\times \quad \text{et} \quad g = \varphi(n)/f.$$

Démonstration. Observons tout d'abord que la proposition 2.12 permet d'expliciter la factorisation de tout nombre premier p dans $\mathcal{O}_{\mathbf{Q}(\zeta_n)} = \mathbf{Z}[\zeta_n]$ (Proposition 1.21) : si $\Phi_n = h_1^{e_1} \cdots h_g^{e_g}$ est la factorisation en produit d'irréductibles de Φ_n dans $\mathbf{F}_p[T]$, alors

$$p\mathcal{O}_{\mathbf{Q}(\zeta_n)} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$$

avec $\mathfrak{P}_i = (p, f_i(\zeta_n))$, où $f_1, \ldots, f_g \in \mathbf{Z}[T]$ sont des relèvements unitaires de $h_1, \ldots, h_g$.

(i) Les diviseurs premiers du discriminant de $\mathbf{Q}(\zeta_n)$ sont ceux de n (Proposition 1.21), donc un nombre premier p est ramifié dans $\mathbf{Q}(\zeta_n)$ si et seulement si $p|n$ en vertu du théorème 2.14. Dans ce cas, on déduit du lemme 1.17 la factorisation

$$\Phi_n = \frac{\Phi_m(T^{p^a})}{\Phi_m(T^{p^{a-1}})} = \Phi_m(T)^{p^{a-1}(p-1)}$$

dans $\mathbf{F}_p[T]$ et Φ_m n'a que des facteurs simples puisque $p \nmid m$.. Ceci fournit l'indice de ramification $e = p^{a-1}(p-1)$, et le calcul du degré résiduel découle du point (iii) ci-dessous.

(ii) Posons $\sigma = (p, \mathbf{Q}(\zeta_n)/\mathbf{Q})$ et choisissons un diviseur premier $\mathfrak{P}$ de p dans $\mathcal{O}_{\mathbf{Q}(\zeta_n)}$. On a

$$\zeta_n^{\chi(\sigma)} = \sigma(\zeta_n) = \zeta_n^p \pmod{\mathfrak{P}}$$

donc $\zeta_n^{\chi(\sigma)}$ et ζ_n^p sont deux racines de Φ_n ayant la même réduction modulo $\mathfrak{P}$. Comme le polynôme Φ_n est séparable modulo p puisque $p \nmid n$, ses racines dans $\kappa(\mathfrak{P})$ sont simples et donc $\zeta_n^{\chi(\sigma)} = \zeta_n^p$ dans $\mathbf{Q}(\zeta_n)$, c'est-à-dire $\chi(\sigma) = p$ dans $(\mathbf{Z}/n\mathbf{Z})^\times$.

(iii) Pour tout diviseur premier $\mathfrak{P}$ de p dans $\mathcal{O}_{\mathbf{Q}(\zeta_n)}$,

$$f(\mathfrak{P}/p) = \text{Card } D(\mathfrak{P}/p) = \text{ord}\left((p, \mathbf{Q}(\zeta_n)/\mathbf{Q})\right) = \text{ord}\left(\chi(p, \mathbf{Q}(\zeta_n)/\mathbf{Q})\right) = \text{ord}(p).$$

□

2.4 La loi de réciprocité quadratique

Soit K un corps de nombres quadratique, donc de la forme $K = \mathbf{Q}(\sqrt{d})$ avec d un entier sans facteur carré distinct de 1 et uniquement déterminé par K. On sait que l'anneau $\mathcal{O}_K$ est engendré par $\tau = \sqrt{d}$, de polynôme minimal $T^2 - d$, si $d \equiv 2, 3 \pmod 4$ et par $\tau = \frac{1+\sqrt{d}}{2}$, de polynôme minimal $f = T^2 - T + \frac{1-d}{4}$, si $d \equiv 1 \pmod 4$. Le discriminant de K coïncide avec celui de f et

$$D_K = \begin{cases} 4d & \text{si } d \equiv 2, 3 \pmod 4 \\ d & \text{si } d \equiv 1 \pmod 4. \end{cases}$$

D'après la proposition 2.12, la factorisation d'un nombre premier p dans $\mathcal{O}_K$ reflète celle de f dans $\mathbf{F}_p[T]$.

(Cas $p = 2$)

(i) Si $d \equiv 2, 3 \pmod 4$, alors $f = (T - d)^2$ dans $\mathbf{F}_2[T]$ et donc 2 est totalement ramifié dans $\mathcal{O}_K$:

$$2\mathcal{O}_K = (2, \tau - d)^2.$$

(ii) Si $d \equiv 1 \pmod 8$, alors $f = T(T-1)$ dans $\mathbf{F}_2[T]$ et donc 2 est totalement décomposé dans $\mathcal{O}_K$:

$$2\mathcal{O}_K = (2, \tau) \cdot (2, \tau - 1).$$

(iii) Si $d \equiv 5 \pmod 8$, alors $f = T^2 - T - 1$ est irréductible dans $\mathbf{F}_2[T]$ et donc 2 est inerte dans $\mathcal{O}_K$.

(Cas $p \geqslant 3$)

En écrivant $f = T^2 - \frac{D_K}{4}$ (resp. $f = \left(T - \frac{1}{2}\right)^2 - \frac{D_K}{4}$) dans $\mathbf{F}_p[T]$ si $d \equiv 2, 3 \pmod 4$ (resp. $d \equiv 1 \pmod 4$), il vient :

(i) p est ramifié dans K si et seulement si $D_K \equiv 0 \pmod{p}$;

(ii) p est totalement décomposé dans K si et seulement si D_K est un carré non nul modulo p ;

(iii) p est inerte dans K si et seulement si D_K n'est pas un carré modulo p.

Nous sommes ainsi confrontés à deux problèmes symétriques naturels : déterminer les entiers qui sont des carrés modulo un nombre premier donné, et déterminer les nombres premiers modulo lesquels un entier donné est un carré.

Dans tout ce qui suit, p désigne un nombre premier différent de 2. Pour $a \in \mathbf{Z}$, on pose

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } a \text{ est un carré non nul modulo } p \\ 0 & \text{si } p|a \\ -1 & \text{si } a \text{ n'est pas un carré modulo } p \end{cases}$$

L'application $\left(\frac{\cdot}{\cdot}\right) : \mathbf{Z} \to \{-1, 0, 1\}$ ainsi définie est évidemment p-périodique ; on l'appelle le *symbole de Legendre*.

Proposition 2.21 — (i) *Pour tout $a \in \mathbf{Z}$,*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

(ii) *Le symbole de Legendre induit un morphisme de groupes $\mathbf{F}_p^\times \to \{-1, 1\}$.*

Démonstration. (i) Le morphisme de groupes $\mathbf{F}_p^\times \to \mathbf{F}_p^\times, x \mapsto x^2$ a pour noyau le sous-groupe $\{-1, 1\}$ qui est d'ordre 2, donc son image $\mathbf{F}_p^{\times,2}$ est d'ordre $\frac{p-1}{2}$; il y a ainsi $\frac{p-1}{2}$ carrés dans $\mathbf{F}_p^\times$. Considérons maintenant le morphisme de groupes $g : \mathbf{F}_p^\times \to \mathbf{F}_p^\times, x \mapsto x^{\frac{p-1}{2}}$. Comme $g(x)^2 = x^{p-1} = 1$ pour tout x, l'image de g est contenue dans $\{-1, 1\}$ et $\ker(g)$ contient $\mathbf{F}_p^{\times,2}$. Ce morphisme étant non trivial, on en déduit $\ker(g) = \mathbf{F}_p^{\times,2}$ et donc

$$g(x) = \left(\frac{x}{p}\right)$$

pour tout $x \in \mathbf{F}_p^\times$. □

Remarque — *Soit q un nombre premier distinct de p. Le groupe de Galois $\mathrm{Gal}(\mathbf{Q}(\sqrt{q})|\mathbf{Q})$ est canoniquement isomorphe à $\{-1, 1\}$ via l'application $\sigma \mapsto \frac{\sigma(\sqrt{d})}{\sqrt{d}}$. Puisqu'il ne divise pas $2q$, le nombre premier p n'est pas ramifié dans $\mathbf{Q}(\sqrt{q})$ et il détermine donc un élément de Frobenius $(p, \mathbf{Q}(\sqrt{q})/\mathbf{Q})$ dans $\mathrm{Gal}(\mathbf{Q}(\sqrt{q})|\mathbf{Q})$. Si $\mathfrak{P}$ est un diviseur premier de p dans $\mathcal{O}_{\mathbf{Q}(\sqrt{q})}$, alors*

$$\sqrt{q}^p = \sqrt{q} \text{ dans } \kappa(\mathfrak{P}) \quad \Longleftrightarrow \quad \sqrt{q} \in \mathbf{F}_p \quad \Longleftrightarrow \quad q \in \mathbf{F}_p^{\times,2}$$

donc

$$\frac{(p, \mathbf{Q}(\sqrt{q})/\mathbf{Q})(\sqrt{d})}{\sqrt{d}} = \left(\frac{q}{p}\right).$$

Autrement dit, l'isomorphisme ci-dessus identifie $(p, \mathbf{Q}(\sqrt{q})/\mathbf{Q})$ et $\left(\frac{q}{p}\right)$.

Théorème 2.22 (Loi de réciprocité quadratique, Gauss) — *Soient p et q deux nombres premiers impairs distincts.*

(i) $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$

(ii) $\left(\frac{-1}{p}\right) = (-1)^{\frac{(p-1)}{2}}$ *(Première loi complémentaire)*

(iii) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ *(Seconde loi complémentaire)*

On peut donner une reformulation plus concrète de cet énoncé de la manière suivante.

Corollaire 2.23 — (i) *Si p et q sont deux nombres premiers impairs distincts, alors :*

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) & \text{si } p \equiv 1 \pmod 4 \text{ ou } q \equiv 1 \pmod 4 \\ -\left(\frac{q}{p}\right) & \text{si } p, q \equiv 3 \pmod 4. \end{cases}$$

(ii) *Si p est premier et impair, alors :*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{si } p \equiv 1 \pmod 4 \\ -1 & \text{si } p \equiv 3 \pmod 4 \end{cases}$$

(iii) *Si p est premier et impair, alors :*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{si } p \equiv \pm 1 \pmod 8 \\ -1 & \text{si } p \equiv \pm 3 \pmod 8 \end{cases}$$

Démonstration du théorème 2.22. Le point (ii) est connu par la proposition 2.21.
(i) et (iii). Fixons deux nombres premiers p et q distincts avec $p \neq 2$ (mais on n'exclut pas $q = 2$). Considérons le corps de nombres $L = \mathbf{Q}(\zeta_p)$, qui est une extension galoisienne de $\mathbf{Q}$ de groupe de Galois G isomorphe à $(\mathbf{Z}/p\mathbf{Z})^\times = \mathbf{F}_p^\times$ via l'application χ définie par $\sigma(\zeta_p) = \zeta_p^{\chi(\sigma)}$. Le groupe G est cyclique d'ordre $p-1$ et $H = \chi^{-1}(\mathbf{F}_p^{\times,2})$ est son unique sous-groupe d'indice 2 ; par la théorie de Galois, $K = L^H$ est l'unique sous-corps quadratique contenu dans L. Le discriminant de L étant une puissance de p (Proposition 1.20), p est l'unique nombre premier ramifié dans L en vertu du théorème 2.14 et donc p est également l'unique nombre premier pouvant se ramifier dans K. Toujours en vertu du théorème 2.14, on en déduit que $|D_K|$ est une puissance de p, puis que l'on a

$$D_K = \begin{cases} p & \text{si } p \equiv 1 \pmod 4 \\ -p & \text{si } p \equiv 3 \pmod 4 \end{cases}$$

compte-tenu de la forme des discriminants quadratiques. Nous avons ainsi déterminé explicitement le corps K :

$$D_K = p^* = \left(\frac{-1}{p}\right) p \text{ et donc } K = \mathbf{Q}(\sqrt{p^*}).$$

Le nombre premier q est non ramifié dans K. En utilisant les proposition 2.18 et 2.20,

$$\begin{aligned} q \text{ est totalement décomposé dans } K &\iff (q, (p, \mathbf{Q}(\zeta_p)/\mathbf{Q}) \in \mathrm{Gal}(\mathbf{Q}(\zeta_p)/K) \\ &\iff q \in \mathbf{F}_p^{\times,2} \\ &\iff \left(\frac{q}{p}\right) = 1. \end{aligned}$$

Comme $p^* \equiv 1 \pmod 4$, on a $\mathcal{O}_K = \mathbf{Z}[\tau]$ avec τ de polynôme minimal $f = T^2 - T + \frac{1-p^*}{4}$ et donc q est totalement décomposé dans K si et seulement si f est scindé sur $\mathbf{F}_q$.

Supposons $q \neq 2$. On a $\mathrm{disc}(f) = p^*$, donc f est scindé sur $\mathbf{F}_q$ si et seulement si p^* est un carré dans $\mathbf{F}_q$, i.e. si et seulement si $\left(\frac{p^*}{q}\right) = 1$. On déduit de cette étude le point (i) :

$$\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right) = \left(\frac{-1}{q}\right)^{\frac{p-1}{2}} \left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{p}{q}\right).$$

Supposons maintenant $q = 2$. Le polynôme f est scindé sur $\mathbf{F}_2$ si et seulement si $\frac{p^*-1}{4} \equiv 0 \pmod 2$, donc si et seulement si $p^* \equiv 1 \pmod 8$. Cette condition équivaut à

$$p \equiv \pm 1 \pmod 8,$$

donc

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

□

Remarques — (i) Il est possible d'expliciter une racine carrée de p^* dans $\mathbf{Q}(\zeta_p)$. Posons

$$g = \sum_{a \in \mathbf{F}_p} \zeta_p^{a^2} = 1 + 2 \sum_{a \in \mathbf{F}_p^{\times,2}} \zeta_p^a = 1 + \sum_{a \in \mathbf{F}_p^{\times,2}} \left(1 + \left(\frac{a}{p}\right)\right) \zeta_p^a = \sum_{a \in \mathbf{F}_p^\times} \left(\frac{a}{p}\right) \zeta_p^a.$$

Il vient

$$g^2 = \sum_{a,b \in \mathbf{F}_p^\times} \left(\frac{ab}{p}\right) \zeta_p^{a+b} = \sum_{a,c \in \mathbf{F}_p^\times} \left(\frac{c}{p}\right) \zeta_p^{a(1+c)} = \left(\frac{-1}{p}\right)(p-1) + \sum_{c \in \mathbf{F}_p \setminus \{0,-1\}} (-1) \left(\frac{c}{p}\right)$$

donc, en observant qu'il y a autant de carrés que de non-carrés dans $\mathbf{F}_p^\times$,

$$g^2 = \left(\frac{-1}{p}\right)(p-1) + \left(\frac{-1}{p}\right) = \left(\frac{-1}{p}\right) p = p^*.$$

(ii) On peut exploiter cette racine carrée afin de donner une autre démonstration de la loi de réciprocité quadratique :

$$\left(\frac{p^*}{q}\right) \equiv {p^*}^{\frac{q-1}{2}} \equiv g^{q-1} \pmod{q\mathbf{Z}[\zeta_p]}$$

et

$$g^q \equiv \sum_{a \in \mathbf{F}_p^\times} \left(\frac{a}{p}\right)^q \zeta_p^{aq} \equiv \left(\frac{q}{p}\right) g \pmod{q\mathbf{Z}[\zeta_p]},$$

donc

$$\left(\frac{p^*}{q}\right) \equiv \left(\frac{q}{p}\right) \pmod{q\mathbf{Z}[\zeta_p]}$$

car g est inversible modulo q. On en déduit finalement

$$\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right)$$

car $2 \notin q\mathbf{Z}[\zeta_p]$ (sinon $2/q$ appartiendrait à $\mathbf{Z}[\zeta_p] \cap \mathbf{Q} = \mathbf{Z}$...)

La démonstration du théorème 2.22 repose sur l'inclusion $\mathbf{Q}(\sqrt{p^*}) \subset \mathbf{Q}(\zeta_p)$. Il s'agit d'un cas particulier du résultat suivant.

Proposition 2.24 — *Tout corps de nombres quadratique K est contenu dans le corps cyclotomique $\mathbf{Q}(\zeta_{|D_K|})$.*

Démonstration. Écrivons $D_K = \pm 2^m p_1 \cdot p_r = \varepsilon 2^m p_1^* \cdots p_r^*$ avec $\varepsilon \in \{-1, 1\}$, $m \in \{0, 2\}$ et $p_1, \ldots, p_r$ des nombres premiers impairs distincts. Deux cas de figure sont possibles :

(i) $D_K \equiv 1 \pmod 4$, c'est-à-dire $m = 0$ et $\varepsilon = 1$ puisque $p_i^* \equiv 1 \pmod 4$;

(ii) $D_K \equiv 0 \pmod 4$, c'est-à-dire $m = 2$.

D'après la démonstration du théorème 2.22, $\mathbf{Q}(\zeta_{p_i})$ contient une racine carré de p_i^*. Dans le premier cas de figure, ceci implique immédiatement $\sqrt{D_K} \in \mathbf{Q}(\zeta_{|D_K|})$. Dans le second cas de figure, on observe que le corps $\mathbf{Q}(\zeta_{|D_K|})$ contient également ζ_4, qui est une racine carrée de -1, et donc contient $\sqrt{D_K}$. □

Nous concluons cette section en décrivant deux applications de la loi de réciprocité quadratique.

Première application : description des nombres premiers p tels que n soit un carré modulo p.

Soit $n \in \mathbf{Z}$ un nombre entier non nul. Peut-on caractériser les nombres premiers p (ne divisant pas n) tels que n soit un carré modulo p ? En écrivant n sous la forme $n = m^2 d$ avec d un entier sans facteur carré, il revient au même de demander que d soit un carré modulo p. En posant $K = \mathbf{Q}(\sqrt{n}) = \mathbf{Q}(\sqrt{d})$, on a $D_K = d$ si $d \equiv 1 \pmod 4$ et $D_K = 4d$ si $d \equiv 2, 3 \pmod 4$, donc les conditions suivantes sont équivalentes pour tout nombre premier impair p ne divisant pas n :

(i) n est un carré modulo p
(ii) d est un carré modulo p
(iii) $4d$ est un carré modulo p
(iv) D_K est un carré modulo p
(v) p est décomposé dans K

Écrivons $D_K = \varepsilon 2^m p_1^* \cdots p_r^*$ avec $\varepsilon \in \{-1, 1\}$, $m \in \{0, 2\}$ et $p_1, \ldots, p_r$ des nombres premiers impairs distincts. En vertu de la loi de réciprocité quadratique,

$$\left(\frac{D_K}{p}\right) = \left(\frac{\varepsilon}{p}\right)\left(\frac{p_1^*}{p}\right)\cdots\left(\frac{p_r^*}{p}\right) = \left(\frac{\varepsilon}{p}\right)\left(\frac{p}{p_1^*}\right)\cdots\left(\frac{p}{p_r^*}\right)$$

et le membre de droite de dépend que des classes de congruences de de p modulo les p_i^* et modulo 4 si $\varepsilon = 1$, donc uniquement de la classe de congruence de p modulo D_K (si $\varepsilon = 1$, alors $m = 2$ et $4|D_K$).

Ainsi, il existe des classes de congruences $C_1, \ldots, C_m$ modulo $|D_K|$ telles que, pour tout nombre premier impair ne divisant pas n,

$$n \text{ est un carré modulo } p \iff p \in C_1 \cup \ldots \cup C_m.$$

Exemples (i) Si $n = -1$, alors $K = \mathbf{Q}(i)$ et $D_K = 4$. Comme

$$\left(\frac{-1}{3}\right) = -1 \quad \text{et} \quad \left(\frac{-1}{5}\right) = 1,$$

on retrouve le fait bien connu que -1 est un carré modulo p impair si et seulement si $p \equiv 1 \pmod 4$.

(ii) Si $n = -3$, alors $K = \mathbf{Q}(\sqrt{-3})$ et $D_K = -3 = 3^*$. Comme

$$\left(\frac{-3}{5}\right) = \left(\frac{-1}{5}\right)\left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1 \quad \text{et} \quad \left(\frac{-3}{7}\right) = \left(\frac{-1}{7}\right)\left(\frac{3}{7}\right) = \left(\frac{7}{3}\right) = 1,$$

on en déduit que -3 est un carré modulo p impair et distinct de 3 si et seulement si $p \equiv 1 \pmod 3$.

(iii) Si $n=-5$, alors $K=\mathbf{Q}(\sqrt{-5})$ et $D_K=-4\times 5$. En calculant

$$\left(\frac{-5}{41}\right)=\left(\frac{-1}{41}\right)\left(\frac{5}{41}\right)=\left(\frac{41}{5}\right)=1,\quad \left(\frac{-5}{3}\right)=\left(\frac{-1}{3}\right)\left(\frac{2}{3}\right)=(-1)^2=1$$

$$\left(\frac{-5}{7}\right)=\left(\frac{-1}{7}\right)\left(\frac{7}{5}\right)=-\left(\frac{2}{5}\right)=1,\quad \left(\frac{-5}{29}\right)=\left(\frac{-1}{29}\right)\left(\frac{5}{29}\right)=\left(\frac{29}{5}\right)=\left(\frac{-1}{5}\right)=1$$

$$\left(\frac{-5}{11}\right)=\left(\frac{-1}{11}\right)\left(\frac{11}{5}\right)=-1,\quad \left(\frac{-5}{13}\right)=\left(\frac{-1}{13}\right)\left(\frac{13}{5}\right)=\left(\frac{3}{5}\right)=\left(\frac{2}{3}\right)=-1$$

et

$$\left(\frac{-5}{17}\right)=\left(\frac{-1}{17}\right)\left(\frac{17}{5}\right)=\left(\frac{2}{5}\right)=-1,\quad \left(\frac{-5}{19}\right)=\left(\frac{-1}{19}\right)\left(\frac{19}{5}\right)=-\left(\frac{-1}{5}\right)=-1.$$

On en déduit que -5 est un carré modulo p impair et distinct de 5 si et seulement si $p\equiv 1,3,7,9 \pmod{20}$.

Deuxième application : symbole de Jacobi et test de primalité.

Pour $m,n\in\mathbf{Z}$ avec $n\geqslant 3$ *impair*, on pose

$$\left(\frac{m}{n}\right)=\prod_{i=1}^{r}\left(\frac{m}{p_i}\right)$$

où $n=p_1\cdots p_r$ est le décomposition de n en produit de nombres premiers (non nécessairement distincts). Il s'agit d'un élément de $\{-1,0,1\}$ appelé *symbole de Jacobi* de m et n qui a les propriétés immédiates suivantes :

$$\left(\frac{m}{n}\right)=0\iff \mathrm{pgcd}(m,n)\neq 1,\quad \left(\frac{mm'}{n}\right)=\left(\frac{m}{n}\right)\left(\frac{m'}{n}\right),\quad \left(\frac{m}{nn'}\right)=\left(\frac{m}{n}\right)\left(\frac{m}{n'}\right)$$

et

$$\left(\frac{m^2}{n}\right)=\left(\frac{m}{n^2}\right)=1\ \text{ si } \mathrm{pgcd}(m,n)=1.$$

Remarque — Attention ! Si n n'est pas premier, alors les conditions $\left(\frac{m}{n}\right)=1$ et $m\in(\mathbf{Z}/n\mathbf{Z})^{\times,2}$ ne sont pas équivalentes. Par exemple, si $n=pq$ avec p,q premiers impairs distincts, alors

$$\left(\frac{m}{n}\right)=1\iff \left(m\in\mathbf{F}_p^{\times,2}\text{ et }m\in\mathbf{F}_q^{\times,2}\right)\ \text{ ou }\ \left(m\notin\mathbf{F}_p^{\times,2}\text{ et }m\notin\mathbf{F}_q^{\times,2}\right)$$

tandis que

$$m\in\left(\mathbf{Z}/n\mathbf{Z}^{\times,2}\right)\iff \left(m\in\mathbf{F}_p^{\times,2}\text{ et }m\in\mathbf{F}_q^{\times,2}\right).$$

Proposition 2.25 — *Soient m et n deux entiers positifs impairs et premiers entre eux.*

(i) $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right)=(-1)^{\frac{(m-1)(n-1)}{4}}$

(ii) $\left(\frac{-1}{n}\right)=(-1)^{\frac{n-1}{2}}$

(iii) $\left(\frac{2}{n}\right)=(-1)^{\frac{n^2-1}{8}}$

Démonstration. Les membres de gauche de ces égalités sont multiplicatifs en m et n et les membres de droite le sont aussi (vérification immédiate). La conclusion découle donc du cas où m et n sont des nombres premiers impairs, auquel cas cet énoncé est précisément la loi de réciprocité quadratique (théorème 2.22). □

On déduit de cette proposition un algorithme efficace pour le calcul des symboles de Jacobi à l'aide de divisions euclidiennes successives : si $m = nq + r$ avec $0 \leqslant r < n$ et $r = 2^a r'$ avec $2 \nmid r'$, alors

$$\left(\frac{m}{n}\right) = \left(\frac{2}{n}\right)^a \left(\frac{r'}{n}\right) = (-1)^{\frac{(n^2-1)}{8}a} \left(\frac{r'}{n}\right) = (-1)^{\frac{n^2-1}{8}a}(-1)^{\frac{(n-1)(r'-1)}{4}} \left(\frac{n}{r'}\right) = ...$$

Par exemple,

$$\left(\frac{14}{51}\right) = \left(\frac{2}{51}\right)\left(\frac{7}{51}\right) = -\left(-\left(\frac{51}{7}\right)\right) = \left(\frac{2}{7}\right) = 1.$$

Le symbole de Jacobi permet d'énoncer un critère de primalité.

Proposition 2.26 (Solovay-Strassen, 1977) — *Soit n un nombre entier positif impair. Si*

$$\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \pmod{n}$$

pour tout entier a premier avec n, alors n est premier.

Démonstration. On vérifie tout d'abord que n est sans facteur carré. S'il existe p premier tel que $n = p^2 m$, alors $(1 + mp)^p \equiv 1 \pmod{n}$ et donc $a = 1 + mp$ est d'ordre p dans $(\mathbf{Z}/n\mathbf{Z})^\times$. Comme $p \nmid n - 1$, il vient $a^{n-1} \not\equiv 1 \pmod{n}$ et donc

$$a^{\frac{n-1}{2}} \not\equiv \pm 1 \pmod{n}.$$

On vérifie ensuite que n n'a qu'un seul facteur premier. Supposons $n = pm$ avec p premier et $m > 1$ non divisible par p. Choisissons un entier u premier avec m tel que $\left(\frac{u}{m}\right) = -1$. Via le théorème chinois des restes, il existe un entier $a \in (\mathbf{Z}/n\mathbf{Z})^\times$ tel que

$$a \equiv 1 \pmod{p} \quad \text{et} \quad a \equiv u \pmod{m}.$$

On a alors

$$\left(\frac{a}{n}\right) = \left(\frac{a}{m}\right) = -1 \quad \text{et} \quad a^{\frac{n-1}{2}} \equiv 1 \pmod{p},$$

donc

$$\left(\frac{a}{n}\right) \not\equiv a^{\frac{n-1}{2}} \pmod{n}.$$

□

Remarques — (i) Puisque

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

(proposition 2.21) pour tous nombre premier impair p et tout entier a premier avec p, la proposition précédente fournit bien un *critère* de primalité.

(ii) Si n n'est pas premier, alors l'ensemble des $a \in (\mathbf{Z}/n\mathbf{Z})^\times$ tels que

$$\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \pmod{n}$$

est un *sous-groupe strict* et donc son cardinal est majoré par $\frac{1}{2}\varphi(n)$.

L'intérêt de la proposition précédente vient de ce qu'elle conduit facilement à un *test probabiliste de (non) primalité*.

Soit en effet n un nombre entier positif et impair donné. Fixons un nombre entier $N \geqslant 1$ et répétons N fois la procédure suivante :

1. *choisir aléatoirement un entier a dans $\{1, \ldots, n\}$ selon la distribution uniforme ;*
2. *exécuter le test*
$$\mathrm{pgcd}(a, n) = 1 \quad et \quad \left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \pmod{n}$$
3. *si ce test échoue, alors n est un entier composé et on a terminé ;*
4. *si ce test réussit, retourner à l'étape 1.*

Si n est composé, la probabilité de réussite du test de l'étape 2 est

$$\frac{\mathrm{Card}\left\{a \in (\mathbf{Z}/\mathbf{Z})^\times \mid \left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \pmod{n}\right\}}{n} \leqslant \frac{\frac{1}{2}\varphi(n)}{n} < \frac{1}{2}$$

et une série de N répétitions indépendante de ce test a donc une probabilité de réussite inférieure à 2^{-N}. Autrement dit, N répétitions de ce test permettent de détecter un nombre composé avec une probabilité supérieure à $1 - 2^{-N}$. Le fait que les symboles de Jacobi puissent se calculer rapidement par application de la division euclidienne et de la loi de réciprocité quadratique rend cet algorithme très performant (voir par exemple le chapitre 5 du *Cours d'algèbre* de Michel Demazure pour une estimation de sa complexité).

Chapitre 3

Groupe des classes et groupe des unités

3.1 Réseaux

Soit V un $\mathbf{R}$-espace vectoriel de dimension $n \geqslant 1$.

Définition 3.1 — *Un* réseau *de V est un sous-groupe discret qui engendre V comme $\mathbf{R}$-espace vectoriel.*

Exemples. (i) Le sous-groupe $\mathbf{Z}^n$ de $\mathbf{R}^n$ est un réseau. À isomorphisme près, tous les réseaux de V sont de cette forme (Proposition 3.2(ii)).

(ii) Le sous-groupe de $\mathbf{R}^2$ formé des couples $(a, b) \in \mathbf{Z}^2$ tels que $a \equiv 2b \pmod 3$ est un réseau. C'est en effet un sous-groupe discret puisque contenu dans $\mathbf{Z}^2$, et il engendre $\mathbf{R}^2$ puisqu'il contient les points $(3, 0)$ et $(0, 3)$.

(iii) Soit K un corps de nombres. L'image de $\mathcal{O}_K$ par l'application canonique $K \to K \otimes_{\mathbf{Q}} \mathbf{R}$ est un réseau. En effet, le choix d'une $\mathbf{Z}$-base de $\mathcal{O}_K$ fournit un isomorphisme $K \otimes_{\mathbf{Q}} \mathbf{R} \simeq \mathbf{R}^n$ identifiant $\Phi(\mathcal{O}_K)$ et $\mathbf{Z}^n$.

Proposition 3.2 — *Soit Λ un sous-groupe de V. Les conditions suivantes sont équivalentes :*

(i) *Λ est un réseau ;*

(ii) *Λ est engendré par une base de V ;*

(iii) *Λ est discret et V/Λ est compact.*

Démonstration. (i) $\Rightarrow$ (ii). Puisque Λ engendre V, il existe une base $(e_1, \dots, e_n)$ formée d'éléments de V. Posant $B = \sum_{i=1}^n [0, 1]e_i$, nous pouvons écrire

$$V = B + \sum_{i=1}^n \mathbf{Z}e_i \quad \text{et} \quad \Lambda = \Lambda \cap B + \sum_{i=1}^n \mathbf{Z}e_i.$$

L'ensemble $\Lambda \cap B$ est fini puisque Λ est discret dans V, donc le sous-groupe $\Lambda_0 = \sum_{i=1}^n \mathbf{Z}e_i$ est d'indice fini dans Λ. Posant $m = (\Lambda : \Lambda_0)$, nous avons obtenu les inclusions

$$\sum_{i=1}^n \mathbf{Z}e_i \subset \Lambda \subset \frac{1}{m} \sum_{i=1}^n \mathbf{Z}e_i$$

qui prouvent que Λ est un groupe abélien libre de rang n. En appliquant le théorème de la base adaptée, la seconde inclusion montre qu'il existe des entiers $d_1, \dots, d_n$ tels que Λ soit engendré par les vecteurs $\frac{d_1}{m}e_1, \dots, \frac{d_n}{m}e_n$.

(ii) $\Rightarrow$ (iii). Le sous-groupe Λ est discret, puisque formé des éléments de V dont les coordonnées dans une base adéquate sont entière. Il en découle que l'espace topologique quotient V/Λ est séparé : si x, y sont deux points de V tels que $y - x \notin \Lambda$, il existe $\varepsilon > 0$ tel que la boule ouverte $B(y-x), \varepsilon)$ soit disjointe de Λ et alors $B(x, \varepsilon/3) + \Lambda$ et $B(y, \varepsilon/3) + \Lambda$ sont des voisinages disjoints de $x + \Lambda$ et $y + \Lambda$ respectivement. Cet espace quotient étant par ailleurs l'image du compact $\sum_{i=1}^{n} [0,1]e_i$ par la projection canonique, il s'agit d'un espace compact.

(iii) $\Rightarrow$ (i). Soit W le sous-espace vectoriel engendré par Λ. L'application naturelle $V/\Lambda \to V/W$ est continue et surjective, donc V/W est compact ; comme il s'agit d'un espace vectoriel, cet espace est nul et $W = V$. □

Supposons que V soit muni d'un produit scalaire ; on dispose alors d'une unique mesure invariante par translation sur V telle que tous les hypercubes construits sur des bases orthonormées soient de volume 1 ; on la notera vol. Lorsque $V = \mathbf{R}^n$ est muni du produit scalaire euclidien standard, la mesure invariante ainsi normalisée est la mesure de Lebesgue $dx_1 \cdots dx_n$.

Lemme 3.3 — *Soit $\Lambda \subset V$ un réseau et soit $(\varepsilon_1, \ldots, \varepsilon_n)$ une base orthonormée de V. Étant donnée une $\mathbf{Z}$-base $(e_1, \ldots, e_n)$ de Λ,*

$$\mathrm{vol}\left(\sum_{i=1}^{n} [0,1]e_i\right) = |\det_{(\varepsilon_1,\ldots,\varepsilon_n)}(e_1, \ldots, e_n)|$$

et cette quantité ne dépend pas du choix de la $\mathbf{Z}$-base de Λ.

Démonstration. L'égalité est un cas particulier de la formule de changement de variables : si A est la matrice des coordonnées des e_i dans la base $(\varepsilon_1, \ldots, \varepsilon_n)$, alors

$$\mathrm{vol}\left(\sum_{i=1}^{n} [0,1]e_i\right) = \mathrm{vol}\left(\sum_{i=1}^{n} [0,1]A\varepsilon_i\right) = |\det(A)|\mathrm{vol}\left(\sum_{i=1}^{n} [0,1]\varepsilon_i\right) = |\det(A)|.$$

L'indépendance par rapport au choix de la base de Λ se déduit également de la formule de changement de variables et du fait que deux $\mathbf{Z}$-bases de Λ se déduisent l'une de l'autre par un élément de $\mathrm{GL}_n(\mathbf{Z})$. □

Définition 3.4 — *Le* covolume *d'un réseau Λ dans V est la mesure commune des pavés construits sur une $\mathbf{Z}$-base de Λ. C'est un nombre réel strictement positif, noté* $\mathrm{covol}(\Lambda)$.

Proposition 3.5 — *Soit $\Lambda \subset V$ un réseau et soit $\Lambda' \subset \Lambda$ un sous-groupe. Les assertions suivantes sont équivalentes :*

(i) *Λ' est un réseau ;*

(ii) *Λ' est d'indice fini dans Λ.*

Si elles sont satisfaites, alors

$$\mathrm{covol}(\Lambda') = (\Lambda : \Lambda')\mathrm{covol}(\Lambda).$$

Démonstration. Notons que Λ' est un sous-groupe discret de V puisque contenu dans le sous-groupe discret Λ.

(i) $\Rightarrow$ (ii). Le groupe quotient Λ/Λ' est le noyau du morphisme canonique $V/\Lambda' \to V/\Lambda$. Comme V/Λ' est compact, le sous-groupe fermé Λ/Λ' est compact et donc fini puisque discret.

(ii) $\Rightarrow$ (i). Posons $m = (\Lambda : \Lambda')$. L'inclusion $m\Lambda \subset \Lambda'$ montre que Λ' engendre V sur $\mathbf{R}$ et donc Λ' est un réseau dans V.

Supposons que Λ' soit d'indice fini m dans Λ. En vertu du théorème de la base adaptée, il existe une base $(e_1, \dots, e_n)$ de Λ et des entiers $d_1, \dots, d_n \geqslant 1$ tels que $(d_1 e_1, \dots, d_n e_n)$ soit une base de Λ'. On a $(\Lambda : \Lambda') = d_1 \cdots d_n$ et

$$\mathrm{covol}(\Lambda') = |\det(d_1 e_1, \dots, d_n e_n)| = |d_1 \cdots d_n||\det(e_1, \dots, e_n)|,$$

c'est-à-dire

$$\mathrm{covol}(\Lambda') = (\Lambda : \Lambda')\mathrm{covol}(\Lambda).$$

□

Exemple. Considérons le sous-groupe $\Lambda = \{(a, b) \in \mathbf{Z}^2 \mid a \equiv 2b \pmod 3\}$ de $\mathbf{R}^2$. En écrivant

$$\Lambda = \ker\left(\mathbf{Z}^2 \to \mathbf{Z}/3\mathbf{Z}, \quad (a, b) \mapsto a - 2b\right),$$

on obtient $(\mathbf{Z}^2 : \Lambda) = 3$ et donc $\mathrm{covol}(\Lambda) = 3$.

Le théorème suivant est un résultat fondamental pour l'étude des réseaux. On rappelle qu'une partie C de V est dite *convexe* si, pour tous $v, v' \in C$ et tout $t \in [0, 1]$, on a $tv + (1 - t)v' \in C$; elle est dite *symétrique* si $-v \in C$ pour tout $v \in C$.

Théorème 3.6 (Minkowski) — *Soit C une partie convexe, symétrique et bornée de V et soit $\Lambda \subset V$ un réseau. Si $\mathrm{vol}(C) > 2^n \mathrm{covol}(\Lambda)$, alors C contient un élément non nul de Λ. Si, de plus, C est compacte, alors l'inégalité large suffit.*

Démonstration. Posons $\Lambda' = 2\Lambda$; c'est un réseau de covolume $2^n \mathrm{covol}(\Lambda)$. Soit $(e_1, \dots, e_n)$ une $\mathbf{Z}$-base de Λ' et posons $\Pi' = \sum_{i=1}^n [0, 1]e_i$. On a

$$V = \bigcup_{\lambda \in \Lambda'} (\lambda + \Pi'),$$

donc

$$C = \bigcup_{\lambda \in \Lambda'} \left(C \cup (\lambda + \Pi')\right) = \bigcup_{\lambda \in \Lambda'} \left(\lambda + (\Pi' \cap (C - \lambda))\right)$$

et

$$\mathrm{vol}(C) \leqslant \sum_{\lambda \in \Lambda'} \mathrm{vol}(\Pi' \cap (C - \lambda)).$$

Si $\mathrm{vol}(C) > \mathrm{covol}(\Lambda') = \mathrm{vol}(\Pi')$, alors les parties $\Pi' \cap (C - \lambda)$ ne sont pas disjointes et il existe donc $\lambda, \mu \in \Lambda'$ distincts ainsi que $v, v' \in C$ tels que $v - \lambda = v' - \mu$. On en déduit que

$$\frac{1}{2}(\lambda - \mu) = \frac{1}{2}(v - v')$$

est un élément de Λ appartenant à C.

Supposons maintenant que C soit de plus compact et que l'on ait $\mathrm{covol}(\Lambda') \leqslant \mathrm{vol}(C)$. Pour tout $\varepsilon > 0$, posons

$$C_\varepsilon = \{v \in V \mid \exists x \in C, \quad ||x - v|| < \varepsilon\}.$$

Il s'agit d'une partie ouverte, bornée, convexe et symétrique telle que $\mathrm{vol}(C_\varepsilon) > \mathrm{vol}(C)$. D'après le cas précédent, l'ensemble $(\Lambda \setminus \{0\}) \cap C_\varepsilon$ est non vide et fini (puisque Λ est discret). Cet ensemble décroissant avec ε, il est constant pour ε suffisamment petit et donc $C \cap (\Lambda \setminus \{0\}) \neq \varnothing$.
□

Le théorème de Minkowski a de nombreuses applications à la théorie des nombres ; en voici une très classique.

Application : le théorème des quatre carrés

Théorème 3.7 (Lagrange) — *Tout entier positif est la somme de quatre carrés.*

Démonstration. L'identité d'Euler

$$(a^2+b^2+c^2+d^2)(u^2+v^2+w^2+x^2) =$$
$$(au+bv+cw+dx)^2+(av-bu-cx+dw)^2+(aw+bx-cu-dv)^2+(ax-bw+cv-du)^2$$

pour tous $a,b,c,d,u,v,w,x \in \mathbf{Z}$ montre qu'il suffit d'établir que tout nombre premier p est la somme de quatre carrés.

Étape 1 : -1 est la somme de deux carrés dans $\mathbf{F}_p$

C'est évident si $p=2$. Pour $p \geqslant 3$, on observe que les deux sous-ensembles de $\mathbf{F}_p$

$$\{1+x^2 \mid x \in \mathbf{F}_p\} \quad \text{et} \quad \{-y^2 \mid y \in \mathbf{F}_p\}$$

sont tous deux de cardinal $(p+1)/2$ et donc ne sont pas disjoints.

Considérons deux nombres entiers u, v tels que $1+u^2+v^2 \equiv 0 \pmod{p}$.

Étape 2 : construction d'un réseau

Le groupe

$$\begin{aligned}\Lambda &= \{(a,b,c,d) \in \mathbf{Z}^4 \mid c \equiv au+bv \pmod{p} \text{ et } d \equiv av-bu \pmod{p}\} \\ &= \ker\left(\mathbf{Z}^4 \to (\mathbf{Z}/p\mathbf{Z})^2\,, \quad (a,b,c,d,) \mapsto (c-au-bv, d-av+bu)\right)\end{aligned}$$

est un réseau dans $\mathbf{R}^4$ de covolume p^2. Pour tout $(a,b,c,d) \in \Lambda$,

$$a^2+b^2+c^2+d^2 \equiv a^2(1+u^2+v^2)+b^2(1+u^2+v^2) \equiv 0 \pmod{p}.$$

Pour $r \geqslant 0$, notons $B(r)$ la boule euclidienne ouverte de centre 0 et de rayon r dans $\mathbf{R}^4$; son volume est $\frac{\pi^2}{2}r^4$.

Étape 3 : application du théorème de Minkowski

La boule $B(\sqrt{2p})$ est une partie bornée, convexe et symétrique de volume $2\pi^2p^2$. Comme

$$\frac{2\pi^2p^2}{2^4p^2} = \frac{\pi^2}{8} > 1,$$

on déduit du théorème de Minkowski que $B(\sqrt{2p})$ contient un élément non nul de Λ.

Soit $(a,b,c,d) \in \Lambda \cap B(\sqrt{2p})$ non nul. On a $a^2+b^2+c^2+d^2 \equiv 0 \pmod{p}$ et $a^2+b^2+c^2+d^2 < 2p$, donc

$$a^2+b^2+c^2+d^2 = p.$$

□

3.2 Finitude du groupe des classes

Soit K un corps de nombres de degré n. On note Σ_r l'ensemble des plongements réels de K et on désigne par Σ'_c un ensemble de représentants des plongements imaginaires de K modulo conjugaison. On a

$$\mathrm{Card}(\Sigma_r) = r_1, \mathrm{Card}(\Sigma'_c) = r_2 \quad \text{et} \quad r_1+2r_2 = n.$$

Soit Φ le plongement canonique de K dans l'espace vectoriel réel $\mathbf{R}^{\Sigma_r} \times \mathbf{C}^{\Sigma'_c} \simeq \mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$, muni de la structure euclidienne standard.

Proposition 3.8 — (i) *L'image de $\mathcal{O}_K$ par Φ est un réseau de covolume $2^{-r_2}|D_K|^{1/2}$.*

(ii) *Pour tout idéal fractionnaire $\mathfrak{a}$ de K, l'image de $\mathfrak{a}$ par Φ est un réseau de covolume $2^{-r_2}|D_K|^{1/2}\mathrm{N}(\mathfrak{a})$.*

Démonstration. (i) Posons $\Sigma_r = \{\sigma_1, \dots, \sigma_{r_1}\}$ et $\Sigma'_c = \{\tau_1, \dots, \tau_{r_2}\}$. L'application Φ envoie une $\mathbf{Z}$-base $(\omega_1, \dots, \omega_n)$ de $\mathcal{O}_K$ sur la famille $(\Phi(\omega_1), \dots, \Phi(\omega_n))$ et

$$\det(\Phi(\omega_1, \dots, \omega(n)) = \begin{vmatrix} \sigma_1(\omega_1) & \dots & \sigma_1(\omega_n) \\ \vdots & & \vdots \\ \sigma_{r_1}(\omega_1) & \dots & \sigma_{r_1}(\omega_n) \\ \mathfrak{Re}\ \tau_1(\omega_1) & \dots & \mathfrak{Re}\ \tau_1(\omega_n) \\ \mathfrak{Im}\ \tau_1(\omega_1) & \dots & \mathfrak{Im}\ \tau_1(\omega_n) \\ \vdots & & \vdots \\ \mathfrak{Re}\ \tau_{r_2}(\omega_1) & \dots & \mathfrak{Re}\ \tau_{r_2}(\omega_n) \\ \mathfrak{Im}\ \tau_{r_2}(\omega_1) & \dots & \mathfrak{Im}\ \tau_{r_2}(\omega_n) \end{vmatrix} = (-2i)^{r_2} \begin{vmatrix} \sigma_1(\omega_1) & \dots & \sigma_1(\omega_n) \\ \vdots & & \vdots \\ \sigma_{r_1}(\omega_1) & \dots & \sigma_{r_1}(\omega_n) \\ \tau_1(\omega_1) & \dots & \tau_1(\omega_n) \\ \overline{\tau_1}(\omega_1) & \dots & \overline{\tau_1}(\omega_n) \\ \vdots & & \vdots \\ \tau_{r_2}(\omega_1) & \dots & \tau_{r_2}(\omega_n) \\ \overline{\tau_{r_2}}(\omega_1) & \dots & \overline{\tau_{r_2}}(\omega_n) \end{vmatrix}$$

donc $|\det(\Phi(\omega_1, \dots, \omega_n)| = 2^{-r_2}|D_K|^{1/2}$. Ainsi, la famille $(\Phi(\omega_1), \dots, \Phi(\omega_n))$ est une base de $\mathbf{R}^{\Sigma_r} \times \mathbf{C}^{\Sigma'_c}$ et $\Phi(\mathcal{O}_K)$ est un réseau de covolume $2^{-r_2}|D_K|^{1/2}$.

(ii) Soit $\mathfrak{a}$ un idéal fractionnaire de K. Il existe un entier $d \geqslant 1$ tel que $d\mathfrak{a} \subset \mathcal{O}_K$ et alors

$$(\mathcal{O}_K : d\mathfrak{a}) = \mathrm{N}(d\mathfrak{a}) = d^n\mathrm{N}(\mathfrak{a}).$$

En vertu de la proposition 3.5, $\Phi(d\mathfrak{a}) = d\Phi(\mathfrak{a})$ est un réseau de covolume $d^n\mathrm{N}(\mathfrak{a})\mathrm{covol}(\Phi(\mathcal{O}_K)$ et donc $\Phi(\mathfrak{a})$ est un réseau de covolume $2^{-r_2}|D_K|^{1/2}\mathrm{N}(\mathfrak{a})$. □

Remarque. Le point (i) fournit une interprétation géométrique (de la valeur absolue) du discriminant d'un corps de nombres.

Pour $R \in \mathbf{R}_{\geqslant 0}$, posons

$$C(r_1, r_2; R) = \{(x_1, \dots, x_{r_1}, z_1, \dots, z_{r_2}) \in \mathbf{R}^{r_1} \times \mathbf{C}^{r_2} \mid |x_1| + \dots + |x_{r_1}| + 2|z_1| + \dots + 2|z_{r_2}| \leqslant R\}.$$

C'est une partie bornée, convexe et symétrique de volume

$$\mathrm{vol}(C(r_1, r_2; R)) = 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2}\frac{R^n}{n!}.$$

Ce dernier point se démontrer par récurrence sur $n = r_1 + 2r_2$.

(a) Initialisation

$$\mathrm{vol}(C(1, 0; R)) = 2R \quad \text{et} \quad \mathrm{vol}(C(0, 1; R)) = \pi\left(\frac{R}{2}\right)^2 = \frac{\pi}{2}\frac{R^2}{2!}$$

(b) Passage de r_1 à $r_1 + 1$

$$\begin{aligned} \mathrm{vol}(C(r_1 + 1, r_2, R)) &= \int_{-R}^{R} \mathrm{vol}(C(r_1, r_2; R - |t|))\ \mathrm{d}t \\ &= 2^{r_1+1}\left(\frac{\pi}{2}\right)^{r_2}\int_0^R (R - t)^n n!\ \mathrm{d}t \\ &= 2^{r_1+1}\left(\frac{\pi}{2}\right)^{r_2}\frac{R^{n+1}}{(n+1)!}. \end{aligned}$$

(b') Passage de r_2 à r_2+1

$$\begin{aligned}
\mathrm{vol}(C(r_1,r_2+1;R)) &= \int_{z\in\mathbf{C},|z|\leqslant R/2} \mathrm{vol}(C(r_1,r_2;R-2|z|)\ \frac{\mathrm{d}z d\overline{z}}{2}\\
&= \int_0^{2\pi}\int_0^{R/2} 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2}\frac{(R-2\rho)^n}{n!}\rho d\rho d\theta\\
&= 2\pi\cdot 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2}\int_0^R (R-t)\frac{t^n}{n!}\frac{\mathrm{d}t}{4}\\
&= 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2+1}\left[\frac{Rt^{n+1}}{(n+1)!}-\frac{t^{n+2}}{(n+2)n!}\right]_0^R\\
&= 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2}\frac{R^{n+2}}{(n+2)!}.
\end{aligned}$$

Théorème 3.9 (Minkowski) — *Soit K un corps de nombres de degré n. Soit r_1 le nombre de plongements réels de K et soit $2r_2$ le nombre de plongements complexes (non réels) de K. Tout idéal fractionnaire $\mathfrak{a}$ de K contient un élément non nul a tel que*

$$|\mathrm{N}(a)|\leqslant \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}|D_K|^{1/2}\mathrm{N}(\mathfrak{a}).$$

Démonstration. D'après la proposition 3.8, $\Phi(\mathfrak{a})$ est un réseau de $\mathbf{R}^{\Sigma_r}\times\mathbf{C}^{\Sigma'_c}$ de covolume $2^{-r_2}|D_K|^{1/2}\mathrm{N}(\mathfrak{a})$. En vertu du calcul qui précède,

$$\frac{\mathrm{vol}(C(r_1,r_2;R))}{2^n\mathrm{covol}(\Phi(\mathfrak{a}))}=\frac{2^{r_1}2^{-r_2}\pi^{r_2}R^n}{n!2^{r_1+2r_2}2^{-r_2}|D_K|^{1/2}\mathrm{N}(\mathfrak{a})}=\left(\frac{\pi}{4}\right)^{r_2}\frac{R^n}{n!|D_K|^{1/2}\mathrm{N}(\mathfrak{a})}.$$

Par ailleurs, si $x\in K$ et $\Phi(x)=(x_1,\dots,x_{r_1},z_1,\dots,z_{r_2})$, alors

$$|\mathrm{N}(x)|=|x_1|\cdots|x_{r_1}||z_1|^2\cdots|z_{r_2}|^2\leqslant\frac{1}{n^n}\left(|x_1|+\ldots+|x_{r_1}|+2|z_1|+\ldots+2|z_{r_2}|\right)^n$$

(inégalité arithmético-géométrique), donc $\mathrm{N}(x)\leqslant R^n/n^n$ si $\Phi(x)\in C(r_1,r_2;R)$. En vertu du second cas du théorème 3.6, il existe donc un élément non nul a de $\mathfrak{a}$ tel que

$$|\mathrm{N}(a)|\leqslant\left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}|D_K|^{1/2}\mathrm{N}(\mathfrak{a}).$$

□

L'expression

$$M_K=\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}|D_K|^{1/2}$$

est la *constante de Minkowski* de K.

Corollaire 3.10 — *Soit K un corps de nombres de degré n.*

(i) *Chaque classe d'idéaux contient un idéal de norme inférieure à M_K.*

(ii) *Le groupe $\mathrm{Cl}(\mathcal{O}_K)$ est fini.*

(iii) *On a la minoration*

$$|D_K|\geqslant\left(\frac{n^n}{n!}\left(\frac{\pi}{4}\right)^{r_2}\right)^2\geqslant\frac{\pi}{4}.$$

En particulier, $|D_K|>1$ si $K\neq\mathbf{Q}$.

Démonstration. (i) Considérons une classe $c \in \mathrm{Cl}(\mathcal{O}_K)$ et un idéal $\mathfrak{a} \subset \mathcal{O}_K$ appartenant à c^{-1}. D'après le théorème précédent, il existe un élément non nul x de $\mathfrak{a}$ tel que $|N(x)| \leqslant M_K \mathrm{N}(\mathfrak{a})$. L'idéal $x\mathfrak{a}^{-1}$ est entier, appartient à c et sa norme est inférieure à M_K.

(ii) Il n'existe qu'un nombre fini d'idéaux dans $\mathcal{O}_K$ de norme bornée (Proposition 2.11, (ii)), donc la conclusion découle immédiatement du point précédent.

(iii) Appliquant le théorème précédent à l'idéal trivial $\mathcal{O}_K$, on obtient l'existence d'un élément non nul x de $\mathcal{O}_K$ tel que $|N(x)| \leqslant M_K$. Comme $|N(x)|$ est un nombre entier strictement positif, on en déduit $M_K \geqslant 1$ et donc

$$|D_K| \geqslant \left(\frac{n^n}{n!}\left(\frac{\pi}{4}\right)^{r_2}\right)^2.$$

En outre, en utilisant la minoration [1] $n^n \geqslant 2^{n-1} n!$ pour tout $n \geqslant 1$, il vient

$$\left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \leqslant \left(\frac{4}{\pi}\right)^{n/2} 2^{1-n} = \left(\frac{4}{\pi}\right)^{1/2}$$

et donc $|D_K| \geqslant \pi^n/4$. □

Le cardinal du groupe $\mathrm{Cl}(\mathcal{O}_K)$ est appelé le *nombre de classes* du corps de nombres K et est noté h_K. Le groupe $\mathrm{Cl}(\mathcal{O}_K)$ est engendré par les idéaux premiers de norme inférieure à M_K.

Corollaire 3.11 — *Si K est un corps de nombres de degré > 1, alors il existe un nombre premier qui se ramifie dans K.*

Démonstration. On a $|D_K| > 1$ d'après le corollaire précédent et tout diviseur premier de $|D_K|$ se ramifie dans K en vertu du théorème 2.14. □

Les résultats précédents fournissent une méthode de calcul du groupe $\mathrm{Cl}(\mathcal{O}_K)$:

1) déterminer tous les idéaux premiers de $\mathcal{O}_K$ de norme inférieure à M_K en factorisant les nombres premiers inférieurs à M_K ; on obtient ainsi un ensemble de générateurs du groupe $\mathrm{Cl}(\mathcal{O}_K)$;
2) déterminer les relations entre ces générateurs en factorisant des éléments de $\mathcal{O}_K$ dont la norme est un produit de nombres premiers inférieurs à M_K.

En pratique, ces calculs ne sont envisageables que pour un corps de nombres de petit degré et petit discriminant...

Exemples de calcul du groupe $\mathrm{Cl}(\mathcal{O}_K)$

(i) $K = \mathbf{Q}(\alpha)$ avec $\alpha^3 - \alpha - 1 = 0$.
Posons $f = T^3 - T - 1$. On a $D_K = -\mathrm{N}(f'(\alpha)) = -23$, donc $r_1 = r_2 = 1$ car $r_1 \geqslant 1$ et $(-1)^{r_2} = -1$. On en déduit

$$M_K = \frac{3!}{3^3}\left(\frac{4}{\pi}\right)\sqrt{23} \simeq 1,36 < 2.$$

Chaque classe dans $\mathrm{Cl}(\mathcal{O}_K)$ contient un idéal entier de norme inférieure à 1, donc contient $\mathcal{O}_K$. Ainsi, $\mathrm{Cl}(\mathcal{O}_K) = \{1\}$ et l'anneau $\mathcal{O}_K$ est principal.

(ii) $K = \mathbf{Q}(\sqrt{-65})$, $\mathcal{O}_K = \mathbf{Z}[\sqrt{-65}] \simeq \mathbf{Z}[T]/(T^2 + 65)$.

1. Si l'on pose $a_n = n^n/n!$, alors $a_{n+1}/a_n = (1 + \frac{1}{n})^n = e^{n\ln(1+1/n)} \geqslant e^{1-1/2n}$, donc $a_{n+1}/a_n \geqslant 2$ et $a_n \geqslant 2^{n-2} a_2 = 2^{n-1}$ pour tout $n \geqslant 2$. Comme par ailleurs $a_1 = 1$, on obtient $a_n \geqslant 2^{n-1}$ pour tout $n \geqslant 1$.

On a $D_K = -4 \times 65$, donc

$$M_K = \frac{2!}{2^2}\left(\frac{4}{\pi}\right)\sqrt{4 \times 65} = \frac{4}{\pi}\sqrt{65} \simeq 10,26 < 11$$

et le groupe $\mathrm{Cl}(\mathcal{O}_K)$ est ainsi engendré par les idéaux premiers de norme inférieure à 10.

En utilisant la proposition 2.12, il vient :

$(2) = \mathfrak{p}_2^2$, avec $\mathfrak{p}_2 = (2, 1 + \sqrt{-65})$

$(3) = \mathfrak{p}_3\mathfrak{p}_3'$ avec $\mathfrak{p}_3 = (3, 1 + \sqrt{-65})$ et $\mathfrak{p}_3' = (3, -1 + \sqrt{-65}) \sim \mathfrak{p}_3^{-1}$

$(5) = \mathfrak{p}_5^2$, avec $\mathfrak{p}_5 = (5, \sqrt{-65})$

(7) est premier, car

$$\left(\frac{-65}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{7}{5}\right) = \left(\frac{2}{5}\right) = -1.$$

Le groupe $\mathrm{Cl}(\mathcal{O}_K)$ est donc engendré par $\mathfrak{p}_2, \mathfrak{p}_3$ et $\mathfrak{p}_5$.

Nous avons déjà obtenu les relations $\mathfrak{p}_2^2 \sim \mathfrak{p}_5 \sim 1$. Nous allons maintenant chercher à en établir d'autres en calculant la norme de quelques éléments de $\mathcal{O}_K$.

Comme $\mathrm{N}(4 + \sqrt{-65}) = 81 = 3^4$, nous pouvons écrire $(4 + \sqrt{-65}) = \mathfrak{p}_3^a{\mathfrak{p}_3'}^b$ avec $a + b = 4$. On observe que $4 + \sqrt{-65}$ n'appartient pas à $\mathfrak{p}_3'$ (cet idéal contiendrait sinon le nombre premier 5), donc $b = 0$ et $a = 4$. On en déduit la relation :

$$\mathfrak{p}_3^4 \sim 1.$$

On a $\mathrm{N}(5 + \sqrt{-65}) = 90 = 2 \cdot 3^2 \cdot 5$ et $5 + \sqrt{-65} \notin \mathfrak{p}_3$ (sinon $4 \in \mathfrak{p}_3$), donc $(5 + \sqrt{-65}) = \mathfrak{p}_2{\mathfrak{p}_3'}^2\mathfrak{p}_5$ et $\mathfrak{p}_5 \sim \mathfrak{p}_2\mathfrak{p}_3^{-2}$. On en déduit que $\mathrm{Cl}(\mathcal{O}_K)$ est engendré par $\mathfrak{p}_2$ et $\mathfrak{p}_3$, vérifiant les relations

$$\mathfrak{p}_2^2 \sim \mathfrak{p}_3^4 \sim 1.$$

Si $\mathfrak{p}_3^2 \sim 1$, alors $\mathfrak{p}_3^2 = (x + y\sqrt{-65})$ avec $x, y \in \mathbf{Z}$ et $x^2 + 65y^2 = \mathrm{N}(\mathfrak{p}_3)^2 = 9$, donc $(x, y) = (\pm 3, 0)$ et $\mathfrak{p}_3^2 = (3) = \mathfrak{p}_3{\mathfrak{p}_3}'$; comme $\mathfrak{p}_3' \neq \mathfrak{p}_3$, ceci est exclu.

Vérifions enfin que (la classe de) $\mathfrak{p}_2$ n'appartient pas au sous-groupe engendré par (la classe de) $\mathfrak{p}_3$. Supposons qu'il existe $i \in \{0, 1, 2, 3\}$ tel que $\mathfrak{p}_2 \sim \mathfrak{p}_3^i$, c'est-à-dire tel que $\mathfrak{p}_3^i = x\mathfrak{p}_2$ avec $x \in K^\times$. Si $d \in \mathbf{Z}_{\geqslant 1}$ est un dénominateur de x, on en déduit l'identité

$$d^2 \cdot 3^i = \mathrm{N}(dx) \cdot 2$$

dans $\mathbf{Z}$ (prendre les normes), ce qui est absurde du point de vue de la valuation 2-adique.

Au final, nous sommes donc parvenus à expliciter le groupe $\mathrm{Cl}(\mathcal{O}_K)$:

$$\mathrm{Cl}(\mathcal{O}_K) = \langle \mathfrak{p}_2 \rangle \times \langle \mathfrak{p}_3 \rangle \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}.$$

(iii) $K = \mathbf{Q}(\zeta_8)$, $\mathcal{O}_K = \mathbf{Z}[\zeta_8] \simeq \mathbf{Z}[T]/(\Phi_8)$, avec $\Phi_8 = T^4 + 1$. On a $D_K = 2^8 = 256$, donc

$$M_K = \frac{4!}{4^4}\left(\frac{4}{\pi}\right)^2\sqrt{256} = \frac{4!}{\pi^2} \simeq 2,42 < 3.$$

Le groupe $\mathrm{Cl}(\mathcal{O}_K)$ est engendré par les idéaux premiers de norme 2.

On a $(2) = \mathfrak{p}_2^4$ avec $\mathfrak{p}_2 = (2, 1+\zeta_8)$. Comme $1+\zeta_8$ divise 2 dans $\mathbf{Z}[\zeta_8]$ en evertu de l'identité $\mathrm{N}(1 + \zeta_8) = \Phi_8(-1) = 2$, l'idéal $\mathfrak{p}_2$ est principal. On en déduit que le groupe $\mathrm{Cl}(\mathbf{Z}[\zeta_8])$ est trivial et donc que l'anneau $\mathbf{Z}[\zeta_8]$ est principal.

3.3 Formes quadratiques binaires et groupes des classes

Gauss a mis en évidence un lien remarquable entre les idéaux fractionnaires d'un corps quadratique et les formes quadratiques binaires à coefficients entiers, ce qui fournit une méthode puissante d'étude du groupe des classes des corps quadratiques.

Définition 3.12 — *Un* discriminant fondamental *est un nombre entier D qui est le discriminant d'un corps quadratique.*

On caractérise aisément les discriminants fondamentaux : ce sont les nombres entiers D distincts de 1 et tels que

$$D \equiv 1 \pmod 4 \quad \text{et} \quad D \text{ est sans facteur carré}$$

ou

$$D \equiv 0 \pmod 4 \quad \text{et} \quad D/4 \text{ est sans facteur carré et } D/4 \equiv 2, 3 \pmod 4.$$

Une *forme quadratique* binaire est une application de la forme

$$q : \mathbf{Z}^2 \to \mathbf{Z}, \quad (x, y) \mapsto ax^2 + bxy + cy^2$$

avec $a, b, c \in \mathbf{Z}$. Les entiers a, b et c sont uniquement déterminés par q :

$$a = q(1, 0),\ c = q(0, 1) \ \text{ et } \ a + b + c = q(1, 1).$$

On note souvent (a, b, c) la forme q ainsi définie. La forme (a, b, c) est dite *primitive* si $\operatorname{pgcd}(a, b, c) = 1$.

Le *discriminant* de q est l'entier

$$\operatorname{disc}(q) = b^2 - 4ac.$$

Exercice — Vérifier que le discriminant d'une forme binaire non nulle q s'écrit toujours sous la forme

$$\operatorname{disc}(q) = D_0 f^2,$$

où f est un nombre entier strictement positif et D_0 est un discriminant fondamental.

On dit qu'une forme q *représente* un entier n s'il existe $(x, y) \in \mathbf{Z}^2 \backslash \{(0, 0)\}$ tel que $q(x, y) = n$. On dit que q *représente primitivement* n si l'on peut de plus choisir x et y premiers entre eux.

Si q est une forme quadratique binaire et $M \in \mathrm{M}_2(\mathbf{Z})$, alors l'application

$$\mathbf{Z}^2 \to \mathbf{Z}, \quad (x, y) \mapsto q((x, y)\ {}^t M)$$

est encore une forme quadratique binaire, notée $q \cdot M$. Deux formes q_1, q_2 sont *équivalentes* s'il existe $P \in \mathrm{GL}_2(\mathbf{Z})$ tel que $q_2 = q_1 \cdot P$; on note alors $q_1 \sim q_2$. Ces formes sont dites *proprement équivalentes* s'il existe $P \in \mathrm{SL}_2(\mathbf{Z})$ tel que $q_2 = q_1 \cdot P$; on note alors $q_1 \overset{+}{\sim} q_2$.

Remarques — (i) Comme $\operatorname{disc}(q \cdot M) = (\det M)^2 \operatorname{disq}(q)$ pour tout $M \in \mathrm{M}_2(\mathbf{Z})$, deux formes équivalentes ont le même discriminant.

(ii) Deux formes équivalentes q et q' représentent les mêmes entiers ; plus précisément, les ensembles $q^{-1}(\{m\})$ et ${q'}^{-1}(\{m\})$ sont en bijection pour tout entier $m \in \mathbf{Z}$.

(iii) Si q est une forme primitive et $q' \sim q$, alors q' est primitive (exercice).

Lemme 3.13 (Équivalence élémentaire) — *Pour tous $a, b, c \in \mathbf{Z}$, on a*

$$(a, b, c) \sim (a, -b, c)$$

et

$$(a, b, c) \overset{+}{\sim} (c, -b, a) \overset{+}{\sim} (a, b + 2a, c + b + a) \overset{+}{\sim} (a, b - 2a, c - b + a)$$

Démonstration. On vérifie immédiatement les identités

$$(a, b, c) \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = (a, -b, c)$$

et

$$(a, b, c) \cdot \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = (c, -b, a), \quad (a, b, c) \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = (a, b + 2a, a + b + c).$$

□

Remarque — Le groupe $\mathrm{SL}_2(\mathbf{Z})$ étant engendré par les matrices $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, l'équivalence propre est engendrée par les équivalences élémentaires. Il en va de même pour l'équivalence puis le groupe $\mathrm{GL}_2(\mathbf{Z})$ est engendré par $\mathrm{SL}_2(\mathbf{Z})$ et la matrice

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Lemme 3.14 — *Soit q une forme de discriminant D.*

(i) *q représente 0 si et seulement si D est un carré.*

(ii) *Tous les entiers représentés par q sont de même signe si et seulement si $D \leqslant 0$.*

Démonstration. Soit $q = (a, b, c)$.

Si $a = 0$, alors q représente 0 et $D = b^2$; de plus, $q(x, y) = bxy + cy^2$ est de signe constant si et seulement si $b = 0$, donc si et seulement si $D \leqslant 0$.

Supposons maintenant $a \neq 0$. En écrivant

$$4aq(x, y) = (2ax + by)^2 - Dy^2$$

On observe que q représente 0 si et seulement si D est un carré dans $\mathbf{Q}$, donc dans $\mathbf{Z}$. Si $D \leqslant 0$, alors $q(x, y)$ est du signe de a pour tout $(x, y) \in \mathbf{Z}^2$; réciproquement, si q est de signe constant, alors D est nécessairement négatif puisque

$$q(1, 0) = a \quad \text{et} \quad q(b, -2a) = -aD.$$

□

Définition 3.15 — *Soit D un discriminant fondamental et soit $K = \mathbf{Q}(\sqrt{D})$ l'unique corps quadratique de discriminant D.*

(i) *On désigne par $\mathcal{F}(D)$ l'ensemble des formes quadratiques binaires de discriminant D. Si $D < 0$, on désigne par $\mathcal{F}^+(D)$ le sous-ensemble de $\mathcal{F}(D)$ formé des formes* définies positives*, c'est-à-dire les formes (a, b, c) telles que $a > 0$.*

(ii) *Posons* $\mathrm{Cl}(D) = \mathrm{Cl}(\mathcal{O}_K)$. *Si* $D > 0$, *on désigne par* $\mathrm{Cl}^+(D)$ *le groupe des classes* au sens restreint *: il s'agit du quotient du groupe* $I(K)$ *des idéaux fractionnaires de* $\mathcal{O}_K$ *par le sous-groupe* $\mathrm{P}^+(K)$ *des idéaux principaux engendrés par les éléments de* norme positive.

Étant donné un corps quadratique K, nous poserons

$$\alpha_K = \begin{cases} \frac{D_K}{2} & \text{si } \mathrm{D}_K \equiv 0 \pmod 4 \\ \frac{1+\sqrt{D_K}}{2} & \text{si } D_K \equiv 1 \pmod 4. \end{cases}$$

Nous utiliserons la description suivante des idéaux de K.

Lemme 3.16 — *Soit* K *un corps quadratique. Tout idéal non nul* $\mathfrak{a}$ *de* $\mathcal{O}_K$ *s'écrit de manière unique sous la forme*

$$\mathfrak{a} = \mathbf{Z} + (b + c\alpha_K)\mathbf{Z}$$

avec $a \in \mathbf{Z}_{>1}$, $0 \leqslant b < a$, $c > 0$ *et* $c|a$, $c|b$. *L'entier* a *est le plus petit entier positif contenu dans* $\mathfrak{a}$ *et* $ac = \mathrm{N}(\mathfrak{a})$.

Démonstration. L'anneau quotient $\mathcal{O}_K/\mathfrak{a}$ étant fini, le noyau du morphisme canonique $\mathbf{Z} \to \mathcal{O}_K/\mathfrak{a}$ est un idéal non nul, engendré par un nombre entier $a > 1$ et $a|\mathrm{N}(\mathfrak{a}) = (\mathcal{O}_K : \mathfrak{a})$. Le groupe $\mathfrak{a}/\mathbf{Z}a$ est libre de rang 1, donc il existe $b \in \mathbf{Z}$ et $c \in \mathbf{Z}_{>0}$ tels que

$$\mathfrak{a} = \mathbf{Z}a + (b + c\alpha_K)\mathbf{Z}.$$

On peut bien évidemment supposer b dans $\{0, \ldots, a-1\}$. La condition $a\alpha_K \in \mathfrak{a}$ implique $c|a$ et, comme $\alpha_K^2 \in \mathbf{Z} + \alpha_K$, la condition $\alpha_K(b + c\alpha_K) \in \mathfrak{a}$ implique $c|b + c$, donc $c|b$. On a enfin

$$\mathrm{N}(\mathfrak{a}) = (\mathcal{O}_K : \mathfrak{a}) = |\det_{(1,\alpha_K)}(a, b + c\alpha_K)| = |ac| = ac.$$

L'unicité de a et c est manifeste ; celle de b s'en déduit immédiatement. □

Il est plus commode de traiter séparément les discriminants positifs et négatifs.

1) Le cas $D < 0$.

Soit $\mathfrak{H}$ le demi-plan supérieur, formé des nombres complexes de partie imaginaire strictement positive. On définit une action (à gauche) de $\mathrm{SL}_2(\mathbf{Z})$ sur $\mathfrak{H}$ en posant

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \cdot z = \frac{\alpha z + \beta}{\gamma z + \delta}$$

pour tout $z \in \mathfrak{H}$ et toute matrice $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z})$. Il est utile d'observer que l'action des générateurs standard de $\mathrm{SL}_2(\mathbf{Z})$:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot z = z + 1 \quad \text{et} \quad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \cdot z = -\frac{1}{z}.$$

Exercice — Vérifier que l'on a effectivement défini une action à gauche de $\mathrm{SL}_2(\mathbf{Z})$ sur $\mathfrak{H}$.

Convenons de désigner par $\sqrt{D}$ la racine carrée de D dans $\mathbf{C}$ de partie imaginaire *positive*. Étant donné une forme quadratique binaire $q = (a, b, c) \in \mathcal{F}^+(D)$, posons

$$\tau(q) = \frac{-b + \sqrt{D}}{2a}.$$

C'est un élément de $\mathfrak{H}$ tel que, pour tout $(x,y) \in \mathbf{Z}^2$,

$$\begin{aligned} q(x,y) &= ax^2+bxy+cy^2 \\ &= a\left(x^2+\frac{b}{a}xy+\frac{c}{a}y^2\right) \\ &= a(x-\tau(q)y)(x-\overline{\tau(q)}y) \end{aligned}$$

Lemme 3.17 — *Pour toute forme quadratique binaire $q \in \mathcal{F}^+(D)$ et toute matrice $M \in \mathrm{SL}_2(\mathbf{Z})$,*

$$\tau(q \cdot M) = M^{-1} \cdot \tau(q).$$

Démonstration. Il suffit de vérifier cette identité pour des générateurs de $\mathrm{SL}_2(\mathbf{Z})$. Posant $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, il vient

$$\tau((a,b,c)\cdot T) = \tau((a,b+2a,a+b+c)) = \frac{-b-2a+\sqrt{D}}{2a} = \tau(q)-1 = T^{-1}\cdot\tau(q)$$

ainsi que

$$\tau((a,b,c)\cdot S) = \tau((c,-b,a)) = \frac{b+\sqrt{D}}{2c}$$

et

$$S\cdot\tau(q) = \frac{2a}{b-\sqrt{D}} = \frac{2a(b+\sqrt{D})}{b^2-D} = \frac{2a(b+\sqrt{D})}{4ac} = \frac{b+\sqrt{D}}{2c} = \tau(S.(a,b,c)).$$

□

Lemme 3.18 — *Soit $q=(a,b,c) \in \mathcal{F}^+(D)$. Le sous-groupe $\mathfrak{a} = \mathbf{Z}a + \mathbf{Z}a\tau(q)$ de K est un idéal fractionnaire de norme a et*

$$q(x,y) = \frac{1}{\mathrm{N}(\mathfrak{a})}\mathrm{N}_{K/\mathbf{Q}}(xa - ya\tau(q)).$$

Démonstration. L'anneau $\mathcal{O}_K$ est un $\mathbf{Z}$-module libre de base $(1,\alpha_K)$, où

$$\alpha_K = \begin{cases} \frac{\sqrt{D}}{2} & \text{si } D \equiv 0 \pmod 4 \\ \frac{1+\sqrt{D}}{2} & \text{si } D \equiv 1 \pmod 4. \end{cases}$$

Si $D \equiv 0 \pmod 4$, alors $b^2 = D+4ac \equiv 0 \pmod 4$, donc $2|b$ et

$$a\tau(q) = \frac{-b}{2} + \frac{\sqrt{D}}{2} \in \mathbf{Z} + \alpha_K.$$

Si $D \equiv 1 \pmod 4$, alors $b^2 = D+4ac \equiv 1 \pmod 4$, donc $2 \nmid b$ et

$$a\tau(q) = -\frac{b+1}{2} + \frac{1+\sqrt{D}}{2} \in \mathbf{Z} + \alpha_K.$$

On en déduit

$$a\alpha_K \in a\tau(q) + a\mathbf{Z} \subset \mathfrak{a} \quad \text{et} \quad a\tau(q)\alpha_K \in (a\tau(q))^2 + a\tau(q)\mathbf{Z} = ac + a\tau(q)\mathbf{Z} \subset \mathfrak{a},$$

ce qui prouve que $\mathfrak{a}$ est un idéal de $\mathcal{O}_K$. On a

$$\mathrm{N}(\mathfrak{a}) = (\mathcal{O}_K : \mathfrak{a}) = |\det_{(1,\alpha_K)}(a, a\tau(q))| = \begin{vmatrix} a & * \\ 0 & 1 \end{vmatrix} = a$$

et, pour tout $(x, y) \in \mathbf{Z}^2$,

$$\frac{1}{\mathrm{N}(\mathfrak{a})}\mathrm{N}_{K/\mathbf{Q}}(xa - ya\tau(q)) = \frac{1}{a}(xa - ya\tau(q))(xa - ya\overline{\tau(q)}) = a(x - \tau(q)y)(x - \overline{\tau(q)}y) = q(x, y).$$

□

Le lemme précédent nous permet de définir l'application

$$\Phi : \mathcal{F}(\mathcal{D}) \to \mathrm{I}(K), \quad q = (a, b, c) \mapsto \mathbf{Z}a + \mathbf{Z}a\tau(q).$$

Posant comme précédemment $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, on déduit du lemme 3.17 les identités

$$\Phi(q \cdot T) = \mathbf{Z}a + \mathbf{Z}a(\tau(q) - 1) = \Phi(q)$$

et

$$\Phi(q \cdot S) = \mathbf{Z}c - \mathbf{Z}\frac{c}{\tau(q)} = \frac{c}{a\tau(q)}\left(\mathbf{Z}a\tau(q) + \mathbf{Z}a\right) = \frac{c}{\tau(q)}\Phi(q),$$

donc Φ induit par passage au quotient une application

$$\varphi : \mathcal{F}^+(D)/\mathrm{SL}_2(\mathbf{Z}) \to \mathrm{Cl}(D).$$

Partons maintenant d'un idéal fractionnaire $\mathfrak{a}$ dans K. Il s'agit d'un $\mathbf{Z}$-module de rang 2 dont on peut choisir une base (ω_1, ω_2) *directe* relativement à l'orientation de K définie par la base $(1, \alpha_K)$. Posons

$$q_{\omega_1,\omega_2}(x, y) = \frac{1}{\mathrm{N}(\mathfrak{a})}\mathrm{N}_{K/\mathbf{Q}}(x\omega_1 - y\omega_2) = \frac{1}{\mathrm{N}(\mathfrak{a})}\left(\mathrm{N}(\omega_1)x^2 + (\omega_1\overline{\omega_2} - \overline{\omega_1}\omega_2)xy + \mathrm{N}(\omega_2)y^2\right).$$

On a

$$\mathrm{N}(\mathfrak{a})|\mathrm{N}(u)$$

pour tout $u \in \mathfrak{a}$ puisqu'alors $(u) = \mathfrak{a}\mathfrak{b}$ avec $\mathfrak{b} = (u)\mathfrak{a}^{-1} \subset \mathcal{O}_K$ et

$$|\mathrm{N}(u)| = \mathrm{N}(\mathfrak{a})\mathrm{N}(\mathfrak{b}) \in \mathrm{N}(\mathfrak{a})\mathbf{Z}$$

donc q_{ω_1,ω_2} est une forme quadratique binaire définie positive. On a

$$q_{z\omega_1,z\omega_2} = q_{\omega_1,\omega_2}$$

pour tout $z \in K^\times$ car $\mathrm{N}_{K/\mathbf{Q}}(z) = \mathrm{N}((z))$ par positivité de la norme, donc nous pouvons supposer $\mathfrak{a} \subset \mathcal{O}_K$ pour calculer le discriminant de q_{ω_1,ω_2}. Sous cette hypothèse, si l'on désigne par M la matrice des coordonnées de $(\omega_1, -\omega_2)$ dans la base $(1, -\alpha_K)$ de $\mathcal{O}_K$, il vient

$$q_{\omega_1,\omega_2}(x, y) = \frac{1}{\mathrm{N}(\mathfrak{a})}q_{1,\alpha_K}((x, y)\ {}^tM),$$

donc

$$\mathrm{disc}(q_{\omega_1,\omega_2}) = \mathrm{N}(\mathfrak{a})^{-2}\det(M)^2\mathrm{disc}(q_{1,\alpha_K}) = \mathrm{disc}(q_{1,\alpha_K})$$

puisque $|\det(M)| = (\mathcal{O}_K : \mathfrak{a}) = \mathrm{N}(\mathfrak{a})$; finalement, puisque

$$q_{1,\alpha_K}(x,y) = \mathrm{N}_{K/\mathbf{Q}}(x-\alpha_K y) = (x-\alpha_K y)(x-\overline{\alpha_K} y) = \begin{cases} x^2 - \frac{D}{4}y^2 & \text{si } D \equiv \pmod 4 \\ x^2 - xy + \frac{1-D}{4}y^2 & \text{si } D \equiv 1 \pmod 4 \end{cases}$$

est une forme de discriminant D, nous obtenons

$$\mathrm{disc}(q_{\omega_1,\omega_2}) = D.$$

Si (ω_1', ω_2') est une autre $\mathbf{Z}$-base directe de $\mathfrak{a}$, alors

$$q_{\omega_1',\omega_2'} = q_{\omega_1,\omega_2} \cdot M$$

avec $M = \mathrm{Mat}_{(\omega_1,-\omega_2)}(\omega_1', -\omega_2') \in \mathrm{SL}_2(\mathbf{Z})$.

Ce qui précède nous permet de définir une application

$$\psi : \mathrm{Cl}(D) \to \mathcal{F}^+(D).$$

Théorème 3.19 — *Les applications φ et ψ sont des bijections réciproques.*

Démonstration. Soit $q = (a,b,c) \in \mathcal{F}^+(D)$. La $\mathbf{Z}$-base $(a, a\tau(q))$ de l'idéal fractionnaire $\Phi(q) = \mathbf{Z}a + \mathbf{Z}a\tau(q)$ est directe et

$$q(x,y) = \frac{1}{\mathrm{N}(\mathfrak{a})}\mathrm{N}_{K/\mathbf{Q}}(xa - ya\tau(q))$$

pour tout $(x,y) \in \mathbf{Z}$, donc $\psi(\varphi(q)) = q$ dans $\mathcal{F}^+(D)$.

Considérons réciproquement un idéal $\mathfrak{a}$ de $\mathcal{O}_K$, que l'on peut écrire sous la forme $\mathfrak{a} = \mathbf{Z}a + \mathbf{Z}(b + c\alpha_K)$ avec $a \in \mathbf{Z}_{>1}$, $b \in \{0, \ldots, a-1\}$, $c \in \mathbf{Z}_{>0}$, et $c|a, c|b$ (lemme 3.16). On a

$$\mathfrak{a} = c\left(\mathbf{Z}\frac{a}{c} + \mathbf{Z}\left(\left(\frac{b}{c} + \alpha_K\right)y\right)\right.$$

et

$$\frac{b}{c} + \alpha_K = \begin{cases} \frac{2b/c+\sqrt{D}}{2} & \text{si } D \equiv 0 \pmod 4 \\ \frac{2b/c+1+\sqrt{D}}{2} & \text{si } D \equiv 1 \pmod 4 \end{cases}$$

donc $\mathfrak{a} = c\ \Phi(q)$, avec

$$q = \begin{cases} (a/c, -2b/c, (4b^2 - Dc^2)/4ac) & \text{si } D \equiv 0 \pmod 4 \\ q = (a/c, -2b/c + 1, (4b^2 - 4bc + (1-D)c^2)/4ac) & \text{si } D \equiv 1 \pmod 4. \end{cases}$$

et

$$\varphi(\psi(\mathfrak{a})) = \mathfrak{a}$$

dans $\mathrm{Cl}(D)$. □

Remarque — Les bijections du théorème précédent associent à la classe triviale dans $\mathrm{Cl}(D)$ la classe d'équivalence propre de la forme quadratique binaire

$$q_{1,\alpha_K}(x,y) = \mathrm{N}_{K/\mathbf{Q}}(x - y\alpha_K) = \begin{cases} x^2 - \frac{D}{4}y^2 & \text{si } D \equiv 0 (\mathrm{mod}\ 4) \\ x^2 - xy + \frac{1-D}{4}y^2 & \text{si } D \equiv 1 (\mathrm{mod}\ 4). \end{cases}$$

appelée *forme principale* de discriminant D.

Définition 3.20 — *Une forme quadratique binaire définie positive (a,b,c) de discriminant D est dite* réduite *si $|b| \leqslant a \leqslant c$ et si de plus $b \geqslant 0$ lorsque l'une des deux inégalités est une égalité.*

Proposition 3.21 — *(i) Chaque classe d'équivalence propre de formes quadratiques binaires définies positives de discriminant D contient une unique forme réduite.*

(ii) *Il n'y a qu'un nombre fini de formes réduites dans* $\mathcal{F}^+(D)$.

(iii) *Le nombre de classes du corps quadratique imaginaire* $\mathbf{Q}(\sqrt{D})$ *est égal au nombre de formes réduites de discriminant* D.

Démonstration. (i) Soit $q = (a,b,c) \in \mathcal{F}^+(D)$. Si $c < a$, alors $q \overset{+}{\sim} (a',b',c') = (c,-b,a)$ et $|a'|+|b'| = |b|+|c| < |a|+|b|$. Si $b \notin]-|a|,|a|]$, alors $q \overset{+}{\sim} (a',b',c') = (a, b \pm 2a, c+a \pm b)$ et $|a'|+|b'| < |a|+|b|$. En particulier, si l'on choisit q dans sa classe d'équivalence propre telle que le nombre entier positif $|a|+|b|$ soit minimal, alors q est réduite.

Supposons maintenant que $q = (a,b,c)$ soit réduite. On a $q(x,0) = ax^2 \geqslant a$ (avec égalité ssi $x = \pm 1$),

$$4aq(x,\pm 1) = (2ax \pm b)^2 - D \geqslant b^2 - D = 4ac, \quad \text{donc} \quad q(x,\pm 1) \geqslant c$$

(avec égalité ssi $x(ax \pm b) = 0$, i.e. $x = 0$ ou $(x,y) = \pm(1,-1)$ si $b = |a|$) et

$$4aq(x,y) = (2ax+by)^2 - Dy^2 \geqslant -Dy^2 \geqslant -4D, \quad \text{donc } aq(x,y) \geqslant -D \geqslant 3ac \quad \text{et } q(x,y) > c$$

pour tous $x \in \mathbf{Z}$ et $y \in \mathbf{Z}$ avec $|y| \geqslant 2$. Ainsi, a est le plus petit entier non nul représenté par q et, si $a < c$, alors c est la deuxième plus petite valeur non nulle de q. En outre, l'équation $q(x,y) = a$ a exactement

- deux solutions $\pm(1,0)$ si $a < c$;
- quatre solutions $\pm(1,0), \pm(0,1)$ si $a = c > |b|$;
- six solutions $\pm(1,0), \pm(0,1), \pm(1,-1)$ si $a = c = |b|$.

De même, si $a < c$, l'équation $q(x,y) = c$ a exactement

- deux solutions $\pm(0,1)$ si $|b| < a$;
- quatre solutions $\pm(0,1), \pm(1,-1)$ si $|b| = a$.

Considérons deux formes réduites proprement équivalentes $q = (a,b,c)$ et $q' = (a',b',c')$, avec $q' = q \cdot M$, $M \in \mathrm{SL}_2(\mathbf{Z})$. Ces formes représentent les mêmes entiers le même nombre de fois, donc $a' = a$.

Si $a < c$, alors $(1,0)\,{}^tM = \pm(1,0)$ et donc $M = \pm \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}$. On a de même $a' < c'$ et $c' = c$, donc $m = 0$ et $b' = b$ si $|b| < a$. Si $|b| = a$, alors $|b'| = a'$ et donc $b' = b$ car $b'^2 = b^2$ et $b', b \geqslant 0$.

Si $a = c$, alors $a' = c'$ puisque l'équation $q'(x,y) = a'$ admet alors au moins quatre solutions et donc $c' = c$. On en déduit $b'^2 = b^2$, donc $b' = b$ puisque $b', b \geqslant 0$.

(ii) Si $q = (a,b,c)$ est une forme réduite de discriminant D, alors $4a^2 \leqslant 4ac = b^2 - D \leqslant a^2 - D$, donc

$$|b| \leqslant a \leqslant \sqrt{|D|/3} \quad \text{et } c = (b^2-D)/4a \leqslant \frac{a^2-D}{4} \leqslant \frac{|D|}{3}.$$

(iii) C'est une conséquence immédiate du théorème 3.19 et des deux précédentes assertions. □

Remarques — (i) Jointe au théorème 3.19, les deux premières assertions de cette proposition fournissent une nouvelle démonstration de la finitude du groupe des classes d'un corps quadratique imaginaire.

(ii) Le sous-espace

$$\mathcal{D} = \left\{ z \in \mathfrak{H} \mid -\frac{1}{2} \leqslant \mathfrak{Re}(z) < \frac{1}{2} \text{ et } |z| > 1 \right\} \cup \left\{ z \in \mathfrak{H} \mid -\frac{1}{2} \leqslant \mathfrak{Re}(z) \leqslant 0 \text{ et } |z| = 1 \right\}$$

est un *domaine fondamental* pour l'action de $\mathrm{SL}_2(\mathbf{Z})$: chaque orbite rencontre $\mathcal{D}$ en exactement un point. Dire qu'une forme quadratique binaire définie négative q est réduite équivaut à dire que le nombre complexe $\tau(q)$ appartient à $\mathcal{D}$.

La proposition précédente fournit une méthode de calcul du nombre de classes du corps quadratique imaginaire $\mathbf{Q}(\sqrt{D})$: il suffit de compter les formes réduites de discriminant D. En écrivant explicitement les idéaux fractionnaires associés à ces dernières, nous pouvons également en déduire des générateurs du groupe des classes.

Exemples. (i) $D = -20$

Toute forme réduite (a, b, c) de discriminant -20 est telle que $a \leqslant \sqrt{20/3} < 3$.

Si $a = 1$, alors $-1 < b \leqslant 1$ et $2|b$, donc $b = 0$ et $c = 5$. Nous avons obtenu la forme réduite $q_1 = (1, 0, 5)$.

Si $a = 2$, alors $-2 < b \leqslant 2$ et $2|b$, donc $b \in \{0, 2\}$. Comme $b^2 - 8c = -20$, on obtient $b = 2$ et $c = 3$, ce qui nous fournit la seconde forme réduite $q_2 = (2, 2, 3)$.

Le groupe des classes du corps quadratique imaginaire est donc d'ordre 2. Les idéaux associés à q_1 et q_2 sont

$$\Phi(q_1) = \mathbf{Z} + \mathbf{Z}\frac{1+\sqrt{-5}}{2} = \mathcal{O}_{\mathbf{Q}(\sqrt{-5})}$$

et

$$\Phi(q_2) = \mathbf{Z}2 + \mathbf{Z}(-1+\sqrt{-5}).$$

Le premier définit la classe triviale, le second fournit un générateur du groupe des classes.

(ii) $D = -11$

Les formes réduites de discriminant -11 sont telles que $a \leqslant \sqrt{1633} < 8$. En calculant b^2+163 pour $b \in \{0, \ldots, 7\}$, on observe que ce nombre n'est divisible par 4 que si $b \in \{1, 3, 5, 7\}$ et alors $(b^2 + 163)/4$ est premier. Cela impose $a = 1$, donc $b = 1$ et $c = 41$; il n'y a donc qu'une seule forme réduite de discriminant -163. On en déduit que l'anneau $\mathbf{Z}\left[\frac{1+\sqrt{-163}}{2}\right]$ est principal.

(iii) $D = -23$

Considérons les idéaux $\mathfrak{a} = (3, \alpha - 1)$ et $\mathfrak{b} = (13, \alpha - 4)$ avec $\alpha = \frac{1+\sqrt{-23}}{2}$.

La forme quadratique binaire associée à $\mathfrak{a}$ muni de la base $(3, \alpha)$ est

$$q_{3,\alpha-1}(x, y) = \frac{1}{3}\mathrm{N}(3x - \alpha y) = \frac{1}{3}(9x^2 - 3xy + 6y^2) = 3x^2 - xy + 2y^2,$$

donc $q = q_{3,\alpha-1} = (3, -1, 2)$.

La forme quadratique binaire associée à $\mathfrak{b}$ muni de la base $(13, \alpha + 4)$ est

$$q_{13,\alpha+4}(x, y) = \frac{1}{13}\mathrm{N}(13x - (\alpha + 4)y) = \frac{1}{13}((13)^2x^2 - (13 \times 9)xy + 26y^2) = 13x^2 - 9xy + 2y^2,$$

donc $q' = q_{13,\alpha+4} = (13, -9, 2)$.

On réduit aisément les formes q et q' :

$$q = (3, -1, 2) \overset{+}{\sim} (2, 1, 3)$$

et

$$q' = (13, -9, 2) \overset{+}{\sim} (2, 9, 13) \overset{+}{\sim} (2, 5, 6) \overset{+}{\sim} (2, 1, 3),$$

donc q et q' sont proprement équivalentes. On en déduit que les idéaux $\mathfrak{a}$ et $\mathfrak{b}$ définissent la même classe dans $\mathrm{Cl}(-23)$. Il est facile de voir qu'il existe exactement trois formes réduites de discriminant -23 (à savoir $(2, 1, 3)$, $(2, -1, 3)$ et $(1, 1, 6)$), donc

$$\mathrm{Cl}(-23) \simeq \mathbf{Z}/3\mathbf{Z}.$$

2) Le cas $D > 0$

Comme toujours, on désigne par $\sqrt{D}$ la racine carrée *positive* de D dans $\mathbf{R}$. La forme quadratique binaire $\mathrm{N}_{K/\mathbf{Q}}(x + y\alpha_K)$ étant de discriminant $D > 0$, elle prend des valeurs positives et négatives ; en particulier, nous pouvons fixer un élément λ de $\mathcal{O}_K^\times$ tel que $N_{K/\mathbf{Q}}(\lambda) < 0$.

Le groupe $\mathrm{SL}_2(\mathbf{Z})$ opère sur $\mathbf{R} \setminus \mathbf{Q}$ via

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \cdot x = \frac{\alpha x + \beta}{\gamma x + \delta}.$$

Étant donnée une forme binaire $q = (a, b, c) \in \mathcal{F}(D)$, posons encore $\tau(q) = \frac{-b+\sqrt{D}}{2a}$ et

$$\Phi(q) = \lambda^{\varepsilon(a)}(\mathbf{Z}a + \mathbf{Z}\tau(q))$$

avec $\varepsilon(a) = (1 - \mathrm{sgn}(a))/2$. On vérifie comme précédemment qu'il s'agit d'un idéal de $\mathcal{O}_K$ de norme $\mathrm{N}_{K/\mathbf{Q}}(\lambda)^{\varepsilon(a)}a$ et tel que

$$q(x, y) = \frac{1}{\mathrm{N}(\Phi(q))}\mathrm{N}_{K/\mathbf{Q}}\left(xa\lambda^{\varepsilon(a)} - y\tau(q)\lambda^{\varepsilon(a)}\right)$$

pour tout $(x, y) \in \mathbf{Z}^2$.

Composée par la projection canonique de $\mathrm{I}(K)$ sur $\mathrm{Cl}^+(D)$, l'application Φ induit une application

$$\varphi : \mathcal{F}^+(D) \to \mathrm{Cl}^+(D)$$

en vertu des identités

$$\Phi(q \cdot T) = \Phi(q)$$

et

$$\Phi(q \cdot S) = \lambda^{\varepsilon(c)-\varepsilon(a)}\frac{c}{\tau(q)}\Phi(q)$$

et φ ne dépend *pas* du choix de λ.

Réciproquement, si $\mathfrak{a}$ est un idéal fractionnaire de $\mathcal{O}_K$ muni d'une base (ω_1, ω_2) directe par rapport à $(1, \alpha_K)$, alors

$$q_{\omega_1,\omega_2}(x, y) = \frac{1}{\mathrm{N}(\mathfrak{a})}\mathrm{N}_{K/\mathbf{Q}}(x\omega_1 - y\omega_2)$$

est une forme binaire de discriminant D (même vérification que précédemment). On a

$$q_{\omega_1',\omega_2'} = q_{\omega_1,\omega_2} \cdot \mathrm{Mat}_{(\omega_1,-\omega_2)}(\omega_1', -\omega_2')$$

si (ω_1', ω_2') est une autre base directe de $\mathfrak{a}$ et

$$q_{z\omega_1,z\omega_2} = \mathrm{sgn}(\mathrm{N}_{K/\mathbf{Q}}(z))q_{\omega_1,\omega_2}$$

pour tout $z \in K^\times$, donc nous obtenons par passage au quotient une application

$$\psi : \mathrm{Cl}^+(D) \to \mathcal{F}(D)/\mathrm{SL}_2(\mathbf{Z}).$$

Théorème 3.22 — *Les applications φ et ψ sont des bijections réciproques.*

Démonstration. Identique à celle du théorème 3.19. □

On démontre comme dans le cas imaginaire que chaque classe d'équivalence propre dans $\mathcal{F}(D)$ contient au moins une forme $q = (a, b, c)$ telle que

$$|b| \leqslant |a| \leqslant |c|$$

et qu'il n'existe qu'un nombre fini de telles formes dans $\mathcal{F}(D)$ puisqu'alors $|b| \leqslant |a| \leqslant \sqrt{D/3}$. On en déduit que le groupe $\mathrm{Cl}^+(D)$ est *fini*, et donc également le groupe $\mathrm{Cl}(\mathcal{O}_{\mathbf{Q}(\sqrt{D})})$ qui en est un quotient. Cependant, il n'y a en général pas unicité de la forme « réduite » dans une classe d'équivalence propre donnée et la situation est donc plus compliquée que dans le cas imaginaire. Pour plus de détails, on pourra consulter le chapitre 5 de [1].

3.4 Le groupe des unités d'un corps de nombres

Soit K un corps de nombres. Le groupe des unités de K est le groupe $\mathcal{O}_K^\times$ des éléments inversibles de $\mathcal{O}_K$; il est formé des éléments $x \in \mathcal{O}_K$ tels que $\left|\mathrm{N}_{K/\mathbf{Q}}(x)\right| = 1$. L'objectif principal de cette section est l'élucidation de la structure de ce groupe.

Théorème 3.23 (Dirichlet) — *Soit K un corps de nombres ayant r_1 plongements réels et r_2 paires de plongements complexes non réels conjugués.*

Le groupe $\mathcal{O}_K^\times$ des de type fini. Son sous groupe de torsion $\mu(K)$ est fini et cyclique, formé des racines de l'unité dans K, et le groupe $\mathcal{O}_K^\times/\mu(K)$ est libre de rang $r = r_1 + r_2 - 1$. Il existe donc r unités multiplicativement indépendantes $\varepsilon_1, \ldots, \varepsilon_r$ telles que

$$\mathcal{O}_K^\times = \mu(K) \times \varepsilon_1^{\mathbf{Z}} \cdot \ldots \cdot \varepsilon_r^{\mathbf{Z}}.$$

Notons $\sigma_1, \ldots, \sigma_{r_1}$ les plongements réels de K et $\sigma_{r_1+1}, \overline{\sigma_{r_1+1}}, \ldots, \sigma_{r_1+r_2}, \overline{\sigma_{r_1+r_2}}$ ses plongements complexes non réels. On sait que l'application

$$\Phi : K \to \mathbf{R}^r \oplus \mathbf{C}^{r_2}$$

identifie $\mathcal{O}_K$ à un réseau du $\mathbf{R}$-espace vectoriel $V = \mathbf{R}^{r_1} \oplus \mathbf{C}^{r_2}$, de covolume $2^{-r_2}|D_K|^{1/2}$. Soit $N : V \to \mathbf{R}$ l'application définie par

$$N(x_1, \ldots, x_{r_1}, z_1, \ldots, z_{r_2}) = x_1 \ldots x_{r_1} z_1 \overline{z_1} \ldots z_{r_2} \overline{z_{r_2}}.$$

On a $N \circ \Phi = \mathrm{N}_{K/\mathbf{Q}}$ et le sous-ensemble $G = \{v \in V \mid |N(v)| = 1\}$ est un sous-groupe de $V^\times = (\mathbf{R}^\times)^{r_1} \times (\mathbf{C}^\times)^{r_2}$ contenant $\Phi(\mathcal{O}_K^\times)$.

Proposition 3.24 — *(i) Pour chaque entier $k \geqslant 1$, les $a \in \mathcal{O}_K$ tels que $|N_{K/\mathbf{Q}}(a)| = k$ se répartissent en un nombre fini d'orbites sous $\mathcal{O}_K^\times$.*

(ii) Le groupe $G/\Phi(\mathcal{O}_K^\times)$ est compact pour la topologie quotient.

Démonstration. (i) Si $\left|N_{K/\mathbf{Q}}(a)\right| = k$, alors $(\mathcal{O}_K : a\mathcal{O}_K) = k$ et donc $k\mathcal{O}_K \subset a\mathcal{O}_K \subset \mathcal{O}_K$. L'anneau $\mathcal{O}_K/k\mathcal{O}_K$ étant fini, il n'existe qu'un nombre fini d'idéaux principaux $a_1\mathcal{O}_K, \ldots, a_m\mathcal{O}_K$ contenant $k\mathcal{O}_K$. Si a est un élément de $\mathcal{O}_K$ tel que $\left|\mathrm{N}_{K/\mathbf{Q}}(a)\right| = k$, alors il existe un indice $i \in \{1, \ldots, m\}$ tel que $a\mathcal{O}_K = a_i\mathcal{O}_K$ et donc $a = a_i\varepsilon$ avec $\varepsilon \in \mathcal{O}_K^\times$.

(ii) Comme $\Phi(\mathcal{O}_K)$ est une partie discrète de V, le sous-espace $\Phi(\mathcal{O}_K^\times)$ est également discret, donc fermé, et le quotient $G/\Phi(\mathcal{O}_K^\times)$ est par conséquent séparé. Fixons une partie convexe compacte et symétrique C dans V volume $\geqslant 2^{r_1+2r_2}\mathrm{covol}(\Phi(\mathcal{O}_K))$. Pour tout $g \in G$, la multiplication par g est un automorphisme linéaire de V de déterminant ± 1, donc $g^{-1}C$ est une partie

convexe compacte et symétrique de même volume que C. En vertu du théorème de Minkowski, il existe donc a dans $\mathcal{O}_K \setminus \{0\}$ tel que $\Phi(a) \in g^{-1}C$.

On a $\left|\mathrm{N}_{K/\mathbf{Q}}(a)\right| = |N(\Phi(a))| \in |N(g^{-1}C)| = |N(C)|$ et $|N(C)|$ est une partie bornée de $\mathbf{R}$ puisque C est compact ; comme $\mathrm{N}_{K/\mathbf{Q}}$ est à valeurs entières sur $\mathcal{O}_K$, $\left|\mathrm{N}_{K/\mathbf{Q}}(a)\right|$ parcourt un ensemble fini. En vertu du point (i), il existe donc une partie finie $\mathcal{F}$ de $\mathcal{O}_K \setminus \{0\}$ telle que chaque partie $g^{-1}C$ rencontre $\Phi(\mathcal{F}\mathcal{O}_K^\times)$, ou encore telle que chaque partie $g\Phi(\mathcal{O}_K^\times)$ rencontre

$$\widetilde{C} = \bigcup_{a \in \mathcal{F}} \Phi(a)^{-1}C.$$

Le sous-espace $\widetilde{C}$ de V est compact, donc $G \cap \widetilde{C}$ l'est également puis G est fermé dans V. L'espace topologique $G/\Phi(\mathcal{O}_K^\times)$ est séparé et image continue d'un compact, donc il est compact. □

Démonstration du théorème 3.23.

Considérons l'application

$$L : V^\times \to \mathbf{R}^{r_1+r_2}, \quad (x_1, \dots, x_{r_1}, z_1, \dots, z_{r_2}) \mapsto (\log|x_1|, \dots, \log|x_{r_1}|, 2\log|z_1|, \dots, 2\log|z_{r_2}|).$$

C'est un homomorphisme de groupes continu et surjectif tel que $G = L^{-1}(H)$, où

$$H = \{(y_1, \dots, y_{r_1+r_2}) \in \mathbf{R}^{r_1+r_2} \mid \sum_{i=1}^{r_1+r_2} y_i = 0\}.$$

(a) L'image du sous-groupe $\Phi(\mathcal{O}_K^\times)$ de G est un *réseau* dans H.

Tout d'abord, $L(\Phi(\mathcal{O}_K^\times))$ est une partie discrète de H car, pour tout nombre réel $R > 0$, l'ensemble

$$\{a \in \mathcal{O}_K^\times \mid |\sigma_i(a)| \leqslant e^R \text{ pour } 1 \leqslant i \leqslant r_1,\ |\sigma_i(a)| \leqslant e^{R/2} \text{ pour } r_1+1 \leqslant i \leqslant r_1+r_2\}$$

est fini car contenu dans l'ensemble

$$\{v \in \Phi(\mathcal{O}_K \mid |v_i| \leqslant e^R \text{ pour } 1 \leqslant i \leqslant r_1 \text{ et } |v_i| \leqslant e^{R/2} \text{ si } r_1+1 \leqslant i \leqslant r_1+r_2\}$$

qui est discret et borné, donc fini.

Ensuite, L induit une application continue et surjective

$$G/\Phi(\mathcal{O}_K^\times) \to H/L(\Phi(\mathcal{O}_K^\times))$$

donc $H/L(\Phi(\mathcal{O}_K^\times))$ est compact en vertu du point (ii) de la proposition précédente.

(b) Notons Ψ l'homomorphisme de groupes $\mathcal{O}_K^\times \to \mathbf{R}^{r_1+r_2}$ induit par $L \circ \Phi$. L'application Φ réalise une bijection entre $\mathrm{Ker}\ \Psi$ et l'intersection de $\Phi(\mathcal{O}_K)$ avec le sous-espace $\mathrm{Ker}\ L = \{\pm 1\}^{r_1} \times (\mathrm{S}^1)^{r_2} \subset V$, donc $\mathrm{Ker}\ \Psi$ est fini puisque $\Phi(\mathcal{O}_K)$ est discret et $\mathrm{Ker}\ L$ est compact.

L'inclusion $\mu(K) \subset \mathrm{Ker}\ \Psi$ est claire puisque $\mathbf{R}^{r_1+r_2}$ est sans torsion. Tout sous-groupe fini du groupe multiplicatif d'un corps étant cyclique et formé de racines de l'unité, $\mathrm{Ker}\ \Psi = \mu(K)$ est cyclique.

(c) Nous avons obtenu une suite exacte de groupes abéliens

$$1 \longrightarrow \mu(K) \longrightarrow \mathcal{O}_K^\times \xrightarrow{\Psi} \Psi(\mathcal{O}_K^\times) \longrightarrow 1$$

et $\Psi(\mathcal{O}_K^\times)$ est libre de rang r_1+r_2-1 puisqu'il s'agit d'un réseau de $H \simeq \mathbf{R}^{r_1+r_2-1}$. □

Remarques — (i) On a vérifié facilement que $\Psi(\mathcal{O}_K^\times)$ est un sous-groupe discret de H. La difficulté principale du théorème 3.23 consiste à établir l'existence de $r_1 + r_2 - 1$ unités multiplicativement indépendantes, ce que l'on a fait en établissant la compacité de $H/\Psi(\mathcal{O}_K^\times)$.

(ii) Si K admet un plongement réel, c'est-à-dire si $r_1 \neq 0$, alors $\mu(K) = \{\pm 1\}$.

Exemples. (i) Si $K = \mathbf{Q}(\sqrt{2})$, alors $(r_1, r_2) = (2, 0)$, $\mathcal{O}_K = \mathbf{Z}[\sqrt{2}]$ et $\mu(K) = \{\pm 1\}$. Notons σ_1 et σ_2 les deux plongements réels de K, avec $\sigma_1(\sqrt{2}) = \sqrt{2}$ et $\sigma_2(\sqrt{2}) = -\sqrt{2}$.

Puisque $\mathrm{N}_{K/\mathbf{Q}(\sqrt{2})}(1 + \sqrt{2}) = -1$, l'élément $\varepsilon = 1 + \sqrt{2}$ de $\mathcal{O}_K$ est une unité ; nous allons démontrer qu'il s'agit d'une *unité fondamentale*, c'est-à-dire d'un générateur de $\mathcal{O}_K^\times/\mu(K)$. Soit $u \in \mathcal{O}_K^\times$ une unité fondamentale et écrivons $\varepsilon = \pm u^k$ avec $k \in \mathbf{Z} \setminus \{0\}$; quitte à remplacer u par u^{-1}, nous pouvons supposer $k \geqslant 1$.

Si $k \geqslant 2$, alors

$$|\sigma_1(u)| = |\sigma_1(\varepsilon)|^{1/k} = (1 + \sqrt{2})^{1/k} \leqslant (1 + \sqrt{2})^{1/2} < 1,6$$

et

$$|\sigma_2(u)| = |\sigma_2(\varepsilon)|^{1/k} = (\sqrt{2} - 1)^{1/k} < 1.$$

En représentant graphiquement le réseau $\Phi(\mathcal{O}_K) = \mathbf{Z}(1, 1) + \mathbf{Z}(\sqrt{2}, -\sqrt{2})$ dans $\mathbf{R}^2$, on observe que la partie de $\mathbf{R}^2$ définie par les conditions $|y_1| \leqslant 1,6$ et $|y_2| < 1$ ne contient pas de point de $\Phi(\mathcal{O}_K)$ autre que 0 et il est donc impossible que k soit supérieur à 2. Nous obtenons ainsi $k = 1$ et $\varepsilon = \pm u$ est bien une unité fondamentale.

(ii) Soit $K = \mathbf{Q}(\alpha)$ avec $f_{\alpha,\min} = f = T^3 - 3T - 1$. On a $\mathrm{disc}(f) = 81 = 3^4$ et $f(1 + T)$ est d'Eisenstein en 3, donc $\mathcal{O}_K = \mathbf{Z}[\alpha]$ (Proposition 1.14 et Corollaire A.3). La constante de Minkowski de ce corps de nombres est $M_K = 3!/3^3\sqrt{D_K} = 2$, donc $\mathrm{Cl}(\mathcal{O}_K)$ est engendré par les idéaux premiers de norme inférieure à 2. Comme f est irréductible modulo 2, l'idéal (2) est premier et il n'existe donc pas d'idéal premier de norme 2 ; par conséquent, le groupe $\mathrm{Cl}(\mathcal{O}_K)$ est trivial et l'anneau $\mathbf{Z}[\alpha]$ est donc principal.

Pour construire des unités, nous pouvons chercher à exhiber des éléments de norme ± 1 dans $\mathcal{O}_K$. Il est facile de le faire à partir de l'identité $\mathrm{N}_{K/\mathbf{Q}}(a\alpha + b) = -a^3 f(-b/a)$, avec $a \in \mathbf{Z} \setminus \{0\}$ et $b \in \mathbf{Z}$. On trouve en particulier

$$\mathrm{N}_{K/\mathbf{Q}}(\alpha) = \mathrm{N}_{K/\mathbf{Q}}(\alpha + 1) = \mathrm{N}_{K/\mathbf{Q}}(\alpha - 2) = 1 \quad \text{et} \quad \mathrm{N}_{K/\mathbf{Q}}(2\alpha + 3) = -1,$$

donc $\alpha, \alpha + 1, \alpha - 2, 2\alpha + 3 \in \mathcal{O}_K^\times$. On vérifie par ailleurs que f est scindé sur K, de racines $\alpha, 2 - \alpha^2$ et $\alpha^2 - \alpha - 2$, et ces dernières sont des unités puisque leur produit est égal à 1 ; ceci nous donne donc deux nouvelles unités.

Numérotons les trois plongements réels de K de telle sorte que l'on ait $\sigma_1(\alpha) < \sigma_2(\alpha) < \sigma_3(\alpha)$ et considérons l'application

$$\Psi : \mathcal{O}_K^\times \to H = \{(y_1, y_2, y_3) \in \mathbf{R}^3 \mid y_1 + y_2 + y_3 = 0\}, \quad x \mapsto (\log\ |\sigma_1(x)|, \log\ |\sigma_2(x)|, \log\ |\sigma_3(x)|)$$

introduite au cours de la preuve du théorème de Dirichlet. En utilisant

$$\sigma_1(\alpha) \approx -1,532, \quad \sigma_2(\alpha) \approx -0,347 \quad \text{et} \quad \sigma_3(\alpha) \approx 1,879,$$

nous obtenons les approximations suivantes

	$\log\ \lvert\sigma_1\rvert$	$\log\ \lvert\sigma_2\rvert$	$\log\ \lvert\sigma_3\rvert$
α	$0,426...$	$-1,058...$	$0,631...$
$\alpha - 2$	$1,262...$	$0,853...$	$-2,112...$
$\alpha + 1$	$-0,631...$	$-0,426...$	$1,057...$
$2\alpha + 3$	$-2,749...$	$0,836...$	$1,911...$
$2 - \alpha^2$	$-1,058...$	$0,631...$	$0,426...$

Ces données suggèrent les identités

$$\Psi(\alpha-2) = -2\Psi(\alpha+1), \text{ donc } \alpha-2 = \pm(\alpha+1)^{-2}$$

$$2\Psi(\alpha) - 3\Psi(\alpha+1) + \Psi(2\alpha+3) = 0, \text{ donc } 2\alpha+3 = \pm\alpha^{-2}(\alpha+1)^3$$

et

$$\Psi(2-\alpha^2) = \Psi(\alpha+1) - \Psi(\alpha), \text{ donc } 2-\alpha^2 = \pm\alpha^{-1}(\alpha+1).$$

On établit sans difficulté chacune des trois égalités de droite, par exemple

$$(\alpha+1)^2(\alpha-2) = \alpha^3 - 3\alpha - 2 = -1, \quad \text{donc } \alpha-2 = -(\alpha+1)^{-2}.$$

Il semble se dégager de ces calculs que α et $\alpha+1$ engendrent $\mathcal{O}_K^\times/\mu(K)$. On peut au moins s'assurer que ces deux unités sont multiplicativement indépendantes : comme

$$\begin{vmatrix} \log\ |\sigma_1(\alpha)| & \log\ |\sigma_2(\alpha)| \\ \log\ |\sigma_1(\alpha+1)| & \log\ |\sigma_2(\alpha+1)| \end{vmatrix} \approx \begin{vmatrix} 0,426 & -1,058 \\ -0,631 & -0,426 \end{vmatrix} = 0,426$$

les deux vecteurs $\Psi(\alpha)$ et $\Psi(\alpha+1)$ sont linéairement indépendants et donc α et $\alpha+1$ sont multiplicativement indépendants.

(iii) Soit $K = \mathbf{Q}(\sqrt{257})$. On a $(r_1, r_2) = (2, 0)$, $\mu(K) = \{\pm 1\}$ et $\mathcal{O}_K = \mathbf{Z}[\alpha]$ avec $\alpha = (1+\sqrt{257})/2$ et $f_{\alpha,\min} = T^2 - T - 64$.

Nous allons illustrer sur cet exemple le lien étroit entre la détermination du groupe des classes et celle du groupe des unités. La borne de Minkowski de K est

$$M_K = \frac{2!}{2^2}\sqrt{257} \approx 8,01$$

donc $\mathrm{Cl}(\mathcal{O}_K)$ est engendré par les idéaux premiers de norme au plus 8. On a

$$(2) = \mathfrak{p}_2\mathfrak{p}_2', \quad \text{avec } \mathfrak{p}_2 = (2, \alpha) \text{ et } \mathfrak{p}_2' = (2, \alpha+1)$$

tandis que les idéaux $(3), (5)$ et (7) sont premiers puisque

$$\left(\frac{257}{3}\right) = \left(\frac{2}{3}\right) = -1, \quad \left(\frac{257}{5}\right) = \left(\frac{2}{5}\right) = -1 \quad \text{et} \quad \left(\frac{257}{7}\right) = \left(\frac{5}{7}\right) = -1.$$

Le groupe des classes de K est donc engendré par (la classe de) $\mathfrak{p}_2$.

On a $\mathrm{N}_{K/\mathbf{Q}}(\alpha-8) = f(8) = -8$ et $\mathrm{N}_{K/\mathbf{Q}}(\alpha-9) = 8$, donc

$$(\alpha-8) = \mathfrak{p}_2^3 \quad \text{et} \quad (\alpha-9) = \mathfrak{p}_2'^3.$$

On en déduit $\mathfrak{p}_2^3 \sim 1$ dans $\mathrm{Cl}(\mathcal{O}_K)$, donc l'ordre de $\mathfrak{p}_2$ divise 3, et $((\alpha-8)(\alpha-9)) = (\mathfrak{p}_2\mathfrak{p}_2')^3 = 8$, donc

$$\varepsilon = \frac{(\alpha-8)(\alpha-9)}{8} = 16 - \sqrt{257}$$

est une unité de $\mathcal{O}_K$.

Il reste à déterminer si $\mathfrak{p}_2$ est, ou non, principal. Pour ce faire, on pourrait songer à prouver que l'équation

$$x^2 - xy - 64y^2 = |\mathrm{N}_{K/\mathbf{Q}}(x+y\alpha)| = \mathrm{N}(\mathfrak{p}_2) = 2$$

n'admet pas de solution ; ce n'est malheureusement pas très évident... Nous allons plutôt exploiter le groupe des unités de K.

On vérifie comme dans l'exemple (i) que ε est une unité fondamentale de K.

Raisonnons par l'absurde en supposant que $\mathfrak{p}_2$ soit principal, engendré par un élément γ de $\mathcal{O}_K$. On a alors $(\gamma^3) = \mathfrak{p}_2^3 = (\alpha - 8)$, donc il existe $k \in \mathbf{Z} \setminus \{0\}$ tel que

$$\alpha - 8 = \varepsilon^k \gamma^3$$

avec $k \in \mathbf{Z} \setminus \{0\}$. En particulier, cette identité montre que $\alpha - 8$ appartient au sous-groupe engendré par ε modulo les cubes. Pour rendre cette observation effective, nous allons réduire cette identité modulo l'idéal $\mathfrak{a} = (5)\mathfrak{p}_{13}$, avec $\mathfrak{p}_{13} = (13, \alpha + 3)$. Comme $\alpha - 8 \in \mathfrak{p}_2$ est premier à $\mathfrak{a}$, cet élément est inversible modulo $\mathfrak{a}$. On a

$$(\mathcal{O}_K/\mathfrak{a})^\times \simeq (\mathcal{O}_K/5\mathcal{O}_K)^\times \times (\mathcal{O}_K/\mathfrak{p}_{13})^\times \simeq \mathbf{F}_{25}^\times \times \mathbf{F}_{13}^\times$$

et

$$\mathbf{F}_{25}^\times/(\mathbf{F}_{25})^3 \simeq (\mathbf{F}_{25})^8 = \{1, -\alpha, \alpha^2\}, \quad \mathbf{F}_{13}^\times/(\mathbf{F}_{13}^\times)^3 \simeq (\mathbf{F}_{13})^4 = \{1, 3, 9\}.$$

Comme

$$(\alpha - 8)^8 \equiv (\alpha + 2)^8 \equiv (\alpha^2 - \alpha - 1)^4 \equiv (-2)^4 \equiv 1 \pmod 5,$$
$$\varepsilon^8 = (17 - 2\alpha)^8 \equiv 2^8((1 - \alpha)^8 \equiv (\alpha^2 - 2\alpha + 1)^4 \equiv (-\alpha)^4 \equiv -\alpha \pmod 5,$$
$$(\alpha - 8)^4 \equiv (-3 - 8)^4 \equiv 2^4 \equiv 3 \pmod{\mathfrak{p}_{13}}$$

et

$$\varepsilon^4 = (17 - 2\alpha)^4 \equiv (-3)^4 \equiv 81 \equiv 3 \pmod{\mathfrak{p}_{13}}$$

le morphisme de groupes

$$(\mathcal{O}_K/\mathfrak{a})^\times \to \mathbf{F}_{25}^\times/(\mathbf{F}_{25}^\times)^3 \times \mathbf{F}_{13}^\times/(\mathbf{F}_{13}^\times)^3 \simeq \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$$

envoie $\alpha - 8$ sur $(0, 1)$ et ε sur $(1, 1)$. Ceci prouve que $\alpha - 8$ n'appartient pas à $\varepsilon^{\mathbf{Z}} \cdot (\mathcal{O}_K)^3$ et donc que l'idéal $\mathfrak{p}_2$ n'est *pas* principal.

Nous sommes finalement parvenus à identifier le groupe des classes de K :

$$\mathrm{Cl}(\mathcal{O}_K) = \langle \mathfrak{p}_2 \rangle \simeq \mathbf{Z}/3\mathbf{Z}.$$

Définition 3.25 — *Soit K un corps de nombres admettant r_1 plongements réels $\sigma_1, \ldots, \sigma_{r_1}$ et r_2 plongements complexes non réels $\sigma_{r_1+1}, \overline{\sigma_{r_1+1}}, \ldots, \sigma_{r_1+r_2}, \overline{\sigma_{r_1+r_2}}$. Le* régulateurs *de K est le nombre réel*

$$R_K = \frac{1}{\sqrt{r_1 + r_2}} \mathrm{covol}(\Psi(\mathcal{O}_K^\times))$$

où $\Psi : \mathcal{O}_K^\times \to H = \{(y_1, \ldots, y_{r_1+r_2}) \in \mathbf{R}^{r_1+r_2} \mid \sum_i y_i = 0\}$ est l'application définie par

$$\Psi(x) = (\log|\sigma_1(x)|, \ldots, \log|\sigma_{r_1}(x), 2\log|\sigma_{r_1+1}(x), \ldots, 2\log|\sigma_{r_1+r_2}(x)|)$$

et l'espace vectoriel H est muni de la structure euclidienne induite par celle de $\mathbf{R}^{r_1+r_2}$.

Remarque — Si $r_1 + r_2 = 1$, alors $K = \mathbf{Q}$ ou K est quadratique imaginaire et $R_K = 1$.

Proposition 3.26 (Méthode de calcul) —*Soit K un corps de nombres, $\sigma_1, \ldots, \sigma_{r_1}$ ses plongements réels et $\sigma_{r_1+1}, \ldots, \sigma_{r_1+r_2}$ des représentants de ses plongements complexes non réels modulo conjugaison. Soit $\varepsilon_1, \ldots, \varepsilon_r$ des unités relevant une base de $\mathcal{O}_K^\times/\mu(K)$. On a*

$$R_K = |\det(\log||\sigma_i(\varepsilon_j)||)_{i \in I,\ 1 \leqslant j \leqslant r}|$$

où I est l'ensemble $\{1,\dots,r_1+r_2\}$ privé d'un élément et

$$||\sigma_i(\cdot)|| = \begin{cases} |\sigma_i(\cdot)| & \text{si } 1 \leqslant i \leqslant r_1 \\ |\sigma_i(\cdot)|^2 & \text{si } r_1+1 \leqslant i \leqslant r_1+r_2. \end{cases}$$

Démonstration. Soit ξ le vecteur $\frac{1}{\sqrt{r+1}}(1,\dots,1) \in \mathbf{R}^{r+1}$, unitaire et orthogonal à l'hyperplan H. On a

$$\begin{aligned} \mathrm{covol}_H(\Psi(\mathcal{O}_K^\times)) &= \mathrm{covol}_{\mathbf{R}^{r+1}}(\mathbf{Z}\xi + \Psi(\mathcal{O}_K^\times)) \\ &= \left| \det \begin{pmatrix} 1/\sqrt{r+1} & \log\ ||\sigma_1(\varepsilon_1)|| & \dots & \log\ ||\sigma_1(\varepsilon_r)|| \\ \vdots & \vdots & & \vdots \\ 1/\sqrt{r+1} & \log\ ||\sigma_r(\varepsilon_1)|| & \dots & \log\ ||\sigma_r(\varepsilon_r)|| \end{pmatrix} \right| \\ &= \left| \det \begin{pmatrix} 1/\sqrt{r+1} & \log\ ||\sigma_1(\varepsilon_1)|| & \dots & \log\ ||\sigma_1(\varepsilon_r)|| \\ \vdots & & \vdots & \\ \sqrt{r+1} & 0 & & 0 \\ 1/\sqrt{r+1} & \log\ ||\sigma_r(\varepsilon_1)|| & \dots & \log\ ||\sigma_r(\varepsilon_r)|| \end{pmatrix} \right| \\ &= \sqrt{r_1+r_2}\,|\det(\log\ ||\sigma_i(\varepsilon_j)||)| \end{aligned}$$

en remplaçant la ligne d'indice $i \notin I$ par la sommes des lignes. □

Exemple. Si K est tel que $r_1+r_2-1=1$ (i.e. $(r_1,r_2)=(2,0),(1,1)$ ou $(0,2)$), alors $\mathcal{O}_K^\times = \mu(K)\times\varepsilon^{\mathbf{Z}}$ et

$$R_K = |\log\ ||\sigma(\varepsilon)|||\,,$$

où σ est n'importe quel plongement de K dans $\mathbf{C}$.

Nous obtenons en particulier

$$\mathrm{R}_{\mathbf{Q}(\sqrt{2})} = \log\,(1+\sqrt{2}) \approx 0,881$$

et

$$\mathrm{R}_{\mathbf{Q}(\sqrt{257})} = |\log\,(\sqrt{257}-16)| \approx 3,467.$$

Application : l'équation de Pell-Fermat

Étant donné $d \in \mathbf{Z}_{>0}$, considérons l'équation diophantienne $X^2 - dY^2 = 1$. Si d est un carré, disons $d=\delta^2$ avec $\delta \in \mathbf{Z}_{>0}$, alors cette équation s'écrit $(X-\delta Y)(X+\delta Y)=1$ et donc $x-\delta y = x+\delta y$ pour toute solution (x,y) dans $\mathbf{Z}^2$; on en déduit $y=0$ et $x=\pm 1$.

Théorème 3.27 (Lagrange) — *Soit $d \in \mathbf{Z}_{>0}$ non carré. L'équation de Pell-Fermat $X^2-dY^2=1$ admet une solution fondamentale (x_1,y_1) dans $\mathbf{Z}_{>0}\times\mathbf{Z}_{>0}$ telle que toutes les autres solutions soient de la forme $(\pm x_n, \pm y_n)$, où $n \in \mathbf{Z}$ et*

$$x_n + y_n\sqrt{d} = (x_1+y_1\sqrt{d})^n.$$

Démonstration. Les solutions entières de l'équation de Pell-Fermat $X^2-dY^2=1$ sont en bijection avec les éléments de norme 1 dans l'anneau $\mathbf{Z}[\sqrt{d}]$. Posons $K=\mathbf{Q}(\sqrt{d})$. Il découle de l'inclusion $\mathbf{Z}[\sqrt{d}] \subset \mathcal{O}_K$ que $\mathbf{Z}[\sqrt{d}]^\times$ est un sous-groupe d'indice fini de $\mathcal{O}_K^\times$; en vertu du théorème de Dirichlet, il existe donc $\varepsilon = u+v\sqrt{d} \in \mathbf{Z}[\sqrt{d}]^\times$ tel que

$$\mathbf{Z}[\sqrt{d}]^\times = \{\pm 1\}\times\varepsilon^{\mathbf{Z}}.$$

Si $\mathrm{N}_{K/\mathbf{Q}}(\varepsilon) = 1$, alors $\mathrm{N}_{K/\mathbf{Q}}(\eta) = 1$ pour tout $\eta \in \mathbf{Z}[\sqrt{d}]^\times$ et il suffit de poser $(x_1, y_1) = (|u|, |v|)$. Si $\mathrm{N}_{K/\mathbf{Q}}(\varepsilon) = -1$, alors $\mathrm{N}_{K/\mathbf{Q}}(\pm\varepsilon^k) = 1$ si et seulement si $2|k$; écrivant $\varepsilon^2 = s + t\sqrt{d}$, il suffit de poser $(x_1, y_1) = (|s|, |t|)$. □

La théorie des *fractions continues* fournit un algorithme permettant de déterminer une solution fondamentale de l'équation de Pell-Fermat, ainsi d'ailleurs que toutes les solutions entières. La raison sous-jacente est que les solutions entières de l'équation $X^2 - dY^2 = \pm 1$ correspondent aux *bonnes* approximations rationnelles de $\sqrt{d}$.

Proposition 3.28 — *Soit $d \in \mathbf{Z}_{>0}$ non carré. Pour tout couple $(x, y) \in \mathbf{Z}_{>0} \times \mathbf{Z}_{>0}$,*

$$x^2 - dy^2 = \pm 1 \iff \left|\frac{x}{y} - \sqrt{d}\right| < \frac{1}{2\sqrt{d}y^2}.$$

Démonstration. Si $x^2 - dy^2 = 1$, alors $x/y > \sqrt{d}$ et

$$0 < \frac{x}{y} - \sqrt{d} = \frac{x^2/y^2 - d}{x/y + \sqrt{d}} < \frac{1}{2\sqrt{d}y^2}.$$

Si $x^2 - dy^2 = -1$, alors

$$-\frac{1}{2\sqrt{d}y^2} < \frac{x}{y} - \sqrt{d} < 0.$$

Réciproquement, si $0 < x/y - \sqrt{d} < 1/2\sqrt{d}y^2$, alors

$$0 < x^2 - dy^2 = y^2\left(\frac{x}{y} - \sqrt{d}\right)\left(\frac{x}{y} - \sqrt{d} + 2\sqrt{d}\right) < \frac{1}{2\sqrt{d}}\left(\frac{1}{2\sqrt{d}y^2} + 2\sqrt{d}\right) < 2$$

et donc $x^2 - dy^2 = 1$ puisqu'il s'agit d'un nombre entier. On vérifie de même que, si $-1/2\sqrt{d}y^2 < x/y - \sqrt{d} < 0$, alors $x^2 - dy^2 = -1$. □

Étant donné $\alpha \in \mathbf{R} \setminus \mathbf{Q}$, on définit deux suites $(a_n) \in \mathbf{Z}^{\mathbf{N}}$ et $(x_n) \in \mathbf{R}^{\mathbf{N}}$ en posant

$$\begin{cases} x_0 = \alpha, \quad a_0 = [\alpha] \\ x_{n+1} = (x_n - a_n)^{-1}, \\ a_{n+1} = [x_{n+1}] \end{cases}$$

Par construction, $a_n \geqslant 1$ pour tout $n \geqslant 1$. Noter également que l'on peut étendre cette définition au cas $\alpha \in \mathbf{Q}$; il existe alors un entier $n_0 \geqslant 0$ tel que $x_{n_0} \in \mathbf{Z}$ et l'on ne définit pas x_n, a_n pour $n > n_0$.

Pour tout $n \in \mathbf{N}$, la fraction

$$\frac{p_n}{q_n} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots + \cfrac{1}{a_n}}}}$$

est la *n-ième réduite* ; on la note $[a_0, \ldots, a_n]$.

Théorème 3.29 — (i) *La suite (p_{2n}/q_{2n}) est croissante et converge vers α. La suite (p_{2n+1}/q_{2n+1}) est décroissante et converge vers α.*

(ii) *Le nombre α est quadratique si et seulement si la suite $(a_n)_{n\geqslant 1}$ est périodique.*

(iii) *Parmi deux réduites consécutives, l'une au moins vérifie*

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{2q_n^2}.$$

(iv) *Réciproquement, si $p \in \mathbf{Z}$ et $q \in \mathbf{Z}_{>0}$ sont tels que $|\alpha - p/q| < 1/2q^2$, alors il existe n tel que $p/q = p_n/q_n$.*

Démonstration. (i) En raisonnant par récurrence, on établit aisément les identités

$$p_{n+1} = a_{n+1}p_n + p_{n-1}, \quad q_{n+1} = a_{n+1}q_n + q_{n-1}$$

et

$$q_n p_{n-1} - p_n q_{n-1} = (-1)^n, \quad q_n p_{n-2} - p_n q_{n-2} = (-1)^{n-1}a_n.$$

On en déduit

$$\frac{p_{n-1}}{q_{n-1}} - \frac{p_n}{q_n} = \frac{(-1)^n}{q_n q_{n-1}} \text{ et } \frac{p_{n-2}}{q_{n-2}} - \frac{p_n}{q_n} = \frac{(-1)^{n-1}a_n}{q_n q_{n-2}}.$$

En observant que $[a_0, a_1, \ldots, a_{n-1}, y]$ est une fonction croissante (resp. décroissante) de y si $2|n$ (resp. $2 \nmid n$), il vient

$$\frac{p_{2n}}{q_{2n}} = [a_0, \ldots, a_{2n}] \leqslant [a_0, \ldots, a_{2n-1}, x_{2n}] = \alpha \leqslant [a_0, \ldots, a_{2n}, a_{2n+1}] = \frac{p_{2n+1}}{q_{2n+1}}$$

puis

$$\frac{p_{2n}}{q_{2n}} < \frac{p_{2n+2}}{q_{2n+2}} < \alpha < \frac{p_{2n+1}}{q_{2n+1}} < \frac{p_{2n-1}}{q_{2n-1}} \text{ et } \left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n q_{n-1}}.$$

(ii) Il s'agit d'un théorème de Lagrange. Pour une démonstration, voir par exemple [2], section 10.12.

(iii) et (iv) Voir [2], section 10.15. □

Corollaire 3.30 — *Soit $d \in \mathbf{Z}_{>0}$ non carré. Si $p, q \in \mathbf{Z}_{>0}$ vérifient $|p^2 - dq^2| < \sqrt{d}$, alors p/q est une réduite de $\sqrt{d}$.*

Démonstration. Supposons tout d'abord $p > q\sqrt{d}$. On a alors

$$|p^2 - dq^2| < \sqrt{d} \Rightarrow \left|\frac{p}{q} - \sqrt{d}\right| < \frac{1}{q^2} \cdot \frac{1}{\frac{p}{q\sqrt{d}} + 1} < \frac{1}{2q^2}$$

et donc p/q est une réduite de $\sqrt{d}$ en vertu du point (iv) du théorème précédent.

Si $p < q\sqrt{d}$, alors

$$|p^2 - dq^2| < \sqrt{d} \Rightarrow \left|\frac{1}{\sqrt{d} - \frac{q}{p}}\right| < \frac{\sqrt{d}}{dp^2} \cdot \frac{1}{\frac{q}{p} + \frac{1}{\sqrt{d}}} = \frac{1}{p^2} \cdot \frac{1}{\frac{q\sqrt{d}}{p} + 1} < \frac{1}{2p^2}$$

et donc q/p est une réduite de $1/\sqrt{d}$.

Si $\sqrt{d} = [a_0, a_1, a_2, \ldots]$, alors $1/\sqrt{d} = [0, a_0, a_1, a_2, \ldots]$; comme

$$[0, a_0, a_1, \ldots, a_n]^{-1} = [a_0, a_1, \ldots, a_n]^{-1},$$

les réduites non nulles de $\frac{1}{\sqrt{d}}$ sont les inverses des réduites de $\sqrt{d}$; en particulier, p/q est bien une réduite de $\sqrt{d}$. □

Nous en déduisons un algorithme de calcul d'une unité fondamentale de $\mathbf{Z}[\sqrt{d}]$: il suffit de déterminer la première réduite p_n/q_n de $\sqrt{d}$ telle que $p_n^2 - dq_n^2 = \pm 1$. De même, pour obtenir une solution fondamentale de l'équation de Pell-Fermat $X^2 - dY^2 = 1$, il suffit de déterminer la première réduite p_n/q_n de $\sqrt{d}$ telle que $p_n^2 - dq_n^2 = 1$.

Remarque — Si $d \equiv 1 \pmod 4$, alors les unités $u + v\frac{1+\sqrt{d}}{4}$ de $\mathcal{O}_{\mathbf{Q}(\sqrt{d})}$ sont paramétrées par les solutions entière de l'équation

$$\mathrm{N}_{\mathbf{Q}(\sqrt{d})/\mathbf{Q}}\left(u + v\frac{1+\sqrt{d}}{2}\right) = u^2 + uv + \frac{1-d}{4}v^2 = \pm 1.$$

Elles sont en bijection avec les solutions entière de l'équation $X^2 - dY^2 = \pm 4$ via l'application $(u, v) \mapsto (2u + v, v)$ (l'application réciproque est $(a, b) \mapsto ((a - b)/2, b)$). Si $4 < \sqrt{d}$, c'est-à-dire si $d \notin \{5, 13\}$, alors le corollaire précédent garantit que nous pouvons obtenir une unité fondamentale de $\mathbf{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ en déterminant la première réduite p_n/q_n de $\sqrt{d}$ telle que $p_n^2 - dq_n^2 = \pm 4$.

Exemples. (i) $d = 2$.

Comme $\sqrt{2} = 1 + x$ avec $0 < x < 1$ et $1/x = 1/(\sqrt{2} - 1) = \sqrt{2} + 1 = 2 + x$, le développement en fraction continue de $\sqrt{2}$ est $[1, \overline{2}]$. On a $p_0/q_0 = 1$, $p_1/q_1 = 3/2$ et $p_0^2 - 2q_0^2 = -1$, $p_1^2 - 2q_1^2 = 1$, donc $\varepsilon = 1 + \sqrt{2}$ est une unité fondamentale de $\mathbf{Z}[\sqrt{2}]$ et $(3, 2)$ est une solution fondamentale de l'équation $X^2 - 2Y^2 = 1$.

(ii) $d = 5$.

En écrivant

$$\sqrt{5} = 2 + (\sqrt{5} - 2) \quad \text{et} \quad \frac{1}{\sqrt{5} - 2} = \sqrt{5} + 2 = 4 + (\sqrt{5} - 2),$$

on obtient $\sqrt{5} = [2, \overline{4}]$. Les premières réduites sont $p_0/q_0 = 2/1$ et $p_1/q_1 = 9/4$; comme $2^2 - 5 = -1$ et $9^2 - 5 \cdot 4^2 = 1$, on en déduit que $\eta = 2 + \sqrt{5}$ est une unité fondamentale de $\mathbf{Z}[\sqrt{5}]$ et que $(9, 4)$ est une solution fondamentale de l'équation de Pell-Fermat $X^2 - 5Y^2 = 1$.

Posons $\varphi = (1 + \sqrt{5})/2$. L'algorithme des fractions continues ne permet pas dans ce cas de déterminer une unité fondamentale de $\mathbf{Z}[\varphi]$ mais, en écrivant

$$\mathrm{N}_{\mathbf{Q}(\sqrt{5})/\mathbf{Q}}(u + v\varphi) = u^2 + uv + v^2,$$

on en obtient immédiatement une en posant $\varepsilon = \varphi$. On observera que l'on a $\varepsilon^3 = \eta$, donc $\mathbf{Z}[\sqrt{5}]^\times$ est un sous-groupe d'indice 3 de $\mathbf{Z}[\varphi]^\times$.

(iii) $d = 7$.

Le développement en fraction continue de $\sqrt{7}$ est $[2, \overline{1, 1, 1, 4}]$ et les premières réduites sont

$$\frac{p_0}{q_0} = \frac{2}{1},\ \frac{p_1}{q_1} = \frac{3}{1},\ \frac{p_2}{q_2} = \frac{5}{2},\ \frac{p_3}{q_3} = \frac{8}{3}.$$

Comme

$$p_0^2 - 7q_0^2 = -3,\ p_1^2 - 7q_1^2 = 2,\ p_2^2 - 7q_2^2 = -3 \text{ et } p_3^2 - 7q_3^2 = 1,$$

on obtient une unité fondamentale de $\mathbf{Z}[\sqrt{7}]$ en posant $\varepsilon = 8 + 3\sqrt{7}$ et $(8, 3)$ est une solution fondamentale de l'équation $X^2 - 7Y^2 = 1$.

(iv) $d = 61$.

Le développement en fraction continue de $\sqrt{61}$ est $[7, \overline{1, 4, 3, 1, 2, 2, 1, 3, 4, 1, 14}]$. On a

$$\frac{p_2}{q_2} = \frac{39}{65} \quad \text{et} \quad 39^2 - 61 \cdot 5^2 = 4,$$

donc $\varepsilon = 17 + 5\frac{1+\sqrt{61}}{2}$ est une unité fondamentale de $\mathbf{Z}[(1 + \sqrt{61})/2]$. Pour obtenir une unité fondamentale de $\mathbf{Z}[\sqrt{61}]$, il faut aller jusqu'à la dixième réduite :

$$\frac{p_{10}}{q_{10}} = \frac{29718}{3805} \quad \text{et} \quad p_{10}^2 - 61q_{10}^2 = -1.$$

En calculant le carré de $29718+3805\sqrt{61}$, on en déduit la plus petite solution entière non triviale de l'équation $X^2 - 61Y^2 = 1$:

$$(x_1, y_1) = (1\ 766\ 319\ 049, 226\ 153\ 980).$$

Chapitre 4

Introduction aux méthodes analytiques

4.1 Séries de Dirichlet, fonction zêta de Riemann

Une *série de Dirichlet* est une série de fonctions de la variable complexe s de la forme

$$f(s) = \sum_{n \geqslant 1} \frac{a_n}{n^s},$$

où les a_n sont des nombres complexes.

Proposition 4.1 — *Si une série de Dirichlet converge pour $s = s_0$, alors elle converge uniformément sur tout cône $s_0 + \left(\mathbf{R}_{\geqslant 0} e^{i\vartheta} + \mathbf{R}_{\geqslant 0} e^{-i\vartheta}\right)$ avec $\vartheta \in [0, \pi/2[$.*

Démonstration. Le changement de variable $\sum a_n n^{-s} = \sum a_n n^{-s_0} n^{-(s-s_0)}$ permet de se ramener au cas $s_0 = 0$; l'hypothèse est alors la convergence de la série $\sum a_n$.

Notons $A_{m,m'}$ la somme partielle $\sum_{n=m}^{m'} a_n$. Soit $\varepsilon > 0$. Il existe un entier $m_0 \geqslant 1$ tel que, pour tous $m' \geqslant m \geqslant m_0$,

$$|A_{m,m'}| \leqslant \varepsilon.$$

En vertu de la transformation d'Abel

$$\sum_{n=m}^{m'} a_n n^{-s} = \sum_{n=m}^{m'-1} A_{m,m'}(n^{-s} - (n+1)^{-s}) + A_{m,m'}(m')^{-s},$$

il vient

$$\left| \sum_{n=m}^{m'} a_n n^{-s} \right| \leqslant \varepsilon \left(\sum_{n=m}^{m'-1} |n^{-s} - (n+1)^{-s}| + |(m')^{-s}| \right)$$

pour tous $m' \geqslant m \geqslant m_0$. Écrivons $s = a + ib$. En observant que l'on a

$$|s| \leqslant ka \quad \text{avec} \quad k = \frac{1}{\cos \vartheta}$$

pour tout s dans le cône $\mathbf{R}_{\geqslant 0} e^{i\vartheta} + \mathbf{R}_{\geqslant 0} e^{-i\vartheta}$, on obtient

$$|n^{-s} - (n+1)^{-s}| = \left| \int_{\log n}^{\log(n+1)} s e^{-st} \, \mathrm{d}t \right| \leqslant k \left| \int_{\log n}^{\log(n+1)} a e^{-at} \, \mathrm{d}t \right| = k(n^{-a} - (n+1)^{-a})$$

et donc

$$\left|\sum_{n=m}^{m'} a_n n^{-s}\right| \leqslant \varepsilon k \left(\sum_{n=m}^{m'-1} (n^{-a} - (n+1)^{-a} + m'^{-a}\right) = \varepsilon k m^{-a} \leqslant k\varepsilon.$$

□

Corollaire 4.2 — *Si la série de Dirichlet converge en s_0, elle converge sur le demi-plan $\mathfrak{Re}(s) > \mathfrak{Re}(s_0)$ et définit sur celui-ci une fonction holomorphe dont les dérivées itérées s'obtiennent en dérivant terme à terme la série initiale.*

Corollaire 4.3 — *Soit $\sum a_n n^{-s}$ une série de Dirichlet. Il existe $\rho \in \mathbf{R} \cup \{\pm\infty\}$ tel que la série diverge si $\mathfrak{Re}(s) < \rho$ et la série converge si $\mathfrak{Re}(s) > \rho$.*

La série de Dirichlet la plus célèbre est la fonction zêta de Riemann

$$\zeta(s) = \sum_{n\geqslant 1} \frac{1}{n^s}.$$

Cette série est convergente sur le demi-plan $\mathfrak{Re}(s) > 1$. Le théorème de factorisation des nombres entiers en produit de facteurs premiers permet d'écrire $\zeta(s)$ comme un produit eulérien

$$\zeta(s) = \prod_p \frac{1}{1 - \frac{1}{p^s}}$$

où le produit porte sur l'ensemble des nombres premiers et est absolument convergent pour $\mathfrak{Re}(s) > 1$. En particulier, la fonction ζ ne s'annule pas sur le demi-plan $\mathfrak{Re}(s) > 1$.

Proposition 4.4 — *La fonction ζ de Riemann admet un prolongement méromorphe sur le demi-plan $\mathfrak{Re}(s) > 0$ ayant un unique pôle, qui est simple, en $s = 1$; son résidu est égal à 1.*

Démonstration. Supposons $\mathfrak{Re}(s) > 1$. En utilisant l'identité

$$\frac{1}{s-1} = \int_1^{+\infty} t^{-s}\, \mathrm{d}t,$$

nous pouvons écrire

$$\zeta(s) = \frac{1}{s-1} + \varphi(s), \quad \text{avec } \varphi(s) = \sum_{n\geqslant 1} \int_n^{n+1} \left(\frac{1}{n^s} - \frac{1}{t^s}\right)\, \mathrm{d}t.$$

Comme

$$\left|\int_n^{n+1} \left(\frac{1}{n^s} - \frac{1}{t^s}\right)\, \mathrm{d}t\right| \leqslant \sup_{n\leqslant t\leqslant n+1} \left|\frac{1}{n^s} - \frac{1}{t^s}\right| \leqslant \frac{|s|}{|n^{s+1}|} = \frac{|s|}{n^{\mathfrak{Re}(s)+1}}$$

la fonction φ est holomorphe sur le demi-plan $\mathfrak{Re}(s) > 0$. □

Remarque — Si l'on pose

$$\xi(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s),$$

avec $\Gamma(s) = \int_0^{+\infty} t^s e^{-t}\, \frac{\mathrm{d}t}{t}$, alors on démontre l'identité $\xi(1-s) = \xi(s)$ pour tout s dans la bande $0\mathfrak{Re}(s) < 1$. Celle-ci permet de prolonger ξ en une fonction méromorphe sur $\mathbf{C}$ tout entier ayant deux pôles, simples, en $s = 0$ et $s = 1$. La fonction Γ admettant un prolongement méromorphe sur $\mathbf{C}$ partout non nul et admettant un pôle simple en chaque entier négatif (déduit de l'équation fonctionnelle $\Gamma(z+1) = z\Gamma(z)$), la fonction ζ elle-même admet un prolongement méromorphe

sur $\mathbf{C}$ tout entier ayant un pôle simple en 1 et un zéro simple en tout entier pair strictement négatif.

Corollaire 4.5 — *Soit $\sum a_n n^{-s}$ une série de Dirichlet.*

(i) *Si la suite (a_n) est bornée, alors la série de Dirichlet converge sur le demi-plan $\mathfrak{Re}(s) > 1$.*

(ii) *Posons $A_N = \sum_{n \leqslant N} a_n$ et supposons qu'il existe $\kappa \in \mathbf{C}$ et $\delta \in]0,1]$ tels que*

$$A_N = \kappa N + \mathrm{O}(N^{1-\delta}).$$

La série de Dirichlet admet alors un prolongement méromorphe sur le demi-plan $\mathfrak{Re}(s) > 1-\delta$, avec au plus un pôle simple, en $s=1$ et de résidu κ.

Démonstration. (i) Il suffit d'observer que l'on a

$$|a_n n^{-s}| = |a_n| n^{-\mathfrak{Re}(s)} = \mathrm{O}(n^{-\mathfrak{Re}(s)}).$$

(ii) Posons $b_n = a_n - \kappa$ et écrivons

$$\sum_{n \geqslant 1} \frac{a_n}{n^s} - \kappa\zeta(s) = \sum_{n \geqslant 1} \frac{b_n}{n^s}.$$

La fonction ζ admettant un prolongement méromorphe sur le demi-plan $\mathfrak{Re}(s) > 0$ ayant un unique pôle, simple, en $s=1$ et de résidu 1, il suffit de prouver que la série de Dirichlet $\sum_{n \geqslant 1} b_n/n^s$ admet un prolongement holomorphe sur le demi-plan $\mathfrak{Re}(s) > 1-\delta$.

Cela se déduit de la transformation d'Abel. En posant $B_n = \sum_{1 \leqslant k \leqslant n} b_k$, il vient, pour $1 < N \leqslant M$,

$$\begin{aligned}\sum_{n=N}^{M} \frac{b_n}{n^s} &= -\frac{B_{N-1}}{(N-1)^s} + \frac{B_M}{M^s} + \sum_{n=N}^{M-1} B_n \left(\frac{1}{n^s} - \frac{1}{(n+1)^s}\right) \\ &= -\frac{B_{N-1}}{(N-1)^s} + \frac{B_M}{M^s} + \sum_{n=N}^{M-1} B_n \int_n^{n+1} s\frac{\mathrm{d}t}{t^{s+1}}.\end{aligned}$$

Comme

$$\left|\frac{B_N}{N^s}\right| = \mathrm{O}(N^{1-\delta-\mathfrak{Re}(s)}), \quad \left|\frac{B_M}{M^s}\right| = \mathrm{O}(M^{1-\delta-\mathfrak{Re}(s)})$$

et

$$\left|B_n \int_n^{n+1} \frac{\mathrm{d}t}{t^{s+1}}\right| = |s|\mathrm{O}(n^{1-\delta-a-1})$$

la série des $b_n n^{-s}$ converge localement uniformément sur le demi-plan $\mathfrak{Re}(s) > 1-\delta$. □

4.2 Fonctions zêta de Dedekind

Définition 4.6 — *Soit K un corps de nombres. La fonction zêta de Dedekind de K est définie par*

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{\mathrm{N}(\mathfrak{a})^s},$$

où $\mathfrak{a}$ parcourt l'ensemble des idéaux non nuls de $\mathcal{O}_K$.

Exemples. On a bien évidemment $\zeta_{\mathbf{Q}}(s) = \zeta(s)$. Par ailleurs,

$$\zeta_{\mathbf{Q}(i)}(s) = \sum_{\substack{a,\, b \,\in\, \mathbf{Z} \\ a \,>\, 0,\ b \,\geqslant\, 0}} \frac{1}{(a^2+b^2)^s} = \sum_{n \geqslant 1} \frac{a_n}{n^s}$$

avec

$$a_n = \mathrm{Card}\{(a,b) \in \mathbf{Z}_{>0} \times \mathbf{Z}_{\geqslant 0} \mid a^2 + b^2 = n\}.$$

Proposition 4.7 — *Soit K un corps de nombres. On a*

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{\mathrm{N}(\mathfrak{a})^s} = \prod_{\mathfrak{p}} \left(1 - \frac{1}{\mathrm{N}(\mathfrak{p})^s}\right)^{-1}$$

où $\mathfrak{a}$ parcourt l'ensemble des idéaux non nuls de $\mathcal{O}_K$ et $\mathfrak{p}$ parcourt l'ensemble des idéaux premiers de $\mathcal{O}_K$. La somme et le produit convergent (localement uniformément) sur le demi-plan $\mathfrak{Re}(s) > 1$.

Démonstration. Posons $[K : \mathbf{Q}] = d$ et soit $s \in \mathbf{C}$ avec $\mathfrak{Re}(s) > 1$.

Il y a au plus d idéaux premiers $\mathfrak{p}$ divisant un nombre premier p donné dans $\mathfrak{O}_K$ et $\mathrm{N}(\mathfrak{p})^{-1} \leqslant p^{-1}$, donc

$$\sum_{\mathrm{N}(\mathfrak{p}) \leqslant X} \frac{1}{|\mathrm{N}(\mathfrak{p})^s|} \leqslant d \sum_{p \leqslant X} \frac{1}{p^{\mathfrak{Re}(s)}} \leqslant d \sum_{n \leqslant X} \frac{1}{n^{\mathfrak{Re}(s)}}$$

et la série $\sum_{\mathfrak{p}} \mathrm{N}(\mathfrak{p})^{-s}$ converge donc normalement sur tout demi-plan $\mathfrak{Re}(s) \geqslant \sigma_0$ avec $\sigma_0 > 1$. On en déduit la convergence du produit infini $\prod_{\mathfrak{p}} (1 - \mathrm{N}(\mathfrak{p})^{-s})^{-1}$ sur le demi-plan $\mathfrak{Re}(s) > 1$. En vertu de la factorisation des idéaux (non nuls) en produit d'idéaux premiers, il vient

$$\sum_{\mathrm{N}(\mathfrak{a}) \leqslant X} \frac{1}{\mathrm{N}(\mathfrak{a})^s} \leqslant \prod_{\mathrm{N}(\mathfrak{p}) \leqslant X} \sum_{k \geqslant 0} \frac{1}{\mathrm{N}(\mathfrak{p})^{ks}} = \prod_{\mathrm{N}(\mathfrak{p}) \leqslant X} \left(1 - \frac{1}{\mathrm{N}(\mathfrak{p})^s}\right)^{-1} \leqslant \prod_{\mathfrak{p}} \left(1 - \frac{1}{\mathrm{N}(\mathfrak{p})^s}\right)^{-1}$$

pour tout $s \in \mathbf{C}$ avec $\mathfrak{Re}(s) > 1$, donc la série des $\mathrm{N}(\mathfrak{a})^{-s}$ converge normalement sur tout demi-plan $\mathfrak{Re}(s) \geqslant \sigma_0$ avec $\sigma_0 > 1$. En outre,

$$\left| \sum_{\mathfrak{a}} \frac{1}{\mathrm{N}(\mathfrak{a})^s} - \prod_{\mathrm{N}(\mathfrak{p}) \leqslant X} \left(1 - \frac{1}{\mathrm{N}(\mathfrak{p})^s}\right)^{-1} \right| \leqslant \sum_{\mathrm{N}(\mathfrak{a}) > X} \frac{1}{\mathrm{N}(\mathfrak{a})^{\mathfrak{Re}(s)}} \to_{X \to +\infty} 0$$

donc

$$\sum_{\mathfrak{a}} \frac{1}{\mathrm{N}(\mathfrak{a})^s} = \prod_{\mathfrak{p}} \left(1 - \frac{1}{\mathrm{N}(\mathfrak{p})^s}\right)^{-1}.$$

□

Exemple. On a

$$\zeta_{\mathbf{Q}(i)}(s) = \left(1 - \frac{1}{2^s}\right)^{-1} \cdot \prod_{p \equiv 1 \pmod 4} \left(1 - \frac{1}{p^s}\right)^{-2} \cdot \prod_{p \equiv 3 \pmod 4} \left(1 - \frac{1}{p^{2s}}\right)^{-1}.$$

Il est commode d'utiliser ici un résultat que nous ne démontrerons que plus tard (théorème 4.13) : la fonction ζ_K admet un prolongement méromorphe sur le demi-plan $\{\mathfrak{Re}(s) > 1 - [K : \mathbf{Q}]^{-1}\}$ ayant un unique pôle, simple, au point 1.

Corollaire 4.8 — *Soit K un corps de nombres.*

$$\sum_{\mathfrak{p}} \frac{1}{\mathrm{N}(\mathfrak{p})^s} \sim \sum_{\mathfrak{p},\ \deg(\mathfrak{p})=1} \frac{1}{\mathrm{N}(\mathfrak{p})^s} \sim \log\ \frac{1}{s-1}$$

quand s tend vers 1 dans le demi-plan $\mathfrak{Re}(s) > 1$.

Démonstration. En vertu de l'écriture de ζ_K sous forme de produit eulérien,

$$\begin{aligned}
\log\ \zeta_K(s) &= -\sum_{\mathfrak{p}} \log\ (1 - \mathrm{N}(\mathfrak{p})^{-1}) \\
&= \sum_{\mathfrak{p}} \sum_{m \geqslant 1} \frac{1}{m\mathrm{N}(\mathfrak{p})^{ms}} \\
&= \sum_{\mathfrak{p},\ \deg(\mathfrak{p})=1} \frac{1}{\mathrm{N}(\mathfrak{p})^s} + \sum_{\mathfrak{p},\ \deg(\mathfrak{p})\geqslant 2} \frac{1}{\mathrm{N}(\mathfrak{p})^s} + \sum_{\mathfrak{p},\ m\geqslant 2} \frac{1}{m\mathrm{N}(\mathfrak{p})^{ms}}.
\end{aligned}$$

On a

$$\sum_{\mathfrak{p},\ \deg(\mathfrak{p})\geqslant 2} \frac{1}{|\mathrm{N}(\mathfrak{p})^s|} \leqslant \sum_p \frac{[K:\mathbf{Q}]}{p^{2\mathfrak{Re}(s)}} \leqslant [K:\mathbf{Q}] \sum_{n\geqslant 1} \frac{1}{n^{2\mathfrak{Re}(s)}},$$

donc la série de gauche converge sur le demi-plan $\mathfrak{Re}(s) > 1/2$. De même,

$$\begin{aligned}
\sum_{m\geqslant 2,\ \mathfrak{p}} \frac{1}{m|\mathrm{N}(\mathfrak{p})^{ms}|} &\leqslant \sum_{\mathfrak{p}} \frac{1}{|\mathrm{N}(\mathfrak{p})^{2s}|} \cdot \frac{1}{1 - |\mathrm{N}(\mathfrak{p})|^{-s}} \\
&\leqslant \sum_{\mathfrak{p}} \frac{1}{|\mathrm{N}(\mathfrak{p})^s|(|\mathrm{N}(\mathfrak{p})^s| - 1)} \\
&\leqslant [K:\mathbf{Q}] \sum_p \frac{1}{p^{\mathfrak{Re}(s)}(p^{\mathfrak{Re}(s)} - 1)} \\
&\leqslant [K:\mathbf{Q}] \sum_{n\geqslant 1} \frac{1}{n^{\mathfrak{Re}(s)}(n^{\mathfrak{Re}(s)} - 1)}
\end{aligned}$$

donc la série de gauche converge également sur le demi-plan $\mathfrak{Re}(s) > 1/2$.

Puisque la fonction $\zeta_K(s)$ admet un prolongement méromorphe sur le demi-plan $\mathfrak{Re}(s) > 1 - [K:\mathbf{Q}]^{-1}$ ayant un pôle simple en $s = 1$ (théorème 4.13),

$$\log\ \zeta_K(s) \sim \log\ \frac{1}{s-1}$$

quand s tend vers 1 dans le demi-plan $\mathfrak{Re}(s) > 1$ et donc

$$\sum_{\mathfrak{p},\ \deg(\mathfrak{p})=1} \frac{1}{\mathrm{N}(\mathfrak{p})^s} \sim \log\ \zeta_K(s) \sim \log\ \frac{1}{s-1}$$

quand s tend vers 1 dans le demi-plan $\mathfrak{Re}(s) > 1$. □

En particulier, il existe une *infinité* d'idéaux premiers de degré 1 dans $\mathcal{O}_K$.

Définition 4.9 — *Soit K un corps de nombres et soit $\mathcal{S}$ un ensemble d'idéaux premiers de $\mathcal{O}_K$. On dit que $\mathcal{S}$ est de* densité analytique *δ si*

$$\lim_{\substack{s\to 1 \\ s\in\mathbf{R}_{>1}}} \frac{\sum_{\mathfrak{p}\in\mathcal{S}} \mathrm{N}(\mathfrak{p})^{-s}}{\log\ \frac{1}{s-1}} = \delta.$$

Si elle existe, la densité analytique d'un ensemble d'idéaux premiers de $\mathcal{O}_K$ est un nombre réel dans $[0,1]$.

Proposition 4.10 — *Soit $K/\mathbf{Q}$ une extension galoisienne finie. L'ensemble des nombres premiers qui sont totalement décomposés dans K est de densité analytique $1/[K:\mathbf{Q}]$.*

Démonstration. Puisqu'il n'existe qu'un nombre fini d'idéaux premiers de $\mathcal{O}_K$ ramifiés,

$$\sum_{p \text{ tot. décomposé}} \frac{1}{p^s} = \frac{1}{[K:\mathbf{Q}]} \sum_{\substack{\mathfrak{p} \text{ non ramifié} \\ \deg(\mathfrak{p})=1}} \frac{1}{\mathrm{N}(\mathfrak{p})^s} \sim \frac{1}{[K:\mathbf{Q}]} \sum_{\mathfrak{p},\ \deg(\mathfrak{p})=1} \frac{1}{\mathrm{N}(\mathfrak{p})^s}$$

donc

$$\lim_{\substack{s\to 1 \\ s\in\mathbf{R}_{>1}}} \frac{\sum_{p \text{ tot. décomposé}} p^{-s}}{\log\ \frac{1}{s-1}} = \frac{1}{[K:\mathbf{Q}]} \lim_{\substack{s\to 1 \\ s\in\mathbf{R}_{>1}}} \frac{\sum_{\mathfrak{p},\ \deg(\mathfrak{p})=1} \mathrm{N}(\mathfrak{p})^{-s}}{\log\ \frac{1}{s-1}} = \frac{1}{[K:\mathbf{Q}]}.$$

□

Exemple. Si K est une extension quadratique de $\mathbf{Q}$, alors les nombres premiers totalement décomposés (resp. inertes) dans K forment un ensemble de densité analytique $1/2$.

Théorème 4.11 — *La fonction zêta d'un corps de nombres détermine sa clôture galoisienne.*

Étant donné un corps de nombres K, notons $\mathcal{S}(K/\mathbf{Q})$ l'ensemble des nombres premiers qui sont non ramifiés et totalement décomposés dans K.

Étant donné deux parties X, Y de $\mathbf{Z}$, nous écrirons $X \subset' Y$ si $X \setminus (X \cap Y)$ est fini, c'est-à-dire s'il existe une partie finie X_0 de X telle que $X \setminus X_0 \subset Y$.

Lemme 4.12 — *Soit $K/\mathbf{Q}$ une extension galoisienne finie. Si $F/\mathbf{Q}$ une extension finie telle que*

$$\mathcal{S}(K/\mathbf{Q}) \subset' \mathcal{S}(F/\mathbf{Q}),$$

alors $F \subset K$.

Démonstration. Considérons une extension galoisienne finie $L/\mathbf{Q}$ contenant K et F et désignons par KF le plus petit sous-corps de L contenant K et F. Si p est un nombre premier non ramifié dans L, alors les conditions suivantes sont équivalentes :

- p est totalement décomposé dans KF ;
- pour tout diviseur premier $\mathfrak{p}$ de p dans L,

$$(\mathfrak{p}, L/\mathbf{Q}) \in \mathrm{Gal}(L/KF) = \mathrm{Gal}(L/K) \cap \mathrm{Gal}(L/F),$$

- p est totalement décomposé dans K et dans F.

Compte-tenu de l'hypothèse $\mathcal{S}(K/\mathbf{Q}) \subset' \mathcal{S}(F/\mathbf{Q})$, on en déduit

$$\sum_{\mathfrak{p}\subset\mathcal{O}_{KF},\ \deg(\mathfrak{p})=1} \mathrm{N}(\mathfrak{p})^{-s} \geqslant [KF:\mathbf{Q}] \sum_{p\in\mathcal{S}(KF/\mathbf{Q})} p^{-s} \sim [KF:\mathbf{Q}] \sum_{p\in S(K/\mathbf{Q})} p^{-s} \sim \frac{[KF:\mathbf{Q}]}{[K:\mathbf{Q}]} \log\ \frac{1}{s-1}$$

et donc

$$\frac{[KF:\mathbf{Q}]}{[K:\mathbf{Q}]} \leqslant 1,$$

c'est-à-dire $F \subset K$. □

Démonstration du théorème 4.11. La fonction ζ_K détermine l'ensemble $\mathcal{S}(K/\mathbf{Q})$, à un nombre fini de nombre premiers près. Pour le voir, il suffit d'écrire $\zeta_K(s) = \sum_{n\geqslant 1} a_n/n^s$ et d'utiliser la formule de Perron :

$$\sum_{n\leqslant x} a_n = \frac{1}{2i\pi}\int_{c-i\infty}^{c+i\infty} \zeta_K(s)\ \frac{x^s}{s}\ \mathrm{d}s$$

valable pour tout $x \in \mathbf{R}_{>0}$ non entier et tout $c \in \mathbf{R}_{>1}$. En particulier, nous pouvons extraire de la fonction ζ_K le coefficient

$$a_p = \mathrm{Card}\{\mathfrak{p} \subset \mathcal{O}_K \mid \mathrm{N}(\mathfrak{p}) = p\}$$

pour chaque nombre premier p, et p est totalement décomposé dans K si et seulement si $a_p = [K : \mathbf{Q}]$.

Si $\widetilde{K}$ désigne la clôture galoisienne de K, alors

$$\mathcal{S}(\widetilde{K}/\mathbf{Q}) =' \mathcal{S}(K/\mathbf{Q})$$

et donc la fonction ζ_K détermine l'ensemble $\mathcal{S}(\widetilde{K}/\mathbf{Q})$, et donc le corps de nombres $\widetilde{K}$. En effet, si F est une extension galoisienne de $\mathbf{Q}$ telle que $\mathcal{S}(F/\mathbf{Q}) =' \mathcal{S}(\widetilde{K}/\mathbf{Q})$, alors $F = \widetilde{K}$ en vertu du lemme précédent. □

On peut reformuler ainsi le théorème 4.11 : si K_1 et K_2 sont deux corps de nombres tels que $\zeta_{K_1} = \zeta_{K_2}$, alors K_1 et K_2 ont la même clôture galoisienne.

4.3 La formule du nombre de classes

Soit K un corps de nombres de degré d. On note r_1 (resp. $2r_2$) le nombre de ses plongements réels (resp. complexes non réels), $w_K = \mathrm{Card}\ \mu(K)$ le nombre des racines de l'unité contenues dans K, D_K le discriminant de K, $h_K = \mathrm{Card}\ \mathrm{Cl}(\mathcal{O}_K)$ son nombre de classes et R_K son régulateur.

Théorème 4.13 (Formule du nombre de classes) — *La fonction ζ_K admet un prolongement méromorphe sur le demi-plan $\mathfrak{Re}(s) > 1 - [K : \mathbf{Q}]^{-1}$ ayant un pôle simple en $s = 1$, de résidu*

$$\mathrm{Res}_{s=1}\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2} R_K h_K}{w_K\sqrt{|D_K|}}.$$

Démonstration. Écrivons

$$\zeta_K(s) = \sum_{n\geqslant 1}\frac{a_n}{n^s} = \sum_{\substack{c\ \in\ \mathrm{Cl}(\mathcal{O}_K)\\ n\ \geqslant\ 1}} \frac{a_{n,c}}{n^s}$$

avec

$$a_n = \mathrm{Card}\{\mathfrak{a} \subset \mathcal{O}_K \mid \mathrm{N}(\mathfrak{a}) = n\} \quad \text{et} \quad a_{n,c} = \mathrm{Card}\{\mathfrak{a} \subset \mathcal{O}_K \mid \mathfrak{a} \in c,\ \ \mathrm{N}(\mathfrak{a}) = n\}.$$

En vertu du corollaire 4.5, il suffit de prouver que la quantité

$$A_{N,c} = \mathrm{Card}\{\mathfrak{a} \subset \mathcal{O}_K \mid \mathfrak{a} \in c \text{ et } \mathrm{N}(\mathfrak{a}) \leqslant N\}$$

vérifie

$$A_{N,c} = \kappa N + \mathrm{O}(N^{1-\delta}), \quad \text{avec } \kappa = \frac{2^{r_1}(2\pi)^{r_2} R_K}{w_K\sqrt{|D_K|}} \text{ et } \delta = [K : \mathbf{Q}]^{-1}.$$

Fixons $\mathfrak{a}_0 \in c$. Les idéaux $\mathfrak{a}$ de $\mathcal{O}_K$ appartenant à c sont de la forme $(x)\mathfrak{a}_0$ avec $x \in \mathfrak{a}_0^{-1} \setminus \{0\}$ et $|\mathrm{N}_{K/\mathbf{Q}}(x)| \leqslant N/\mathrm{N}(\mathfrak{a}_0)$. Ainsi,

$$A_{N,c} = \mathrm{Card}\left(\{x \in \mathfrak{a}_0^{-1} \setminus \{0\} \mid |\mathrm{N}_{K/\mathbf{Q}}(x)| \leqslant N.\mathrm{N}(\mathfrak{a}_0)^{-1}\}/\mathcal{O}_K^\times\right).$$

Posons $n = [K : \mathbf{Q}]$ et notons $\sigma_1, \ldots, \sigma_{r_1}$ les plongements réels de K et $\tau_1, \overline{\tau_1}, \ldots, \tau_{r_2}, \overline{\tau_{r_2}}$ ses plongements complexes non réels. Soit Ψ l'application

$$K^\times \to \mathbf{R}^{r_1+r_2}, \quad x \mapsto (\log|\sigma_1(x)|, \ldots, \log|\sigma_{r_1}(x)|, 2\log|\tau_1(x)|, \ldots, 2\log|\tau_{r_2}(x)|)$$

et posons $W_0 = (1, \ldots, 1)$ et $W = (1, ..., 1, 2, ..., 2)$ dans $\mathbf{R}^{r_1} \times \mathbf{R}^{r_2}$. En vertu du théorème 3.23, Ψ induit un isomorphisme du groupe $\mathcal{O}_K^\times/\mu(K)$ sur un réseau de l'hyperplan $H = (\mathbf{R}W_0)^\perp$; en outre, comme $\mathrm{N}_{K/\mathbf{Q}}\left(x^n\mathrm{N}_{K/\mathbf{Q}}(x)^{-1}\right) = 1$ tout $x \in K^\times$, on a $\Psi(x^d \cdot \mathrm{N}_{K/\mathbf{Q}}(x)^{-1}) \in H$ et donc

$$\Psi(x) = \frac{1}{d}\left(\Psi\left(x^d \cdot \mathrm{N}_{K/\mathbf{Q}}(x)^{-1}\right) + \log|\mathrm{N}_{K/\mathbf{Q}}(x)|W\right) \in H + \mathbf{R}W$$

pour tout $x \in K^\times$. On en déduit que, si P désigne un parallélépipède fondamental dans H pour $\Psi(\mathcal{O}_K^\times)$, alors

$$w_K \cdot A_{N,K} = \mathrm{Card}\left(\left\{x \in \mathfrak{a}_0^{-1} \setminus \{0\} \mid |\mathrm{N}_{K/\mathbf{Q}}(x)| \leqslant \mathrm{N}(\mathfrak{a}_0)^{-1} \cdot N \text{ et } \Psi(x) \in P + \mathbf{R}W\right\}\right).$$

Posons

$$\Gamma = \left\{(\underline{x}, \underline{z}) \in (\mathbf{R}^\times)^{r_1} \times (\mathbf{C}^\times)^{r_2} \;\middle|\; \begin{array}{c}\log|x_1| + \ldots + \log|x_{r_1}| + 2\log|z_1| + \ldots + 2\log|z_{r_2}| \leqslant 0 \\ \text{et } (\log|x_1|, \ldots, \log|x_{r_1}|, 2\log|z_1|, \ldots, 2\log|z_{r_2}|) \in P + \mathbf{R}W\end{array}\right\}.$$

En désignant comme d'habitude par Φ le plongement de K dans $\mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$ défini par $\sigma_1, \ldots, \sigma_{r_1}$ et $\tau_1, \ldots, \tau_{r_2}$, il vient

$$w_K \cdot A_{N,c} = \mathrm{Card}\left(\Phi(\mathfrak{a}_0^{-1} \cap (N/N(\mathfrak{a}_0))^{1/n}\Gamma\right).$$

On voit facilement que le domaine Γ est *borné*. En effet, pour tout point $(\underline{x}, \underline{z}) \in \Gamma$,

$$(\log|x_1|, \ldots, \log|x_{r_1}|, 2\log|z_1|, \ldots, 2\log|z_{r_2}|) = p + \lambda W$$

avec $p \in P$ (borné) et

$$\lambda = \log|x_1| + \ldots + \log|x_{r_1}| + 2\log|z_1| + \ldots + 2\log|z_{r_2}| \in \mathbf{R}_{\leqslant 0},$$

donc toutes les fonctions $\log|x_i|, \log|z_j|$ sont majorées sur Γ.

Le bord de Γ est défini par les conditions

$$\log|x_1| + \ldots \log|x_{r_1}| + 2\log|z_1| + \ldots 2\log|z_{r_2}| = 0$$

et

$$(\log|x_1|, \ldots, \log|x_{r_1}|, 2\log|z_1|, \ldots, 2\log|z_{r_2}|) \in \partial P + \mathbf{R}W,$$

donc est recouvert par les images d'un nombre fini d'applications de classe C^1 de $[0,1]^{n-1}$ dans $\mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$. En vertu du lemme ci-dessous, on obtient

$$w_K \cdot A_{N,c} = \frac{\mathrm{vol}(\Gamma)}{\mathrm{covol}(\Phi(\mathfrak{a}_0^{-1}))} \cdot \frac{N}{N(\mathfrak{a}_0)} + \mathrm{O}(N^{1-1/n}).$$

Le domaine Γ de $(\mathbf{R}^\times)^{r_1} \times (\mathbf{C}^\times)^{r_2}$ est invariant par l'action de $\{\pm 1\}^{r_1}$, donc

$$\mathrm{vol}(\Gamma) = 2^{r_1}\mathrm{vol}(\Gamma^+)$$

avec

$$\Gamma^+ = \Gamma \cap ((\mathbf{R}_{>0})^{r_1} \times (\mathbf{C}^\times)^{r_2}).$$

Considérons l'application

$$\begin{array}{rcl} f : (\mathbf{R}_{>0})^{r_1} \times (\mathbf{C}^\times)^{r_2} & \to & \mathbf{R}^{r_1+r_2} \\ (x_1, \ldots, x_{r_1}, z_1, \ldots, z_{r_2}) & \mapsto & (\log x_1, \ldots, \log x_{r_1}, 2\log|z_1|, \ldots, 2\log|z_{r_2}|). \end{array}$$

Par définition de Γ,

$$f(\Gamma) = P + \mathbf{R}_{\leqslant 0}W.$$

Si $\mathrm{d}\mu$ désigne la mesure de Lebesgue sur $\mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$, alors

$$f_*\mathrm{d}\mu = (2\pi)^{r_2} \cdot 2^{-r_2} \cdot e^{u_1} \cdots e^{u_{r_1+r_2}} \mathrm{d}u_1 \ldots \mathrm{d}u_{r_1+r_2},$$

donc

$$\mathrm{vol}(\Gamma^+) = \int_{\Gamma^+} \mathrm{d}\mu = \int_{P+\mathbf{R}_{\leqslant 0}W} f_*\mathrm{d}\mu = \pi^{r_2} \int_{P+\mathbf{R}_{\leqslant 0}W} e^{u_1+\ldots+u_{r_1+r_2}}\ \mathrm{d}u_1 \ldots \mathrm{d}u_{r_1+r_2}.$$

En faisant le changement de variables

$$v_1 = u_1, \ldots, v_{r_1+r_2-1} = u_{r_1+r_2-1}, \quad v_{r_1+r_2} = u_1 + \ldots + u_{r_1+r_2},$$

il vient

$$\begin{array}{rcl} \mathrm{vol}(\Gamma^+) & = & \pi^{r_2} \displaystyle\int_{P+\mathbf{R}_{\leqslant 0}W} e^{v_{r_1+r_2}}\ \mathrm{d}v_1 \ldots \mathrm{d}v_{r_1+r_2-1}\mathrm{d}v_{r_1+r_2} \\ & = & \pi^{r_2} \displaystyle\int_{-\infty}^{0} e^t \left(\int \mathbf{1}_{P+\mathbf{R}W}(v_1, \ldots, v_{r_1+r_2-1}, t)\ \mathrm{d}v_1 \ldots \mathrm{d}v_{r_1+r_2-1} \right) \mathrm{d}t \\ & = & \pi^{r_2} \displaystyle\int_{-\infty}^{0} e^t \lambda(t)\ \mathrm{d}t \end{array}$$

où $\lambda(t)$ désigne la mesure de la projection P_t de $(P + \mathbf{R}W) \cap \{v_{r_1+r_2} = t\}$ sur l'hyperplan $\{u_{r_1+r_2} = 0\}$. Il s'agit d'un translaté du projeté P' de $P_0 = P$ sur cet hyperplan, donc

$$\lambda(t) = \mathrm{covol}(P') = R_K$$

en vertu de la proposition 3.26. Ainsi,

$$\mathrm{vol}(\Gamma) = 2^{r_1}\pi_2^r R_K.$$

Au final, puisque $\Phi(\mathfrak{a}_0^{-1})$ est un réseau de covolume $2^{-r_2}|D_K|^{1/2}\mathrm{N}(\mathfrak{a}_\mathfrak{o}{}^{-1})$, nous avons obtenu

$$\begin{array}{rcl} A_{N,c} & = & \dfrac{\mathrm{vol}(\Gamma)}{w_K \mathrm{covol}(\Phi(\mathfrak{a}_\mathfrak{o}{}^{-1}))} \cdot \dfrac{N}{\mathrm{N}(\mathfrak{a}_\mathfrak{o})} + \mathrm{O}(N^{1-1/n}) \\ & = & \dfrac{2^{r_1}(2\pi)^{r_2} R_K}{w_K |D_K|^{1/2}} N + \mathrm{O}(N^{1-1/n}). \end{array}$$

□

Lemme 4.14 — *Soit $\Lambda \subset \mathbf{R}^n$ un réseau et soit $\Gamma \subset \mathbf{R}^n$ une partie bornée dont le bord est recouvert par les images d'un nombre fini d'applications lipschitziennes $\varphi : [0,1]^{n-1} \to \mathbf{R}^n$. On a*

$$\mathrm{Card}(\Lambda \cap t\Gamma) = \frac{\mathrm{vol}(\Gamma)}{\mathrm{covol}(\Lambda)} t^n + \mathrm{O}(t^{n-1})$$

quand $t \in \mathbf{R}_{>0}$ tend vers $+\infty$,

Démonstration. Soit P un parallélépipède fondamental pour Λ. Désignons par $m(t)$ (resp. $b(t)$) le nombre de points de Λ tels que $\lambda + P \subset t\overset{\circ}{\Gamma}$ (resp. tels que $(\lambda + P) \cap t\partial\Gamma \neq \varnothing$). Les inclusions

$$\bigcup_{\substack{\lambda \in \Lambda \\ (\lambda+P) \subset t\overset{\circ}{\Gamma}}} (\lambda + P) \subset t\Gamma \subset \bigcup_{\substack{\lambda \in \Lambda \\ (\lambda+P) \cap t\Gamma \neq \varnothing}} (\lambda + P)$$

impliquent

$$m(t)\mathrm{vol}(P) \leqslant \mathrm{vol}(t\Gamma) \leqslant (m(t) + b(t))\mathrm{vol}(P)$$

et donc

$$m(t) \leqslant \frac{\mathrm{vol}(\Gamma)}{\mathrm{covol}(\Lambda)} t^n \leqslant m(t) + b(t).$$

Pour conclure, il reste à établir l'estimation

$$b(t) = \mathrm{O}(t^{n-1}).$$

Soit $\varphi : [0,1]^{n-1} \to \mathbf{R}^n$ une application lipschitzienne, de constante de Lipschitz $\delta \in \mathbf{R}_{>0}$. Étant donné $t \in \mathbf{R}_{\geqslant 1}$, on peut subdiviser $[0,1]^{n-1}$ en $[t]^{n-1}$ cubes C de côté $1/[t]$ et $t\varphi(C)$ est alors une partie de diamètre inférieur à $\delta' = 2\sqrt{2}\delta$. En posant $N = \mathrm{Card}(\Lambda \cap B(0, \delta'))$, on en déduit

$$\mathrm{Card}(\Lambda \cap t\varphi(C)) \leqslant N$$

et donc

$$b(t) \leqslant N t^{n-1}$$

puisque le bord de Γ est recouvert par les images d'un nombre fini de telles applications φ. □

Exemple : le cas des corps quadratiques.

Si K est un corps quadratique imaginaire, alors

$$\lim_{\substack{s \to 1 \\ \Re\mathrm{e}(s) > 1}} \zeta_K(s) = \frac{2\pi h_K}{w_K \sqrt{|D_K|}}.$$

On a $w_{\mathbf{Q}(i)} = 4$, $w_{\mathbf{Q}(j)} = 6$ et $w_K = 2$ sinon.

Si K est un corps quadratique réel, alors

$$\lim_{\substack{s \to 1 \\ \Re\mathrm{e}(s) > 1}} \zeta_K(s) = \frac{2h_D \log\, \sigma_1(\varepsilon)}{\sqrt{D_K}}$$

où ε désigne une unité fondamentale telle que $\sigma_1(\varepsilon) > 1$.

En guise de complément, mentionnons sans démonstration le résultat suivant, établi par Hecke en 1910.

Théorème 4.15 — *La fonction*

$$Z_K(s) = |D_K|^{s/2} \left(\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\right)^{r_1} \left((2\pi)^{-s}\Gamma(s)\right)^{r_2} \zeta_K(s)$$

admet un prolongement méromorphe sur $\mathbf{C}$ *ayant deux pôles simples en* $s = 0$ *et* $s = 1$ *et satisfaisant à l'équation fonctionnelle*

$$Z_K(1-s) = Z_K(s).$$

4.4 Caractères et fonctions L de Dirichlet

Définition 4.16 — *Soit* $N \geqslant 1$ *un nombre entier. Un* caractère de Dirichlet *est un morphisme de groupes* $\chi : (\mathbf{Z}/N\mathbf{Z})^\times \to \mathbf{C}^\times$. *On note encore* χ *la fonction* N*-périodique de* $\mathbf{Z}$ *dans* $\mathbf{C}$ *définie par*

$$\chi(n) = \begin{cases} 0 & \text{si } \operatorname{pgcd}(n,N) \neq 1 \\ \chi(n \pmod N) & \text{si } \operatorname{pgcd}(n,N) = 1. \end{cases}$$

Il peut arriver qu'un caractère de Dirichlet modulo N se factorise par $(\mathbf{Z}/M\mathbf{Z})^\times$ avec $M|N$ et $M \neq N$, c'est-à-dire que χ provienne d'un caractère de Dirichlet modulo M via la projection canonique

$$(\mathbf{Z}/N\mathbf{Z})^\times \to (\mathbf{Z}/M\mathbf{Z})^\times .$$

Cette observation motive la définition suivante.

Définition 4.17 — *Le* conducteur *d'un caractère de Dirichlet* χ *est le plus petit entier* M *(au sens de la divisibilité) tel que* χ *se factorise à travers* $(\mathbf{Z}/M\mathbf{Z})^\times$. *On dit qu'un caractère de Dirichlet modulo* N *est* primitif *si son conducteur est égal à* N.

Exemple : caractères de Dirichlet modulo 8.

Le groupe $(\mathbf{Z}/8\mathbf{Z})^\times$ est abélien d'ordre 4, donc isomorphe à $(\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/2\mathbf{Z})$ car tous ses éléments sont d'ordre 2. Un caractère de Dirichlet modulo 8 envoie tout élément de $(\mathbf{Z}/8\mathbf{Z})^\times$ sur un élément d'ordre 2 dans $\mathbf{C}^\times$, donc sur 1 ou -1, et il est entièrement déterminé par son noyau. Ces observations permettent de dresser aisément la liste de tous les caractères de Dirichlet modulo 8 :

	1	-1	3	-3	conducteur
χ_1	1	1	1	1	1
χ_2	1	-1	-1	1	4
χ_3	1	1	-1	-1	8
χ_4	1	-1	1	-1	8

Les caractères qui se factorisent à travers $(\mathbf{Z}/4\mathbf{Z})^\times$ sont ceux qui sont triviaux sur le noyau $\{1, -3\}$ de la projection canonique $(\mathbf{Z}/8\mathbf{Z})^\times \to (\mathbf{Z}/4\mathbf{Z})^\times$.

Soit $N \geqslant 1$ un nombre entier et soit χ un caractère de Dirichlet modulo N. La *fonction L de Dirichlet* associée à χ est la série de Dirichlet

$$L(\chi, s) = \sum_{n \geqslant 1} \frac{\tilde{\chi}(n)}{n^s}$$

où $\tilde{\chi}$ désigne le caractère *primitif* induisant χ.

Remarque — On a $\chi(n) = \tilde{\chi}(n)$ pour tout entier n premier avec N ; par contre, $\chi(n) = 0$ et $\tilde{\chi}(n) \neq 0$ si $\mathrm{pgcd}(n, N) > 1$ mais $\mathrm{pgcd}(n, \mathrm{cond}(\chi)) = 1$. En particulier, si χ est le caractère trivial, alors $L(\chi, s) = \zeta(s)$.

Lemme 4.18 — (i) *La série $L(\chi, s)$ converge sur le demi-plan $\mathfrak{Re}(s) > 1$.*

(ii) *(Produit eulérien) Pour tout $s \in \mathbf{C}$ tel que $\mathfrak{Re}(s) > 1$,*

$$L(\chi, s) = \prod_p \frac{1}{1 - \tilde{\chi}(p)p^{-s}}$$

où $\tilde{\chi}$ désigne le caractère primitif induisant χ.

(iii) *Si χ n'est pas le caractère trivial, alors $L(\chi, s)$ converge sur le demi-plan $\mathfrak{Re}(s) > 0$ et y définit une fonction holomorphe.*

Démonstration. (i) On a $|\chi(n)| \leqslant 1$, donc il suffit d'invoquer le corollaire 4.5.

(ii) La convergence du produit infini se déduit du fait que l'on a $|\chi(p)| \leqslant 1$ (cf. preuve de l'identité analogue pour la fonction ζ de Riemann). L'égalité découle formellement de la multiplicativité de χ.

(iii) Si χ est non trivial, alors

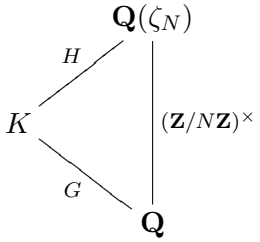
$$\sum_{a \in (\mathbf{Z}/N\mathbf{Z})^\times} \chi(a) = 0$$

et donc

$$\sum_{n=1}^{M} \chi(n) = \mathrm{O}(1)$$

quand M tend vers $+\infty$. La conclusion découle alors du corollaire 4.5. □

Considérons un entier $N \geqslant 1$ et un sous-corps K de $\mathbf{Q}(\zeta_N)$. L'extension $K/\mathbf{Q}$ est galoisienne, de groupe de Galois G.



Le groupe dual $\widehat{G}$ s'identifie au sous-groupe de $\mathrm{Gal}(\mathbf{Q}(\zeta_N)|\mathbf{Q})$ formé des caractères triviaux sur H. On rappelle également l'isomorphisme canonique $\iota : \mathrm{Gal}(\mathbf{Q}(\zeta_N)|\mathbf{Q}) \to (\mathbf{Z}/N\mathbf{Z})^\times$ défini par

$$\sigma(\zeta_N) = \zeta_N^{\iota(\sigma)},$$

ce qui nous permet d'identifier $\widehat{G}$ à un sous-groupe de $(\mathbf{Z}/N\mathbf{Z})^\times$.

Proposition 4.19 — *Avec les notations précédentes,*

$$\zeta_K(s) = \prod_{\chi \in \widehat{G}} L(\chi, s).$$

Démonstration. Par comparaison des produits eulériens, il suffit de prouver l'identité

$$\prod_{\mathfrak{p}|p}(1-\mathrm{N}(\mathfrak{p})^{-s})^{-1}=\prod_{\chi\in\widehat{G}}(1-\tilde{\chi}(p)p^{-s})^{-1}$$

pour tout nombre premier p (on rappelle que $\tilde{\chi}$ désigne le caractère primitif induisant χ).

Premier cas : $p\nmid N$, i.e. p n'est pas ramifié dans $\mathbf{Q}(\zeta_N)$.

On a $p\mathcal{O}_K=\mathfrak{p}_1\dots\mathfrak{p}_g$ avec $\deg(\mathfrak{p}_i)=f=\mathrm{Card}\langle(p,K/\mathbf{Q})\rangle$ et $g=[K:\mathbf{Q}]/f$. Par suite,

$$\prod_{\mathfrak{p}|p}(1-\mathrm{N}(\mathfrak{p})^{-s})^{-1}=(1-p^{-fs})^{-g}.$$

De l'autre côté, les éléments de $\widehat{G}$ s'identifient aux caractères $\chi:(\mathbf{Z}/N\mathbf{Z})^\times\to\mathbf{C}^\times$ se factorisant à travers la projection $(\mathbf{Z}/N\mathbf{Z})^\times\to G$. La classe de p dans $(\mathbf{Z}/N\mathbf{Z})^\times$ s'identifie à l'élément de Frobenius $(p,\mathbf{Q}(\zeta_N)/\mathbf{Q})$, donc l'image de p dans $\mathrm{Gal}(K|\mathbf{Q})$ est $(p,K/\mathbf{Q})$, d'ordre f. On en déduit que $\chi(p)$ que parcourt les racines f-ièmes de l'unité lorsque χ parcourt $\widehat{G}$, chacune étant obtenue g fois (voir le point 2 de l'appendice C). L'identité

$$\prod_{\chi\in\widehat{G}}(1-\tilde{\chi}(p)p^{-s})^{-1}=\prod_{\chi}(1-\chi(p)p^{-s})^{-1}=\prod_{\xi\in\mu_f}(1-\xi p^{-s})^{-1}=(1-p^{-fs})^{-g}$$

en découle.

Second cas : $p|N$, i.e. p est ramifié dans $\mathbf{Q}(\zeta_N)$.

Écrivons $N=p^km$ avec $\mathrm{pgcd}(p,m)=1$. L'extension $\mathbf{Q}(\zeta_m)/\mathbf{Q}$ (resp. $\mathbf{Q}(\zeta_N)/\mathbf{Q}(\zeta_m)$) est non ramifiée en p (resp. totalement ramifiée en chaque idéal premier au-dessus de p), donc le sous-groupe d'inertie $I_p=\mathrm{Gal}(\mathbf{Q}(\zeta_N)|\mathbf{Q}(\zeta_m))$ de $\mathrm{Gal}(\mathbf{Q}(\zeta_N)|\mathbf{Q})$ s'identifie au noyau de la projection canonique $(\mathbf{Z}/N\mathbf{Z})^\times\to(\mathbf{Z}/m\mathbf{Z})^\times$. Posons

$$K_0=K^{\mathrm{I}_p}=K\cap\mathbf{Q}(\zeta_m)\ \text{ et }\ G_0=\mathrm{Gal}(K_0|\mathbf{Q}).$$

En vertu de la proposition 2.18, l'extension $K_0/\mathbf{Q}$ (resp. K/K_0) est non ramifiée en p (resp. est totalement ramifiée en chaque idéal premier au-dessus de p), donc

$$\prod_{\substack{\mathfrak{p}\subset\mathcal{O}_K\\ \mathfrak{p}|p}}(1-\mathrm{N}(\mathfrak{p})^{-s})^{-1}=\prod_{\substack{\mathfrak{p}'\subset\mathcal{O}_{K_0}\\ \mathfrak{p}'|p}}(1-\mathrm{N}(\mathfrak{p}')^{-s})^{-1}.$$

Considérons un caractère $\chi\in\widehat{G}\subset\widehat{(\mathbf{Z}/N\mathbf{Z})^\times}$, induit par un caractère primitif $\tilde{\chi}$. On a $\tilde{\chi}(p)\neq0$ si et seulement si $\mathrm{pgcd}(p,\mathrm{cond}(\chi))=1$, donc si et seulement si χ se factorise à travers la projection canonique de $(\mathbf{Z}/N\mathbf{Z})^\times$ sur $(\mathbf{Z}/m\mathbf{Z})^\times$, c'est-à-dire si et seulement si χ se factorise à travers la projection de G sur G_0, c'est-à-dire appartient au sous-groupe $\widehat{G_0}$ de $\widehat{G}$. On en déduit :

$$\prod_{\chi\in\widehat{G}}(1-\tilde{\chi}(p)p^{-s})^{-1}=\prod_{\chi\in\widehat{G_0}}(1-\tilde{\chi}(p)p^{-s})^{-1}.$$

Les deux expressions à comparer sont celles associées à l'extension K_0/K, non ramifiée en p, donc la conclusion découle du premier cas. □

Corollaire 4.20 — *Soit K un corps de nombres contenu dans une extension cyclotomique de $\mathbf{Q}$, de groupe de Galois G. On a*

$$\prod_{\substack{\chi\in\widehat{G}\\ \chi\neq1}}L(\chi,1)=\frac{2^{r_1}(2\pi)^{r_2}h_KR_K}{w_K\cdot|D_K|^{1/2}}.$$

En particulier, $L(\chi,1)\neq 0$ *si* $\chi\neq 1$.

Démonstration. C'est une conséquence immédiate de la proposition précédente et du théorème 4.13. □

Théorème 4.21 (Dirichlet) — *Soit* $N\in\mathbf{Z}_{>0}$ *et* $a\in\mathbf{Z}$ *avec* $\mathrm{pgcd}(a,N)=1$. *Il existe une infinité de nombres premiers congrus à* a *modulo* N.

Démonstration. Désignons par $\mathcal{P}$ l'ensemble des nombres premiers et par $\mathcal{P}_{(a,N)}$ le sous-ensemble des nombres premiers congrus à a modulo N. La série de Dirichlet

$$\sum_{p\in\mathcal{P}_{(a,N)}}\frac{1}{p^s}$$

converge sur le demi-plan $\mathfrak{Re}(s)>1$ et l'on peut écrire

$$\sum_{p\in\mathcal{P}_{(a,N)}}\frac{1}{p^s}=\sum_{p\in\mathcal{P}}\frac{\mathbf{1}_{\{\overline{a}\}}(p)}{p^s}$$

où

$$\mathbf{1}_{\{\overline{a}\}}:(\mathbf{Z}/N\mathbf{Z})^\times\to\mathbf{C}^\times$$

désigne la fonction caractéristique du singleton $\{\overline{a}\}$. On peut recourir à l'analyse harmonique sur le groupe abélien $(\mathbf{Z}/N\mathbf{Z})^\times$ afin d'écrire $\mathbf{1}_{\{\overline{a}\}}$ à l'aide des caractères :

$$\mathbf{1}_{\{\overline{a}\}}=\frac{1}{\varphi(N)}\sum_{\chi}\overline{\chi(a)}\chi.$$

On en déduit

$$\begin{aligned}\sum_{p\in\mathcal{P}_{(a,N)}}\frac{1}{p^s} &= \frac{1}{\varphi(N)}\sum_{p,\chi}\overline{\chi(a)}\frac{\chi(p)}{p^s}\\ &= \frac{1}{\varphi(N)}\left(\sum_{p\in\mathcal{P}}\frac{1}{p^s}+\sum_{\chi\neq 1}\overline{\chi(a)}f_\chi(s)\right)\end{aligned}$$

avec

$$f_\chi(s)=\sum_{p\in\mathcal{P}}\frac{\chi(p)}{p^s}.$$

Le théorème sera démontré si l'on prouve que $f_\chi(s)$ est bornée au voisinage de $s=1$. Pour ce faire, on peut remplacer $f_\chi(s)$ par

$$f_\chi(s)+\sum_{p\in\mathcal{P},\ m\geqslant 2}\frac{\chi(p)^m}{mp^{ms}}=\sum_{p\in\mathcal{P},\ m\geqslant 1}\frac{\chi(p)^m}{mp^{ms}}=-\log\prod_p(1-\chi(p)p^{-s})^{-1}.$$

Aux facteurs $(1-\tilde{\chi(p)}p^{-s})$ près pour p divisant N, le membre de droite coïncide avec $-\log L(\chi,s)$.

Si le caractère χ n'est pas trivial, la fonction $L(\chi,s)$ se prolonge en une fonction holomorphe sur le demi-plan $\mathfrak{Re}(s)>0$ (lemme 4.18) et $L(\chi,1)\neq 0$ (corollaire 4.20) ; on en déduit que la fonction f_χ est bornée au voisinage de 1 et ceci achève la démonstration du théorème. □

Remarques. (i) La démonstration précédente donne un résultat plus fort :

$$\lim_{\substack{s\to 1\\ s\in\mathbf{R}_{>1}}}\frac{\sum_{p\in\mathcal{P}_{(a,N)}}1/p^s}{\sum_{p\in\mathcal{P}}1/p^s}=\frac{1}{\varphi(N)}$$

donc l'ensemble $\mathcal{P}_{(a,N)}$ admet une densité analytique, égale à $1/\varphi(N)$.

(ii) Le théorème précédent peut se reformuler en utilisant l'isomorphisme canonique entre $(\mathbf{Z}/n\mathbf{Z})^\times$ et $G = \mathrm{Gal}(\mathbf{Q}(\zeta_n)|\mathbf{Q})$: *étant donné un élément a de G, l'ensemble des nombres premiers p non ramifiés dans $\mathbf{Q}(\zeta_n)$ tels que $(p, \mathbf{Q}(\zeta_n)/\mathbf{Q}) = a$ a pour densité analytique* $1/\mathrm{Card}(G)$. Sous cette forme, une vaste généralisation a été établie par Tchebotariov en 1922 : *étant donné une extension finie galoisienne K de $\mathbf{Q}$ et une classe de conjugaison C dans $G = \mathrm{Gal}(K|\mathbf{Q})$, l'ensemble des nombres premiers p non ramifiés dans K tels que $(p, K/\mathbf{Q}) \in C$ a pour densité analytique* $\mathrm{Card}(C)/\mathrm{Card}(G)$.

Complément C. Analyse harmonique sur un groupe abélien fini.

Soit G un groupe abélien fini.

1. Un *caractère* de G est un morphisme de groupes $\chi : G \to \mathbf{C}^\times$. L'ensemble

$$\widehat{G} = \mathrm{Hom}_{\mathbf{Gr}}(G, \mathbf{C}^\times)$$

des caractères de G est un groupe pour la multiplication usuelle des fonctions (i.e. $(\chi_1\chi_2)(x) = \chi_1(x)\chi_2(x)$), appelé *groupe dual* et non canoniquement isomorphe à G. Son élément neutre est le caractère *trivial*, qui envoie G sur $\{1\}$; on le note 1.

Exemple. Si $G = \mathbf{Z}/N\mathbf{Z}$, alors on dispose d'un isomorphisme canonique $\widehat{\mathbf{Z}/N\mathbf{Z}} \tilde{\to} \mu_N, \quad \chi \mapsto \chi(1)$. Choisir un isomorphisme entre $\widehat{\mathbf{Z}/N\mathbf{Z}}$ et $\mathbf{Z}/N\mathbf{Z}$ revient à choisir une racine N-ième de l'unité primitive.

2. [Fonctorialité] Si $f : G \to G'$ est un morphisme de groupes abéliens, alors l'application $f^* : \widehat{G'} \to \widehat{G}, \quad \chi \mapsto \chi \circ f$, est un morphisme de groupes. Étant donné un sous-groupe H de G, la suite exacte naturelle

$$1 \longrightarrow H \xrightarrow{\iota} G \xrightarrow{\pi} G/H \longrightarrow 1$$

induit une suite *exacte*

$$1 \longrightarrow \widehat{G/H} \xrightarrow{\pi^*} \widehat{G} \xrightarrow{\iota^*} \widehat{H} \longrightarrow 1\ .$$

Autrement dit : tout caractère de H se prolonge en un caractère de G, et les caractères du groupe quotient G/H s'identifient aux caractères de G qui sont triviaux sur H.

En particulier, si a est un élément de G d'ordre f, alors

(i) $\chi(a)$ est une racine f-ième de l'unité dans $\mathbf{C}$ pour tout caractère χ de G ;

(ii) lorsque χ parcourt l'ensemble $\widehat{G}$, chaque racine f-ième de l'unité apparaît exactement $|G|/f$ fois parmi les $\chi(a)$.

Pour le vérifier, il suffit de considérer la suite exacte courte

$$1 \longrightarrow \langle a\rangle^\perp \longrightarrow \widehat{G} \longrightarrow \widehat{\langle a\rangle} \longrightarrow 1$$

où $\langle a\rangle^\perp = \{\chi \in \widehat{G} \mid \chi(a) = 1\}$, et de remarquer que l'application $\chi \mapsto \chi(a)$ réalise un isomorphisme entre $\widehat{\langle a\rangle}$ et $\mu_f(\mathbf{C})$.

3. Les caracères de G forment une *base orthonormée* du $\mathbf{C}$-espace vectoriel des fonctions complexes sur G relativement au produit scalaire hermitien

$$(f|g) = \frac{1}{|G|}\sum_{x\in G} \overline{f(x)}g(x).$$

En particulier (*relations d'orthogonalité*) :

(i) pour tout $\chi \in \widehat{G}$,

$$\sum_{x\in G} \chi(x) = |G|(1|\chi) = \begin{cases} |G| & \text{si } \chi = 1 \\ 0 & \text{sinon.} \end{cases}$$

(ii) pour tout $x \in G$,

$$\sum_{\chi \in \widehat{G}} \chi(x) = \begin{cases} |G| & \text{si } x = 1 \\ 0 & \text{sinon.} \end{cases}$$

On peut le justifier ainsi :

$$\begin{aligned} \sum_{\chi \in \widehat{G}} \chi(x) &= \left(\sum_{\chi \in \widehat{G}} \chi(x)\chi \right)(1) \\ &= |G| \left(\sum_{\chi \in \widehat{G}} (\mathbf{1}_{\{x\}}|\chi)\chi \right)(1) \\ &= |G|\mathbf{1}_{\{x\}}(1) \end{aligned}$$

où $\mathbf{1}_{\{x\}}$ désigne la fonction caractéristique du singleton $\{x\}$.

On peut aussi invoquer la *bidualité* : le morphisme de groupes canonique

$$G \to \widehat{\widehat{G}}, \quad x \mapsto (\chi \mapsto \chi(x))$$

est un isomorphisme et (ii) est une reformulation de (i) en remplaçant G par $\widehat{G}$.

Complément D. La formule du nombre de classes pour un corps quadratique

D.1. Le caractère de Dirichlet d'un corps quadratique

Considérons un corps de nombres quadratique K, de discriminant D_K.

Nous savons que K est contenu dans le corps cyclotomique $\mathbf{Q}(\zeta_{|D_K|})$ (proposition 2.24). Le caractère χ_K est le caractère de Dirichlet modulo $|D_K|$ défini via le diagramme commutatif

$$\begin{array}{ccc} \mathrm{Gal}(\mathbf{Q}(\zeta_{|D_K|})|\mathbf{Q}) & \longrightarrow & \mathrm{Gal}(K|\mathbf{Q}) \\ {\scriptstyle \mathrm{cyc}}\downarrow{\scriptstyle \simeq} & & {\scriptstyle \simeq}\downarrow{\scriptstyle \iota} \\ (\mathbf{Z}/|D_K|\mathbf{Z})^\times & \xrightarrow[\chi_K]{} & \{\pm 1\} \end{array}$$

où les flèches verticales sont les isomorphismes canoniques, définis par

$$\sigma(\zeta_{|D_K|}) = \zeta_{|D_K|}^{\mathrm{cyc}(\sigma)} \quad \text{et} \quad \iota(\tau) = \frac{\tau(\sqrt{D_K})}{\sqrt{D_K}}$$

pour tous $\sigma \in \mathrm{Gal}(\mathbf{Q}(\zeta_{|D_K|})|\mathbf{Q})$, $\tau \in \mathrm{Gal}(K|\mathbf{Q})$. Pour tout entier n premier à D_K, nous avons donc

$$\chi_K(n) = \frac{\sigma_n(\sqrt{D_K})}{\sqrt{D_K}}$$

où σ_n est l'automorphisme de $\mathbf{Q}(\zeta_{|D_K|})$ envoyant $\zeta_{|D_K|}$ sur $\zeta_{|D_K|}^n$.

Lemme D.1 — (i)

$$\chi_K(-1) = \begin{cases} 1 & \text{si } D_K > 0, \textit{ i.e. si } K \textit{ est réel}; \\ -1 & \text{si } D_K < 0, \textit{ i.e. si } K \textit{ est imaginaire}. \end{cases}$$

(ii) *Pour tout nombre premier p ne divisant pas D_K,*

$$\chi_K(p) = \begin{cases} 1 & \text{si } p \textit{ est décomposé dans } K; \\ -1 & \text{si } p \textit{ est inerte dans } K. \end{cases}$$

En particulier :

$$\chi_K(p) = \left(\frac{D_K}{p}\right)$$

pour tout p premier impair ne divisant pas 2 et, si $D_K \equiv 1 \pmod 4$, alors

$$\chi_K(2) = \begin{cases} 1 & \text{si } D_K \equiv 1 \pmod 8 \\ -1 & \text{si } D_K \equiv 5 \pmod 8 \end{cases}$$

Démonstration. (i) Fixons un plongement de $\mathbf{Q}(\zeta_{|D_K|})$ dans $\mathbf{C}$ et désignons par c la conjugaison complexe, qui induit par restriction des automorphismes de $\mathbf{Q}(\zeta_{|D_K|})$ et de K. Puisque $\zeta_{|D_K|}^{-1} = c(\zeta_{|D_K|})$, on a $\sigma_{-1} = c$ et donc

$$\chi_K(-1) = \frac{c(\sqrt{D_K})}{\sqrt{D_K}}.$$

La conclusion est maintenant immédiate.

(ii) L'automorphisme σ_p est l'élément de Frobenius $(p, \mathbf{Q}(\zeta_{|D_K|})/\mathbf{Q})$, donc

$$\chi_K(p) = \frac{(p, \mathbf{Q}(\zeta_{|D_K|})/\mathbf{Q})(\sqrt{D_K})}{\sqrt{D_K}} = \frac{(p, K/\mathbf{Q})(\sqrt{D_K})}{\sqrt{D_K}}.$$

L'élément de Frobenius $(p, K/\mathbf{Q})$ est trivial si et seulement si p est décomposé dans K. Lorsque $p > 2$, cette condition équivaut au fait que D_K soit un carré modulo p ; si $D_K \equiv 1 \pmod 4$ et $p = 2$, il revient au même de demander que le polynôme $X^2 - X + (1 - D_K)/4$ se réduise sur $X^2 + X$ modulo 2. □

Proposition D.2 — *Le caractère χ_K est primitif, i.e. son conducteur est $|D_K|$*

Démonstration. Pour tout diviseur f de $|D_K|$, le corps $\mathbf{Q}(\zeta_f)$ est contenu dans $\mathbf{Q}(\zeta_{|D_K|})$ et le diagramme naturel

$$\begin{array}{ccc} \mathrm{Gal}(\mathbf{Q}(\zeta_{|D_K|}|\mathbf{Q}) & \longrightarrow & \mathrm{Gal}(\mathbf{Q}(\zeta_f)/\mathbf{Q}) \\ \simeq\downarrow & & \downarrow\simeq \\ (\mathbf{Z}/|D_K|\mathbf{Z})^\times & \longrightarrow & (\mathbf{Z}/f\mathbf{Z})^\times \end{array}$$

est commutatif. Il en découle que le caractère χ_K se factorise à travers $(\mathbf{Z}/f\mathbf{Z})^\times$ si et seulement si K est contenu dans $\mathbf{Q}(\zeta_f)$.

Soit f un diviseur de $|D_K|$ tel que $K \subset \mathbf{Q}(\zeta_f)$. Si un nombre premier p divise $|D_K|$, alors p est ramifié dans K, donc dans $\mathbf{Q}(\zeta_f)$, et ainsi $p|f$. Les entiers $|D_K|$ et f ont donc les mêmes facteurs premiers.

Rappelons que D_K est soit un entier sans facteur carré et congru à 1 modulo 4, soit de la forme $4d$ avec d sans facteur carré et congru à 2 ou 3 modulo 4. Dans le premier cas de figure, nous pouvons directement conclure à l'égalité

$$\mathrm{cond}(\chi_K) = f = |D_K|.$$

Supposons que l'on ait $D_K = 4d$ avec d sans facteur carré et $d \equiv 3 \pmod 4$; il nous faut vérifier que K n'est pas contenu dans $\mathbf{Q}(\zeta_{2|d|})$. Comme $|d|$ est impair, $-\zeta_{|d|}$ est une racine primitive d'ordre $2|d|$, donc $\mathbf{Q}(\zeta_{2|d|}) = \mathbf{Q}(\zeta_{|d|})$ et 2 n'est *pas* ramifié dans $\mathbf{Q}(\zeta_{|d|})$. Puisque 2 est ramifié dans K, l'inclusion $K \subset \mathbf{Q}(\zeta_{2|d|})$ est exclue et donc

$$\mathrm{cond}(\chi_K) = f = |D_K|.$$

Supposons finalement que l'on ait $D_K = 8\delta$ avec δ impair et sans facteur carré ; il nous faut vérifier que K n'est pas contenu dans $\mathbf{Q}(\zeta_{4|\delta|})$, c'est-à-dire $\sqrt{D_K} = 2\sqrt{2\delta} \notin \mathbf{Q}(\zeta_{4|\delta|})$. Puisque $\sqrt{\delta} \in \mathbf{Q}(\zeta_{4|\delta|})$ en vertu de la proposition 2.24, il revient au même d'établir que $\mathbf{Q}(\zeta_{4|\delta|})$ ne contient pas $\sqrt{2}$. Si tel était le cas, alors ce corps cyclotomique contiendrait également

$$\zeta_8 = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$$

car il contient $i = \zeta_4$ et l'on aurait donc

$$\mathbf{Q}(\zeta_{4|\delta|}) = \mathbf{Q}(\zeta_{8|\delta|})$$

puisque δ est impair. Comme

$$[\mathbf{Q}(\zeta_{4|\delta|}) : \mathbf{Q}] = \varphi(4)\varphi(|\delta|) = 2\varphi(|\delta|) \quad \text{et} \quad [\mathbf{Q}(\zeta_{8|\delta|}) : \mathbf{Q}] = \varphi(8)\varphi(|\delta|) = 4\varphi(|\delta|),$$

ces corps cyclotomiques sont distincts et donc

$$\mathrm{cond}(\chi_K) = f = |D_K|.$$

□

Remarque — Si $D_K \equiv 1 \pmod 4$, alors

$$\chi_K = \left(\frac{\cdot}{D_K}\right).$$

En effet, pour tout nombre premier p ne divisant pas D_K,

$$\chi_K(p) = \left(\frac{D_K}{p}\right) = \left(\frac{p}{D_K}\right)$$

en vertu de la loi de réciprocité quadratique.

Proposition D.3 —

$$\zeta_K(s) = \zeta(s)L(\chi_K, s)$$

Démonstration. C'est un cas particulier de la proposition 4.19 dont on peut donner une démonstration directe :

$$\begin{aligned}
\zeta_K(s) &= \prod_{p|D_K} (1-p^{-s})^{-1} \cdot \prod_{\substack{p \nmid D_K \\ p \text{ décomposé}}} (1-p^{-s})^{-2} \cdot \prod_{\substack{p \nmid D_K \\ p \text{ inerte}}} (1-p^{-2s})^{-1} \\
&= \prod_{p|D_K} (1-p^{-s})^{-1} \cdot \prod_{p \nmid D_K} (1-p^{-s})^{-1} \cdot (1-\chi_K(p)p^{-s})^{-1} \\
&= \zeta(s) \cdot \prod_{p \nmid D_K} (1-\chi(p)p^{-s})^{-1} \\
&= \zeta(s)L(\chi_K, s)
\end{aligned}$$

en utilisant le fait que χ_K est primitif. □

Corollaire D.4 — *La fonction $L(\chi_K, s)$ est holomorphe sur le demi-plan $\mathfrak{Re}(s) > 0$ et*

$$L(\chi_K, 1) = \begin{cases} \frac{h_K R_K}{\sqrt{D_K}} & \text{si } D_K > 0 \\ \frac{\pi h_K}{\sqrt{|D_K|}} & \text{si } D_K < -4 \end{cases}$$

On a en outre

$$L(\chi_{\mathbf{Q}(i)}, 1) = \frac{\pi}{4} \quad \text{et} \quad L(\chi_{\mathbf{Q}(j)}, 1) = \frac{\pi}{3\sqrt{3}}.$$

Démonstration. Compte-tenu de la proposition précédente, il s'agit de la formule du nombre de classes dans le cas particulier d'un corps quadratique. Notons que l'on a $w_K = 2$ lorsque K est réel et

$$w_K = \begin{cases} 4 & \text{si } K = \mathbf{Q}(i), \text{ i.e. si } D_K = -4 \\ 6 & \text{si } K = \mathbf{Q}(j), \text{ i.e. si } D_K = -3 \\ 2 & \text{sinon, i.e. si } D_K < -4. \end{cases}$$

□

D.2. Calcul direct de $L(\chi_K, 1)$

Soit χ un caractère de Dirichlet de conducteur $f \geqslant 3$ et soit $\omega_f = e^{2i\pi/f}$. La *somme de Gauss* associée à χ est définie par

$$G(\chi) = \sum_{a \in \mathbf{Z}/f\mathbf{Z}} \chi(a)\omega^a.$$

Plus généralement, pour tout $c \in \mathbf{Z}$, posons

$$G(\chi, c) = \sum_{a \in \mathbf{Z}/f\mathbf{Z}} \chi(a)\omega^{ar}.$$

Lemme D.5 — (i) $G(\chi, r) = \overline{\chi(r)}G(\chi)$.

(ii) $G(\chi)G(\overline{\chi}) = \chi(-1)f$

(iii) $|G(\chi)| = \sqrt{f}$

Démonstration. (i) Si $\mathrm{pgcd}(r, f) = 1$, alors

$$G(\chi, r) = \sum_{a \in (\mathbf{Z}/f\mathbf{Z})^\times} \chi(a^{-1})\chi(ar)\omega_f^{ar} = \chi(r^{-1})G(\chi) = \overline{\chi(r)}G(\chi)$$

puisque $\chi(r)$ est une racine de l'unité dans $\mathbf{C}$.

Si $\mathrm{pgcd}(a, r) > 1$, alors $\chi(r) = 0$. D'autre par, en écrivant $r = \delta r'$, $f = \delta f'$ avec $\delta = \mathrm{pgcd}(r, f)$, il vient $\omega_f^\delta = \omega_{f'}$ et

$$G(\chi, r) = \sum_{a \in \mathbf{Z}/f\mathbf{Z}} \chi(a)\omega_{f'}^{r'a} = \sum_{a' \in \mathbf{Z}/f'\mathbf{Z}} \left(\sum_{\substack{a' \in \mathbf{Z}/f'\mathbf{Z} \\ a \equiv a' \pmod{f'}}} \chi(a) \right) \omega_{f'}^{r'a'}.$$

La somme entre parenthèse est nulle : c'est immédiat si $\mathrm{pgcd}(a', f') > 1$, car alors $\mathrm{pgcd}(a, f) > 1$ pour tout a congru à a' modulo f' ; si $\mathrm{pgcd}(a', f') = 1$, alors

$$\sum_{\substack{a' \in \mathbf{Z}/f'\mathbf{Z} \\ a \equiv a' \pmod{f'}}} \chi(a) = \chi(a_0) \cdot \sum_{\substack{b \in \mathbf{Z}/f\mathbf{Z} \\ b \equiv 1 \pmod{f'}}} \chi(b) = 0$$

en vertu des relations d'orthogonalité (Complément C) car χ se restreint en un caractère non trivial du noyau de la projection canonique de $(\mathbf{Z}/f\mathbf{Z})^\times$ sur $(\mathbf{Z}/f'\mathbf{Z})^\times$ puisque χ est de conducteur f.

(ii) On a

$$\begin{aligned}
G(\chi)G(\overline{\chi}) &= \sum_{r \in \mathbf{Z}/f\mathbf{Z}} \overline{\chi(r)}G(\chi)\omega_f^r \\
&= \sum_{r \in \mathbf{Z}/f\mathbf{Z}} G(\chi, r)\omega_f^r \\
&= \sum_{a,r \in \mathbf{Z}/f\mathbf{Z}} \chi(a)\omega_f^{r(1+a)} \\
&= \chi(-1)f + \sum_{\substack{a \in \mathbf{Z}/f\mathbf{Z} \\ a \not\equiv -1}} \left(\sum_{r \in \mathbf{Z}/f\mathbf{Z}} \omega_f^{(1+a)r} \right) \\
&= \chi(-1)f
\end{aligned}$$

(iii) On a

$$\overline{G(\overline{\chi})} = \sum_{a\in\mathbf{Z}/f\mathbf{Z}} \chi(a)\omega_f^{-a} = G(\chi,-1) = \chi(-1)G(\chi),$$

donc

$$|G(\overline{\chi})|^2 = \chi(-1)G(\chi)G(\overline{\chi}) = f$$

et

$$|G(\chi)| = f/|G(\overline{\chi})| = \sqrt{f}.$$

□

Théorème D.6 — *Soit χ un caractère de Dirichlet de conducteur $f \geqslant 3$.*

$$|L(\chi,1)| = \frac{1}{\sqrt{f}}\left|\sum_{a\in(\mathbf{Z}/f\mathbf{Z})^\times} \overline{\chi(a)}\log\left(\sin\frac{\pi a}{f}\right)\right| \quad \text{si } \chi(-1)=1$$

et

$$|L(\chi,1)| = \frac{\pi}{f\sqrt{f}}\left|\sum_{a\in\mathbf{Z}/f\mathbf{Z}} \overline{\chi(a)}a\right| \quad \text{si } \chi(-1)=-1.$$

Démonstration.

$$L(\chi,s) = \sum_{n\geqslant 1}\chi(n)n^{-s} = \sum_{t\in(\mathbf{Z}/f\mathbf{Z})^\times}\chi(t)\sum_{n\geqslant 1}a_n(t)n^{-s}$$

avec

$$a_n(t) = \begin{cases} 1 & \text{si } n\equiv t \pmod f \\ 0 & \text{sinon}\end{cases} = \frac{1}{f}\sum_{r=0}^{f-1}\omega_f^{(t-n)r},$$

donc

$$\begin{aligned} L(\chi,s) &= \frac{1}{f}\sum_{t\in(\mathbf{Z}/f\mathbf{Z})^\times}\sum_{r=0}^{f-1}\chi(t)\omega_f^{tr}\sum_{n\geqslant 1}\omega_f^{-nr}n^{-s} \\ &= \frac{1}{f}\sum_{r=0}^{f-1}G(\chi,r)\sum_{n\geqslant 1}\omega_f^{-nr}n^{-s} \\ &= \frac{G(\chi)}{f}\sum_{r\in(\mathbf{Z}/f\mathbf{Z})^\times}\overline{\chi(r)}\sum_{n\geqslant 1}\omega_f^{-nr}n^{-s}. \end{aligned}$$

En faisant tendre s vers 1, il vient

$$L(\chi,1) = -\frac{G(\chi)}{f}\sum_{r\in(\mathbf{Z}/f\mathbf{Z})^\times}\overline{\chi(r)}\log(1-\omega_f^{-r}).$$

En considérant la détermination principal du logarithme sur $\mathbf{C}\setminus\mathbf{R}_{\leqslant 0}$, il vient

$$\log(1-\omega_f^{-r}) = \log\left(2\sin\frac{\pi r}{f}e^{\pi/2-\pi r/f}\right) = \log\left(2\sin\frac{\pi r}{f}\right) - i\frac{\pi r}{f}.$$

Si $\chi(-1)=1$, alors χ est pair et donc

$$\begin{aligned} L(\chi,1) &= -\frac{G(\chi)}{f}\sum_{r\in(\mathbf{Z}/f\mathbf{Z})^\times}\overline{\chi(r)}\frac{\log(1-\omega_f^r)+\log(1-\omega_f^{-r})}{2} \\ &= -\frac{G(\chi)}{f}\sum_{r\in(\mathbf{Z}/f\mathbf{Z})^\times}\overline{\chi(r)}\log\left(2\sin\frac{\pi r}{f}\right) \\ &= -\frac{G(\chi)}{f}\sum_{r\in(\mathbf{Z}/f\mathbf{Z})^\times}\overline{\chi(r)}\log\left(\sin\frac{\pi r}{f}\right) \end{aligned}$$

car $\sum_{r\in(\mathbf{Z}/f\mathbf{Z})^\times}\overline{\chi(r)}=0$ puisque χ est un caractère non trivial de $(\mathbf{Z}/f\mathbf{Z})^\times$. On conclut en passant aux modules et en utilisant $|G(\chi)|=\sqrt{f}$ (lemme D.5).

Si $\chi(-1)=-1$, alors χ est impair et donc

$$\begin{aligned} L(\chi,1) &= -\frac{G(\chi)}{f}\sum_{r\in(\mathbf{Z}/f\mathbf{Z})^\times}\overline{\chi(r)}\frac{\log(1-\omega_f^r)-\log(1-\omega_f^{-r})}{2} \\ &= -\frac{G(\chi)}{f}\sum_{r\in(\mathbf{Z}/f\mathbf{Z})^\times}\overline{\chi(r)}i\frac{\pi r}{f} \\ &= -\frac{i\pi G(\chi)}{f^2}\sum_{r\in(\mathbf{Z}/f\mathbf{Z})^\times}\overline{\chi(r)}r. \end{aligned}$$

On conclut en passant aux modules et en utilisant $|G(\chi)|=\sqrt{f}$ (lemme D.5). □

En exploitant conjointement le corollaire D.4 et le théorème D.6, nous obtenons une formule du nombre de classe « explicite » pour les corps quadratiques.

Corollaire D.7 — *Soit K un corps quadratique, de caractère de Dirichlet associé χ_K.*

(i) *Si K est imaginaire, alors*

$$h_K=\frac{w_K}{2|D_K|}\left|\sum_{a\in(\mathbf{Z}/D_K\mathbf{Z})^\times}\chi_K(a)a\right|.$$

(ii) *Si K est réel, alors*

$$h_KR_K=\left|\sum_{a\in(\mathbf{Z}/D_K\mathbf{Z})^\times}\chi_K(a)\log\left(\sin\frac{\pi a}{D_K}\right)\right|.$$

Exemples. (i) Considérons $K=\mathbf{Q}(\sqrt{-5})$, avec $D_K=-20$. Le caractère de Dirichlet associé à K est

$$\chi_K:(\mathbf{Z}/20\mathbf{Z})^\times\to\{\pm1\},\quad a\mapsto\begin{cases}1 & \text{si } a=1,3,7,9\\ -1 & \text{si } a=11,13,17,19\end{cases}$$

et donc

$$h_K=\frac{1}{20}\left|1+3+7+9-11-13-17-19\right|=\frac{40}{20}=2.$$

(ii) Considérons $K=\mathbf{Q}(\sqrt{-39})$, avec $D_K=-39$. Le caractère de Dirichlet associé à K est

$$\chi_K=\left(\frac{\cdot}{3}\right)\left(\frac{\cdot}{13}\right)$$

et $\chi_K(a) = 1$ si et seulement si

$$a \equiv 1, 2, 4, 5, 8, 10, 11, 16, 20, 22, 25, 32 \pmod{39}.$$

On en déduit

$$h_K = \frac{|156 - 312|}{39} = 4.$$

Bibliographie

[1] H. Cohen. *A Course in Computational Algebraic Number Theory.* Springer, 1993.

[2] G. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers.* Oxford University Press, 1938.

[3] Ireland, K. et Rosen, M. *A classical Introduction to Modern Number Theory.* Springer, 1990.

[4] J. Neukirch. *Algebraic Number Theory.* Springer, 2007.

[5] Samuel, P. *Théorie algébrique des nombres.* Hermann.

[6] H.P.F. Swinnerton-Dyer. *A Brief Guide to Algebraic Number Theory.* London Mathematical Society, 2001.

Table des matières