Introduction à la Théorie Algébrique des Nombres

Gilles Auriol

auriolg@free.fr — http ://auriolg.free.fr

Table des matières

Chapitre 1

Entiers algébriques

Dans ce chapitre, nous allons introduire l'anneau des entiers d'une extension finie de $\mathbb{Q}$, ainsi que ses propriétés fondamentales, notamment que tout idéal se factorise de façon unique en produit d'idéaux. On retrouvera ainsi une notion de factorialité, introduite par Dedekind, qui fait défaut dans la plupart des anneaux d'entiers. On déterminera de façon élémentaire quelques exemples d'anneaux d'entiers qui sont euclidiens ou seulement principaux.

1.1 Exemples de défaut de factorialité

Dans cette section, nous allons mettre en évidence quelques points que vise à éclaircir et à généraliser la notion d'entiers algébriques.

On appellera norme sur un sous-anneau A de $\mathbb{C}$ une application de $A \longrightarrow \mathbb{Z}$ multiplicative, c'est-à-dire vérifiant

$$\forall \alpha, \beta \in A,\ \mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\mathrm{N}(\beta).$$

Par exemple pour les anneaux $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d}, a, b \in \mathbb{Z}\}$ où $d \in \mathbb{Z}$, on peut prendre l'application N définie par $\mathrm{N}(z) = a^2 - db^2$, où $z = a + b\sqrt{d}$.

La proposition suivante résume les propriétés de la norme.

1.1 Proposition (Norme). — *Soit A un sous-anneau de $\mathbb{C}$, $\alpha, \beta \in A$, et* N *une norme sur A. Si α divise β dans A, alors $N(\alpha)$ divise $N(\beta)$ dans $\mathbb{Z}$. En particulier si $N(\alpha)$ est premier dans $\mathbb{Z}$, alors α est irréductible dans A. De plus α est une unité de A si, et seulement si, $N(\alpha) = \pm 1$.*

1.2 Exemple (Anneau des entiers de Gauss). — Désignons $\sqrt{-1}$ par i. On introduit l'anneau des entiers de Gauss $\mathbb{Z}[i]$ qui a joué un rôle clé dans la recherche des nombres premiers somme de deux carrés d'entiers. Il jouit d'une propriété remarquable, il est euclidien (voir proposition 6.7). Par conséquent il est factoriel, c'est-à-dire que tout de $\mathbb{Z}[i]$ s'écrit comme produit de facteurs irréductibles de $\mathbb{Z}[i]$ et ce de façon unique à l'ordre des facteurs près.

1.3 Exemple (Un anneau non factoriel). — Considérons $\mathbb{Z}[\sqrt{-5}]$, et $\mathrm{N}(a + b\sqrt{-5}) = a^2 + 5b^2$ sa norme. On a deux factorisations pour 6,

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

Chacun des nombres $2, 3, 1 + \sqrt{-5}$ et $1 - \sqrt{-5}$ est irréductible, comme on le vérifie aisément avec la norme. Montrons-le par exemple pour 2. Si α divise 2 dans $\mathbb{Z}[\sqrt{-5}]$, d'après la proposition précédente $\mathrm{N}(\alpha)$ divise $\mathrm{N}(2) = 4$ dans $\mathbb{Z}$. Donc $\mathrm{N}(\alpha) \in \{1, 2, 4\}$. Si $\mathrm{N}(\alpha) = 4$ ou 1, c'est que 2 et α sont associés, ou que α est une unité. De plus l'équation $\mathrm{N}(\alpha) = 2$ n'a pas de solution dans $\mathbb{Z}$,

donc 2 n'admet pas de diviseurs propres.
D'autre part l'équation $\mathrm{N}(\alpha) = 1$ admet pour seules solutions ± 1, donc les unités de $\mathbb{Z}[\sqrt{-5}]$ sont ± 1, ainsi aucun des facteurs $2, 3, 1+\sqrt{-5}$ et $1-\sqrt{-5}$ ne sont associés, ce qui montre que $\mathbb{Z}[\sqrt{-5}]$ n'est pas factoriel.

Tout n'est pas perdu cependant ! Kummer réalisa qu'il manque à cet anneau certains éléments. Il répara la factorialité en remplaçant les nombres par les "nombres idéaux". En termes modernes, il factorisa les idéaux en produit d'idéaux premiers. On retrouve alors l'unicité à l'ordre près.

Voyons ce que cela donne avec $\mathbb{Z}[\sqrt{-5}]$ et 6. Posons

$$\mathfrak{a}_1 = (2, 1+\sqrt{-5}), \quad \mathfrak{a}_2 = (3, 1+\sqrt{-5}) \quad \text{et} \quad \mathfrak{a}_3 = (3, 1-\sqrt{-5}).$$

Notons qu'on peut écrire aussi $\mathfrak{a}_1 = (2, 1-\sqrt{5})$ puisque $2 \in \mathfrak{a}_1$. Il vient

$$\begin{aligned} \mathfrak{a}_1^2 &= (2\times 2, 2\times(1-\sqrt{-5}), (1+\sqrt{-5})\times 2, (1+\sqrt{-5})\times(1-\sqrt{-5})) \\ &= (4, 2-2\sqrt{-5}, 2+2\sqrt{-5}, 6) \\ &= (2) \end{aligned}$$

puisque $2 = 6 - 4 \in \mathfrak{a}_1^2$ et que chaque générateur est divisible par 2. De même, on trouve

$$\mathfrak{a}_1\mathfrak{a}_2 = (1+\sqrt{5}) \quad \mathfrak{a}_1\mathfrak{a}_3 = (1-\sqrt{-5}) \quad \text{et} \quad \mathfrak{a}_2\mathfrak{a}_3 = (3).$$

En particulier,

$$(6) = (2)(3) = (\mathfrak{a}_1\mathfrak{a}_1)(\mathfrak{a}_2\mathfrak{a}_3)$$

et

$$(6) = (1+\sqrt{-5})(1-\sqrt{5}) = (\mathfrak{a}_1\mathfrak{a}_2)(\mathfrak{a}_1\mathfrak{a}_3)$$

sont en fait les mêmes factorisations en termes d'idéaux. Démontrons par exemple que $\mathfrak{a}_1$ est premier. Tout d'abord on remarque que

$$\mathfrak{a}_1 = \{a + b\sqrt{-5} \,|\, a \equiv b \bmod (2)\}.$$

En effet, en prenant $(a,b) = (2,0)$ et $(a,b) = (1,1)$ on voit que $\mathfrak{a}_1 \subset \{a + b\sqrt{-5} \,|\, a \equiv b \bmod (2)\}$, et réciproquement si $a \equiv b \bmod (2)$, il existe $\lambda \in \mathbb{Z}$ tel que $a = b + 2\lambda$, d'où $a + b\sqrt{-5} = b + 2\lambda + b\sqrt{-5} = 2\lambda + b(1+\sqrt{-5}) \in \mathfrak{a}_1$, d'où l'égalité.
Soit $x = a + b\sqrt{-5}, y = c + d\sqrt{-5} \in \mathcal{O}_K$, et supposons que $x \notin \mathfrak{a}_1$ et $y \notin \mathfrak{a}_1$. Alors a et b (resp. c et d) sont de parité différente. Or

$$xy = (ac - 5bd) + (ad + bc)\sqrt{-5}.$$

On vérifie que dans tous les cas, $ac - 5bd$ et $ad + bc$ sont de parité différente, donc $xy \notin \mathfrak{a}_1$, ce qui prouve que $\mathfrak{a}_1$ est premier. On procède de même pour $\mathfrak{a}_2$ et $\mathfrak{a}_3$, en remarquant par exemple que

$$\mathfrak{a}_2 = \{a + b\sqrt{-5} \,|\, a \equiv b \bmod (3)\} \quad \text{et} \quad \mathfrak{a}_3 = \{a + b\sqrt{-5} \,|\, a \equiv 2b \bmod (3)\}.$$

Comme on l'a montré, $\mathbb{Z}[\sqrt{-5}]$ n'est pas principal, sinon il serait factoriel. Mais cela n'empêche pas $\mathbb{Z}[\sqrt{-5}]$ de posséder des idéaux principaux ! Nous allons montrer que $\mathfrak{a}_1$ n'est pas principal, cela nous resservira plus loin. Supposons $\mathfrak{a}_1$ principal, et notons β un générateur. Alors $\beta | 2$ et $\beta | (1+\sqrt{-5})$, donc en prenant les normes $\mathrm{N}(\beta) | 4$ et $\mathrm{N}(\beta) | 6$, d'où $\mathrm{N}(\beta) \in \{1, 2\}$. Si $\mathrm{N}(\beta) = 1$, c'est que β est inversible, et que $\mathfrak{a}_1 = \mathbb{Z}[\sqrt{-5}]$, ce qui n'est pas le cas puisque $\mathfrak{a}_1^2 = (2)$. Il est d'autre part clair qu'il n'existe pas d'élément de norme 2.

1.4 Exemple. — Pour finir, plaçons-nous dans $\mathbb{Z}[\sqrt{-3}]$. On a

$$4 = 2 \times 2 = (1+\sqrt{3}) \times (1-\sqrt{3})$$

et on vérifie facilement que $2, (1+\sqrt{3})$ et $(1-\sqrt{3})$ sont irréductibles, et non associés (les unités sont encore ± 1). Cela montre que $\mathbb{Z}[\sqrt{-3}]$ n'est pas factoriel.

Cependant ici on n'a pas la factorisation unique en terme d'idéaux. Posons $\mathfrak{a} = (2, 1+\sqrt{-3})$. Il vient

$$\mathfrak{a}^2 = (4, 2+2\sqrt{-3}, (1+\sqrt{-3})^2) = (4, 2+2\sqrt{-3}, -2+2\sqrt{-3}) = (4, 2+2\sqrt{-3}) = 2\mathfrak{a}.$$

Mais $\mathfrak{a} \neq (2)$ puisque $1+\sqrt{-3} \notin (2)$. Nous avons donc un exemple de factorisation non unique en produit d'idéaux.

Heureusement, comme nous le verrons au théorème 1.50, l'anneau à considérer dans le cas présent est $\mathbb{Z}\left[\dfrac{-1+\sqrt{-3}}{2}\right]$, qui en plus d'être un anneau où la factorisation en produit d'idéaux fonctionne est factoriel. Notons que dans cet anneau $(2, 1+\sqrt{-3}) = (2)$ puisque 2 divise $1+\sqrt{3}$.

1.2 Quelques quantités

1.2.1 Trace, norme et polynôme caractéristique

Soit L/K une extension de corps séparable, $n = [L : K]$ et Ω une clôture algébrique de K et L. On note σ_i, $1 \leqslant i \leqslant n$ les K-morphismes de L dans Ω.

Pour tout $x \in L$, soit m_x l'application K-linéaire $L \longrightarrow L, u \longmapsto ux$.

1.5 Définition (Trace, norme, polynôme caractéristique). — *On appelle trace (resp. norme, polynôme caractéristique) de $x \in L$ sur K et on note $\mathrm{Tr}_{L/K}(x)$ (resp. $\mathrm{N}_{L/K}(x)$, $\mathrm{P}_{L/K,x}(X)$) la trace (resp. le déterminant, le polynôme caractéristique) de m_x.*

On a donc $\mathrm{P}_{L/K,x}(X) = \det_K(X\mathrm{Id}_L - m_x)$.

1.6 Remarque. — Notons que pour $x, y \in L$ et $\alpha \in K$, on a $m_x + m_y = m_{x+y}$, $m_x \circ m_y = m_{xy}$ et $\alpha m_x = m_{\alpha x}$.

1.7 Proposition. — *Soit $x \in L$. On $\mathrm{P}_{L/K,x}(x) = 0$.*

Preuve. — Ecrivons $\mathrm{P}_{L/K,x}(X) = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_0$. Par le théorème de Cayley-Hamilton, $\mathrm{P}_{L/K,x}(m_x)$ est nulle. D'autre part par la remarque 1.6,

$$\begin{aligned}
\mathrm{P}_{L/K,x}(m_x) &= a_n m_x^n + a_{n-1}m_x^{n-1} + \cdots + a_0 I \\
&= a_n m_{x^n} + a_{n-1}m_{x^{n-1}} + \cdots + a_0 m_1 \\
&= m_{a_n x^n} + m_{a_{n-1}x^{n-1}} + \cdots + m_{a_0} \\
&= m_{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0} \\
&= m_{\mathrm{P}_{L/K,x}(x)}.
\end{aligned}$$

Ainsi $m_{\mathrm{P}_{L/K,x}(x)}$ est nulle, et en particulier $\mathrm{P}_{L/K,x}(x) = m_{\mathrm{P}_{L/K,x}(x)}(1) = 0$. ∎

Il en résulte qu'une condition nécessaire et suffisante pour que les polynômes caractéristique et minimal de $x \in L$ sur K soient égaux est que x soit un élément primitif de L/K.

Les propriétés immédiates de la norme sont résumées dans la proposition suivante.

1.8 Proposition. — *L'application trace* $\mathrm{Tr}_{L/K} : L \longmapsto K$ *est une forme linéaire du* K*-espace vectoriel* L*. L'application norme* $\mathrm{N}_{L/K} : L \longmapsto K$ *induit un morphisme de groupes multiplicatifs de* $L^\times$ *vers* $K^\times$*. Pour tout* $x \in K$*, on a* $\mathrm{Tr}_{L/K}(x) = nx$ *et* $\mathrm{N}_{L/K}(x) = x^n$*.*

Preuve. — Ceci résulte des propriétés du déterminant et de la remarque 1.6. Par exemple

$$\mathrm{N}_{L/K}(xy) = \det(m_{xy}) = \det(m_x \circ m_y) = \det(m_x)\det(m_y) = \mathrm{N}_{L/K}(x)\mathrm{N}_{L/K}(y).$$

D'autre part si $x \in K$, la matrice de l'application m_x dans une base de K est $x\mathrm{Id}_n$, d'où les valeurs de $\mathrm{Tr}_{L/K}(x)$ et $\mathrm{N}_{L/K}(x)$ dans ce cas. ∎

1.9 Proposition. — *Soit* $K \subset M \subset L$ *des corps,* $m = [M : K]$*,* $r = [L : M]$ *et* $n = [L : K] = mr$*. Pour tout* $x \in M$*, on a*

$$\mathrm{P}_{L/K,x}(X) = (\mathrm{P}_{M/K,x}(X))^r.$$

Preuve. — Soit $(e_1, \ldots, e_n)$ une base de L sur M et $(f_1, \ldots, f_n)$ une base de M sur K. En tant que K-espaces vectoriels, on a $L = Me_1 \oplus \cdots \oplus Me_r$ et Me_j a $(f_1e_j, \ldots, f_me_j)$ pour base sur K. Pour $x \in M$, les sous-K-espaces vectoriels Me_j sont stables par $m_x : L \longrightarrow L$, $u \longmapsto ux$. Soit B la matrice de m_x dans la base des (f_ie_j) et A la matrice de $\widetilde{m}_x : M \longrightarrow M, u \longmapsto ux$ dans la base $(f_1, \ldots, f_m)$. Alors B est diagonale par blocs avec r blocs diagonaux égaux à A. En prenant les déterminants, on en déduit le résultat. ∎

1.10 Corollaire. — *Soit* L *une extension finie de* K*. Pour tout* $x \in K$*, le polynôme caractéristique de* x *sur* K *est une puissance de son polynôme minimal.*

Preuve. — Il suffit d'appliquer la proposition précédente aux extensions $K \subset K(x) \subset L$. ∎

1.11 Proposition. — *Soit* L *une extension finie séparable de* K *de degré* n *et* σ_i*,* $1 \leqslant i \leqslant n$ *les* K*-morphismes de* L *dans une clôture algébrique de* K *et* L*. Pour tout* $x \in L$*, le polynôme caractéristique de* x *sur* K *est*

$$\mathrm{P}_{L/K,x}(X) = \prod_{i=1}^{n}(X - \sigma_i(x)).$$

Preuve. — On a la tour d'extension $K \subset M = K(x) \subset L \subset \Omega$ où Ω est une clôture algbérique de L.

Supposons d'abord $L = K(x)$. Les σ_i sont distincts et le polynôme minimal de x sur K est $\prod_{i=1}^{n}(X - \sigma_i(x))$, qui coïncide avec le polynôme caractéristique puisque x est primitif.

Si $L \neq K(x)$, posons $m = [M : K]$ et $r = [L : M]$. On a alors $\mathrm{P}_{L/K,x}(X) = (\mathrm{P}_{M/K,x}(X))^r$. Comme x est primitif de M sur K, on a

$$\mathrm{P}_{M/K,x}(X) = \prod_{j=1}^{m}(X - \varphi_j(x)).$$

où les φ_j, $1 \leqslant j \leqslant m$ sont les K-morphismes de M dans Ω. On sait que tout φ_j se prolonge de r façons différentes à des σ_i. Ceci permet de conclure en regroupant dans le produit $\prod_{i=1}^{n}(X - \sigma_i(x))$ les r σ_i dont la restriction à M est la même. ∎

1.12 Corollaire. — *Soit* $x \in L$*. On a*

$$\mathrm{Tr}_{L/K}(x) = \sum_{i=1}^{n}\sigma_i(x) \quad \textit{et} \quad \mathrm{N}_{L/K}(x) = \prod_{i=1}^{n}\sigma_i(x).$$

Preuve. — Le résultat est immédiat d'après les relations entre les coefficients et les racines d'un polynôme et la proposition précédente. ∎

1.2.2 Discriminant

Soit L/K une extension de corps.

1.13 Définition (Discriminant). — *Soit $(x_1, \dots, x_n)$ des éléments de L. Le discriminant $\mathrm{D}_{L/K}(x_1, \dots, x$ de ce n-uplet est défini par*

$$\mathrm{D}_{L/K}(x_1, \dots, x_n) = (\det(\sigma_i(x_j)))^2.$$

1.14 Proposition. — *Pour $(x_1, \dots, x_n) \in L^n$, on a*

$$\mathrm{D}_{L/K}(x_1, \dots, x_n) = \det(\mathrm{Tr}_{L/K}(x_i x_j))$$

et $\mathrm{D}_{L/K}(x_1, \dots, x_n) \in K$.

Preuve. — Soit $A = (\sigma_i(x_j))$. Puisque $\det A^t = \det A$ (où A^t désigne la transposée de A), on voit que $\mathrm{D}_{L/K}(x_1, \dots, x_n) = \det(A^t A)$ et le coefficient ij de cette matrice est

$$\sum_{k=1}^{n} \sigma_k(x_i)\sigma_k(x_j) = \sum_{k=1}^{n} \sigma_k(x_i x_j) = \mathrm{Tr}_{L/K}(x_i x_j) \in K,$$

d'où le résultat. ∎

1.15 Proposition. — *Soit L/K une extension séparable et x un élément primitif de L/K. Soit f le polynôme minimal de x sur K. Alors*

$$\mathrm{D}_{L/K}(1, x, \dots, x^{n-1}) = (-1)^{n(n-1)/2} \prod_{i \neq j} (\sigma_i(x) - \sigma_j(x)) = (-1)^{n(n-1)/2}\ \mathrm{N}_{L/K}(f'(x)).$$

En particulier $\mathrm{D}_{L/K}(1, x, \dots, x^{n-1}) \neq 0$.

Preuve. — Par définition $\mathrm{D}_{L/K}(1, x, \dots, x^{n-1}) = (\det(\sigma_i(x^j)))^2$. Or $(\sigma_i(x^j)) = ((\sigma_i(x))^j)$ est la matrice de Vandermonde du n-uplet $(\sigma_1(x), \dots \sigma_n(x))$, donc $\det(\sigma_i(x^j)) = \prod_{i<j} (\sigma_i(x) - \sigma_j(x))$, puis

$$\begin{aligned} \mathrm{D}_{L/K}(1, x, \dots, x^{n-1}) = \prod_{i<j} (\sigma_i(x) - \sigma_j(x))^2 &= (-1)^{n(n-1)/2} \prod_{i \neq j} (\sigma_i(x) - \sigma_j(x)) \\ &= (-1)^{n(n-1)/2} \prod_{i=1}^{n} \prod_{j \neq i} (\sigma_i(x) - \sigma_j(x)). \end{aligned}$$

D'autre part on sait que $f(X) = \prod_{i=1}^{n} (X - \sigma_i(x))$, donc

$$f'(X) = \sum_{i=1}^{n} \prod_{j \neq i} (X - \sigma_i(x)),$$

d'où pour tout $1 \leqslant i \leqslant n$,

$$\sigma_i(f'(x)) = f'(\sigma_i(x)) = \prod_{j \neq i} (\sigma_i(x) - \sigma_j(x)).$$

Par conséquent

$$\mathrm{D}_{L/K}(1, x, \dots, x^{n-1}) = (-1)^{n(n-1)/2} \prod_{i} \sigma_i(f'(x)) = (-1)^{n(n-1)/2}\ \mathrm{N}_{K/\mathbb{Q}}(f'(x)).$$

Enfin comme les $\sigma_i(x)$ sont distincts, on a bien $\mathrm{D}_{L/K}(1, x, \dots, x^{n-1}) \neq 0$. ∎

1.16 Exemple. — Soit $f(X) = X^3 + pX + q$ irréductible avec $p, q \in \mathbb{Q}$ et α une racine de $f(X)$. Alors $(1, \alpha, \alpha^2)$ est une base du $\mathbb{Q}$-espace vectoriel $\mathbb{Q}(\alpha)$. La matrice de $m_{f(\alpha)}$ dans la base $(1, \alpha, \alpha^2)$ est

$$\begin{pmatrix} p & -3q & 0 \\ 0 & 2p & -3q \\ 3 & 0 & 2p \end{pmatrix}$$

et son déterminant vaut $4p^3 + 27q^2$. Par la proposition qui précède, il vient donc $D_{K/\mathbb{Q}}(1, \alpha, \alpha^2) = -(4p^3 + 27q^2)$.

1.17 Lemme. — *Soit L/K une extension séparable de degré n et $x_1, \ldots, x_n \in L$. Si $B = (b_{jk})$ est une matrice $n \times n$ à coefficients dans K et $y_j = \sum_{k=1}^{n} b_{jk} x_k$, alors*

$$\mathrm{D}_{L/K}(y_1, \ldots y_n) = (\det(B))^2 \mathrm{D}_{L/K}(x_1, \ldots x_n).$$

Preuve. — On a $\mathrm{D}_{L/K}(x_1, \ldots, x_n) = (\det(\sigma_k(x_j)))^2$ et $\sigma_k(y_j) = \sum_{k=1}^{n} b_{ji} \sigma_k(y_i)$, si bien que

$$(\sigma_k(y_j)) = B \times (\sigma_k(x_j))$$

d'où le résultat en prenant les déterminants et en mettant au carré. ∎

1.18 Proposition. — *Soit L/K une extension séparable de degré n $y_1, \ldots y_n$ des éléments de L. Alors les y_i forment une base de L si et seulement si $\mathrm{D}_{L/K}(y_1, \ldots, y_n) \neq 0$.*

Preuve. — Soit $x \in L$ tel que $L = K(x)$, alors $(1, x, \ldots x^{n-1})$ est une base du K-espace vectoriel L. On peut donc écrire $y_j = \sum_{k=1}^{n} b_{jk} x^{k-1}$ avec $b_{jk} \in K$. Soit B la matrice ayant les b_{jk} comme coefficients. Par le lemme il vient

$$\mathrm{D}_{L/K}(y_1, \ldots y_n) = (\det(B))^2 \ \mathrm{D}_{L/K}(1, x, \ldots x^{n-1}).$$

Par la proposition 1.15, $\mathrm{D}_{L/K}(1, x, \ldots x^{n-1}) \neq 0$, donc $\mathrm{D}_{L/K}(y_1, \ldots y_n) \neq 0$ si et seulement si $\det B \neq 0$, soit encore si et seulement si les y_i forment une base du K-espace vectoriel L. ∎

1.19 Corollaire. — *Soit L/K une extension séparable. L'application*

$$\Theta_{L/K} : L \times L \longrightarrow K,\ (x, y) \longmapsto \mathrm{Tr}_{L/K}(xy)$$

est une forme K-bilinéaire symétrique propre.

Preuve. — Il est clair que $\Theta_{L/K}$ est symétrique, montrons par exemple qu'elle est K-linéaire par rapport à la première variable. Soit $\alpha \in K$ et $x, y, z \in L$; on a

$$\begin{aligned} \Theta_{L/K}(\alpha x + y, z) &= \sum_{i=1}^{n} \sigma_i((\alpha x + y)z) = \sigma_i(z) \sum_{i=1}^{n} (\alpha \sigma_i(x) + \sigma_i(y)) \\ &= \sum_{i=1}^{n} \alpha \sigma_i(xy) + \sum_{i=1}^{n} \sigma_i(z) = \alpha \Theta_{L/K}(x, y) + \Theta_{L/K}(z, y) \end{aligned}$$

Le discriminant de $\Theta_{L/K}$ par rapport à une base $(x_1, \ldots, x_n)$ est

$$\det(\mathrm{Tr}_{L/K}(x_i x_j)) = \mathrm{D}_{L/K}(x_1, \ldots, x_n),$$

quantité non nulle d'après la proposition précédente. ∎

1.3 Intégralité

1.3.1 Généralités

1.20 Définition (Entier). — *Soit L un corps et $A \subset L$ un sous-anneau de L. On dit que $\alpha \in L$ est entier sur A s'il existe $P \in A[X]$ unitaire tel que $P(\alpha) = 0$.*

1.21 Exemple. — Soit $\alpha = \dfrac{\sqrt{3}+\sqrt{7}}{2} \in \mathbb{R}$. On vérifie que $\alpha^4 - 5\alpha^2 + 1 = 0$, ce qui prouve que α est entier sur $\mathbb{Z}$.

Le théorème fondamental qui suit permet de manipuler de façon théorique les entiers ; on aura comme corollaire immédiat que l'ensemble des entiers sur un anneau A est un anneau.

1.22 Théorème. — *Soit L un corps, A un sous-anneau de L, et $\alpha \in A$. Les conditions suivantes sont équivalentes :*

(i) α est entier sur A ;

(ii) l'anneau $A[\alpha]$ engendré par A et α est un sous-A-module de type fini de L ;

(iii) il existe un sous-anneau B de L contenant α et A qui est un sous-A-module de type fini de L ;

(iv) il existe un sous-A-module non nul E de type fini de L tel que $\alpha E \subset E$.

Preuve. — Montrons que chaque propriété entraîne la suivante.

Supposons que α est entier sur A. Il existe donc $f(X) \in A[X]$ unitaire de degré n tel que $f(\alpha) = 0$. Soit $g(X) \in A[X]$. Comme $f(X)$ est unitaire, on peut effectuer la division euclidienne par $f(X)$ dans $A[X]$; il existe donc $q(X)$ et $r(X)$ avec $\deg(r) \leqslant n-1$ tel que $g(X) = q(X)f(X)+r(X)$, d'où $g(\alpha) = r(\alpha)$. Ainsi le sous-A-module $A[\alpha] \subset L$ admet $(1, x, \ldots, x^{n-1})$ comme système générateur et $(i) \Longrightarrow (ii)$.

Les implications $(ii) \Longrightarrow (iii) \Longrightarrow (iv)$ sont triviales.

Il reste à prouver que (iv) entraîne (i). Supposons donc qu'il existe sous-A-module de type fini non nul E de L tel que $\alpha E \subset E$, engendré par $(e_1, \ldots, e_n)$. Les relations $\alpha e_i \in E$ se traduisent par l'existence d'une matrice $M = (a_{ij})_{1 \leqslant 1, j \leqslant n}$ à coefficients dans A telle que

$$\left\{ \begin{array}{rcl} \alpha e_1 & = & a_{11}e_1 + \cdots + a_{1n}e_n \\ \vdots & & \vdots \\ \alpha e_n & = & a_{n1}e_1 + \cdots + a_{nn}e_n \end{array} \right.$$

Comme $E \neq 0$, il existe m tel que $e_m \neq 0$. Les formules de Cramer donnent $\det(x\mathrm{Id}_n - M)u_i = 0$. Les u_i n'étant pas tous nuls car $E \neq 0$, on a $\det(x\mathrm{Id}_n - M) = 0$. En développant on obtient une relation de dépendance intégrale pour x, d'où (i). ∎

1.23 Définition (Anneau entier, fini). — *Soit L un corps et $A \subset B$ deux sous-anneaux de L. On dit que B est entier sur A si tout $y \in B$ est entier sur A. On dit que B est fini sur A si c'est un A-module de type fini.*

Par le théorème 1.22, si B est fini sur A, alors il est entier sur A.

1.24 Définition (Fermeture et clôture intégrale). — *L'ensemble C des $x \in L$ entiers sur A est la fermeture intégrale de A dans L. Si A est intègre, sa fermeture intégrale dans son corps des fractions s'appele sa clôture intégrale.*

1.25 Définition (Intégralement clos). — *On dit qu'un anneau intègre A est intégralement clos si sa clôture intégrale est A lui-même.*

1.26 Lemme. — *Avec les notations précédentes, si B est fini sur A, tout B-module de type fini est un A-module de type fini.*

Preuve. — Si B est engendré par $(b_1, \ldots, b_n)$ comme A-module et si E est un B-module engendré par $(e_1, \ldots, e_n)$, le système $(b_j e_i)_{1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n}$ de cardinal mn engendre E comme A-module. ∎

1.27 Théorème. — *Soit L un corps et $A \subset L$ un anneau. Soit C la fermeture intégrale de A dans L. Alors C est un anneau intégralement clos contenant A.*

Preuve. — Soit $x, y \in C$. Alors $A[x]$ est fini sur A, et $A[x, y] = (A[x])[y]$ est fini sur $A[x]$, donc aussi sur A d'après le lemme. Or $x + y$ et xy étant dans $A[x, y]$, ils sont entiers sur A d'après le théorème 1.22, donc appartiennent à C.

Soit $x \in L$ entier dans C. Il existe une relation de dépendance intégrale

$$x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0 = 0$$

où les c_i sont entiers sur A. Dans la suite d'inclusion

$$A \subset A[c_0] \subset \ldots A[c_0, \ldots, c_{n-1}] \subset A[c_0, \ldots, c_{n-1}, x]$$

chaque anneau est entier sur celui qui le précède. Par application répétée du lemme, il vient que $A[c_0, \ldots, c_{n-1}, x]$ est fini sur A, donc $x \in C$. ∎

1.28 Proposition. — *Soit A un anneau factoriel. Alors il est intégralement clos.*

Preuve. — Soit K l'anneau des fractions de A, et soit $x = \dfrac{r}{s} \in K$ avec $r, s \in A$ et r et s premiers entre eux. Soit

$$\left(\frac{r}{s}\right)^n + a_{n-1}\left(\frac{r}{s}\right)^{n-1} + \cdots + a_0 = 0$$

une relation de dépendance intégrale pour x. Alors

$$r^n + a_{n-1}sr^{n-1} + \cdots + a_0 s^n = 0$$

d'où

$$s(-a_{n-1}r^{n-1} - sa_{n-2}r^{n-2} - \cdots - a_0 s^{n-1}) = r^n.$$

Ainsi s divise r^n, donc $s = 1$ puisque r et s sont premiers entre eux. Finalement $x \in A$. ∎

1.29 Exemple. — $\mathbb{Z}$ est factoriel, donc intégralement clos. La réciproque de la proposition est fausse. On a vu que $\mathbb{Z}[-\sqrt{5}]$ n'est pas factoriel (exemple 1.3), bien qu'il soit intégralement clos (voir théorème 1.27 et théorème 1.50).

1.30 Proposition. — *Soit A un anneau intégralement clos, K son corps des fractions supposé de caractéristique 0, L une extension finie de K et B la fermeture intégrale de A dans L. Alors*

(i) L est le corps des fractions de B ;

(ii) il existe un élément primitif de L sur K appartenant à B ;

(iii) un élément $z \in L$ est dans B si et seulement si son polynôme caractéristique (resp. minimal) est à coefficients dans A.

Preuve. — (*i*) Soit $y \in L$ de polynôme minimal $f(X) \in K[X]$. En multipliant par un dénominateur commun a des coefficients, la relation $f(y) = 0$ peut s'écrire

$$ay^n + a_{n-1}y^{n-1} + \cdots + a_1 y + a_0 = 0$$

où les a_i sont dans A. En posant $b = ay$ et en multipliant par a^{n-1}, on a

$$b^n + a_{n-1}b^{n-1} + \cdots + a_1 a^{n-2} b + a_0 a^{n-1} = 0.$$

Tout $y \in L$ est du type $y = \dfrac{b}{a}$ où $a \in A$, $b \in B$ donc L est le corps des fractions de B.

(*ii*) L'extension L/K est séparable car K est de caractéristique 0. Soit y un élément primitif de L sur K, Avec les notations précédente il existe $a \in A$ tel que $b = ay \in B$ et l'élément b est aussi primitif de L sur K.

(*iii*) Puisque L/K est séparable de degré n, il y a exactement n K-morphismes de L dans Ω une clôture algébrique de K et L ; notons-les σ_i pour $1 \leqslant i \leqslant n$. Si $x \in L$, l'application K-linéaire $m_x : L \longrightarrow L, u \longmapsto ux$ a pour polynôme caractéristique par la proposition 1.11,

$$p_x(X) = p_{L/K,x}(X) = \prod_{i=1}^{n} (X - \sigma_i(x)).$$

Soit $x \in L$. Si $p_x(X)$ est à coefficients dans A, la relation $p_x(x) = 0$ est une relation de dépendance intégrale de x sur A, donc $x \in B$.
Réciproquement, si $x \in B$, les $\sigma_i(x)$ sont aussi entiers sur A car vérifiant les mêmes relations de dépendance intégrale que x. Les coefficients de $p_x(X)$ sont les fonctions symétriques fondamentales de $\sigma_i(x)$, donc appartiennent à K et sont entiers sur A, donc sont dans A puisque A est intégralement clos.
Donc pour tout $x \in L$, $p_x(X) \in A[X]$ si et seulement si $z \in B$. L'assertion sur le polynôme minimal résulte de l'application de ce qui précède au cas où $L = K(x)$. ∎

1.31 Corollaire. — *Les hypothèses sont celles de la proposition. Alors pour tout $\alpha \in B$ et $\alpha_1, \ldots, \alpha_n \in B$, on a $\mathrm{Tr}_{L/K}(\alpha), \mathrm{N}_{L/K}(\alpha) \in A$ et $\mathrm{D}_{L/K}(\alpha_1, \ldots, \alpha_n) \in A$.*

Preuve. — L'extension L/K est séparable car de caractéristique 0. Les nombres $\mathrm{Tr}_{L/K}(\alpha)$ et $\mathrm{N}_{L/K}(\alpha)$ sont au signe près des coefficients du polynôme caractéristique de α sur K, que l'on sait être à coefficients dans A par la proposition, d'où le résultat. ∎

1.3.2 Cas noethérien de caractéristique nulle

1.32 Théorème. — *Soit A un anneau noethérien, intégralement clos, K son corps des fractions de caractéristique 0, L une extension finie de K et B la fermeture intégrale de A dans L. Alors B est une A-algèbre de type finie admettant L pour corps des fractions, et B est un anneau noethérien.*

Preuve. — Posons

$$\Theta_{L/K} : L \times L \longrightarrow K,\ (x, y) \longmapsto \mathrm{Tr}_{L/K}(xy).$$

Pour $y \in L$, la forme K-linéaire $L \longrightarrow K$, $x \longmapsto \Theta_{L/K}(x, y) = \mathrm{Tr}_{L/K}(xy)$ sera notée $\Theta_{L/K}(\cdot, y)$. Comme par le corollaire 1.19 $\Theta_{L/K}$ est propre, l'application $y \longmapsto \Theta_{L/K}(\cdot, y)$ est une bijection K-linéaire de L sur son K-espace vectoriel dual. Soit $(x'_1, \ldots, x'_n)$ l'image réciproque par cette bijection de la base duale d'une base $(x_1, \ldots, x_n)$ de L sur K. Elle est telle que

$$\mathrm{Tr}_{L/K}(x_i x'_j) = \delta_{ij} = \begin{cases} 0 & \text{si } i \neq j \\ 1 & \text{si } i = j \end{cases}.$$

Soit y un élément primitif de L/K ; par la proposition 1.30 (ii) on peut le prendre entier sur A. Alors $(1, y, \ldots, y^{n-1})$ est une base de L sur K et par ce qui précède il existe une base $(\varepsilon_1, \ldots, \varepsilon_n)$ de L sur K telle que $\mathrm{Tr}_{L/K}(y^i \varepsilon_j) = \delta_{ij}$. Soit $b \in B$ exprimé dans cette base

$$b = \alpha_1 \varepsilon_1 + \cdots + \alpha_n \varepsilon_n$$

où les $\mathrm{Tr}_{L/K}(y^i b) = \alpha_i \in K$ sont entiers sur A, donc appartiennent à A puisque A est intégralement clos. Ainsi B est contenu dans le sous-A-module libre de type fini de L de base $(\varepsilon_1, \ldots \varepsilon_n)$. Comme A est noethérien, B est un A-module de type fini car sous-A-module d'un A-module de type fini.

Enfin B est noethérien car tout idéal $J \subset B$ étant un sous-A-module de B, c'est un aussi un A-module de type fini, donc de type fini sur B. ∎

1.33 Corollaire. — *Dans les conditions du théorème précédent, si de plus A est principal alors B est un A-module libre de rang $n = [L : K]$.*

Preuve. — D'après la démonstration précédente, on a

$$B \subset A\varepsilon_1 \oplus \cdots \oplus A\varepsilon_n.$$

Ainsi B est un A-module libre de rang inférieur ou égal à n.

Or par l'assertion (i) de la proposition 1.30, il existe $a \in A$ et $\beta_1, \ldots, \beta_n \in B$ tels que $\varepsilon_i = \dfrac{\beta_i}{a}$ pour tout i. Par conséquent,

$$A\beta_1 \oplus \cdots \oplus A\beta_n \subset B$$

ce qui prouve que le rang de B est supérieur ou égal à n. Il y a donc égalité. ∎

1.4 Entiers algébriques

Appliquons ce qui précède à $A = \mathbb{Z}$ (avec les notations de la proposition 1.30).

1.4.1 Généralités et structure des idéaux de $\mathcal{O}_K$

1.34 Définition (Corps de nombres). — *On appelle corps de nombres K une extension finie (donc algébrique) de $\mathbb{Q}$. Le degré de K est $[K : \mathbb{Q}]$. On notera $\mathcal{O}_K$ la fermeture intégrale de $\mathbb{Z}$ dans K. Si $\alpha \in K$ est entier sur $\mathbb{Z}$, on parlera plus simplement d'entier s'il n'y a pas de risque de confusion avec les éléments de $\mathbb{Z}$, qu'on appelera entier rationnel.*

1.35 Lemme. — *Soit L/K une extension de corps de nombres. Alors $\mathcal{O}_L \cap K = \mathcal{O}_K$*

Preuve. — En effet $x \in \mathcal{O}_L \cap K$ si et seulement si $x \in K$ et x vérifie une relation de dépendance intégrale sur $\mathbb{Z}$, donc si et seulement si $x \in K \cap \mathcal{O}_K$. Or $K \cap \mathcal{O}_K = \mathcal{O}_K$ car $\mathcal{O}_K$ est intégralement clos. ∎

Enonçons l'assertion (ii) du corollaire 1.30 dans ce cadre.

1.36 Proposition. — *Soit $\alpha \in K$. Il existe un $a \in \mathbb{Z}$ tel que $a\alpha \in \mathcal{O}_K$.*

D'après le corollaire 1.33 appliqué à $A = \mathbb{Z}$, l'anneau $\mathcal{O}_K$ est un $\mathbb{Z}$-module libre de rang n.

1.37 Définition (Base intégrale). — *Une $\mathbb{Z}$-base de $\mathcal{O}_K$ en tant que $\mathbb{Z}$-module s'appelle une base intégrale de K.*

Mais il y a mieux ; en fait tout idéal non nul de $\mathcal{O}_K$ est un $\mathbb{Z}$-module libre de rang n. Montrons d'abord un lemme.

1.38 Lemme. — *Soit $\mathfrak{a}$ un idéal non nul de de $\mathcal{O}_K$. Alors $\mathfrak{a} \cap \mathbb{Z} \neq \{0\}$.*

Preuve. — Prenons α non nul dans $\mathfrak{a}$, et soit $\alpha^d + a_{d-1}\alpha^{d-1} + \cdots + a_0 = 0$ une relation de dépendance intégrale avec $a_0 \neq 0$ (si $a_0 = 0$, c'est qu'on peut mettre α en facteur dans la relation...). On déduit

$$a_0 = \alpha(-a_1 - \cdots - a_{d-1}\alpha^{d-2} - \alpha^{d-1})$$

donc $a_0 = \alpha\beta$ avec $\beta \in \mathcal{O}_K$. D'où $a_0 \in \mathbb{Z} \cap \mathfrak{a}$, et $a_0 \neq 0$. ∎

1.39 Proposition. — *Soit $\mathfrak{a}$ un idéal non nul de $\mathcal{O}_K$. Alors $\mathfrak{a}$ est un $\mathbb{Z}$-module libre de rang n d'indice fini dans $\mathcal{O}_K$. Si de plus $\mathfrak{a} = (\gamma)$, alors $\mathcal{O}_K/(\gamma)$ est d'ordre $|\gamma|^n$.*

Preuve. — Soit $\beta_1, \ldots, \beta_n$ une base intégrale de $\mathcal{O}_K$, et γ non nul dans $\mathbb{Z} \cap \mathfrak{a}$ (par le lemme précédent). Alors les $\gamma\beta_i$ sont dans (γ), et sont $\mathbb{Q}$-linéairement indépendants. Comme $(\gamma) \subset \mathcal{O}_K$, il s'ensuit que (γ) est un $\mathbb{Z}$-module libre de rang n. Mais $(\gamma) \subset \mathfrak{a} \subset \mathcal{O}_K$, donc $\mathfrak{a}$ est libre de rang n, puisqu'il est coincé entre deux $\mathbb{Z}$-modules libres de rang n.

La finitude de $[\mathcal{O}_K : \mathfrak{a}]$ résulte de la formule $[\mathcal{O}_K : (\gamma)] = [\mathcal{O}_K : \mathfrak{a}] \times [\mathfrak{a} : (\gamma)]$, compte tenu du fait que

$$\mathcal{O}_K/(\gamma) = \bigoplus_{i=1}^{n} \mathbb{Z}\beta_i \Big/ \bigoplus_{i=1}^{n} \mathbb{Z}\gamma\beta_i \simeq (\mathbb{Z}/\gamma\mathbb{Z})^n,$$

qui est fini d'ordre $|\gamma|^n$. ∎

1.40 Proposition. — *Soit $(\beta_1, \ldots \beta_n)$ et $(\gamma_1, \ldots \gamma_n)$ deux bases d'un idéal $\mathfrak{a}$ de $\mathcal{O}_K$. Alors on a $\mathrm{D}_{K/\mathbb{Q}}(\beta_1, \ldots \beta_n) = \mathrm{D}_{K/\mathbb{Q}}(\gamma_1, \ldots \gamma_n)$.*

Preuve. — On peut écrire $\gamma_j = \sum_{k=1}^{n} b_{jk}\beta_k$ et $\beta_j = \sum_{k=1}^{n} c_{jk}\gamma_k$ où les b_{jk} et c_{jk} sont entiers. Soit B et C les matrices ayant b_{jk} et c_{jk} respectivement pour coefficients de rang (j, k). On a

$$\beta_j = \sum_{k=1}^{n} c_{jk}\gamma_k = \sum_{k=1}^{n}\sum_{i=1}^{n} c_{jk}b_{ki}\beta_i = \sum_{i=1}^{n} d_{ji}\beta_i$$

où $d_{ji} = \sum_{k=1}^{n} c_{jk}b_{ki} \in \mathbb{Z}$. Puisque l'écriture dans la base (β_i) est unique, il vient $d_{jj} = 1$ et $d_{ji} = 0$ si $j \neq i$. Mais d_{ji} est le coefficient (j, i) de la matrice CB, donc $CB = \mathrm{Id}_n$, la matrice identité. Ainsi $\det(C)\det(B) = 1$, et comme $\det(B)$ et $\det(C)$ sont entiers, on a $\det(B) = \pm 1$. Par le lemme 1.17, il vient finalement $\mathrm{D}_{K/\mathbb{Q}}(\gamma_1, \ldots \gamma_n) = \det(B)^2\mathrm{D}_{K/\mathbb{Q}}(\beta_1, \ldots \beta_n) = \mathrm{D}_{K/\mathbb{Q}}(\beta_1, \ldots \beta_n)$.

1.41 Définition (Discriminant d'un idéal). — *L'entier ainsi défini qui ne dépend pas de la base de $\mathfrak{a}$ choisie pour le calculer s'appelle le discriminant de $\mathfrak{a}$ et se note $\mathrm{D}_{\mathfrak{a}}$. En particulier si $\mathfrak{a} = \mathcal{O}_K$, on l'appelle le discriminant de K, et on le notera D_K.*

La proposition qui suit peut s'avérer utile pour déterminer l'anneau des entiers d'un corps de nombres.

1.42 Proposition. — *Soit $(x_1, \ldots, x_n)$ des entiers de K formant une base de K. Si le discriminant $\mathrm{D}_{K/\mathbb{Q}}(x_1, \ldots, x_n)$ est sans facteurs carrés, alors $(x_1, \ldots, x_n)$ est une base intégrale de $\mathcal{O}_K$.*

Preuve. — En effet, si $(\beta_1, \ldots, \beta_n)$ est une base intégrale de $\mathcal{O}_K$, en écrivant $x_i = \sum_{j=1}^{n} a_{ij}\beta_j$, le lemme 1.17 montre que

$$\mathrm{D}_{K/\mathbb{Q}}(x_1, \ldots x_n) = (\det(a_{ij}))^2 \mathrm{D}_{K/\mathbb{Q}}(\beta_1, \ldots \beta_n).$$

Comme $\mathrm{D}_{K/\mathbb{Q}}(x_1, \ldots, x_n)$ est sans facteurs carrés $\det(a_{ij}) = \pm 1$ et $(x_1, \ldots, x_n)$ est une base intégrale de $\mathcal{O}_K$. ∎

1.43 Exemple. — Soit $K = \mathbb{Q}(\alpha)$ où α est une racine du polynôme $X^3 + 2X^2 + 1$. D'après l'exemple 1.16, $D_{K/\mathbb{Q}}(1, \alpha, \alpha^2) = 59$. Or 59 est premier (a fortiori sans facteurs carrés), donc $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

1.4.2 Norme d'un idéal

Soit K un corps de nombre. Pour $x \in K$, la norme $\mathrm{N}_{K/\mathbb{Q}}(x)$ de x est le déterminant de l'application $\mathbb{Q}$-linéaire $m_x : K \longrightarrow K, x \longmapsto ux$. Si $x \in \mathcal{O}_K$, alors $\mathrm{N}_{K/\mathbb{Q}}(x) \in \mathbb{Z}$. On va maintenant parler de la norme d'un idéal de $\mathcal{O}_K$ qui généralise en un certain sens la norme $\mathrm{N}_{K/\mathbb{Q}}$ restreinte à $\mathcal{O}_K$. On pose la définition suivante, rendue légitime par la proposition 1.39.

1.44 Définition (Norme d'un idéal). — *Soit $\mathfrak{a}$ un idéal non nul de $\mathcal{O}_K$. Le nombre $[\mathcal{O}_K : \mathfrak{a}]$ s'appelle la norme de $\mathfrak{a}$ et se note $\mathrm{N}_K(\mathfrak{a})$.*

Pour les idéaux principaux, la situation est particulièrement simple.

1.45 Proposition. — *Soit $\alpha \in \mathcal{O}_K$ non nul et $\mathfrak{a} = (\alpha)$. Alors $\mathrm{N}_K(\mathfrak{a}) = |\mathrm{N}_{K/\mathbb{Q}}(\alpha)|$.*

Preuve. — Soit $(\theta_1, \ldots, \theta_n)$ une base intégrale de $\mathcal{O}_K$ adaptée à $\mathfrak{a}$. Il existe donc $q_1 | \ldots | q_n$ dans $\mathbb{Z}\backslash\{0\}$ tels que $(q_1\theta_1, \ldots, q_n\theta_n)$ est une $\mathbb{Z}$-base de $\mathfrak{a}$, donc

$$\mathcal{O}_K/\mathfrak{a} = \bigoplus_{i=1}^{n} \mathbb{Z}\theta_i \Big/ \bigoplus_{i=1}^{n} \mathbb{Z}q_i\theta_i \simeq \prod_{i=1}^{n} \mathbb{Z}\theta_i/\mathbb{Z}q_i\theta_i \simeq \prod_{i=1}^{n} \mathbb{Z}/q_i\mathbb{Z},$$

d'où $\mathrm{N}_K(\mathfrak{a}) = [\mathcal{O}_K : \mathfrak{a}] = |q_1 \ldots q_n|$. D'autre part en notant D_K le discriminant de K,

$$\mathrm{D}_{K/\mathbb{Q}}(q_1\theta_1, \ldots, q_n\theta_n) = \det(\sigma_i(q_j\theta_j))^2 = \prod_{j=1}^{n} q_j^2 \mathrm{D}_K$$

d'où

$$\mathrm{D}_{K/\mathbb{Q}}(q_1\theta_1, \ldots, q_n\theta_n) = (\mathrm{N}_K(\mathfrak{a}))^2 \mathrm{D}_K. \tag{1.1}$$

Mais $(\alpha\theta_1, \ldots, \alpha\theta_n)$ est une autre $\mathbb{Z}$-base de $\mathfrak{a}$ donc

$$\mathrm{D}_{K/\mathbb{Q}}(q_1\theta_1, \ldots, q_n\theta_n) = \mathrm{D}_{K/\mathbb{Q}}(\alpha\theta_1, \ldots, \alpha\theta_n).$$

Comme

$$\mathrm{D}_{K/\mathbb{Q}}(\alpha\theta_1, \ldots, \alpha\theta_n) = \det(\sigma_i(\alpha\theta_j))^2 = \det(\sigma_i(\alpha)\sigma_i(\theta_j))^2 = \prod_{j=1}^{n} \sigma_i(\alpha)^2 \mathrm{D}_K,$$

il vient bien $\mathrm{N}_K(\mathfrak{a}) = |\mathrm{N}_{K/\mathbb{Q}}(\alpha)|$ en comparant avec 1.1, puisque $\mathrm{D}_K \neq 0$. ∎

1.46 Corollaire. — *Soit $\mathfrak{a}$ un idéal non nul de $\mathcal{O}_K$. Alors $\mathrm{D}_{\mathfrak{a}} = (\mathrm{N}_K(\mathfrak{a}))^2 \mathrm{D}_K$.*

Preuve. — Le résultat découle de l'équation 1.1 puisque l'entier $\mathrm{D}_{\mathfrak{a}}$ ne dépend pas de la base choisie pour le calculer. ∎

A l'instar de la norme pour les éléments de $\mathcal{O}_K$, la norme des idéaux est multiplicative. La preuve de cette proposition sera faite page 24 puisque celle-ci utilise la factorisation en idéaux premiers qui fait l'objet du prochain chapitre.

1.47 Proposition. — *Soit $\mathfrak{a}$ et $\mathfrak{b}$ deux idéaux non nuls de $\mathcal{O}_K$. Alors*

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

1.5 Entiers quadratiques

Soit K une extension quadratique de $\mathbb{Q}$, c'est-à-dire une extension de degré 2 de $\mathbb{Q}$. Nous allons étudier l'ensemble des entiers de K. Tout d'abord, on simplifie la situation par la proposition suivante.

1.48 Proposition. — *Soit K une extension quadratique de $\mathbb{Q}$. Il existe $d \in \mathbb{Z}\backslash\{0,1\}$ et d sans facteurs carrés tel que $K = \mathbb{Q}(\sqrt{d})$ (où d désigne un complexe dont le carré est d).*

Preuve. — Soit u un élément primitif de l'extension $K/\mathbb{Q}$, et $M(X) = X^2+bX+c$ son polynôme minimal, avec $b, c \in \mathbb{Q}$. On a

$$M(X) = \left(X + \frac{b}{2}\right)^2 - \frac{b^2-4c}{4}$$

donc $v = 2u + b$ vérifie $v^2 = b^2 - 4c$, et clairement $K = \mathbb{Q}(u) = \mathbb{Q}(v)$. Mais $b^2 - 4c \in Q$, notons $b^2 - 4c = r/s$ avec $r \in \mathbb{Z}$ et $s \in \mathbb{N}$, non nuls, alors $w = sv$ vérifie $w^2 = rs^2$ et $K = \mathbb{Q}(v) = \mathbb{Q}(w)$. Dans $\mathbb{Z}\backslash\{0\}$, rs se décompose ainsi : $rs = m^2d$ avec d ne possédant pas de facteurs carrés. Donc $K = \mathbb{Q}(w) = \mathbb{Q}(w/m)$, et comme $d = (w/m)^2$, on a $K = \mathbb{Q}(\sqrt{d}) = \mathbb{Q}(-\sqrt{d})$. Enfin $d \notin \{0,1\}$ car $K \neq \mathbb{Q}$. ∎

1.49 Définition (Corps quadratiques réels, complexes). — *On dit que $\mathbb{Q}(\sqrt{d})$ est un corps quadratique réel (resp. complexe) si $d > 0$ (resp $d < 0$).*

1.50 Théorème (Entiers quadratiques). — *Soit $d \in \mathbb{Z}\backslash\{0,1\}$ sans facteurs carrés. Une $\mathbb{Z}$-base d'entiers de $\mathbb{Q}(\sqrt{d})$ est donnée par $(1, \sqrt{d})$ si $d \equiv 2, 3 \bmod (4)$, et par $\left(1, \dfrac{1+\sqrt{d}}{2}\right)$ si $d \equiv 1 \bmod (4)$. Les discriminants de ces corps sont $4d$ si $d \equiv 2, 3 \bmod (4)$ et d si $d \equiv 1 \bmod (4)$.*

Preuve. — Posons $K = \mathbb{Q}(\sqrt{d})$. Les deux isomorphismes de K sont l'identité et $\sigma : a + b\sqrt{d} \mapsto a - b\sqrt{d}$ (qui est un automorphisme puisque $K/\mathbb{Q}$ est normale). Soit $x = a + b\sqrt{d} \in \mathcal{O}_K$, avec $a, b \in \mathbb{Q}$. On a donc, par le corollaire 1.31,

$$\mathrm{Tr}_{K/\mathbb{Q}}(x) = x + \sigma(x) = 2a \in \mathbb{Z} \text{ et } \mathrm{N}_{K/\mathbb{Q}}(x) = x\sigma(x) = a^2 - db^2 \in \mathbb{Z}.$$

Réciproquement si $\mathrm{Tr}_{K/\mathbb{Q}}(x), \mathrm{N}_{K/\mathbb{Q}}(x) \in \mathbb{Z}$, une relation de dépendance intégrale pour x est

$$x^2 - \mathrm{Tr}_{K/\mathbb{Q}}(x)x + \mathrm{N}_{K/\mathbb{Q}}(x) = 0.$$

Distinguons deux possibilités.

(*i*) On suppose que $a \in \mathbb{Z}$. On a alors $db^2 \in \mathbb{Z}$; écrivons $b = u/v$ avec u et v entiers premiers entre eux. Alors $db^2 = du^2/v^2$, d'où $v^2|d$, et enfin $v = \pm 1$ puisque d est sans facteurs carrés. On a donc $b \in \mathbb{Z}$. Comme la réciproque est évidente, le cas (i) donne donc les élements de $\mathbb{Z}[\sqrt{d}]$.

(*ii*) On suppose que $a \notin \mathbb{Z}$. On a donc $a = \alpha/2$ avec α entier impair. Mais

$$a^2 - db^2 = \frac{\alpha^2 - 4db^2}{4}$$

d'où $\alpha^2 - 4db^2 \in 4\mathbb{Z}$. On a donc $4db^2 = d(2b)^2 \in \mathbb{Z}$, et comme ci-dessus, on en déduit que $2b \in \mathbb{Z}$ d'où $b = \beta/2$, avec $\beta \in \mathbb{Z}$.

Pour la réciproque, distinguons deux cas selon les valeurs de d modulo 4.

(*iia*) $d \equiv 2, 3 \bmod (4)$. On a $\alpha^2 - 4db^2 = \alpha^2 - d\beta^2 \in 4\mathbb{Z}$. Comme $\alpha^2 \equiv 1 \bmod (4)$ et $\beta^2 \equiv 0$ ou $1 \bmod (4)$, il vient $\alpha^2 - db^2 \equiv 1, 2$ ou $3 \bmod (4)$, ce qui est absurde, donc dans ce cas, il n'est pas possible que $a \notin \mathbb{Z}$, et (i) donne tous les entiers possibles.

(*iib*) $d \equiv 1 \bmod (4)$. Dans ce cas on a $\alpha^2 - d\beta^2 \equiv 1 - \beta^2 \bmod (4)$, d'où β impair, et $x = (\alpha + \beta\sqrt{d})/2$ avec α, β impairs. Réciproquement, un tel x est entier car racine du polynôme

$$X^2 - \alpha X + \frac{\alpha^2 - d\beta^2}{4} \in \mathbb{Z}[X].$$

On peut écrire dans ce cas $x = \dfrac{\alpha - \beta}{2} + \beta\dfrac{1 + \sqrt{d}}{2} = \gamma + \beta\dfrac{1 + \sqrt{d}}{2}$ avec $\gamma, \beta \in \mathbb{Z}$. Comme $(1+\sqrt{d})/2$ est entier (prendre le polynôme ci-dessus avec $\alpha = \beta = 1$), le résultat est démontré.

Il reste à calculer les discriminants. Si $d \equiv 2, 3$ (resp. $d \equiv 1$) $\bmod (4)$, on a

$$D = \begin{vmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{vmatrix}^2 = 4d \quad \left(\text{resp. } D = \begin{vmatrix} 1 & \dfrac{1+\sqrt{d}}{2} \\ 1 & -\dfrac{1+\sqrt{d}}{2} \end{vmatrix}^2 = d\right)$$

ce qui achève la preuve du théorème. ∎

1.51 Remarque. — Si $d \equiv 1 \bmod(4)$, on a $\mathcal{O}_K = \left\{ \dfrac{\alpha + \beta\sqrt{d}}{2}, \alpha \text{ et } \beta \text{ de même parité} \right\}$. En particulier $\mathcal{O}_K \subset \{\alpha + \beta\sqrt{d}, \alpha, \beta \in \mathbb{Z}\}$.

1.52 Remarque. — L'anneau des entiers de $\mathbb{Q}(\sqrt{-3})$ est $\mathbb{Z}[j]$, où $\omega = e^{\frac{i\pi}{3}}$, et non $\mathbb{Z}[\sqrt{-3}]$ puisque $-3 \equiv 1 \bmod (4)$. C'est pour cette raison que l'anneau $\mathbb{Z}[\sqrt{-3}]$ est pathologique comme nous l'avons vu dans l'exemple 1.4. Cependant il joue un rôle dans la résolution de l'équation de Fermat $x^3 + y^3 = z^3$, voir section 5.5.2.

1.53 Remarque. — Les cas $d > 0$ et $d < 0$ sont très différents. Si $d > 0$, l'anneau $\mathcal{O}_K$ est dense dans $\mathbb{R}$ car ce n'est pas un sous-groupe additif monogène. Si $d < 0$, $\mathcal{O}_K$ est un réseau du plan complexe (voir définition 4.7).

Si $d < 0$ et $d \equiv 2, 3 \bmod (4)$, une base de ce réseau est $(1, \sqrt{d})$. Ces deux vecteurs sont orthogonaux car $\sqrt{d}$ est imaginaire pur. Les mailles de ce réseau sont donc des rectangles.

Si $d < 0$ et $d \equiv 1 \bmod (4)$, une base de ce réseau est $(1, \alpha)$ où $\alpha = \dfrac{1 + \sqrt{d}}{2}$. Mais $\alpha + \overline{\alpha} = 1$, donc $(\alpha, \overline{\alpha})$ est aussi une base de ce réseau dont les mailles sont donc des losanges.

Déterminons le groupe des unités de l'anneau des entiers d'un corps quadratique imaginaire.

1.54 Proposition. — *Soit $d < 0$ un entier sans facteurs carrés et $K = \mathbb{Q}(\sqrt{d})$. Alors $\mathcal{O}_K^\times = \{-1, +1\}$ sauf dans les deux cas suivants.*

(i) $d = -1$, donc $\mathcal{O}_K = \mathbb{Z}[\sqrt{-1}]$, et alors $\mathcal{O}_K^\times = \{-1, 1, i, -i\}$;

(ii) $d = -3$, donc $\mathcal{O}_K = \mathbb{Z}\left[\dfrac{1+\sqrt{-3}}{2}\right]$, et alors $\mathcal{O}_K^\times = \left\{\omega^k,\, 0 \leqslant k \leqslant 5\right\}$ où $\omega = e^{\frac{i\pi}{3}}$.

Preuve. — *(i)* $d \equiv 2, 3 \bmod (4)$. Dans ce cas $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$. Soit $\varepsilon = \alpha + \beta\sqrt{d} \in \mathcal{O}_K$. Alors $\mathrm{N}_{K/\mathbb{Q}}(\varepsilon) = \alpha^2 - b\beta^2$. On a

$$\varepsilon \in \mathcal{O}_K^\times \Longleftrightarrow \alpha^2 - d\beta^2 = 1 \Longleftrightarrow \left\{ \begin{array}{rcl} \alpha^2 & = & 1 \\ -d\beta^2 & = & 0 \end{array} \right. \text{ ou } \left\{ \begin{array}{rcl} \alpha^2 & = & 0 \\ -d\beta^2 & = & 1 \end{array} \right.$$

Le premier système conduit à ($\alpha = \pm 1$ et $\beta = 0$) et le second à ($\alpha = 0$, $d = -1$ et $\beta = \pm 1$), d'où les unités $\pm 1, \pm\sqrt{-1}$ de $\mathbb{Z}[\sqrt{-1}]$.

(ii) $d \equiv 1 \bmod (4)$. Dans ce cas $\mathcal{O}_K = \mathbb{Z}\left[\dfrac{1+\sqrt{d}}{2}\right]$. Soit $\varepsilon = \dfrac{\alpha + \beta\sqrt{d}}{2} \in \mathcal{O}_K$, avec α et β de même parité. Alors $\mathrm{N}_{K/\mathbb{Q}}(\varepsilon) = \dfrac{\alpha^2 - d\beta^2}{4}$. Supposons α et β pairs. On a

$$\varepsilon \in \mathcal{O}_K^\times \Longleftrightarrow \alpha^2 - d\beta^2 = 4 \Longleftrightarrow \left\{ \begin{array}{rcl} \alpha^2 & = & 4 \\ -d\beta^2 & = & 0 \end{array} \right. \text{ ou } \left\{ \begin{array}{rcl} \alpha^2 & = & 0 \\ -d\beta^2 & = & 4 \end{array} \right.$$

Le premier système conduit à ($\alpha = \pm 1$ et $\beta = 0$) et le second n'a pas de solution. Donc dans ce cas on récupère les unités ± 1. Supposons α et β impairs. On a

$$\varepsilon \in \mathcal{O}_K^\times \Longleftrightarrow \alpha^2 - d\beta^2 = 4 \Longleftrightarrow \left\{ \begin{array}{rcl} \alpha^2 & = & 1 \\ d\beta^2 & = & -3 \end{array} \right. \text{ ou } \left\{ \begin{array}{rcl} \alpha^2 & = & 3 \\ d\beta^2 & = & 1 \end{array} \right.$$

Le premier système conduit à ($\alpha = \pm 1$, $d = -3$ et $\beta = \pm 1$), d'où des unités de $\mathbb{Z}[\omega]$

$$\frac{1+\sqrt{-3}}{2} = \omega,\ \frac{1-\sqrt{-3}}{2} = \omega^5,\ \frac{-1+\sqrt{-3}}{2} = \omega^2 \text{ et } \frac{-1-\sqrt{-3}}{2} = \omega^4.$$

Le second système n'a pas de solution car $d \equiv 1 \bmod (4)$. ∎

1.6 Entiers cyclotomiques

Rappelons quelques faits sur les corps et polynômes cyclotomiques.

Soit $m \geqslant 1$ un entier. On appelle racine primitive m-ième de l'unité un générateur du groupe des racines m-ième de l'unité. Soit $\mathcal{P}_m$ l'ensemble de ces éléments. Le cardinal de $\mathcal{P}_m$ est $\varphi(m)$ où φ désigne l'indicatrice d'Euler. On définit le m-ième polynôme cyclotomique par

$$\Phi_m(X) = \prod_{\xi \in \mathcal{P}_m} (X - \xi).$$

Puisque les $\mathcal{P}_d(\mathbb{C})$, d décrivant l'ensemble des diviseurs de m dans $\mathbb{N}^*$, forment une partition de $\mathbb{U}_m$, il vient que $X^m - 1 = \prod_{d|m} \Phi_d(X)$. En particulier, si p est premier, on a

$$\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1.$$

Le critère d'Eisenstein montre qu'il est irréductible, après changement de variable $X = Y + 1$. Plus généralement, on a le théorème suivant (on renvoie à n'importe quel ouvrage d'algère pour la preuve, par exemple [Goz97]).

1.55 Théorème. — *Le m-ième polynôme cyclotomique est un polynôme irréductible de degré $\varphi(m)$ de $\mathbb{Z}[X]$.*

On appelle m-ième corps cyclotomique le corps engendré par les racines m-ièmes de l'unité. C'est un corps de nombre de degré $\varphi(m)$ d'après ce qui précède, extension galoisienne de $\mathbb{Q}$. Dans la suite, on notera ξ_m une racine primitive m-ième de l'unité. Le m-ième corps cyclotomique est donc $\mathbb{Q}(\xi_m)$. Le théorème sur l'anneau des entiers de $\mathbb{Q}(\xi_m)$ est le suivant.

1.56 Théorème. — *Soit $p \geqslant 1$, alors l'anneau des entiers de $K = \mathbb{Q}(\xi_p)$ est $\mathbb{Z}[\xi_p]$.*

La démonstration dans le cas général utilise des outils qui n'ont pas été introduits ici (voir [Rib01]). On se contente de montrer le résultat pour p premier. Commençons par un lemme sur un calcul de trace. Posons pour alléger les notations $\xi = \xi_p$.

1.57 Lemme. — *(i) On a $\mathrm{Tr}_{K/\mathbb{Q}}(\xi^i) = -1$ pour $1 \leqslant i \leqslant p-1$ et $\mathrm{Tr}_{K/\mathbb{Q}}(1-\xi) = p$.*
(ii) Pour tout $x \in \mathcal{O}_K$, on a $\mathrm{Tr}_{K/\mathbb{Q}}(x(1-\xi)) \in p\mathbb{Z}$.

Preuve. — Le polynôme minimal de ξ est

$$\Phi_p(X) = X^{p-1} + \cdots + X + 1 = (X-\xi)(X-\xi^2)\dots(X-\xi^{p-1})$$

donc les $p-1$ isomorphismes de $\mathbb{Q}(\xi)$ dans $\mathbb{C}$ (qui sont en fait des automorphismes car $\mathbb{Q}(\xi)/\mathbb{Q}$ est normale) sont définis par $\sigma_i(\xi) = \xi^i$ pour $1 \leqslant i \leqslant p-1$.

Par irréductibilité du polynôme cyclotomique Φ_p, on a $\mathrm{Tr}_{K/\mathbb{Q}}(\xi^i) = -1$ pour tout $1 \leqslant i \leqslant p-1$, et comme de plus $\mathrm{Tr}_{K/\mathbb{Q}}(1) = p-1$, il vient

$$\mathrm{Tr}_{K/\mathbb{Q}}(1-\xi) = \mathrm{Tr}_{K/\mathbb{Q}}(1-\xi^2) = \cdots = \mathrm{Tr}_{K/\mathbb{Q}}(1-\xi^{p-1}) = 1 + (p-1) = p.$$

ce prouve (i). D'autre part

$$\Phi_p(1) = p = (1-\xi)(1-\xi^2)\dots(1-\xi^{p-1}) = \sigma_1(1-\xi)\sigma_2(1-\xi)\dots\sigma_{p-1}(1-\xi). \tag{1.2}$$

Montrons maintenant que $\mathcal{O}_K(1-\xi) \cap \mathbb{Z} = p\mathbb{Z}$. D'après 1.2, on a $p \in \mathcal{O}_K(1-\xi)$, donc $\mathcal{O}_K(1-\xi) \cap \mathbb{Z} \supset p\mathbb{Z}$. Comme $p\mathbb{Z}$ est un idéal maximal de $\mathbb{Z}$, si on n'avait pas égalité, c'est que $\mathcal{O}_K(1-\xi) \cap \mathbb{Z} = \mathbb{Z}$, donc $1 \in \mathcal{O}_K(1-\xi)$, et $1-\xi$ serait inversible, et ses conjugués aussi. Par suite toujours d'après 1.2, p serait inversible dans $\mathcal{O}_K$, donc $1/p$ serait entier sur $\mathbb{Z}$, ce qui impossible car $\mathbb{Z}$ est intégralement clos.

Soit $x \in \mathcal{O}_K$. Pour tout $1 \leqslant i \leqslant p$, on a $\sigma_i(x(1-\xi)) = x_i(1-\xi^i)$ avec $x_i \in \mathcal{O}_K$. Mais $1-\xi^i = (1-\xi)(1+\xi+\cdots+\xi^{i-1})$, donc tous les $\sigma_i(x(1-\xi))$ sont des multiples de $1-\xi$ dans $\mathcal{O}_K$. Ainsi

$$\mathrm{Tr}_{K/\mathbb{Q}}(x(1-\xi)) \in \mathcal{O}_K(1-\xi).$$

De plus $\mathrm{Tr}_{K/\mathbb{Q}}(x(1-\xi)) \in \mathbb{Z}$ (trace d'un entier) d'où $\mathrm{Tr}_{K/\mathbb{Q}}(x(1-\xi)) \in \mathcal{O}_K(1-\xi) \cap \mathbb{Z} = p\mathbb{Z}$. ∎

Preuve (du théorème 1.56 avec p premier). — Soit $x = a_{p-2}\xi^{p-2} + \cdots + a_1\xi + a_0$ un élément de $\mathcal{O}_K$ avec les $a_i \in \mathbb{Q}$. On a alors

$$x(1-\xi) = a_{p-2}(\xi^{p-2} - \xi^{p-1}) + \cdots + a_1(\xi - \xi^2) + a_0(1-\xi).$$

En prenant les traces, il résulte de l'assertion (i) du lemme que

$$\mathrm{Tr}_{K/\mathbb{Q}}(x(1-\xi)) = a_0\mathrm{Tr}_{K/\mathbb{Q}}(1-z) = a_0 p$$

car pour tout $1 \leqslant j \leqslant p-2$, on a $\mathrm{Tr}_{K/\mathbb{Q}}(a_j(\xi^j - \xi^{j+1})) = a_j(-1-(-1)) = 0$.

Par l'assertion (ii) du lemme, il vient $pa_0 \in p\mathbb{Z}$, puis $a_0 \in \mathbb{Z}$. Comme $z^{-1} = z^{p-1}$, on a $z^{-1} \in \mathcal{O}_K$, d'où

$$(x - a_0)z^{-1} = a_{p-2}z^{p-3} + \cdots + a_2 z + a_1 \in \mathcal{O}_K.$$

En appliquant la première partie du raisonnement à cet élément, on voit que $a_1 \in \mathbb{Z}$. Par applications successives de ce procédé, on voit que $a_i \in \mathbb{Z}$ pour tout i. ∎

1.58 Proposition. — *Soit p un nombre premier. Alors le discriminant* D *de $\mathbb{Q}(\xi_p)$ est*

$$\mathrm{D} = \begin{cases} (-1)^{(p-1)/2}p^{p-2} & \text{si } p \text{ impair} \\ 1 & \text{si } p = 2 \end{cases}$$

Preuve. — Posons $\xi = \xi_p$. Une base de $K = \mathbb{Q}(\xi)$ est $(1, \xi, \xi^2, \ldots x^{p-2})$, et le polynôme minimal de ξ est $\Phi_p(X)$. Par la proposition 1.15, il suffit de calculer $\mathrm{N}_{K/\mathbb{Q}}(\Phi_p'(\xi))$. On a

$$\Phi_p(X) = \frac{X^p - 1}{X - 1}, \quad \text{donc} \quad \Phi_p'(X) = \frac{pX^{p-1}(X-1) - (X^p - 1)}{(X-1)^2},$$

d'où pour tout $1 \leqslant k \leqslant p - 1$,

$$\Phi_p'(\xi^k) = \frac{p(\xi^k)^{p-1}}{\xi^k - 1} = \frac{p}{\xi^k(\xi^k - 1)},$$

et

$$\mathrm{N}_{K/\mathbb{Q}}(\Phi_p'(\xi)) = \prod_{k=1}^{p-1} \Phi_p'(\xi^k) = \frac{p^{p-1}}{\prod_{k=1}^{p-1} \xi^k \times \prod_{k=1}^{p-1}(\xi^k - 1)}.$$

Or les relations entre coefficients et racines d'un polynôme montrent que $\displaystyle\prod_{k=1}^{p-1} \xi^k = (-1)^{p-1}$, et comme les $\xi^k - 1$, $1 \leqslant k \leqslant p - 1$ sont racines de $\Phi_p(X + 1)$, on a $\displaystyle\prod_{k=1}^{p-1}(\xi^k - 1) = (-1)^{p-1}p$. Par suite, $\mathrm{N}_{K/\mathbb{Q}}(\Phi_p'(\xi)) = p^{p-2}$. Finalement,

$$\mathrm{D} = (-1)^{(p-1)(p-2)/2}p^{p-2}$$

d'où le résultat si $p = 2$. Si p est impair, $p - 1$ est pair et $p - 2$ est impair donc

$$(-1)^{(p-1)(p-2)/2} = \left((-1)^{(p-1)/2}\right)^{p-2} = (-1)^{(p-1)/2}$$

d'où $\mathrm{D} = (-1)^{(p-1)/2}p^{p-2}$. ∎

Chapitre 2

Anneaux de Dedekind et factorisation d'idéaux

Notre but est maintenant de montrer que les anneaux d'entiers ont la propriété de factorisation en produit d'idéaux premiers. La preuve donnée fontionne pour une classe plus large d'anneaux, les anneaux de Dedekind.

2.1 Définition (Anneau de Dedekind). — *Un anneau est dit de Dedekind s'il est intégralement clos (donc intègre), noethérien et si tout idéal premier non nul est maximal (c'est-à-dire que l'anneau est de dimension $\leqslant 1$).*

2.2 Théorème. — *Soit A un anneau de Dedekind de corps des fractions K. On suppose la caractéristique de K nulle. Soit L une extension finie de degré n de K. Alors la clôture intégrale B de A dans L est un anneau de Dedekind.*

Preuve. — Le théorème 1.32 montre que $\mathcal{O}_K$ est intégralement clos, noethérien de corps des fractions égal à K. Il reste à prouver que tout idéal premier non nul est maximal.

Soit $\mathfrak{p}$ un idéal premier non nul de B. Montrons que l'idéal $\mathfrak{q} = \mathfrak{p} \cap A$ est non nul, donc maximal. Soit $x \in \mathfrak{p}$. On a une relation de dépendance intrégrale $x^d + a_{d-1}x^{d-1} + \cdots + a_0 = 0$ où on peut supposer $a_0 \neq 0$ en divisant éventuellement par des puissances de x. Alors $a_0 = -x(x^{d-1} + a_{k-1}x^{k-2} + \cdots + a_1)$ appartient à $\mathfrak{q} = \mathfrak{p} \cap A$.

Soit $(b_1, \ldots, b_n)$ un système générateur de B comme A-module (théorème 1.32). Les classes $(\overline{b_1}, \ldots, \overline{b_n})$ des b_i mod $(\mathfrak{q})$ forment un système générateur de $B/\mathfrak{q}$ en tant que $A/\mathfrak{p}$-espace vectoriel. Ainsi $B/\mathfrak{q}$ est une $A/\mathfrak{p}$ algèbre intègre finie, c'est donc un corps et l'idéal $\mathfrak{q}$ est maximal dans B.■

Avec $A = \mathbb{Z}$, $K = \mathbb{Q}$, obtient le corollaire suivant.

2.3 Corollaire. — *L'anneau des entiers d'un corps de nombres est de Dedekind.*

2.1 Idéaux inversibles

Soit A un anneau de Dedekind, K son corps des fractions et $\mathfrak{a}$ un idéal non nul de A. La clé dans la preuve de l'existence et l'unicité de la factorisation en idéaux est de montrer qu'il existe un autre idéal $\mathfrak{b}$ de A tel que $\mathfrak{ab}$ est principal. Commençons par quelques lemmes

2.4 Lemme. — *Soit A un anneau, $\mathfrak{p}$ un idéal premier et $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ des idéaux de A. Supposons que $\mathfrak{p} \supset \mathfrak{a}_1 \ldots \mathfrak{a}_n$. Alors $\mathfrak{p} \supset \mathfrak{a}_i$ pour un certain i.*

Preuve. — Supposons qu'il n'existe aucun i tel que $\mathfrak{p} \supset \mathfrak{a}_i$. Il existe alors $\pi_i \in \mathfrak{a}_i$ tel que $\pi_i \notin \mathfrak{p}$ pour tout i. Mais alors $\pi_1 \dots \pi_k \notin \mathfrak{p}$ puisque $\mathfrak{p}$ est premier, et ceci contredit l'inclusion $\mathfrak{a}_1 \dots \mathfrak{a}_k \subset \mathfrak{p}$. ∎

2.5 Lemme. — *Soit $\mathfrak{a}$ un idéal non nul de A. Alors il existe des idéaux premiers non nuls (pas nécessairement distincts) $\mathfrak{p}_1, \dots \mathfrak{p}_k$ de A tels que $\mathfrak{a} \supset \mathfrak{p}_1 \dots \mathfrak{p}_k$.*

Preuve. — Soit $\mathcal{S}$ l'ensemble des idéaux non nuls de A qui ne contiennent pas un produit d'idéaux premiers non nuls. Supposons que $\mathcal{S}$ est non vide. Puisque A est noethérien, $\mathcal{S}$ a un élément maximal, disons $\mathfrak{a}$. Cet idéal n'est pas premier, sinon il contiendrait un produit d'idéaux premiers (à savoir : lui-même). Ainsi il existe $\alpha, \beta \in \mathcal{O}_K$ tel que $\alpha, \beta \notin \mathfrak{a}$, mais $\alpha\beta \in \mathfrak{a}$. Considérons maintenant les idéaux $\mathfrak{a} + (\alpha)$ et $\mathfrak{a} + (\beta)$ qui contiennent strictement $\mathfrak{a}$ et donc qui ne sont pas dans $\mathcal{S}$. Ils contiennent un produit d'idéaux premiers non nuls par définitions de $\mathcal{S}$, et il en est de même du produit

$$(\mathfrak{a} + (\alpha))(\mathfrak{a} + (\beta)) = \alpha^2 + \alpha\mathfrak{a} + \beta\mathfrak{a} + \alpha\beta \subset \mathfrak{a}.$$

C'est une contradiction, donc $\mathcal{S}$ est vide. ∎

2.6 Lemme. — *Soit $\mathfrak{a}$ un idéal non nul de A tel que $\mathfrak{a} \neq A$. Alors il existe $\gamma \in K$ tel que $\gamma \notin A$ et $\gamma\mathfrak{a} \subset A$.*

Le lemme dit que $\mathfrak{a}$ est significativement distinct de A dans le sens où il y a un élément non entier de K que l'on peut multiplier par cet idéal laissant entier cet idéal. C'est faux pour K lui-même.

Preuve. — Fixons α non nul dans $\mathfrak{a}$. Par le lemme 2.5, l'idéal principal (α) contient un produit d'idéaux premiers non nuls. Choisissons les $\mathfrak{p}_1, \dots, \mathfrak{p}_k$ avec k minimal tels que $(\alpha) \supset \mathfrak{p}_1 \dots \mathfrak{p}_k$ (les $\mathfrak{p}_i$ ne sont pas nécessairement distincts). Mais $\mathfrak{a}$ est aussi contenu dans un idéal maximal $\mathfrak{p}$. Ainsi

$$\mathfrak{p} \supset \mathfrak{a} \supset (\alpha) \supset \mathfrak{p}_1 \dots \mathfrak{p}_k.$$

Par le lemme 2.4, on a que $\mathfrak{p}$ contient l'un des $\mathfrak{p}_i$. Sans perte de généralité, supposons que $\mathfrak{p}_1 \subset \mathfrak{p}$. Puisque A est un anneau de Dedekind, $\mathfrak{p}_1$ est maximal, et donc $\mathfrak{p} = \mathfrak{p}_1$.

Puisque (α) ne contient pas de produit de $k-1$ idéaux premiers, il existe un $\beta \in \mathfrak{p}_2 \dots \mathfrak{p}_k$ tel que $\beta \notin (\alpha)$. Soit $\gamma = \beta/\alpha$ et montrons que γ vérifie les conditions du lemme. Tout d'abord $\gamma \notin A$ puisque $\beta \notin (\alpha)$. Pour l'autre partie, si $\alpha' \in \mathfrak{a}$, alors

$$\gamma\alpha' = \frac{\beta\alpha'}{\alpha}.$$

Mais $\alpha' \in \mathfrak{a} \subset \mathfrak{p} = \mathfrak{p}_1$, donc

$$\beta\alpha' \in \mathfrak{p}_1 \dots \mathfrak{p}_k \subset (\alpha)$$

et ainsi $\gamma\alpha' = \beta\alpha'/\alpha \in A$, comme annoncé. ∎

Nous pouvons maintenant démontrer que chaque idéal de A est inversible en utilisant les deux lemmes précédents, et le fait que A est intégralement clos (remarquons qu'on a utilisé le fait que A est noethérien dans le lemme 2.5 et le fait que A est de dimension $\leqslant 1$ dans le lemme 2.6).

2.7 Proposition. — *Soit A un anneau de Dedekind, et $\mathfrak{a}$ un idéal non nul de A. Alors il existe un idéal non nul $\mathfrak{b}$ de A tel que $\mathfrak{ab}$ est principal.*

Preuve. — Fixons un $\alpha \in \mathfrak{a}$ non nul, et posons

$$\mathfrak{b} = \{\beta \in A | \beta\mathfrak{a} \subset (\alpha)\}.$$

Il est clair que $\mathfrak{b}$ est un idéal non nul de A (il contient α), et par définition $\mathfrak{ab} \subset (\alpha)$. On va montrer qu'on a égalité. Pour cela, posons

$$\mathfrak{c} = \frac{1}{\alpha}\mathfrak{ab}.$$

C'est un idéal de A, et montrer que $\mathfrak{ab} = (\alpha)$ revient à montrer que $\mathfrak{c} = A$. Supposons $\mathfrak{c} \neq A$. Par le lemme 2.6 on peut trouver $\gamma \in K$ avec $\gamma \notin A$ tel que $\gamma\mathfrak{c} \subset A$.

Puisque $\alpha \in \mathfrak{a}$, on a $\mathfrak{b} \subset \mathfrak{c}$, et donc $\gamma\mathfrak{b} \subset \gamma\mathfrak{c} \subset A$. Montrons que $\gamma\mathfrak{b} \subset \mathfrak{b}$. Prenons un élément arbitraire $\beta \in \mathfrak{b}$; on veut montrer que $\gamma\beta \in \mathfrak{b}$; pour cela on va prouver que pour tout $\alpha' \in \mathfrak{a}$, on a $\gamma\beta\alpha' \in (\alpha)$, ce qui impliquera bien $\gamma\beta \in \mathfrak{b}$ par définition de $\mathfrak{b}$ (en notant que $\gamma\beta \in A$ puisque $\gamma\beta \in \gamma\mathfrak{b} \subset \gamma\mathfrak{c} \subset A$). Soit donc $\alpha' \in \mathfrak{a}$. Alors $\beta\alpha' \in (\alpha)$ par définition de $\mathfrak{b}$ donc on peut écrire $\beta\alpha' = \alpha\delta$ pour un certain $\delta \in A$. Mais clairement $\delta \in \mathfrak{c}$, donc $\gamma\delta \in \gamma\mathfrak{c} \subset A$. Finalement,

$$\gamma\beta\alpha' = (\gamma\delta)\alpha \in (\alpha),$$

et on a bien $\gamma\beta \in \mathfrak{b}$, puis $\gamma\mathfrak{b} \subset \mathfrak{b}$.

Ainsi $\mathfrak{b}$ est stable par la multiplication par γ, mais $\mathfrak{b}$ étant un sous-A-module de type fini de K (car A est noethérien) l'assertion (iv) du théorème 1.22 montre que γ est entier sur A, donc $\gamma \in A$ puisque A est intégralement clos. Ceci contredit $\gamma \notin A$ et termine la preuve. ∎

2.2 Factorisation des idéaux

Avec la proposition 2.7, il ne va pas être difficile de prouver l'existence et l'unicité de la factorisation des idéaux. On donne en premier quelques résultats préliminaires.

2.8 Lemme. — *Soit $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ des idéaux de A. Alors si $\mathfrak{ab} = \mathfrak{ac}$, on a $\mathfrak{b} = \mathfrak{c}$.*

Preuve. — Soit $\mathfrak{a}'$ un idéal de A tel que $\mathfrak{aa}'$ est principal (par la proposition 2.7), et notons α un générateur de $\mathfrak{aa}'$. Il vient $\mathfrak{a}'\mathfrak{ab} = \mathfrak{a}'\mathfrak{ac}$, puis $\alpha\mathfrak{b} = \alpha\mathfrak{c}$ et finalement $\mathfrak{b} = \mathfrak{c}$. ∎

Ce lemme est faux si A n'est pas un anneau de Dedekind ; voir l'exemple 1.4 de $\mathbb{Z}[\sqrt{3}]$.

Si $\mathfrak{a}$ et $\mathfrak{b}$ sont des idéaux de A, on dit que $\mathfrak{b}$ divise $\mathfrak{a}$ s'il existe un idéal $\mathfrak{c}$ tel que $\mathfrak{a} = \mathfrak{bc}$. En particulier $\mathfrak{b} \supset \mathfrak{a}$; dans les anneaux de Dedekind, il y a équivalence.

2.9 Lemme. — *Soit $\mathfrak{a}$ et $\mathfrak{b}$ des idéaux de A. Alors $\mathfrak{b}$ divise $\mathfrak{a}$ si, et seulement, si $\mathfrak{b} \supset \mathfrak{a}$.*

Preuve. — Supposons $\mathfrak{b} \supset \mathfrak{a}$, et soit $\mathfrak{b}'$ tel que $\mathfrak{bb}'$ est principal, disons $\mathfrak{bb}' = (\beta)$. On vérifie que $\mathfrak{c} = \frac{1}{\beta}\mathfrak{b}'\mathfrak{a}$ est un idéal de A (en utilisant le fait que $\mathfrak{b} \supset \mathfrak{a}$). Il vient

$$\mathfrak{bc} = \frac{1}{\beta}\mathfrak{bb}'\mathfrak{a} = \frac{1}{\beta}(\beta)\mathfrak{a} = \mathfrak{a},$$

et donc $\mathfrak{b}$ divise $\mathfrak{a}$. ∎

Nous allons maintenant prouver le théorème de factorisation. On dira qu'un ideal $\mathfrak{a}$ de A se factorise en idéaux premiers si on peut écrire $\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_k$ où les $\mathfrak{p}_i$ sont des idéaux premiers non nuls de A. On dira que $\mathfrak{a}$ se factorise de façon unique en idéaux premiers si deux telles factorisations sont les mêmes à l'ordre des facteurs près (la langage est simplifié ici par rapport aux anneaux factoriels, car les unités et associés sont absorbés par les idéaux).

2.10 Théorème. — *Soit A un anneau de Dedekind. Alors tout idéal non nul de A se factorise de façon unique en idéaux premiers.*

Preuve. — Voyons d'abord que tout idéal non nul se factorise en idéaux premiers. Soit $\mathcal{S}$ l'ensemble des idéaux non nuls qui ne se factorisent pas en idéaux premiers, et supposons que $\mathcal{S}$ est non vide. Puisque A est noethérien, $\mathcal{S}$ a un élément maximal, disons $\mathfrak{a}$. On sait que $\mathfrak{a}$ est contenu dans un idéal maximal $\mathfrak{p}$; par le lemme 2.9 ceci implique $\mathfrak{a} = \mathfrak{p}\mathfrak{b}$ pour un idéal $\mathfrak{b}$ de A. Le même lemme implique $\mathfrak{b} \supset \mathfrak{a}$; en fait, on a $\mathfrak{b} \neq \mathfrak{a}$ car sinon le lemme 2.8 impliquerait $A = \mathfrak{p}$, ce qui n'est pas. Donc $\mathfrak{b} \notin \mathcal{S}$ puisque $\mathfrak{a}$ est maximal, donc $\mathfrak{b}$ se factorise en idéaux premiers. Mais $\mathfrak{a} = \mathfrak{p}\mathfrak{b}$ se factorise alors en idéaux premiers, ce qui est une contradiction. Ainsi $\mathcal{S}$ est vide.

Montrons maintenant l'unicité d'une telle factorisation. Soit $\mathfrak{a}$ un idéal avec deux factorisations, disons

$$\mathfrak{p}_1 \dots \mathfrak{p}_r = \mathfrak{q}_1 \dots \mathfrak{q}_s.$$

Le lemme 2.9 montre que $\mathfrak{p}_1 \supset \mathfrak{q}_1 \dots \mathfrak{q}_s$, et par le lemme 2.4 il vient que $\mathfrak{p}_1 \supset \mathfrak{q}_i$ pour un certain i. Quitte à réordonner les $\mathfrak{q}_j$, on peut supposer que $\mathfrak{p}_1 \supset \mathfrak{q}_1$. Puisque tout idéal premier non nul est maximal, on a $\mathfrak{p}_1 = \mathfrak{q}_1$. En utilisant le lemme 2.8, on peut simplifier le terme $\mathfrak{p}_1 = \mathfrak{q}_1$ de chaque côté, et on a

$$\mathfrak{p}_2 \dots \mathfrak{p}_r = \mathfrak{q}_2 \dots \mathfrak{q}_s.$$

En continuant ainsi, on trouve que $r = s$ et les facteurs de chaque côté sont identiques. ∎

Finissons par une proposition qui démontre que dans un anneau de Dedekind, la factorialité équivaut à la principalité, ce qui est faux en général.

2.11 Proposition. — *Soit A un anneau de Dedekind. Alors A est factoriel si, et seulement si, il est principal.*

Preuve. — On sait que tout anneau principal est factoriel, donc seule la réciproque est à montrer. Supposons A factoriel, et soit $\mathfrak{a}$ un idéal non nul de A ; on doit montrer qu'il est principal. Prenons $\alpha \in \mathfrak{a}$ non nul et écrivons $\alpha = \pi_1 \dots \pi_n$ sa décomposition en irréductibles. Puisque A est factoriel, chacun des idéaux π_i est premier, et donc l'équation

$$(\alpha) = (\pi_1) \dots (\pi_n)$$

donne une factorisation de (α) en idéaux premiers. Comme $(\alpha) \subset \mathfrak{a}$, l'idéal $\mathfrak{a}$ divise (α). En particulier, en utilisant l'unicité de la factorisation en idéaux premiers, cela implique que tous les facteurs idéaux premiers de $\mathfrak{a}$ sont principaux, donc $\mathfrak{a}$ est le produit d'idéaux principaux, donc est lui-même principal. ∎

Terminons par la preuve de la proposition 1.47 rappelée ici.

Proposition. — *Soit $\mathfrak{a}$ et $\mathfrak{b}$ deux idéaux non nuls de $\mathcal{O}_K$. Alors* $\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a}\mathfrak{b}) = \mathrm{N}_K(\mathfrak{a})\mathrm{N}_K(\mathfrak{b})$.

Preuve. — Remarquons que si $\mathfrak{a}$ et $\mathfrak{b}$ sont premiers entre eux, par le théorème chinois on a

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

et le résultat est clair. En utilisant la factorisation en idéaux premiers et cette remarque, on voit qu'il est suffisant de montrer que pour tout idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ on a $\mathrm{N}_K(\mathfrak{p}^m) = \mathrm{N}_K(\mathfrak{p})^m$. Or

$$\mathrm{N}_K(\mathfrak{p}^m) = \#(\mathcal{O}_K/\mathfrak{p}^m) = \#(\mathcal{O}_K/\mathfrak{p}) \times \#(\mathfrak{p}/\mathfrak{p}^2) \times \dots \times \#(\mathfrak{p}^{m-1}/\mathfrak{p}^m),$$

donc il est suffisant de montrer que $\#(\mathfrak{p}^k/\mathfrak{p}^{k+1}) = \#(\mathcal{O}_K/\mathfrak{p})$ pour tout k. Par unicité de la factorisation en idéaux premiers, on a $\mathfrak{p}^{k+1} \subsetneq \mathfrak{p}^k$. Soit alors $\gamma \in \mathfrak{p}^k \backslash \mathfrak{p}^{k+1}$. On montre que l'application $\varphi : \mathcal{O}_K/\mathfrak{p} \longrightarrow \mathfrak{p}^k/\mathfrak{p}^{k+1}, \alpha \longmapsto \alpha\gamma$ est un isomorphisme, d'où le résultat. ∎

2.3 Idéaux fractionnaires

Soit K un corps de nombre, et $\mathcal{O}_K$ son anneau des entiers. L'ensemble des idéaux de $\mathcal{O}_K$ est un monoïde, mais pas un groupe, car les idéaux n'ont pas d'inverse. Nous allons plonger l'ensemble de ces idéaux dans le groupe des idéaux dits fractionnaires de K.

2.12 Définition (Idéal fractionnaire). — *Soit $\mathfrak{r}$ un $\mathcal{O}_K$-module de K. Un tel $\mathfrak{r}$ est appelé idéal fractionnaire de K s'il existe $\gamma_1, \dots, \gamma_m \in \mathfrak{r}$ tels que*

$$\mathfrak{r} = \{\alpha_1\gamma_1 + \cdots + \alpha_m\gamma_m \,|\, \alpha_i \in \mathcal{O}_K\}.$$

Chaque idéal non nul $\mathfrak{a}$ de $\mathcal{O}_K$ est un idéal fractionnaire. En effet $\mathfrak{a}$ est un $\mathcal{O}_K$-module par définition, et il est finiment engendré puisque $\mathcal{O}_K$ est noethérien. Pour éviter les confusions on parlera d'idéaux entiers dorénavant.

Une seconde sorte d'idéaux fractionnaires sont très importants, ce sont ceux de la forme $\gamma\mathcal{O}_K$, avec $\gamma \in K^*$ (il est immédiat que $\gamma\mathcal{O}_K$ est un $\mathcal{O}_K$-module et que γ est un générateur). Un tel idéal fractionnaire est appelé idéal fractionnaire principal. Notons que les idéaux principaux de $\mathcal{O}_K$ sont précisément les idéaux fractionnaires principaux entiers.

Plus généralement, si $\mathfrak{a}$ est un idéal quelconque de $\mathcal{O}_K$ et γ un élément de K^*, alors $\gamma\mathfrak{a}$ est un idéal fractionnaire. La réciproque est vraie.

2.13 Lemme. — *Soit $\mathfrak{r}$ un $\mathcal{O}_K$-module de K. Alors $\mathfrak{r}$ est un idéal fractionnaire si et seulement s'il existe $\gamma \in K^*$ tel que $\gamma\mathfrak{r}$ est un idéal entier (en fait on peut prendre $\gamma \in \mathbb{Z}$).*

Preuve. — Seul le sens direct est à vérifier. Si $\mathfrak{r}$ est un idéal fractionnaire, on peut écrire

$$\mathfrak{r} = \{\alpha_1\gamma_1 + \cdots + \alpha_m\gamma_m \,|\, \alpha_i \in \mathcal{O}_K\}$$

pour des $\gamma_1, \dots, \gamma_m \in \mathfrak{r}$. Par la proposition 1.36, il existe $a_1, \dots, a_m \in \mathbb{Z}$ tels que $a_i\gamma_i \in \mathcal{O}_K$. Alors $a_1 \dots a_m\mathfrak{r}$ est un idéal entier, ce qui prouve le lemme avec $\gamma = a_1 \dots a_m$. ∎

On notera I_K l'ensemble des idéaux fractionnaires de K. Si $\mathfrak{r}, \mathfrak{s} \in I_K$, on définit le produit $\mathfrak{rs}$ comme le $\mathcal{O}_K$-module engendré par tous les produits d'éléments de $\mathfrak{r}$ et $\mathfrak{s}$. Si $\mathfrak{r}$ est engendré par $\gamma_1, \dots, \gamma_m$ et $\mathfrak{s}$ par $\delta_1, \dots, \delta_k$, alors $\mathfrak{rs}$ est engendré par les $\gamma_i\delta_j$. En particulier $\mathfrak{rs}$ est un idéal fractionnaire.

2.14 Corollaire. — *L'ensemble I_K est un groupe commutatif pour la multiplication des idéaux fractionnaires.*

Preuve. — Nous avons vu ci-dessus que I_K est stable pour la multiplication. La commutativité est la distributivité sont claires. Le neutre est $\mathcal{O}_K$. Il reste à trouver l'inverse d'un idéal fractionnaire $\mathfrak{r}$. Soit $\gamma \in K^*$ tel que $\gamma\mathfrak{r}$ soit un idéal entier. Par la proposition 2.7, il existe un idéal entier $\mathfrak{b}$ tel que $\gamma\mathfrak{rb}$ est principal disons engendré par $\alpha \in \mathcal{O}_K$, avec $\alpha \neq 0$. Posons $\mathfrak{s} = \dfrac{\gamma}{\alpha}\mathfrak{b}$. C'est un idéal fractionnaire et

$$\mathfrak{rs} = \frac{\gamma}{\alpha}\mathfrak{rb} = \frac{1}{\alpha}(\alpha) = \mathcal{O}_K$$

Ainsi $\mathfrak{s}$ est un inverse pour $\mathfrak{r}$ dans I_K. ∎

On peut aussi caractériser les idéaux fractionnaires en termes de factorisation unique en idéaux.

2.15 Proposition. — *Tout idéal fractionnaire $\mathfrak{r}$ peut s'écrire $\mathfrak{r} = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$ où les $\mathfrak{p}_i$ sont des idéaux premiers distincts et les e_i des entiers (éventuellement négatifs). Cette factorisation est unique à l'ordre des facteurs près. De plus $\mathfrak{r}$ est un idéal entier si et seulement si tout les e_i sont positifs.*

Preuve. — Soit $\mathfrak{r}$ un idéal fractionnaire et soit $a \in \mathbb{Z}$ non nul tel que $a\mathfrak{r}$ soit un idéal entier. Alors on peut écrire de façon unique à l'ordre des facteurs près et ajout de facteurs avec un exposant 0,

$$(a) = \mathfrak{p}_1^{e'_1} \dots \mathfrak{p}_r^{e'_r} \quad \text{et} \quad a\mathfrak{r} = \mathfrak{p}_1^{e''_1} \dots \mathfrak{p}_r^{e''_r}$$

avec éventuellement des e'_i et e''_i nuls. Ainsi, puisque I_K est un groupe,

$$\mathfrak{r} = \mathfrak{p}_1^{e''_1 - e'_1} \dots \mathfrak{p}_r^{e''_r - e'_r}.$$

Ce qui montre que $\mathfrak{r}$ s'écrit sous la forme annoncé. L'unicité provient du fait que les factorisations de (a) et $a\mathfrak{r}$ sont uniques. Enfin le fait que $\mathfrak{r}$ est un idéal entier si et seulement si tout les e_i sont positifs est clair par unicité de la factorisation en idéaux. ∎

La décomposition des idéaux fractionnaires en idéaux premiers est totalement analogue à la décomposition des nombres rationnels en entiers rationnels.

Chapitre 3

Factorisation effective en idéaux premiers

3.1 Lemme. — *Soit $\mathfrak{p}$ un idéal premier non nul de $\mathcal{O}_K$. Alors $\mathfrak{p}$ contient un unique entier rationnel premier.*

Preuve. — Par le lemme 1.38, on sait que $\mathfrak{p}$ contient un entier rationnel non nul. Soit n le plus petit entier positif contenu dans $\mathfrak{p}$. Puisque $\mathfrak{p} \neq \mathcal{O}_K$, on a $n > 1$. Supposons que n n'est pas premier dans $\mathbb{Z}$. Alors $n = ab$ avec $n > a, b > 1$, et comme $\mathfrak{p}$ est premier, c'est que $a \in \mathfrak{p}$ ou $b \in \mathfrak{p}$ ce qui contredit la minimalité de n. Supposons que p' soit un deuxième entier premier contenu dans $\mathfrak{p}$. Alors il existe $u, v \in \mathbb{Z}$ tels que $up + vp' = 1$, donc $1 \in \mathfrak{p}$, ce qui est absurde. ∎

La proposition qui suit nous donne un moyen de trouver tous les idéaux premiers de $\mathcal{O}_K$.

3.2 Proposition. — *Soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$. Alors $\mathfrak{p}$ apparaît dans la factorisation de $p\mathcal{O}_K$ pour un unique p premier rationnel. De plus $\mathrm{N}_K(\mathfrak{p})$ est une puissance de p.*

Preuve. — Par le lemme, il existe p premier rationnel dans $\mathfrak{p}$, donc $\mathfrak{p} \supset p\mathcal{O}_K$. Ainsi $\mathfrak{p}$ divise $p\mathcal{O}_K$, et par le lemme 2.9, $\mathfrak{p}$ figure dans la décomposition en idéaux premiers de $p\mathcal{O}_K$.
Puisque $\mathfrak{p} \supset p\mathcal{O}_K$, l'entier $\mathrm{N}_K(\mathfrak{p})$ est un facteur de $\mathrm{N}_K(p\mathcal{O}_K) = p^n$. Ainsi $\mathrm{N}_K(\mathfrak{p}) = p^k$ pour un $1 \leqslant k \leqslant n$. Ceci montre aussi l'unicité de p. ∎

Ainsi pour trouver les idéaux premiers de $\mathcal{O}_K$, il nous suffit de factoriser les idéaux $p\mathcal{O}_K$ pour les p premiers dans $\mathbb{N}$, c'est l'objet de ce chapitre.

3.1 Localisation des anneaux d'entiers

Faisons quelques rappels sur la localisation. On se place dans le cas particulier des anneaux intègres qui est suffisant pour notre propos.

3.3 Définition. — *Soit A un anneau intègre, K son corps des fractions et S une partie de A stable pour la multiplication contenant 1 et ne contenant pas 0 (appelée partie multiplicative de A dans la suite). On appelle localisé en S de A et on note $S^{-1}A$ l'ensemble des éléments $\dfrac{a}{s} \in K$ avec $a \in A$ et $s \in S$.*

3.4 Proposition. — *Soit A un anneau intègre et S une partie multiplicative de A. On pose $A' = S^{-1}A$. Pour tout idéal $\mathfrak{P}$ de A', on a $(\mathfrak{P} \cap A)A' = \mathfrak{P}$, de sorte que $\varphi : \mathfrak{P} \mapsto \mathfrak{P} \cap A$ est une injection croissante (pour l'inclusion) de l'ensemble des idéaux de A' dans l'ensemble des idéaux de A.*

Preuve. — Soit $\mathfrak{P}$ un idéal de A'. On a $\mathfrak{P} \cap A \subset \mathfrak{P}$, donc $(\mathfrak{P} \cap A)A' \subset \mathfrak{P}$. Réciproquement, soit $x \in \mathfrak{P}$; on a $x = a/s$ avec $a \in A$ et $s \in S$. Or $sx \in \mathfrak{P}$ car $\mathfrak{P}$ est un idéal et $A \subset A'$, d'où $a \in \mathfrak{P}$ et $a \in \mathfrak{P} \cap A$. Ainsi $x = a/s \in (\mathfrak{P} \cap A)A'$ d'où l'égalité $(\mathfrak{P} \cap A)A' = \mathfrak{P}$. En notant $\theta : \mathfrak{P} \mapsto A'\mathfrak{P}$, on a $\theta \circ \varphi = \mathrm{Id}$, donc φ est injective ; elle est clairement croissante. ∎

3.5 Proposition. — *Soit A un anneau intègre, S une partie multiplicative et $\mathfrak{a}$ un idéal maximal de A ne rencontrant pas S. Alors $S^{-1}A/\mathfrak{a}S^{-1}A \simeq A/\mathfrak{a}$.*

Preuve. — L'homomorphisme composé $A \hookrightarrow S^{-1}A \twoheadrightarrow S^{-1}A/\mathfrak{a}S^{-1}A$ a pour noyau $\mathfrak{a}S^{-1}A \cap A = \mathfrak{a}$ d'après la proposition 3.4, d'où une injection $\varphi : A/\mathfrak{a} \hookrightarrow S^{-1}A/\mathfrak{a}S^{-1}A$. Montrons que φ est surjective. Soit $x = \dfrac{a}{s} \in S^{-1}A$ avec $a \in A$ et $s \in S$. Comme $s \notin \mathfrak{a}$ (puisque $\mathfrak{a} \cap S = \varnothing$) et comme $\mathfrak{a}$ est maximal, s est inversible mod $(\mathfrak{a})$ et il existe b tel que $bs \equiv 1 \bmod (\mathfrak{a})$. Alors $\dfrac{a}{s} - ab = \dfrac{a}{s}(1 - bs) \in \mathfrak{a}S^{-1}A$, de sorte que l'image par φ de la classe de ab est égale à la classe de $\dfrac{a}{s} = x$. ∎

3.6 Proposition. — *Soit K un corps, A un sous-anneau, $S \subset A$ une partie multiplicative, B la fermeture intégrale de A dans K. Alors $S^{-1}B$ est la fermeture intégrale de $S^{-1}A$ dans K.*

Preuve. — Soit $b' = \dfrac{b}{s} \in S^{-1}B$ où $b \in B$ et $s \in S$. On a une relation de dépendance intégrale

$$b^m + a_{m-1}b^{m-1} + \cdots + a_1 b + a_0 = 0$$

où les a_i sont dans A. On en déduit

$$\left(\frac{b}{s}\right)^m + \frac{a_{m-1}}{s}\left(\frac{b}{s}\right)^{m-1} + \cdots + \frac{a_1}{s^{m-1}}\left(\frac{b}{s}\right) + \frac{a_0}{s^m} = 0$$

ce qui montre que que $S^{-1}B$ est entier sur $S^{-1}A$.

Soit $z \in K$ entier sur $S^{-1}B$. On a une relation de dépendance intégrale

$$z^n + b'_{n-1}z^{n-1} + \ldots b'_1 z + b'_0 = 0.$$

En réduisant les b'_i au même dénominateur, on peut écrire $b'_i = \dfrac{b_i}{s}$ où $b_i \in B$ et $s \in S$. En multipliant la relation précédente par s^n, il vient

$$(sz)^n + b_{n-1}(sz)^{n-1} + b_{n-2}s(sz)^{n-2} + \cdots + b_1 s^{n-2}(sz) + b_0 s^{n-1} = 0.$$

Ainsi sz est entier sur B, donc sz appartient à B car B est intégralement clos, d'où $z \in S^{-1}B$ et $S^{-1}B$ est la fermeture intégrale de $S^{-1}A$ dans K. ∎

Soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$. On note $\mathcal{O}_{K,\mathfrak{p}}$ le localisé de $\mathcal{O}_K$ par rapport à la partie multiplicative $S = \mathcal{O}_K \backslash \mathfrak{p}$, c'est-à-dire

$$\mathcal{O}_{K,\mathfrak{p}} = \left\{ \frac{\alpha}{\beta} \in K \,|\, \alpha \in \mathcal{O}_K,\, \beta \in \mathcal{O}_K \backslash \mathfrak{p} \right\}.$$

Les idéaux de $\mathcal{O}_{K,\mathfrak{p}}$ ont une forme particulièrement simple comme le montre le lemme suivant.

3.7 Lemme. — *Tout idéal de $\mathcal{O}_{K,\mathfrak{p}}$ est de la forme $\mathfrak{p}^n\mathcal{O}_{K,\mathfrak{p}}$ pour $n \geqslant 0$.*

Preuve. — Soit $\mathfrak{a}$ un idéal de $\mathcal{O}_{K,\mathfrak{p}}$. D'après la proposition 3.4, on a $\mathfrak{a} = (\mathfrak{a} \cap \mathcal{O}_K)\mathcal{O}_{K,\mathfrak{p}}$. Considérons maintenant la factorisation de $\mathfrak{a} \cap \mathcal{O}_K$ dans $\mathcal{O}_K$. On l'écrit sous la forme

$$\mathfrak{a} \cap \mathcal{O}_K = \mathfrak{p}^n \mathfrak{b}$$

pour un certain $n \geqslant 0$ et un idéal $\mathfrak{b}$ premier avec $\mathfrak{p}$. L'idéal $\mathfrak{b}$ n'est pas contenu dans l'idéal $\mathfrak{p}$ puisque $\mathfrak{b}$ n'est pas divisible par $\mathfrak{p}$. En particulier, $\mathfrak{b}$ contient des éléments de $\mathcal{O}_K \backslash \mathfrak{p}$; ce sont des unités de $\mathcal{O}_{K,\mathfrak{p}}$, donc $\mathfrak{b}\mathcal{O}_{K,\mathfrak{p}} = \mathcal{O}_{K,\mathfrak{p}}$. Ainsi

$$\mathfrak{a} = (\mathfrak{a} \cap \mathcal{O}_K)\mathcal{O}_{K,\mathfrak{p}} = \mathfrak{p}^n \mathfrak{b}\mathcal{O}_{K,\mathfrak{p}} = \mathfrak{p}^n \mathcal{O}_{K,\mathfrak{p}},$$

ce qui est le résultat annoncé. ∎

3.8 Proposition. — *L'anneau $\mathcal{O}_{K,\mathfrak{p}}$ est de Dedekind.*

Preuve. — Soit $\mathfrak{p}_1 \subset \mathfrak{p}_2 \subset \dots$ une suite croissante d'idéaux de $\mathcal{O}_{K,\mathfrak{p}}$. D'après la proposition 3.4, $\varphi(\mathfrak{p}_1) \subset \varphi(\mathfrak{p}_2) \subset \dots$ est une suite croissante d'idéaux de $\mathcal{O}_K$, mais cet anneau est noethérien, donc cette suite stationne à partir d'un certain rang, et par injectivité il en est de même de la suite $\mathfrak{p}_n$, ceci prouve que $\mathcal{O}_{K,\mathfrak{p}}$ est noethérien.

D'après le lemme précédent, le seul idéal premier de $\mathcal{O}_{K,\mathfrak{p}}$ est $\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}}$. Soit $\mathfrak{a}$ un idéal maximal contenant $\mathfrak{p}$, alors $\mathfrak{a} = \mathfrak{p}^n \mathcal{O}_K$ pour un certain n. Mais comme $\mathfrak{p}\mathcal{O}_K \subset \mathfrak{a}$, il vient $\mathfrak{a} = \mathfrak{p}\mathcal{O}_K$, ce qui prouve que $\mathfrak{p}\mathcal{O}_K$ est maximal.

En appliquant la proposition 3.6 avec $A = B = \mathcal{O}_K$, puisque K est le corps des fractions de $\mathcal{O}_K$, il vient que la fermeture intégrale de $\mathcal{O}_{K,\mathfrak{p}}$ dans K est $\mathcal{O}_{K,\mathfrak{p}}$, donc en particulier $\mathcal{O}_{K,\mathfrak{p}}$ est intégralement clos. ∎

3.9 Proposition. — *L'anneau $\mathcal{O}_{K,\mathfrak{p}}$ est principal.*

Preuve. — Notons $\mathfrak{q} = \mathfrak{p}\mathcal{O}_{K,\mathfrak{p}}$ son unique idéal premier non nul. Tout idéal est de la forme $\mathfrak{q}^n$, donc il suffit de voir que $\mathfrak{q}$ lui-même est principal. Soit π un élément de $\mathfrak{q}$ n'appartenant pas à $\mathfrak{q}^2$. Il existe donc $n \geqslant 1$ tel que $\pi\mathcal{O}_{K,\mathfrak{p}} = \mathfrak{q}^n$. Mais on ne peut pas avoir $n \geqslant 2$, sinon π appartiendrait à $\mathfrak{q}^2$. Donc $n = 1$ et $\mathfrak{q} = \pi\mathcal{O}_{K,\mathfrak{p}}$. ∎

Considérons maintenant L/K une extension de corps de nombres de degré n et $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$. Notons $\mathcal{O}_{L,\mathfrak{p}}$ l'anneau

$$\mathcal{O}_{L,\mathfrak{p}} = \left\{ \frac{\alpha}{\beta} \in L \,|\, \alpha \in \mathcal{O}_L,\, \beta \in \mathcal{O}_K \backslash \mathfrak{p} \right\},$$

qui n'est autre que le localisé de $\mathcal{O}_L$ en $\mathcal{O}_K \backslash \mathfrak{p}$.

3.10 Lemme. — *Dans les conditions ci-dessus, on a*
(i) $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \simeq \mathcal{O}_{L,\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{L,\mathfrak{p}}$.
(ii) $\mathcal{O}_{L,\mathfrak{p}}$ *est un* $\mathcal{O}_{K,\mathfrak{p}}$*-module libre de rang* n.

Preuve. — L'anneau $\mathcal{O}_L$ est de Dedekind, donc $\mathfrak{p}\mathcal{O}_L$, qui est premier, est maximal. Par la proposition 3.5 appliquée avec $A = \mathcal{O}_L$ et $S = \mathcal{O}_K \backslash \mathfrak{p}$, on a l'isomorphisme de (i).

L'assertion (ii) résulte du corollaire 1.33 avec $A = \mathcal{O}_{K,\mathfrak{p}}$ qui est un anneau de Dedekind principal, K le corps des fractions de A et B la fermeture intégrale de $\mathcal{O}_{K,\mathfrak{p}}$ dans L qui d'après la proposition 3.6 est $\mathcal{O}_{L,\mathfrak{p}}$. ∎

3.11 Proposition. — *Soit $\mathfrak{p}$ un idéal non nul de $\mathcal{O}_K$. Alors $\#(\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L) = (\#(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K))^n$.*

Preuve. — Remarquons d'abord que d'après la proposition 1.39, le nombre $\#(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)$ est fini. Le lemme ci-dessus montre que $\mathcal{O}_{L,\mathfrak{p}}$ est un $\mathcal{O}_{K,\mathfrak{p}}$-module libre de rang n. Ainsi $\mathcal{O}_{L,\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{L,\mathfrak{p}}$ est un $\mathcal{O}_{K,\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}}$-module libre de rang n d'où

$$\#(\mathcal{O}_{L,\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{L,\mathfrak{p}}) = (\#(\mathcal{O}_{K,\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}}))^n.$$

Mais ces anneaux sont respectivement isomorphes à $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ et $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$, toujours grâce au lemme. D'où le résultat. ∎

3.12 Théorème. — *Soit L/K une extension de corps de nombres de degré n et soit $\mathfrak{a}$ un idéal non nul de $\mathcal{O}_K$. Alors*

$$N_L(\mathfrak{a}\mathcal{O}_L) = N_K(\mathfrak{a})^n.$$

Preuve. — Puisque la norme est multiplicative, il suffit de prouver ce résultat pour les idéaux premiers. C'est ce qui a été fait dans la proposition précédente. ∎

3.2 Factorisation dans les extensions

3.2.1 Ramification

On considère toujours une extension L/K de corps de nombres de degré n.

3.13 Lemme. — *Soit $\mathfrak{p}$ un idéal premier non nul de $\mathcal{O}_K$ et soit $\mathfrak{P}$ un idéal premier non nul de $\mathcal{O}_L$. Les cinq conditions suivantes sont équivalentes.*

(i) $\mathfrak{P}$ *divise* $\mathfrak{p}\mathcal{O}_L$ *;*
(ii) $\mathfrak{P} \supset \mathfrak{p}\mathcal{O}_L$ *;*
(iii) $\mathfrak{P} \supset \mathfrak{p}$ *;*
(iv) $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$ *;*
(v) $\mathfrak{P} \cap K = \mathfrak{p}$.

Preuve. — Montrons que chaque assertion est équivalente à la suivante. L'équivalence de (i) et (ii) est le lemme 2.9 et celle de (ii) et (iii) vient de la définition de l'idéal $\mathfrak{p}\mathcal{O}_L$ engendré par $\mathfrak{p}$. Il est clair que (iv) implique (iii) ; réciproquement supposons que $\mathfrak{P} \supset \mathfrak{p}$. Alors l'idéal $\mathfrak{P} \cap \mathcal{O}_K$ de $\mathcal{O}_K$ contient $\mathfrak{p}$. Puisque $\mathfrak{p}$ est maximal, ceci implique soit $\mathfrak{P} \cap \mathcal{O}_K = \mathcal{O}_K$, soit $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$. La première possibilité ne peut pas se produire, car alors $\mathfrak{P}$ contiendrait 1 et serait $\mathcal{O}_L$, d'où (iii) implique (iv). Enfin (v) implique clairement (iv). Réciproquement, supposons que $\mathfrak{P} \cap K = \mathfrak{p}$; on a $\mathfrak{P} \cap \mathcal{O}_K \subset \mathfrak{p}$ et l'inclusion inverse résulte du lemme 1.35. ∎

3.14 Définition. — *Si $\mathfrak{p}$ et $\mathfrak{P}$ satisfont les propriétés équivalents du lemme, on dit que $\mathfrak{P}$ est au-dessus de $\mathfrak{p}$ ou que $\mathfrak{p}$ est au-dessous de $\mathfrak{P}$.*

3.15 Proposition. — *Chaque idéal premier $\mathfrak{P}$ de $\mathcal{O}_L$ est au-dessus d'un unique idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$, et chaque idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ est au-dessous d'au moins un idéal premier $\mathfrak{P}$ de $\mathcal{O}_L$.*

Preuve. — Soit $\mathfrak{P}$ un idéal premier de $\mathcal{O}_L$. Alors $\mathfrak{P} \cap \mathcal{O}_K$ est un idéal premier non nul de $\mathcal{O}_K$ (le fait qu'il soit premier résulte de la définition, et qu'il soit non nul du fait que $\mathfrak{P}$ contient un entier non nul). Le lemme 3.13 montre que cet idéal est nécessairement unique.

Considérons l'idéal $\mathfrak{p}\mathcal{O}_L$. Par le lemme 2.6, il existe $\gamma \in K\backslash\mathcal{O}_K$ tel que $\gamma\mathfrak{p} \subset \mathcal{O}_K$. Il vient que $\gamma\mathfrak{p}\mathcal{O}_L \subset \mathcal{O}_L$. Si $1 \in \mathfrak{p}\mathcal{O}_L$, cette inclusion conduit à $\gamma \in \mathcal{O}_L$, ce qui impossible puisque $\gamma \notin \mathcal{O}_L$ (en effet $\mathcal{O}_L \cap K = \mathcal{O}_K$ et $\gamma \in K\backslash\mathcal{O}_K$). Ainsi $\mathfrak{p}\mathcal{O}_L \neq \mathcal{O}_L$. Il existe donc un idéal maximal $\mathfrak{P}$ contenant $\mathfrak{p}\mathcal{O}_L$ et par le lemme 3.13 $\mathfrak{P}$ est au-dessus de $\mathfrak{p}$. ∎

Notons également que par le lemme 3.13, les idéaux premiers au-dessus de $\mathfrak{p}$ sont précisément ceux qui interviennent dans la factorisation de $\mathfrak{p}\mathcal{O}_L$. En notant $e(\mathfrak{P}/\mathfrak{p})$ la puissance exacte de $\mathfrak{P}$ qui divise $\mathfrak{p}\mathcal{O}_L$, on peut écrire

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

Soit p l'unique l'unique entier positif premier contenu dans $\mathfrak{p}$ et $\mathfrak{P}$. Alors $\mathcal{O}_K/\mathfrak{p}$ et $\mathcal{O}_L/\mathfrak{P}$ sont des corps finis de caractéristique p. De plus l'injection naturelle $\mathcal{O}_K \hookrightarrow \mathcal{O}_L$ induit une injection $\mathcal{O}_K/\mathfrak{p} \hookrightarrow \mathcal{O}_L/\mathfrak{P}$ puisque $\mathfrak{P}\cap\mathcal{O}_K = \mathfrak{p}$ par le lemme 3.13. Ainsi $\mathcal{O}_L/\mathfrak{P}$ est une extension de $\mathcal{O}_K/\mathfrak{p}$. On note $f(\mathfrak{P}/\mathfrak{p})$ le degré de cette extension.

3.16 Définition (Indice de ramification, degré d'inertie). — *$e(\mathfrak{P}/\mathfrak{p})$ et $f(\mathfrak{P}/\mathfrak{p})$ s'appellent respectivement l'indice de ramification de $\mathfrak{P}/\mathfrak{p}$ et le degré d'inertie de $\mathfrak{P}/\mathfrak{p}$.*

Remarquons que $\mathrm{N}_L(\mathfrak{P}) = \mathrm{N}_K(\mathfrak{p})^{f(\mathfrak{P}/\mathfrak{p})}$.

3.17 Théorème. — *Soit L/K une extension de corps de nombres de degré n et soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$. Soit*

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}$$

la factorisation de $\mathfrak{p}\mathcal{O}_L$ en idéaux premiers de $\mathcal{O}_L$. Posons $f_i = f(\mathfrak{P}_i/\mathfrak{p})$. Alors

$$\sum_{i=1}^{r} e_i f_i = n.$$

Preuve. — En prenant la norme des deux côtés de la factorisation de $\mathfrak{p}\mathcal{O}_L$, on trouve

$$\mathrm{N}_L(\mathfrak{p}\mathcal{O}_L) = \mathrm{N}_L(\mathfrak{P}_1)^{e_1} \dots \mathrm{N}_L(\mathfrak{P}_r)^{e_r} = \mathrm{N}_K(\mathfrak{p})^{f_1 e_1} \dots \mathrm{N}_K(\mathfrak{p})^{f_r e_r}.$$

Par le théorème 3.12, $\mathrm{N}_L(\mathfrak{p}\mathcal{O}_L) = \mathrm{N}_K(\mathfrak{p})^n$, d'où le résultat en comparant les degrés. ∎

3.18 Définition (Ramifié, inerte, décomposé). — *Avec les notations du théorème,*
(i) si l'un des e_i n'est pas égal à 1, on dit que $\mathfrak{p}$ est ramifié sur L, et totalement ramifié si $r = 1$ et $e_1 = n$ (donc $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}^n$);
(ii) si $r = 1$ et $e_1 = 1$, on dit que $\mathfrak{p}$ est inerte sur L.
(iii) $e_i = f_i = 1$ pour tout i, on dit que $\mathfrak{p}$ est décomposé sur L ($\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1 \dots \mathfrak{P}_n$).

Signalons enfin le théorème suivant, donné sans preuve.

3.19 Théorème. — *Soit K un corps de nombre et* D *son discriminant. Soit p un rationnel premier. Alors p se ramifie dans K si, et seulement si, p divise* D.

3.2.2 Cas des extensions galoisiennes

Soit L/K une extension galoisienne. La présence d'automorphisme de K donne une factorisation plus régulière que dans une extension quelconque ; nous appliquerons les résultats de cette partie aux extensions cyclotomiques.

3.20 Lemme. — *Soit L/K une extension galoisienne et $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$. Alors le groupe $Gal(L/K)$ agit transitivement sur l'ensemble des idéaux premiers au-dessus de $\mathfrak{p}$.*

Preuve. — Soit $\mathfrak{P}$ un idéal premier au-dessus de $\mathfrak{p}$ et $\sigma \in \mathrm{Gal}(L/K)$. Comme σ est surjective, $\sigma(\mathfrak{P})$ est un idéal. Soit $x, y \notin \sigma(\mathfrak{P})$. Il existe $x', y' \notin \mathfrak{P}$ tels que $x = \sigma(x')$ et $y = \sigma(y')$. Mais $x'y' \notin \mathfrak{P}$, donc $xy = \sigma(x'y') \notin \sigma(\mathfrak{P})$, donc $\sigma(\mathfrak{P})$ est premier. Ceci montre que $\mathrm{Gal}(L/K)$ agit sur l'ensemble des idéaux premiers au-dessus de $\mathfrak{p}$.

Soit $\mathfrak{P}$ et $\mathfrak{P}'$ deux idéaux premiers au-dessus de $\mathfrak{p}$. Supposons que pour tout $\sigma \in \mathrm{Gal}(L/K)$ on ait $\sigma(\mathfrak{P}) \neq \mathfrak{P}'$. Par le théorème chinois on peut trouver $\alpha \in \mathcal{O}_L$ tel que

$$\alpha \equiv 0 \bmod (\mathfrak{P}') \quad \text{et} \quad \alpha \equiv 1 \bmod (\sigma(\mathfrak{P}))$$

pour tout $\sigma \in \mathrm{Gal}(L/K)$. Considérons

$$\mathrm{N}_{L/K}(\alpha) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\alpha) \in \mathcal{O}_K.$$

Puisque $\alpha \in \mathfrak{P}'$, sa norme appartient à $\mathfrak{P}' \cap \mathcal{O}_K = \mathfrak{p}$.

D'autre part, puisque $\alpha \equiv 1 \bmod (\sigma(\mathfrak{P}))$ pour tout $\sigma \in \mathrm{Gal}(L/K)$, on a aussi $\alpha \notin \sigma(\mathfrak{P})$; ainsi $\sigma^{-1}(\alpha) \notin \mathfrak{P}$ pour tout σ. Quand σ parcourt $\mathrm{Gal}(L/K)$, σ^{-1} parcourt aussi $\mathrm{Gal}(L/K)$, donc

$$\mathrm{N}_{L/K}(\alpha) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma^{-1}(\alpha).$$

Puisque qu'aucun des facteurs n'appartient à $\mathfrak{P}$ et que $\mathfrak{P}$ est premier, on a $\mathrm{N}_{L/K}(\alpha) \notin \mathfrak{P}$. Par suite $\mathrm{N}_{L/K}(\alpha) \notin \mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$, ce qui est une contradiction. ∎

3.21 Théorème. — *Soit L/K une extension galoisienne de degré n et $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$. Soit*

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}$$

la factorisation de $\mathfrak{p}$ dans $\mathcal{O}_L$, et soit $f_i = f(\mathfrak{P}_i/\mathfrak{p})$. Alors

$$f_1 = \dots = f_r \quad \text{et} \quad e_1 = \dots = e_r.$$

En particulier $re_if_i = n$ pour tout i.

Preuve. — Si $r = 1$, le résultat est clair. Supposons $r \geqslant 2$ et prouvons que $e_1 = e_2$ et $f_1 = f_2$; le cas général est similaire. Par le lemme il existe $\sigma \in \mathrm{Gal}(L/K)$ tel que $\sigma(\mathfrak{P}_1) = \mathfrak{P}_2$. En appliquant σ à notre factorisation et en utilisation le fait $\sigma(\mathfrak{p}) = \mathfrak{p}$, il vient

$$\mathfrak{p}\mathcal{O}_L = \sigma(\mathfrak{P}_1)^{e_1}\sigma(\mathfrak{P}_2)^{e_2} \dots \sigma(\mathfrak{P}_r)^{e_r} = \mathfrak{P}_2^{e_1}\sigma(\mathfrak{P}_2)^{e_2} \dots \sigma(\mathfrak{P}_r)^{e_r}.$$

De plus si $\sigma(\mathfrak{P}_i) = \mathfrak{P}_2$, alors $\mathfrak{P}_i = \sigma^{-1}(\mathfrak{P}_2) = \mathfrak{P}_1$; donc $\sigma(\mathfrak{P}_i) \neq \mathfrak{P}_2$ pour $i \geqslant 2$. Ainsi $\mathfrak{P}_2^{e_1}$ est la seule occurrence de $\mathfrak{P}_2$ dans la factorisation de $\mathfrak{p}\mathcal{O}_K$; par unicité, on a bien $e_1 = e_2$.

Enfin σ induit un isomorphisme $\mathcal{O}_L/\mathfrak{P}_1 \simeq \mathcal{O}_L/\mathfrak{P}_2$, donc $f_1 = f_2$. ∎

3.2.3 Norme relative d'un idéal

Soit L/K une extension de corps de nombres de degré n et $\mathfrak{P}$ un idéal premier de $\mathcal{O}_L$. Posons $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$ et $f = f(\mathfrak{P}/\mathfrak{p})$. On appelle norme relative de l'idéal $\mathfrak{P}$ l'idéal $\mathrm{N}_{L/K}(\mathfrak{P}) = \mathfrak{p}^f$.
Soit $\mathfrak{A}$ un idéal de $\mathcal{O}_L$. Notons $\mathfrak{A} = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}$ la factorisation de $\mathfrak{A}$ en idéaux premiers de $\mathcal{O}_L$. Posons $f_i = f(\mathfrak{P}_i/\mathfrak{p})$. On étend la définition de la façon suivante.

3.22 Définition (Norme relative d'un idéal). — *On appelle norme relative de l'idéal $\mathfrak{A}$ de $\mathcal{O}_L$ l'idéal $\mathrm{N}_{L/K}(\mathfrak{A}) = N_{L/K}(\mathfrak{P}_1)^{e_1} \dots N_{L/K}(\mathfrak{P}_r)^{e_r}$ de $\mathcal{O}_K$.*

3.23 Proposition. — *Soit L/K une extension galoisienne et $\sigma_1, \ldots, \sigma_n$ les K-automorphismes de L et $\mathfrak{A}$ un idéal de $\mathcal{O}_L$. Alors* $\prod_{i=1}^{n} \sigma_i(\mathfrak{A}) = \mathrm{N}_{L/K}(\mathfrak{A})\mathcal{O}_L$.

Preuve. — Par multiplicativité de la norme, il suffit de prouver le résultat pour les idéaux premiers de $\mathcal{O}_L$, supposons donc $\mathfrak{A}$ premier. Posons $\mathfrak{p} = \mathfrak{A} \cap \mathcal{O}_K$. D'après le théorème 3.21, la décomposition en produit d'idéaux premiers de $\mathfrak{p}\mathcal{O}_L$ dans $\mathcal{O}_L$ s'écrit

$$\mathfrak{p}\mathcal{O}_L = (\mathfrak{P}_1 \ldots \mathfrak{P}_r)^e$$

où $e = e(\mathfrak{P}_i/\mathfrak{p})$ pour n'importe quel i. Posons $f = f(\mathfrak{P}_i/\mathfrak{p})$, qui ne dépend pas de i. Par le lemme 3.13, on a $\mathfrak{A} \in \{\mathfrak{P}_1, \ldots, \mathfrak{P}_r\}$. Alors

$$\prod_{i=1}^{n} \sigma_i(\mathfrak{A}) = (\mathfrak{P}_1 \ldots \mathfrak{P}_r)^{ef} = \mathfrak{p}^f \mathcal{O}_L = \mathrm{N}_{L/K}(\mathfrak{A})\mathcal{O}_L,$$

puisque $\mathrm{Gal}(L/K)$ agit transitivement sur les $\mathfrak{P}_i$. ∎

3.24 Lemme. — *Soit $\mathfrak{a}$ un idéal de $\mathcal{O}_K$. Alors $\mathfrak{a}\mathcal{O}_L \cap K = \mathfrak{a}$.*

Preuve. — Si $\mathfrak{a} = 0$, le résultat est clair. Supposons donc $\mathfrak{a} \neq 0$. On considère l'idéal fractionnaire $\mathfrak{a}^{-1}$. On a

$$\mathcal{O}_L = \mathcal{O}_K\mathcal{O}_L = (\mathfrak{a}\mathfrak{a}^{-1})\mathcal{O}_L = (\mathfrak{a}\mathcal{O}_L)(\mathfrak{a}^{-1}\mathcal{O}_L),$$

donc, d'après le lemme 1.35,

$$\mathcal{O}_K = \mathcal{O}_L \cap K = (\mathfrak{a}\mathcal{O}_L)(\mathfrak{a}^{-1}\mathcal{O}_L) \cap K \supset (\mathfrak{a}\mathcal{O}_L \cap K)(\mathfrak{a}^{-1}\mathcal{O}_L \cap K).$$

Puisque $\mathfrak{a}\mathcal{O}_L \cap K$ est un idéal fractionnaire, il en découle $\mathfrak{a}^{-1}\mathcal{O}_L \cap K \subset (\mathfrak{a}\mathcal{O}_L \cap K)^{-1}$. D'autre part $\mathfrak{a} \subset \mathfrak{a}\mathcal{O}_L \cap K$, donc

$$(\mathfrak{a}\mathcal{O}_L \cap K)^{-1} \subset \mathfrak{a}^{-1} \subset \mathfrak{a}^{-1}\mathcal{O}_L \cap K,$$

d'où $(\mathfrak{a}\mathcal{O}_L \cap K)^{-1} = \mathfrak{a}^{-1}$ et $\mathfrak{a}\mathcal{O}_L \cap K = \mathfrak{a}$. ∎

3.25 Proposition. — *Soit L/K une extension galoisienne et $x \in \mathcal{O}_L$. Alors* $\mathrm{N}_{L/K}(x\mathcal{O}_L) = \mathrm{N}_{L/K}(x)\mathcal{O}_K$.

Preuve. — Soit $\sigma_1, \ldots, \sigma_n$ les K-automorphismes de L. D'après la proposition précédente

$$\mathrm{N}_{L/K}(x\mathcal{O}_L)\mathcal{O}_L = \prod_{i=1}^{n} \sigma_i(x\mathcal{O}_L) = \prod_{i=1}^{n} \mathcal{O}_L\sigma_i(x) = \mathcal{O}_L \prod_{i=1}^{n} \sigma_i(x) = \mathrm{N}_{L/K}(x)\mathcal{O}_L.$$

d'où d'après le lemme

$$\mathrm{N}_{L/K}(x\mathcal{O}_L) = \mathrm{N}_{L/K}(x\mathcal{O}_L)\mathcal{O}_L \cap K = (\mathrm{N}_{L/K}(x)\mathcal{O}_K)\mathcal{O}_L \cap K = \mathrm{N}_{L/K}(x)\mathcal{O}_K.$$ ∎

3.3 Calculs de factorisation

Venons-en au calcul effectif de factorisation d'idéaux en idéaux premiers. Dans la première section on démontre un théorème clé, dans les suivantes on l'applique au cas des anneaux d'entiers quadratiques et cyclotomiques.

3.3.1 Théorème fondamental

On note $\overline{f}(x) \in \mathbb{F}_p[x]$ la réduction modulo p du polynôme $f(x) \in \mathbb{Z}[x]$, et étant donné un polynôme $\overline{g}(x) \in \mathbb{F}_p[x]$, on désignera par g n'importe quel polynôme de $\mathbb{Z}[x]$ dont la réduction modulo p est $\overline{g}(x)$.

3.26 Théorème. — *Soit K un corps de nombre de degré n et p un nombre premier. Supposons qu'il existe $\alpha \in \mathcal{O}_K$ tel que $\mathcal{O}_K = \mathbb{Z}[\alpha]$ et notons $f(x) \in \mathbb{Z}[x]$ son polynôme minimal. Soit $\overline{f}(x) = \overline{g}_1(x)^{e_1} \dots \overline{g}_r(x)^{e_r}$ la factorisation de $f(x)$ en polynôme irréductible de $\mathbb{F}_p[x]$. Notons f_i le degré de $\overline{g}_i$.*
Alors la décomposition en idéaux premiers de $p\mathcal{O}_K$ s'écrit

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r} \quad \text{où} \quad \mathfrak{p}_i = (p, g_i(\alpha)).$$

De plus $f(\mathfrak{p}_i/p) = f_i$.

L'hypothèse qu'il existe $\alpha \in \mathcal{O}_K$ tel que $\mathcal{O}_K = \mathbb{Z}[\alpha]$ nous suffira pour les exemples que nous allons étudier, à savoir les entiers quadratiques et cyclotomiques.

Pour démontrer ce théorème, nous aurons besoin d'un lemme

3.27 Lemme. — *Avec les notations du théorème, si $f(x)$ et $g(x)$ sont deux polynômes tel que $\overline{f}(x), \overline{g}(x) \in \mathbb{F}_p[x]$ sont premiers entre eux, alors les idéaux $(p, f(\alpha))$ et $(p, g(\alpha))$ sont premiers entre eux dans $\mathcal{O}_K$.*

Preuve. — Comme $\overline{f}(x)$ et $\overline{g}(x)$ sont irréductibles dans $\mathbb{F}_p[x]$, ils sont premiers entre eux, et il existe $\overline{u}(x), \overline{v}(x) \in \mathbb{F}_p[x]$ tels que

$$\overline{f}(x)\overline{u}(x) + \overline{g}(x)\overline{v}(x) = 1.$$

En remontant dans $\mathbb{Z}[x]$, on a $f(x)u(x) + g(x)v(x) = 1 + pc(x)$ pour un certain $c(x) \in \mathbb{Z}[x]$. En évaluant ceci en α, il vient

$$f(\alpha)u(\alpha) + g(\alpha)v(\alpha) = 1 + pc(\alpha).$$

Considérons l'idéal

$$\mathfrak{q} = (p, f(\alpha)) + (p, g(\alpha)).$$

$f(\alpha)u(\alpha)$ est contenu dans le premier idéal de la somme, $g(\alpha)v(\alpha)$ dans le second, et $pc(\alpha)$ dans chacun d'eux. Ainsi $\mathfrak{q}$ contient 1, donc $\mathfrak{q} = \mathcal{O}_K$. ∎

Preuve (du théorème). — Puisque $\overline{g}_i(x)$ divise $\overline{f}(x)$ dans $\mathbb{F}_p[x]$, on a les isomorphismes

$$\mathcal{O}_K/\mathfrak{p}_i = \mathbb{Z}[\alpha]/(p, g_i(a)) \simeq \mathbb{Z}[x]/(f(x), p, g_i(x)) \simeq \mathbb{F}_p[x]/(\overline{f}(x), \overline{g}_i(x)) \simeq \mathbb{F}_p[x]/(\overline{g}_i(x)).$$

Comme $\overline{g}_i(x)$ est irréductible de degré f_i, $\mathbb{F}_p[x]/(\overline{g}_i(x))$ est un corps d'ordre p^{f_i}, ce qui montre d'une part que $f(\mathfrak{p}_i/p) = f_i$ et d'autre part que l'idéal $\mathfrak{p}_i$ est premier.

Prouvons maintenant l'assertion sur la factorisation de $p\mathcal{O}_K$. Cet idéal est le noyau de la surjection canonique $\mathcal{O}_K \longrightarrow \mathcal{O}_K/\mathfrak{p}$. Nous allons calculer ce noyau d'une autre façon. Remarquons que

$$\mathcal{O}_K/p\mathcal{O}_K = \mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha] \simeq \mathbb{Z}[x]/(p, f(x)) \simeq \mathbb{F}_p[x]/(\overline{f}(x)).$$

Par le lemme et le théorème chinois, il vient

$$\mathbb{F}_p[x]/(\overline{f}(x)) \simeq \mathbb{F}_p[x]/(\overline{g}_1(x)^{e_1}) \times \dots \times \mathbb{F}_p[x]/(\overline{g}_r(x)^{e_r}).$$

On peut donc considérer la surjection canonique $\mathcal{O}_K \longrightarrow \mathcal{O}_K/\mathfrak{p}$ comme l'application

$$\mathcal{O}_K \longrightarrow \mathbb{F}_p[x]/(\overline{g}_1(x)^{e_1}) \times \cdots \times \mathbb{F}_p[x]/(\overline{g}_r(x)^{e_r})$$

qui envoie α sur $(x, \ldots, x)$. Le noyau de chacun des facteurs est $(p, g_i(\alpha))$ si bien que le noyau de cette application est

$$(p, g_1(\alpha)^{e_1}) \cap \cdots \cap (p, g_r(\alpha)^{e_r}).$$

Comme ces idéaux sont premiers deux à deux, il vient bien

$$p\mathcal{O}_K = (p, g_1(\alpha)^{e_1}) \ldots (p, g_r(\alpha)^{e_r}).$$

Il nous reste à "sortir" les e_i. Comme chaque générateur de $\mathfrak{p}_i^{e_i} = (p, g_i(\alpha))^{e_i}$ est divisible par p sauf $g_i(\alpha)$, on peut dire que chaque générateur de $\mathfrak{p}_i^{e_i}$ appartient à $(p, g_i(\alpha)^{e_i})$, donc $(p, g_i(\alpha)^{e_i}) \supset \mathfrak{p}_i^{e_i}$. Le lemme 2.9 assure alors que $(p, g_i(\alpha)^{e_i})$ divise $\mathfrak{p}_i^{e_i}$.

Puisque les idéaux $(p, g_i(\alpha)^{e_i})$ sont premiers entre eux, il vient que $p\mathcal{O}_K$ divise $\mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_r^{e_r}$. Or

$$\mathrm{N}_K(\mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_r^{e_r}) = p^{f_1 e_1} \ldots p^{f_r e_r} = p^n$$

ce qui est aussi la norme de $p\mathcal{O}_K$. Donc $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_r^{e_r}$. ∎

3.28 Exemple. — Soit α une racine de $X^3 + 2X + 1$ et $K = \mathbb{Q}(\alpha)$. D'après l'exemple 1.43, $\mathcal{O}_K = \mathbb{Z}[\alpha]$, donc on peut appliquer le théorème 3.26. Factorisons $p\mathcal{O}_K$ pour quelques valeurs de p (premier rationnel).

Pour $p = 2$, on a $X^3 + 2X + 1 \equiv (X + 1)(X^2 + X + 1) \bmod (2)$, si bien que

$$2\mathcal{O}_K = (2, \alpha + 1)(2, \alpha^2 + \alpha + 1).$$

Le premier facteur a un degré d'inertie égal à 1 et le second un degré d'inertie égal à 2. Pour $p = 3$, $f(X)$ est irréductible dans $\mathbb{F}_3[X]$, donc $3\mathcal{O}_K$ se factorise en $(3, f(\alpha)) = (3)$, c'est-à-dire $3\mathcal{O}_K$ reste premier dans $\mathcal{O}_K$, ou encore que 3 est inerte sur K. On vérifie que 5 et 7 sont également inertes sur K. Pour $p = 11$, on a $X^3 + 2X + 1 \equiv (X + 2)(X^2 - 2X + 6) \bmod (11)$, donc

$$11\mathcal{O}_K = (11, \alpha + 2)(11, \alpha^2 - 2\alpha + 6)$$

$13\mathcal{O}_K$ reste premier, tandis que $X^3 + 2X + 1 \equiv (X - 3)(X - 5)(X - 9) \bmod (17)$, donc $17\mathcal{O}_K$ se décompose en

$$17\mathcal{O}_K = (17, \alpha - 3)(17, \alpha - 5)(17, \alpha - 9).$$

Le théorème 3.19 montre que le seul p qui se ramifie dans K est 59, puisque 59 est premier. On peut d'ailleurs vérifier que $X^3 + 2X + 1 \equiv (X - 14)^2(X - 31) \bmod (59)$, donc

$$59\mathcal{O}_K = (59, \alpha - 14)^2(59, \alpha - 31).$$

3.3.2 Factorisation dans les anneaux d'entiers quadratiques

Soit $K = \mathbb{Q}(\sqrt{d})$ un corps quadratique avec d sans facteurs carrés et $\mathcal{O}_K = \mathbb{Z}[\alpha]$ son anneau des entiers où $\alpha = \sqrt{d}$ si $d \equiv 2, 3 \bmod (4)$ et $\alpha = (1 + \sqrt{d})/2$ si $d \equiv 1 \bmod (4)$. Soit p un nombre premier et $\mathfrak{p}\mathcal{O}_K = \mathfrak{P}_1^{e_1} \ldots \mathfrak{P}_r^{e_r}$ sa décomposition en idéaux premiers dans $\mathcal{O}_K$. Le théorème 3.17 nous dit que $\sum_{i=1}^{r} e_i f_i = 2$, donc $r \leqslant 2$ et trois cas seulement peuvent se produire :

(i) $r = 2$, $e_1 = e_2 = 1$, $f_1 = f_2 = 1$; donc $p\mathbb{Z}$ est décomposé dans K ;

(ii) $r = 1$, $e_1 = 1$, $f_1 = 2$; donc $p\mathbb{Z}$ est inerte dans K ;

(iii) $r = 1$, $e_1 = 2$, $f_1 = 1$; donc $p\mathbb{Z}$ se ramifie dans K.
On dira par extension que l'entier p est décomposé, inerte ou ramifié.

3.29 Exemple. — Soit $K = \mathbb{Q}(\sqrt{-5})$ et $\mathcal{O}_K = \mathbb{Z}[-\sqrt{5}]$. On va factoriser quelques entiers premiers. Prenons d'abord $p = 2$. Alors $X^2 + 5 \equiv (X + 1)^2 \bmod (2)$, donc $2\mathcal{O}_K$ se ramifie :

$$2\mathcal{O}_K = (2, \sqrt{-5} + 1)^2.$$

Pour $p = 3$, on a $X^2 + 5 \equiv (X + 1)(X + 2) \bmod (3)$, donc $3\mathcal{O}_K$ est décomposé en

$$3\mathcal{O}_K = (3, \sqrt{-5} + 1)(3, \sqrt{-5} + 2).$$

Pour $p = 5$, on a $X^2 + 5 \equiv X^2 \bmod (5)$, donc

$$5\mathcal{O}_K = (5, \sqrt{-5})^2.$$

Remarquons que l'idéal $(5, \sqrt{-5})$ n'est autre que l'idéal $(\sqrt{-5})$ puisque $\sqrt{-5}$ divise 5 dans $\mathcal{O}_K$. Ceci illustre le fait que dans la factorisation donnée par le théorème 3.26, on ne sait pas si les idéaux qui interviennent sont principaux ou pas.

Continuons avec $p = 7$. On a $X^2 + 5 \equiv (X + 3)(X + 4) \bmod (7)$, donc

$$7\mathcal{O}_K = (7, \sqrt{-5} + 3)(7, \sqrt{-5} + 4).$$

Ensuite $X^2 + 5$ est irréductible dans $\mathbb{F}_{11}[X]$, donc $11\mathcal{O}_K$ est inerte dans K.

La proposition suivante résume tout ce qui peut se passer dans les corps quadratiques.

3.30 Proposition. — *Soit $K = \mathbb{Q}(\sqrt{d})$ un corps de quadratique, avec d sans facteurs carrés.*
(i) Sont décomposés dans K les nombres premiers impairs p tels que d soit un résidu quadratique $\bmod (p)$*, et 2 si $d \equiv 1 \bmod (8)$;*
(ii) Sont inertes dans K les nombres premiers impairs p tels que d soit un non-résidu quadratique $\bmod (p)$*, et 2 si $d \equiv 5 \bmod (8)$;*
(iii) Se ramifient dans K les diviseurs premiers impairs de d si $d \equiv 1 \bmod (4)$. Si $d \equiv 2, 3 \bmod (4)$, outre les diviseurs premiers impairs de d, le premier 2 se ramifie également.

Preuve. — Si $d \equiv 2, 3 \bmod (4)$, le polynôme minimal de α est $X^2 - d$ dont les racines sont $\pm\sqrt{d}$. Si $d \equiv 1 \bmod (4)$, le polynôme minimal de α est $X^2 - X + \dfrac{1-d}{4}$ dont les racines sont $\dfrac{1 \pm \sqrt{d}}{2}$.

Supposons d'abord p impair. Ces polynômes ont une racine double si et seulement si $d \equiv 0 \bmod (p)$ et le théorème 3.26 montre que p est ramifié. Ces polynômes sont irréductibles (resp. réductibles) si et seulement si d n'est pas un carré mod (p) (resp. est un carré), donc si et seulement si p est inerte (resp. décomposé) dans K.

Traitons maintenant le cas $p = 2$. Si $d \equiv 2, 3 \bmod (4)$, la réduction mod (2) de $X^2 - d$ est soit X^2, soit $X^2 + 1 = (X + 1)^2$ qui sont des carrés dans le deux cas, donc p se ramifie dans K. Si $d \equiv 1 \bmod (4)$, la réduction mod (2) du polynôme minimal de α est $X^2 + X + \delta$ où δ est la classe de $(d - 1)/4$. Pour $d \equiv 1 \bmod (8)$, on a $\delta = 0$ et $X^2 + X + \delta = X(X + 1)$ de sorte que 2 est décomposé ; pour $d \equiv 5 \bmod (8)$, on a $\delta = 1$ et $X^2 + X + 1$ est irréductible dans $\mathbb{F}_2[X]$, de sorte que 2 est inerte. ∎

3.31 Remarque. — En se souvenant que le discriminant de $\mathcal{O}_K$ vaut $4d$ si $d \equiv 2, 3 \bmod (4)$ et d si $d \equiv 1 \bmod (4)$, on constate que p se ramifie dans $\mathcal{O}_K$ si et seulement si p divise le discriminant. C'est exactement le théorème 3.19.

Nous avons vu dans un exemple ci-dessus que le théorème 3.26 ne disait rien sur la principalité des idéaux. Le lemme suivant donne un élément de réponse dans des cas bien particuliers ; il sera utilisé plus loin.

3.32 Lemme. — *Soit $d \leqslant -15$ un entier sans facteurs carrés, $d \equiv 1 \bmod (4)$, $K = \mathbb{Q}(\sqrt{d})$ et $\alpha = \dfrac{1+\sqrt{d}}{2}$ de telle sorte que $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Soit q un nombre premier avec $q^2 \leqslant -d$ et $\beta \in \mathbb{Z}$. Supposons que l'idéal $\mathfrak{a} = (q, \alpha+\beta)$ est premier dans $\mathcal{O}_K$. Alors $\mathfrak{a}$ est n'est pas principal.*

Preuve. — Supposons l'idéal $\mathfrak{a}$ principal et notons γ un générateur. Comme $\gamma | q$ dans $\mathcal{O}_K$, on a $\mathrm{N}_{K/\mathbb{Q}}(\gamma) | \mathrm{N}_{K/\mathbb{Q}}(q) = q^2$ dans $\mathbb{Z}$. Or q est premier donc $\mathrm{N}_{K/\mathbb{Q}}(\gamma) \in \{1, q, q^2\}$.

(*i*) Le cas $\mathrm{N}_{K/\mathbb{Q}}(\gamma) = 1$ est impossible car $\mathfrak{a}$ est premier, donc γ n'est pas inversible.

(*ii*) En posant $\gamma = a + b\alpha$, si $|b| \geqslant 1$, on a

$$\mathrm{N}_{K/\mathbb{Q}}(\gamma) = \mathrm{N}_{K/\mathbb{Q}}(a+b\alpha) = \left(a + \frac{b}{2}\right)^2 + b^2\frac{|d|}{4} \geqslant \frac{1}{4} + \frac{|d|}{4} > \sqrt{|d|} \geqslant q,$$

l'avant-dernière inégalité résultant de

$$\forall n \in \mathbb{N},\ n \geqslant 14 \Longrightarrow \frac{1+n}{4} > \sqrt{n}.$$

Ceci montre que $\mathrm{N}_{K/\mathbb{Q}}(\gamma) \neq q$ sous l'hypothèse $\gamma \notin \mathbb{Z}$. Mais si $\gamma \in \mathbb{Z}$, γ ne peut engendrer l'idéal $(q, \alpha+\beta)$ car l'équation $\gamma(a+b\alpha) = \alpha + \beta$ entraîne que γ est inversible, ce qui n'est pas.

(*iii*) Enfin le cas $\mathrm{N}_{K/\mathbb{Q}}(\gamma) = q^2 = \mathrm{N}_{K/\mathbb{Q}}(q)$ ne peut se produire, car sinon γ et q seraient associés dans $\mathcal{O}_K$, donc $\gamma \in \mathbb{Z}$ (car les unités de $\mathcal{O}_K$ dans ce cas sont ± 1, voir proposition 1.54), et ceci est impossible comme on vient de le voir. ∎

3.3.3 Factorisation dans les anneaux d'entiers cyclotomiques

Le théorème 3.26 donne une procédure calculatoire pour factoriser les polynômes cyclotomiques, mais les calculs deviennent difficiles à cause du degré qui devient grand. Heureusement dans de nombreux cas, on peut donner une bonne description de la factorisation des polynômes cyclotomiques même s'il est difficile d'écrire les facteurs. La clé réside dans le lemme suivant qui dit que le m-ième polynôme cyclotomique est le polynôme "universel" pour tester si un élément d'un corps est une racine primitive m-ième de l'unité.

3.33 Lemme. — *Soit m un entier positif et K un corps de caractéristique ne divisant pas m. Soit α un élément de K. Alors $\Phi_m(\alpha) = 0$ si et seulement si α est une racine primitive m-ième de l'unité.*

Preuve. — Rappelons-nous que dans $\mathbb{Z}[X]$, on a

$$X^m - 1 = \prod_{d|m} \Phi_d(X).$$

Dans $K[X]$ cette factorisation a encore un sens. Notons aussi que $X^m - 1$ n'a que des racines simples (la dérivée de ce polynôme est non nulle).

Supposons d'abord que α est une racine primitive m-ième de l'unité. Alors α est racine de $X^m - 1$, donc de l'un des $\Phi_d(X)$ avec d divisant m. Mais si $d < n$, comme $\Phi_d(X)$ divise $X^d - 1$, on a $\alpha^d - 1 = 0$, ce qui contredit que α est une racine pritimive m-ième de l'unité. Donc α est une racine de $\Phi_m(X)$.

Réciproquement, supposons que $\Phi_m(\alpha) = 0$. Puisque $\Phi_m(X)$ divise $X^m - 1$, ce implique que $\alpha^m = 1$, c'est-à-dire α est une racine m-ième de l'unité. Supposons que α est en fait une racine primitive d-ième de l'unité pour $d < m$ et d divisant m. L'argument donné dans la preuve du sens direct montre que $\Phi_d(\alpha) = 0$. Ainsi α est racine double de $X^m - 1$, ce qui est absurde. Ainsi α est une primitive m-ième de l'unité. ∎

Voici la proposition utile en pratique pour factoriser les polynômes cyclotomiques

3.34 Proposition. — *Soit $K = \mathbb{Q}(\xi_m)$ un corps cyclotomique, p un entier premier ne divisant pas m et $\mathfrak{p}$ un idéal de $\mathbb{Z}[\xi_m]$ au-dessus de p. Alors $e(\mathfrak{p}/p) = 1$, $f(\mathfrak{p}/p)$ est l'ordre de p dans $(\mathbb{Z}/m\mathbb{Z})^\times$ et il y exactement $\varphi(m)/f(\mathfrak{p}/p)$ idéaux premiers de $\mathbb{Z}[\xi_m]$ au-dessus de p.*

Preuve. — Notons $e = e(\mathfrak{p}/p)$ et $f = f(\mathfrak{p}/p)$. L'extension $\mathbb{Q}(\xi_m)/\mathbb{Q}$ étant galoisienne, le théorème 3.21 montre que ces nombres sont indépendants du choix de $\mathfrak{p}$. Autrement dit, $\Phi_m(X)$ se factorise dans $\mathbb{F}_p[X]$ en

$$\Phi_m(X) = (g_1(X) \dots g_r(X))^e$$

où $\deg g_i = f$ pour tout i et $efr = \varphi(m)$.

Puisque $X^m - 1$ n'a que des racines simples dans $\mathbb{F}_p[X]$, c'est aussi le cas de $\Phi_m(X)$. En particulier on a $e = 1$. Nous allons calculer f et r ; avant de faire le cas général, examinons le cas $f = 1$ pour illustrer l'idée. Si $f = 1$, alors $\Phi_m(X)$ se factorise en facteurs du premier degré dans $\mathbb{F}_p[X]$, donc $\Phi_m(X)$ a des racines dans $\mathbb{F}_p$. Par le lemme 3.33, ceci implique que $\mathbb{F}_p$ a des racines primitives m-ièmes de l'unité. Mais $\mathbb{F}_p^*$ est un groupe cyclique d'ordre $p-1$, donc il a un élément d'ordre m si et seulement si m divise $p-1$, c'est-à-dire si et seulement si $p \equiv 1 \bmod (m)$. L'argument est réversible, donc on a montré qu'un entier premier p se décompose dans $\mathbb{Q}(\xi_m)$ si et seulement si $p \equiv 1 \bmod (m)$.

Dans le cas général, soit $g(X)$ un des facteurs irréductibles de $\Phi_m(X)$ dans $\mathbb{F}_p[X]$. Le degré de $g(X)$ est f. Soit α une racine de $g(X)$ et posons $F = \mathbb{F}_p(\alpha) \simeq \mathbb{F}_p[X]/(g(X))$; c'est une extension de $\mathbb{F}_p$ de degré f. Notons que α est une racine primitive m-ième de l'unité dans F (nous avons tout fait pour) et que c'est la plus petite. Ainsi f est le degré de la plus petite extension de $\mathbb{F}_p$ contenant une racine primitive m-ième de l'unité.

Déterminons cette extension par une autre méthode. Soit F_i l'unique extension de $\mathbb{F}_p$ de degré i. Alors F_i^* est cyclique d'ordre $p^i - 1$, donc il contient une racine primitive m-ième de l'unité si et seulement si m divise $p^i - 1$. Ainsi la plus petite extension de $\mathbb{F}_p$ contenant une racine primitive m-ième de l'unité sera F_i, où i est le plus petit entier strictement positif tel que $p^i \equiv 1 \bmod (m)$, c'est-à-dire que i est l'ordre de p dans $(\mathbb{Z}/m\mathbb{Z})^\times$. ∎

3.35 Exemple. — Soit $K = \mathbb{Q}(\xi_5)$. Le comportement d'un entier rationnel p premier dans $\mathcal{O}_K$ est entièrement déterminé par la classe de $p \bmod (5)$. Si $p \equiv 1 \bmod (5)$ (par exemple $p = 11$), alors p est décomposé dans $\mathcal{O}_K$. Si $p \equiv 4 \bmod (5)$, alors p se factorise en 2 facteurs premiers, chacun avec un degré d'inertie 2. Si $p \equiv 2, 3 \bmod (5)$, alors p est inerte dans $\mathcal{O}_K$.

Pour des exemples explicites, considérons les premiers rationnels $3, 7, 11, 19$. Pour $p = 3, 7$, l'argument ci-dessus montre que $\Phi_5(X) = X^4 + X^3 + X^2 + X + 1$ est irréductible mod (p), et donc que $3\mathcal{O}_K$ et $7\mathcal{O}_K$ sont premiers dans $\mathcal{O}_K$. Pour $p = 19$, on trouve

$$X^4 + X^3 + X^2 + X + 1 = (X^2 + 5X + 1)(X^2 + 15X + 1) \bmod (19),$$

donc

$$19\mathcal{O}_K = (19, \xi_5^2 + 5\xi_5 + 1)(19, \xi_5^2 + 15\xi_5 + 1).$$

Pour finir, mod (11), on a

$$X^4 + X^3 + X^2 + X + 1 = (X + 2)(X + 6)(X + 7)(X + 8) \bmod (11),$$

donc

$$11\mathcal{O}_K = (11, \xi_5 + 2)(11, \xi_5 + 6)(11, \xi_5 + 7)(11, \xi_5 + 8).$$

3.36 Remarque. — Soit p un nombre premiers. Déterminons la factorisation dans $\mathbb{F}_p[X]$ de

$$\Phi_p(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + 1.$$

Comme $X^p - 1 \equiv (X - 1)^p \bmod (p)$, on a $\Phi_p(X) = (X - 1)^{p-1}$, d'où

$$p\mathcal{O}_K = (p, \xi_p - 1)^{p-1}.$$

De plus

$$\mathcal{O}_K/(p, \xi_p - 1) = \mathbb{Z}[\xi_p]/(p, \xi_p - 1) \simeq \mathbb{Z}/p\mathbb{Z},$$

donc $(p, \xi_p - 1)$ est premier de degré d'inertie 1. Ainsi $p\mathcal{O}_K$ est totalement ramifié dans $\mathbb{Q}(\xi_p)$. Le discriminant de $\mathbb{Q}(\xi_p)$ étant $\mathrm{D} = (-1)^{(p-1)/2}p^{p-2}$, ceci est cohérent avec le théorème 3.19 (qui montre de plus que p est le seul premier rationnel qui se ramifie dans $\mathbb{Q}(\xi_p)$).

3.37 Proposition. — *Soit p un nombre premier impair. Le corps $\mathbb{Q}(\xi_p)$ contient le corps quadratique $\mathbb{Q}(\sqrt{\varepsilon p})$ où $\varepsilon = (-1)^{(p-1)/2}$.*

Preuve. — Posons $L = \mathbb{Q}(\xi_p)$. Le groupe $\mathrm{Gal}(L/\mathbb{Q})$ est isomorphe au groupe $(\mathbb{Z}/p\mathbb{Z})^*$ par l'application

$$\begin{array}{ccc} (\mathbb{Z}/p\mathbb{Z})^* & \longrightarrow & \mathrm{Gal}(L/\mathbb{Q}) \\ q & \longmapsto & \sigma_q \end{array}$$

où σ_q est défini par $\sigma_q(\xi_p) = \xi_p^q$. Comme $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique d'ordre $p-1$, il existe un unique sous-groupe d'indice 2, c'est l'ensemble des carrés de $(\mathbb{Z}/p\mathbb{Z})^*$. Notons S le sous-groupe correspondant de $\mathrm{Gal}(L/\mathbb{Q})$ et K le sous-corps de L fixé par S. On a alors $[K : \mathbb{Q}] = 2$, donc K est un corps quadratique.

L'entier p est totalement ramifié dans L, il existe donc un unique idéal $\mathfrak{P}$ de $\mathcal{O}_L$ au-dessus de p tel que $(p) = \mathfrak{P}^{p-1}$. Soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$ au-dessus de p. Alors $\mathfrak{P}$ est au-dessus de $\mathfrak{p}$ (par unicité de $\mathfrak{P}$) et $e(\mathfrak{P}/p) = e(\mathfrak{P}/\mathfrak{p})e(\mathfrak{p}/p)$. Puisque $e(\mathfrak{P}/p) = p - 1$ et que le degré de ramification est majoré par le degré de l'extension, il vient $e(\mathfrak{P}/\mathfrak{p}) = \dfrac{p-1}{2}$ et $e(\mathfrak{p}/p) = 2$, en particulier $\mathfrak{p}$ est le seul idéal de K au-dessus de p, et il est totalement ramifié.
Soit $\mathfrak{Q}$ un autre idéal premier de $\mathcal{O}_L$. Notons $\mathfrak{q}$ l'idéal de $\mathcal{O}_K$ au-dessous de $\mathfrak{Q}$ et q le premier rationnel au-dessous de $\mathfrak{q}$. Comme $e(\mathfrak{Q}/q) = 1$ (proposition 3.34), on a $e(\mathfrak{q}/q) = 1$, donc q n'est pas ramifié dans K.
Ainsi p est le seul premier rationnel qui se ramifie dans K, donc d'après la proposition 3.30, $K = \mathbb{Q}(\sqrt{\varepsilon p})$ où $\varepsilon = \pm 1$ de telle sorte que $\varepsilon p \equiv 1 \bmod (4)$. On voit que $\varepsilon = (-1)^{(p-1)/2}$ convient, d'où le résultat. ∎

Rappelons qu'étant donné p un nombre premier impair, on définit pour tout $a \in \mathbb{Z}$ le symbole de Legendre par

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

On a $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod (p)$ et $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

3.38 Théorème (Loi de réciprocité quadratique). — *Soit p et q deux nombres premiers impairs. Alors*

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

Preuve. — Posons $L = \mathbb{Q}(\xi)$, $\tau = \sqrt{\varepsilon p}$ et $K = \mathbb{Q}(\tau)$. La proposition ci-dessus montre que $\tau \in L$. Soit $\sigma_q \in \mathrm{Gal}(L/\mathbb{Q})$; il est défini par $\sigma_q(\xi_p) = \xi_p^q$. Les conjugués de τ étant $\pm\tau$, on a $\sigma_q(\tau) = \pm\tau$. Notons S le sous-groupe de $\mathrm{Gal}(L/\mathbb{Q})$ défini par $\sigma_q(\tau) = \tau$ si et seulement si $\sigma_q \in H$ (donc K est le sous-corps fixé par S). C'est l'unique sous-groupe d'indice 2 de $\mathrm{Gal}(L/\mathbb{Q})$, on peut l'identifier à l'ensemble des carrés de $(\mathbb{Z}/p\mathbb{Z})^*$. Ainsi $\sigma_q(\tau) = \tau$ si et seulement si q est un carré dans $(\mathbb{Z}/p\mathbb{Z})^*$, autrement dit

$$\sigma_q(\tau) = \left(\frac{q}{p}\right)\tau.$$

Soit $\mathfrak{q}$ un idéal premier de $\mathcal{O}_L$ au-dessus de q. Ecrivons $\tau = a_0 + a_1\xi_p + \cdots + a_{p-2}\xi_p^{p-2}$ avec $a_i \in \mathbb{Z}$. En utilisant $\sigma_q(\xi_p) = \xi_p^q$ et $a^q = a$ pour tout $a \in \mathbb{F}_q$, il vient

$$\begin{aligned} \sigma_q(\tau) &= a_0 + a_1\xi_p^q + \cdots + a_{p-2}\xi_p^{(p-2)q} \\ &\equiv a_0^q + a_1^q\xi_p^q + \cdots + a_{p-2}^q\xi_p^{(p-2)q} \bmod (\mathfrak{q}) \\ &\equiv (a_0 + a_1\xi_p + \cdots + a_{p-2}\xi_p^{(p-2)})^q \bmod (\mathfrak{q}) \\ &\equiv \tau^q \bmod (\mathfrak{q}). \end{aligned}$$

Donc $\left(\frac{q}{p}\right)\tau \equiv \tau^q \bmod (\mathfrak{q})$. Puisque $\mathfrak{q}$ est premier, on a $\tau \notin \mathfrak{q}$, donc on peut simplifier par $\mathfrak{q}$ et on a

$$\left(\frac{q}{p}\right) \equiv \tau^{q-1} \equiv (\varepsilon p)^{\frac{p-1}{2}} \equiv \left(\frac{\varepsilon p}{q}\right) \bmod (\mathfrak{q}).$$

D'où

$$\left(\frac{q}{p}\right) - \left(\frac{\varepsilon p}{q}\right) \in \mathfrak{q} \cap \mathbb{Z} = q\mathbb{Z}.$$

Mais

$$\left|\left(\frac{q}{p}\right) - \left(\frac{\varepsilon p}{q}\right)\right| \leqslant 2 < q$$

Donc on a l'égalité $\left(\frac{q}{p}\right) = \left(\frac{\varepsilon p}{q}\right)$. D'autre part

$$\left(\frac{\varepsilon}{q}\right) = \left(\frac{(-1)^{(p-1)/2}}{q}\right) = (-1)^{\frac{p-1}{2}\,\frac{q-1}{2}},$$

ce qui termine la preuve. ∎

Chapitre 4

Groupes des classes d'idéaux

4.1 Définition

Soit K un corps de nombres d'anneau d'entiers $\mathcal{O}_K$. On a vu que $\mathcal{O}_K$ peut ne pas être un anneau factoriel, mais que par contre la factorisation en idéaux premiers fonctionne toujours. Nous avons aussi vu que $\mathcal{O}_K$ est factoriel si, et seulement si, il est principal, c'est-à-dire si tous ses idéaux sont principaux (proposition 2.11).

Tout ceci suggère qu'il serait intéressant d'avoir un moyen de déterminer si un idéal est principal. Bien qu'en pratique ceci soit assez difficile, on peut procéder abstraitement de façon satisfaisante. Appelons P_K le sous-groupe de I_K des idéaux fractionnaires principaux. Notons que les idéaux entiers de P_K sont précisément les idéaux principaux de $\mathcal{O}_K$.

4.1 Définition (Groupe des classes d'idéaux). — *Pour un corps de nombres K, avec les notations ci-dessus, on définit le groupe quotient $\mathcal{C}_K = I_K/P_K$ appelé groupe des classes d'idéaux.*

Les éléments de $\mathcal{C}_K$ seront appelés classes d'idéaux. Par définition de $\mathcal{C}_K$, deux idéaux fractionnaires $\mathfrak{a}$ et $\mathfrak{b}$ appartiennent à la même classe d'idéaux s'il existe $\gamma \in K^*$ tel que $\gamma\mathfrak{a} = \mathfrak{b}$. On écrira cette relation $\mathfrak{a} \sim \mathfrak{b}$. Ainsi $\mathfrak{r} \in P_K \iff \mathfrak{r} \sim \mathcal{O}_K$.

Le lemme qui suit montre que la notion d'idéaux fractionnaires n'est pas vraiment essentielle dans la définition du groupe des classes d'idéaux.

4.2 Lemme. — *Soit $\mathfrak{A}$ une classe d'idéaux. Alors il existe un idéal entier dans $\mathfrak{A}$.*

Preuve. — Soit $\mathfrak{r}$ un idéal fractionnaire de $\mathfrak{A}$. Il existe par le lemme 2.13 $\gamma \in K^*$ tel que $\gamma\mathfrak{r}$ est un idéal entier. Puisque $(\gamma) \in P_K$, on a $\gamma\mathfrak{r} \in \mathfrak{A}$. ∎

Voici une proposition qui motive le calcul des groupes de classes d'idéaux.

4.3 Proposition. — *Le groupe $\mathcal{C}_K$ est trivial si, et seulement si, $\mathcal{O}_K$ est principal.*

Preuve. — Le groupe $\mathcal{C}_K$ est trivial si et seulement si $I_K = P_K$, c'est-à-dire si et seulement si tout idéal fractionnaire est principal. Ceci implique en particulier que tous les idéaux entiers sont principaux, et donc que $\mathcal{O}_K$ est principal. Réciproquement, supposons $\mathcal{O}_K$ principal, et soit $\mathfrak{r} \in I_K$. Il existe par le lemme 2.13 $\gamma \in K^*$ tel que $\gamma\mathfrak{r}$ est un idéal entier, disons (α). Alors $\mathfrak{r} = (\alpha/\gamma)$, et $\mathfrak{r}$ est principal. ∎

4.4 Exemple. — Reprenons $\mathbb{Z}[\sqrt{-5}]$ (voir exemple 1.3), et les idéaux

$$\mathfrak{a}_1 = (2, 1+\sqrt{-5}), \quad \mathfrak{a}_2 = (3, 1+\sqrt{-5}) \quad \text{et} \quad \mathfrak{a}_3 = (3, 1-\sqrt{-5}).$$

Puisque $\mathfrak{a}_1$ n'est pas principal on a $\mathfrak{a}_1 \nsim \mathcal{O}_K$. Comme

$$\mathfrak{a}_1^2 = (2) \quad \mathfrak{a}_1\mathfrak{a}_2 = (1+\sqrt{5}) \quad \mathfrak{a}_1\mathfrak{a}_3 = (1-\sqrt{-5}) \quad \text{et} \quad \mathfrak{a}_2\mathfrak{a}_3 = (3)$$

on a $\mathfrak{a}_1^2 \sim \mathfrak{a}_1\mathfrak{a}_2 \sim \mathfrak{a}_1\mathfrak{a}_3 \sim \mathfrak{a}_2\mathfrak{a}_3 \sim \mathcal{O}_K$, d'où $\mathfrak{a}_1 \sim \mathfrak{a}_2 \sim \mathfrak{a}_3$ en simplifiant (par exemple $\mathfrak{a}_1\mathfrak{a}_2 \sim \mathfrak{a}_1\mathfrak{a}_3 \Longrightarrow \mathfrak{a}_2 \sim \mathfrak{a}_3$, les éléments manipulés n'étant rien d'autres que des classes). Cela montre au passage que $\mathfrak{a}_2$ et $\mathfrak{a}_3$ ne sont pas principaux. On a donc déjà deux élements dans $\mathcal{C}_{\mathbb{Q}(\sqrt{-5})}$, à savoir la classe de $\mathcal{O}_K$, et celle de $\mathfrak{a}_1$. On démontrera plus loin que ce sont les seuls, ainsi $\mathcal{C}_{\mathbb{Q}(\sqrt{-5})} \simeq \{-1, 1\}$.

4.2 Réseaux de $\mathbb{R}^n$

4.2.1 Premières propriétés

4.5 Définition (Sous-groupe discret de $\mathbb{R}^n$). — *Un sous-groupe additif H de $\mathbb{R}^n$ est dit discret si pour tout compact K de $\mathbb{R}^n$, l'intersection $H \cap K$ est finie.*

Un exemple typique de sous-groupe discret de $\mathbb{R}^n$ est $\mathbb{Z}^n$. C'est à peu près le seul d'après le théorème qui suit.

4.6 Théorème. — *Soit H un sous-groupe discret de $\mathbb{R}^n$. Alors H est un $\mathbb{Z}$-module libre de rang $r \leqslant n$.*

Preuve. — Choisissons un système libre $(e_1, \ldots, e_r)$ de H tel que r soit maximal. Soit

$$\mathcal{P} = \left\{ \sum_{i=1}^{r} \alpha_i e_i \,|\, 0 \leqslant \lambda_i \leqslant 1 \right\} \subset \mathbb{R}^n$$

le parallélotope construit sur ces vecteurs. Il est clair que P est compact, donc que $P \cap H$ est fini. Soit alors $x \in H$. Vu la maximalité de $(e_i)_i$, x s'écrit $x = \sum_{i=1}^{r} \lambda_i e_i$ avec $\lambda_i \in \mathbb{R}$. Pour $j \in \mathbb{Z}$, considérons l'élément

$$x_j = jx - \sum_{i=1}^{r} [j\lambda_i] e_i,$$

où $[\mu]$ est la partie entière de $\mu \in \mathbb{R}$. On a alors

$$x_j = \sum_{i=1}^{r} (j\lambda_i - [j\lambda_i]) e_i,$$

d'où $x_j \in \mathcal{P}$ et $x \in H$ puisque H est un sous-groupe de $\mathbb{R}^n$. Ainsi $x_j \in \mathcal{P} \cap H$. En remarquant que $x = x_1 + \sum_{i=1}^{r} [\lambda_i] e_i$, on voit que le $\mathbb{Z}$-module H est engendré par $\mathcal{P} \cap H$, donc est de type fini.

D'autre part, comme $\mathcal{P} \cap H$ est fini et $\mathbb{Z}$ infini, il existe deux entiers distincts j et k tel que $x_j = x_k$. Pour ces entiers, on a donc $(j-k)\lambda_i = [j\lambda_i] - [k\lambda_i]$, ce qui démontre que les λ_i sont rationnels. Ainsi le $\mathbb{Z}$-module H est engendré par un nombre fini d'éléments qui sont combinaisons linéaires à coefficients rationnels de e_i. Soit d un dénominateur commun entier de ces coefficients ; on a alors $dH \subset \sum_{i=1}^{r} \mathbb{Z} e_i$. Ainsi il existe une base (f_i) du $\mathbb{Z}$-module $\sum_{i=1}^{r} \mathbb{Z} e_i$ et des $\alpha_i \in \mathbb{Z}$ tels que $(\alpha_1 f_1, \ldots, \alpha_r f_r)$ engendrent dH. Comme le $\mathbb{Z}$-module a même rang que H et que $H \supset \sum_{i=1}^{r} \mathbb{Z} e_i$, le

rang de dH est supérieur ou égal à r ; il est donc égal à r et les α_i sont non nuls. Or les f_i sont, comme les e_i, $\mathbb{R}$-linéairement indépendants. Donc dH, et par conséquent H, est engendré sur $\mathbb{Z}$ par r éléments indépendants sur $\mathbb{R}$. ∎

4.7 Définition (Réseaux de $\mathbb{R}^n$). — *Un sous-groupe discret de rang n de $\mathbb{R}^n$ est appelé un réseau de $\mathbb{R}^n$.*

4.8 Définition (Parallélotope). — *Soit G un réseau et $e = (e_1, \ldots, e_n)$ une $\mathbb{Z}$-base. On appelle parallélotope fondamental associé à cette base l'ensemble*

$$\mathcal{P}_e = \left\{ \sum_{i=1}^{n} \alpha_i e_i \,|\, 0 \leqslant \alpha_i < 1 \right\} \subset \mathbb{R}^n.$$

Pour toute partie intégrable S de $\mathbb{R}^n$, on désigne par $\mu(S)$ sa mesure de Lebesgue (appelée aussi volume).

4.9 Lemme. — *Le volume $\mu(\mathcal{P}_e)$ est indépendant de la base choisie.*

Preuve. — Soit $f = (f_1, \ldots, f_n)$ une autre base de H. On a $f_i = \sum_{j=1}^{n} \alpha_{ij} e_j$ avec $\alpha_{ij} \in \mathbb{Z}$. L'effet d'une transformation linéaire sur les volumes montre que $\mu(\mathcal{P}_f) = |\det(\alpha_{ij})| \mu(\mathcal{P}_e)$. Or comme c'est un déterminant de changement de $\mathbb{Z}$-base, $\det(\alpha_{ij})$ est inversible dans $\mathbb{Z}$, donc vaut ± 1. Ainsi $\mu(\mathcal{P}_f) = \mu(\mathcal{P}_e)$. ∎

4.10 Définition (Volume d'un réseau). — *Le volume de l'un quelconque de ces $\mathcal{P}_e$ est appelé (abusivement) volume du réseau et est noté $v(H)$.*

4.2.2 Théorème de Minkowski

4.11 Lemme. — *Soit H un réseau de $\mathbb{R}^n$ et S une partie intégrable de R^n. Si $\mu(S) > v(H)$, il existe x, y distincts dans S tels que $x - y \in H$.*

Preuve. — Soit $e = (e_1, \ldots, e_n)$ une base de H, et $\mathcal{P}_e$ le parallélotope fondamental de H. Pour $u \in H$, l'ensemble des $\mathcal{P}_e + u$ forment une partition de $\mathbb{R}^n$ quand u décrit H. On a donc

$$\mu(S) = \sum_{u \in H} \mu(S \cap (\mathcal{P}_e + u)).$$

Mais la translation de vecteur $-u$ transforme $S \cap (\mathcal{P}_e + u)$ en $(S - u) \cap \mathcal{P}_e$, de même volume, donc

$$\mu(S) = \sum_{u \in H} \mu((S - u) \cap \mathcal{P}_e).$$

Si les ensembles $(S - u) \cap \mathcal{P}_e$ étaient tous disjoints, on aurait

$$\sum_{u \in H} \mu((S - u) \cap \mathcal{P}_e) \leqslant \mu(\mathcal{P}_e) = v(H),$$

donc $\mu(S) \leqslant v(H)$, contrairement à l'hypothèse.

Il existe donc u et v distincts dans H, tels que $(S - u) \cap (S - v) \cap \mathcal{P}_e$ soit non vide. Un élément z de cet ensemble est de la forme $z = x - u = y - v$ où $x, y \in S$. Ainsi il existe x, y distincts dans S tels que $x - y = u - v \in H$. ∎

4.12 Théorème (Minkowski). — *Soit H un réseau de $\mathbb{R}^n$ et S une partie de $\mathbb{R}^n$ intégrable, compacte, symétrique par rapport à 0 et convexe de. Si $\mu(S) \geqslant 2^n v(H)$, alors $S \cap H$ contient un point autre que* 0.

Preuve. — (i) Supposons d'abord qu'on a seulement $\mu(S) > 2^n v(H)$, et considérons l'ensemble $S' = \dfrac{1}{2}S$. On a $\mu(S') = \dfrac{1}{2^n}\mu(S)$, donc $\mu(S') > v(H)$. D'après le lemme, il existe x, y distincts dans S' tels que

$$x - y = \frac{1}{2}(2x - 2y) = \frac{1}{2}(2x + (-2y)) = w \in H.$$

Comme S est symétrique par rapport à 0, on a $-2y \in S$. Comme S est convexe, le milieu w de $[-2x, -2y]$ est dans S. Enfin $w \neq 0$ car $x \neq y$, donc $w \in H \cap S$ convient.
(ii) Supposons maintenant $\mu(S) = 2^n v(H)$. Pour $k > 1$ réel, posons $S_k = kS$. On a donc $\mu(S_k) = k^n \mu(S) > 2^n v(H)$. Comme $H\backslash\{0\}$ est fermé, l'ensemble non vide $(H\backslash\{0\}) \cap S_k = F_k$ est compact car S_k est compact. Il en résulte que

$$(H\backslash\{0\}) \cap S = \cap_{k>1} F_k$$

est non vide comme intersection décroissante de compacts non vides. ∎

4.2.3 Plongement canonique d'un corps de nombres dans $\mathbb{R}^n$

Soit K un corps de nombre et n son degré. L'extension $K/\mathbb{Q}$ étant séparable, il y a exactement n $\mathbb{Q}$-isomorphismes $\sigma_i : K \mapsto \mathbb{C}$. En notant $\alpha : \mathbb{C} \mapsto \mathbb{C}$ la conjugaison complexe. Pour tout i, $\alpha \circ \sigma_i$ est l'un des σ_j, et est égal à σ_i si et seulement si $\sigma_i(K) \subset \mathbb{R}$. Notons r_1 les nombres d'indices i tel que $\sigma_i(K) \subset \mathbb{R}$; les autres indices sont en nombre pair $2r_2$ et on a $r_1 + 2r_2 = n$.

On numérote les σ_i de sorte que $\sigma_i(K) \subset \mathbb{R}$ pour $1 \leqslant i \leqslant r_1$ et que $\sigma_{j+r_2} = \overline{\sigma_j}$ pour $r_1 + 1 \leqslant j \leqslant r_1 + r_2$.

4.13 Définition (Plongement canonique). — *On définit l'application $\mathbb{Q}$-linéaire injective suivante*

$$\begin{array}{rcl} \sigma : K & \longrightarrow & \mathbb{R}^{r_1} \times \mathbb{R}^{2r_2} \\ x & \longmapsto & (\ldots, \sigma_k(x), \ldots ; \ldots, \Re(\sigma_{r_1+l}(x)), \Im(\sigma_{r_1+l}(x)), \ldots) \end{array}$$

avec $1 \leqslant k \leqslant r_1$ et $1 \leqslant l \leqslant r_2$. Cette application s'appelle le plongement canonique de K dans $\mathbb{R}^n$.

4.14 Proposition. — *Si M est un sous-$\mathbb{Z}$-module libre de rang n de $\mathcal{O}_K$ et si $(x_i)_{1\leqslant i\leqslant n}$ est une $\mathbb{Z}$-base de M, alors $\sigma(M)$ est un réseau de $\mathbb{R}^n$ dont le volume est donné par*

$$v(\sigma(M)) = 2^{-r_2} |\det(\sigma_i(x_j))|.$$

Preuve. — Une base de $v(M)$ est donc formée des $v(\alpha_j)$ pour $j = 1, \ldots, n$ que l'on connaît par ses composantes sur la base canonique de $\mathbb{R}^n$; on a donc, en écrivant par commodité les transposées des déterminants

$$v(M) = \begin{vmatrix} \ldots & \sigma_k(\alpha_1) & \ldots & \ldots & \dfrac{\sigma_{r_1+l}(\alpha_1) + \overline{\sigma_{r_1+l}(\alpha_1)}}{2} & \dfrac{\sigma_{r_1+l}(\alpha_1) - \overline{\sigma_{r_1+l}(\alpha_1)}}{2} & \ldots \\ & \vdots & & & \vdots & \vdots & \\ \ldots & \sigma_k(\alpha_j) & \ldots & \ldots & \dfrac{\sigma_{r_1+l}(\alpha_j) + \overline{\sigma_{r_1+l}(\alpha_j)}}{2} & \dfrac{\sigma_{r_1+l}(\alpha_j) - \overline{\sigma_{r_1+l}(\alpha_j)}}{2} & \ldots \\ & \vdots & & & \vdots & \vdots & \\ \ldots & \sigma_k(\alpha_n) & \ldots & \ldots & \dfrac{\sigma_{r_1+l}(\alpha_n) + \overline{\sigma_{r_1+l}(\alpha_n)}}{2} & \dfrac{\sigma_{r_1+l}(\alpha_n) - \overline{\sigma_{r_1+l}(\alpha_n)}}{2} & \ldots \end{vmatrix}$$

$$= \begin{vmatrix} \dots & \sigma_k(\alpha_1) & \dots & \dots & \sigma_{r_1+l}(\alpha_1) & \overline{\sigma_{r_1+l}(\alpha_1)} & \dots \\ & \vdots & & & \vdots & \vdots & \\ \dots & \sigma_k(\alpha_j) & \dots & \dots & \sigma_{r_1+l}(\alpha_j) & \overline{\sigma_{r_1+l}(\alpha_j)} & \dots \\ & \vdots & & & \vdots & \vdots & \\ \dots & \sigma_k(\alpha_n) & \dots & \dots & \sigma_{r_1+l}(\alpha_n) & \overline{\sigma_{r_1+l}(\alpha_n)} & \dots \end{vmatrix} \times \begin{vmatrix} \ddots & & & & & & \\ & 1 & & & & & \\ & & \ddots & & & & \\ & & & \ddots & & & \\ & & & & 1/2 & 1/2 & \\ & & & & 1/2 & -1/2 & \\ & & & & & & \ddots \end{vmatrix},$$

le dernier déterminant étant constitué de r_1 blocs diagonaux 1 et de r_2 blocs diagonaux

$$\begin{vmatrix} 1/2 & 1/2 \\ 1/2 & -1/2 \end{vmatrix}.$$

On obtient bien la valeur $v(\sigma(M)) = 2^{-r_2}|\det(\sigma_i(x_j))|$.

4.15 Proposition. — *Soit $\mathfrak{a}$ un idéal entier non nul de $\mathcal{O}_K$. Alors $\sigma(\mathcal{O}_K)$ et $\sigma(\mathfrak{a})$ sont des réseaux, et on a*

$$v(\sigma(\mathcal{O}_K)) = 2^{-r_2}\sqrt{|D_K|} \text{ et } v(\sigma(\mathfrak{a})) = 2^{-r_2}\sqrt{|d|}\ \mathrm{N}_K(\mathfrak{a}).$$

Preuve. — Il suffit d'établir le résultat pour $\mathcal{O}_K$ puisqu'alors

$$v(\mathfrak{a}) = [\mathcal{O}_K : \mathfrak{a}]v(\mathcal{O}_K) = \mathrm{N}_K(\mathfrak{a})v(\mathcal{O}_K).$$

Or dans le cas de $\mathcal{O}_K$, $(\alpha_1, \dots, \alpha_n)$ est une base d'entiers, et $\det(\sigma_i(x_j)) = \sqrt{|\mathrm{D}_K|}$. ∎

4.3 Finitude du groupe des classes d'idéaux

Une propriété remarquable du groupe des classes d'idéaux d'un corps de nombre K est sa finitude. Nous présentons deux démonstration de ce résultat. L'une, particulière simple, donne une majoration assez grossière de son cardinal mais néanmoins suffisante pour la théorie. L'autre résulte d'un théorème de Minkowski sur les réseaux et fournit une majoration satisfaisante pour les calculs effectifs.

4.3.1 Une preuve élémentaire

4.16 Théorème. — *Soit K un corps de nombres. Il existe une constante λ_K dépendant seulement de K tel que chaque idéal non nul $\mathfrak{a}$ de $\mathcal{O}_K$ contienne un élément non nul α avec*

$$|\mathrm{N}_{K/\mathbb{Q}}(\alpha)| \leqslant \lambda_K \mathrm{N}_K(\mathfrak{a}).$$

Preuve. — Soit $\alpha_1, \dots, \alpha_n$ une base intégrale de $\mathcal{O}_K$, et $\sigma_1, \dots, \sigma_n$ les isomorphismes de K dans $\mathbb{C}$. Soit $\mathfrak{a}$ un idéal non nul de $\mathcal{O}_K$ et m l'unique entier positif tel que

$$m^n \leqslant \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a}) < (m+1)^n.$$

Considérons l'ensemble suivant à $(m+1)^n$ éléments

$$A = \left\{ \sum_{j=1}^{n} m_j\alpha_j \,|\, 0 \leqslant m_j \leqslant m,\ m_j \in \mathbb{Z} \right\}.$$

La proposition 1.39 nous indique $\mathcal{O}_K/\mathfrak{a}$ a pour ordre m^n, donc il existe deux éléments de A congru mod $(\mathfrak{a})$. En prenant leur différence, on a un élément $\alpha = \sum_{j=1}^{n} m'_j \alpha_j \in \mathfrak{a}$ avec $|m'_j| \leqslant m$. Calculons la norme de cet élément. Par l'inégalité triangulaire, il vient

$$|\mathrm{N}_{K/\mathbb{Q}}(\alpha)| = \prod_{i=1}^{n} |\sigma_i(\alpha)| = \prod_{i=1}^{n} \left| \sigma_i \left(\sum_{j=1}^{n} m'_j \alpha_j \right) \right| = \prod_{i=1}^{n} \left| \sum_{j=1}^{n} m'_j \sigma_i(\alpha_j) \right| \leqslant \prod_{i=1}^{n} \sum_{j=1}^{n} m |\sigma_i(\alpha_j)|$$

Continuons en posant $\lambda_K = \prod_{i=1}^{n} \sum_{j=1}^{n} |\sigma_i(\alpha_j)|$,

$$|\mathrm{N}_{K/\mathbb{Q}}(\alpha)| \leqslant m^n \lambda_K \leqslant \lambda_K \mathrm{N}_K(\mathfrak{a}),$$

ce qui est bien le résultat attendu, vu que λ_K ne dépend que de n et des α_i et σ_i (donc de K). ∎

4.17 Corollaire. — *Toute classe d'idéaux de $\mathcal{C}_K$ contient un idéal entier de norme $\leqslant \lambda_K$.*

Preuve. — Soit $\mathfrak{A}$ une classe d'idéaux, et soit $\mathfrak{b}$ un idéal entier de $\mathfrak{A}$ (un tel idéal existe par le lemme 4.2). Par le théorème qui précède, on peut trouver $\beta \in \mathfrak{b}$ avec $|\mathrm{N}_{K/\mathbb{Q}}(\beta)| \leqslant \lambda_K \mathrm{N}_K(\mathfrak{b})$. L'idéal principal $\beta\mathcal{O}_K$ est contenu dans $\mathfrak{b}$, donc par le lemme 2.9, il existe un idéal $\mathfrak{a}$ tel que $\mathfrak{a}\mathfrak{b} = \beta\mathcal{O}_K$. Puisque $\beta\mathcal{O}_K$ est principal, on a $\mathfrak{a} \in \mathfrak{A}$, et $\mathrm{N}_K(\mathfrak{a}) = \dfrac{|\mathrm{N}_{K/\mathbb{Q}}(\beta)|}{\mathrm{N}_K(\mathfrak{b})} \leqslant \lambda_K$. ∎

4.18 Lemme. — *Soit $m \in \mathbb{N}$. Il n'y a qu'un nombre fini d'idéaux $\mathfrak{a}$ de norme inférieure à m.*

Preuve. — Soit $\mathfrak{a}$ un idéal de $\mathcal{O}_K$ tel que $\mathrm{N}_K(\mathfrak{a}) < m$ et $\mathfrak{p}_1^{n_1} \dots \mathfrak{p}_r^{n_r}$ sa factorisation en idéaux premiers. Soit p_i le nombre premier au-dessous de $\mathfrak{p}_i$ et f_i son degré d'inertie. Alors $\mathrm{N}_K(\mathfrak{a}) = p_1^{f_1 n_1} \dots p_r^{f_r n_r}$. En particulier pour chaque p_i, on a $p_i < m$ et $n_i < \log_{p_i} m$.
Ceci nous montre qu'il n'y a qu'un nombre fini de choix pour les p_i et que pour chaque p_i il n'y a qu'un nombre fini de choix pour les n_i. De plus il y a au plus $n = [K : \mathbb{Q}]$ idéaux premiers de $\mathcal{O}_K$ au-dessus de chaque p_i, et donc seulement un nombre fini de choix pour les $\mathfrak{p}_i$. Puisqu'il n'y qu'un nombre fini de choix pour les $\mathfrak{p}_i$ et les n_i, il vient qu'il n'y qu'un nombre fini de possibilités pour $\mathfrak{a}$. ∎

4.19 Théorème. — *Le groupe de classe d'idéaux $\mathcal{C}_K$ est fini.*

Preuve. — Par le corollaire ci-dessus, toute classe d'idéaux contient un idéal entier de norme au plus λ_K. Mais par le lemme il n'y a qu'un nombre fini d'idéaux de norme inférieure à λ_K, d'où le résultat. ∎

La borne λ_K n'est pas très efficace pour les calculs. Nous allons maintenant parler des réseaux, et du théorème de Minkowski, qui nous donnera une borne bien meilleure.

4.3.2 Par le théorème de Minkowski

Commençons par un calcul de volume dans $\mathbb{R}^n$.

4.20 Proposition. — *Soit $r_1, r_2 \in \mathbb{N}$, $n = r_1 + 2r_2$, et $t \geqslant 0$ un réel. Soit*

$$B_t = \{(y_1, \ldots, y_{r_1}, z_1, \ldots, z_{r_2}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \text{ tel que } \sum_{i=1}^{r_1} |y_i| + 2\sum_{j=1}^{r_2} \leqslant t\}.$$

Alors pour la mesure de Lebesgue μ on a

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

Preuve. — Posons $\mu(B_t) = V(r_1, r_2, t)$ et procédons par double récurrence sur r_1 et r_2. On a $V(1, 0, t) = 2t$ (volume du segment $[-t, t]$), et $V(0, 1, t) = \dfrac{\pi t^2}{4}$ (volume du disque de rayon t de centre 0), ce qui est conforme au résultat.

Passons de r_1 à $r_1 + 1$. L'ensemble $B_t \subset \mathbb{R} \times \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ correspondant à $r_1 + 1$ et r_2 est défini par

$$|y| + \sum_{i=1}^{n} |y_i| + 2\sum_{j=1}^{r_2} \leqslant t$$

avec $y \in \mathbb{R}$. En intégrant par tranches,

$$V(r_1 + 1, r_2, t) = \int_{\mathbb{R}} V(r_1, r_2, t - |y|)\ \mathrm{d}y = \int_{-t}^{t} V(r_1, r_3, t - |y|)\ \mathrm{d}y.$$

D'après l'hypothèse de récurrence, il vient

$$V(r_1{+}1, r_2, t) = 2\int_0^t 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{(t-y)^n}{n!}\ \mathrm{d}y = 2^{r_1+1} \left(\frac{\pi}{2}\right)^{r_2} \left[-\frac{(t-y)^{n+1}}{(n+1)!}\right]_0^t = 2^{r_1+1} \left(\frac{\pi}{2}\right)^{r_2} \frac{t^{n+1}}{(n+1)!},$$

comme attendu.

Passons maintenant de r_2 à $r_2 + 1$. L'ensemble $B_t \subset \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \times \mathbb{C}$ correspondant à r_1 et $r_2 + 1$ est défini par

$$\sum_{i=1}^{n} |y_i| + 2\sum_{j=1}^{r_2} +2|z| \leqslant t$$

avec $z \in \mathbb{C}$. L'intégration par tranches conduit ici à

$$V(r_1, r_2 + 1, t) = \int_C V(r_1, r_2, t - 2|z|)\ \mathrm{d}\mu(z) = \int_{|z| \leqslant \frac{t}{2}} V(r_1, r_2, t - 2|z|)\ \mathrm{d}\mu(z)$$

où $\mathrm{d}\mu(z)$ désigne la mesure de Lebesgue de $\mathbb{C}$. En posant $z = \rho e^{i\alpha}$ ($\rho \in \mathbb{R}_+$ et $0 \leqslant \alpha \leqslant 2\pi$), on a $\mathrm{d}\mu(z) = \rho\ \mathrm{d}\rho\ \mathrm{d}\alpha$.
D'après l'hypothèse de récurrence, il vient

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

Pour calculer $\displaystyle\int_0^{\frac{t}{2}} (t-2\rho)^n \rho\ \mathrm{d}\rho$, on intègre par parties en intégrant $(t-2\rho)^n$ et en dérivant ρ,

$$\int_0^{\frac{t}{2}} (t-2\rho)^n \rho\ \mathrm{d}\rho = \left[\frac{(t-2\rho)^{n+1}\rho}{-2(n+1)}\right]_0^{\frac{t}{2}} + \frac{1}{2(n+1)} \int_0^{\frac{t}{2}} (1-2\rho)^{n+1}\ \mathrm{d}\rho = \frac{t^{n+2}}{4(n+1)(n+2)}.$$

Par suite, $V(r_1, r_2 + 1, t) = 2^{r_1} \left(\dfrac{\pi}{2}\right) \dfrac{t^{n+2}}{(n+2)!}$, ce qui est conforme à la formule voulue, vu que $r_1 + 2(r_2 + 1) = n + 2$. ∎

4.21 Proposition. — *Soit K un corps de nombres, n son degré, r_1 et r_2 comme ci-dessus et $\mathfrak{a}$ un idéal entier non nul de K. Alors $\mathfrak{a}$ contient un élément non nul α tel que*

$$|\mathrm{N}_{K/\mathbb{Q}}(\alpha)| \leqslant \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n}\sqrt{|D_K|}\ \mathrm{N}_K(\mathfrak{a}).$$

Preuve. — L'ensemble B_t défini dans la proposition précédente est un ensemble compact, convexe et symétrique par rapport à 0 de $\mathbb{R}^n$. Soit $t > 0$ tel que $\mu(B_t) = 2^n v(\sigma(\mathfrak{a}))$, c'est-à-dire, d'après la proposition précédente, tel que

$$2^{r_1}\left(\frac{\pi}{2}\right)^{r_2}\frac{t^n}{n!} = 2^{n-r_2}\sqrt{|\mathrm{D}_K|}\ \mathrm{N}_K(\mathfrak{a}),$$

ou encore $t^n = 2^{n-r_1}\pi^{-r_2}n!\sqrt{|\mathrm{D}_K|}\ \mathrm{N}_K(\mathfrak{a})$. D'après le théorème 4.12, il existe un élément non nul α de $\mathfrak{a}$ tel que $\sigma(\alpha) \in B_t$. Sa norme vaut $\mathrm{N}_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^{r_1}|\sigma_i(\alpha)| \prod_{j=r_1+1}^{r_1+r_2}|\sigma_j(\alpha)|^2$, et par l'inégalité arithmético-géométrique, on a

$$|\mathrm{N}_{K/\mathbb{Q}}(\alpha)| \leqslant \left[\frac{1}{n}\sum_{i=1}^{r_1}|\sigma_i(\alpha)| + \frac{2}{n}\sum_{j=r_1+1}^{r_1+r_2}|\sigma_j(\alpha)|\right]^n \leqslant \frac{t^n}{n^n} = \frac{1}{n^n}2^{n-r_1}\pi^{-r_2}n!\sqrt{|\mathrm{D}_K|}\ \mathrm{N}_K(\mathfrak{a}),$$

d'où le résultat car $r_1 = n - 2r_2$. ∎

L'énoncé de la proposition que l'on vient d'obtenir et le même que celui du théorème 4.16, à ceci près que la constante λ_K a été remplacé par la constante μ_K définie par

$$\mu_K = \left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}\sqrt{|\mathrm{D}_K|}.$$

On obtient alors sans aucun effort une copie du corollaire 4.17 dans la preuve duquel seule l'existence de λ_K intervient, et non sa construction.

4.22 Corollaire. — *Toute classe d'idéaux de $\mathcal{C}_K$ contient un idéal entier de norme $\leqslant \mu_K$.*

L'avantage de cette nouvelle constante μ_K est qu'elle est bien petite que λ_K, et donc qu'elle simplifie le nombre de cas à envisager pour les calculs de groupes de classes d'idéaux.

Finissons par une définition.

4.23 Définition (Nombre de classes). — *Le cardinal de $\mathcal{C}_K$ s'appelle le nombre de classes de K et se note h_K.*

4.4 Calcul des groupes de classes d'idéaux

Nous avons maintenant tous les outils pour déterminer les groupes de classes d'idéaux. Pour tout $p \leqslant \mu_K$ premier rationnel, on détermine la factorisation de $p\mathcal{O}_K$ en idéaux premier comme dans le chapitre 3. Si p est inerte, l'idéal $p\mathcal{O}_K$ est principal, donc il appartient à la classe de $\mathcal{O}_K$ dans $\mathcal{C}_K$. Il suffit donc de considérer l'ensemble des p décomposés ou ramifiés dans K. Soit P_0 l'ensemble des idéaux premiers de $\mathcal{O}_K$ au-dessus de ces p.

Démontrons que P_0 contient des générateurs du groupe de classe d'idéaux $\mathcal{C}_K$. Soit $\mathfrak{A}$ une classe quelconque d'idéaux. D'après le corollaire 4.22, il existe un idéal $\mathfrak{a} \in \mathfrak{A}$ tel que $\mathrm{N}_K(\mathfrak{a}) \leqslant \mu_K$. Par unicité de la factorisation des idéaux, $\mathfrak{a}$ se factorise en idéaux premiers de norme $\leqslant \mu_K$; mais

d'après le corollaire 3.2, les idéaux premiers de norme $\leqslant \mu_K$ s'obtiennent par factorisation des $p\mathcal{O}_K$ avec $p \leqslant \mu_K$ (puisque leur norme est une puissance p). Ceci montre que la classe d'idéaux $\mathfrak{A}$ est engendrée des idéaux premiers de P_0, et donc P_0 engendre $\mathcal{C}_K$.

Il reste alors à déterminer lesquels de ces générateurs sont égaux. Des considérations élémentaires aboutissent, mais elles deviennent lourdes dès que le cardinal de P_0 augmente. Nous verrons plus loin une méthode algorithmique pour effectuer ces comparaisons dans le cas des corps quadratiques imaginaires.

4.24 Exemple. — Finissons l'étude $\mathcal{O}_K$ où $K = \mathbb{Q}(\sqrt{-5})$. Ce corps est imaginaire, donc $r_1 = 1$. La constante de Minkowski de K est $\mu_K \approx 2,21$. Il suffit donc de considérer la factorisation de $2\mathcal{O}_K$. Or $X^2 + 5 \equiv (X+1)^2 \bmod (5)$, donc

$$2\mathcal{O}_K = (2, \sqrt{-5} + 1)^2.$$

D'après l'exemple 4.4 $(2, \sqrt{-5}+1)$ n'est pas un idéal principal, donc $\mathcal{C}_K$ est le groupe cyclique à deux éléments engendré par $(2, \sqrt{-5}+1)$.

4.25 Exemple. — Soit $K = \mathbb{Q}(\sqrt{-47})$. Alors $\mathrm{D}_K = -47$ et $\mathcal{O}_K = \mathbb{Z}[\alpha]$ où $\alpha = \dfrac{1+\sqrt{-47}}{2}$. Le polynôme minimal de α est $X^2 - X + 14$, et $\mu_K \approx 4,36$, donc $\mathcal{C}_K$ est généré par les idéaux premiers de norme au plus 4. Comme $X^2 - X + 14 \equiv X(X-1) \bmod (2)$ et $X^2 - X + 14 \equiv X(X-1) \bmod (3)$, on a d'après le théorème 3.26,

$$2\mathcal{O}_K = (2, \alpha)(2, \alpha - 1) \quad \text{et} \quad 3\mathcal{O}_K = (3, \alpha)(3, \alpha - 1).$$

Posons $\mathfrak{p}_2 = (2, \alpha)$, $\mathfrak{q}_2 = (2, \alpha - 1)$, $\mathfrak{p}_3 = (3, \alpha)$ et $\mathfrak{q}_3 = (3, \alpha - 1)$. On a bien sûr $\mathfrak{q}_2 \sim \mathfrak{p}_2^{-1}$ et $\mathfrak{q}_3 \sim \mathfrak{p}_3^{-1}$.

Nous allons trouver des relations entre $\mathfrak{p}_2$ et $\mathfrak{p}_3$ en considérant les idéaux premiers de norme petite.

(*i*) On a $\mathrm{N}_{K/\mathbb{Q}}(\alpha) = 12$, donc l'idéal $\alpha\mathcal{O}_K$ est le produit d'idéaux premiers de norme 2 et 3. On a aussi $\alpha \in \mathfrak{p}_2$ et $\alpha \in \mathfrak{p}_3$ d'où $\alpha\mathcal{O}_K \subset \mathfrak{p}_2\mathfrak{p}_3$, et donc $\alpha\mathcal{O}_K = \mathfrak{p}_2^2\mathfrak{p}_3$ ou $\alpha\mathcal{O}_K = \mathfrak{p}_2\mathfrak{q}_2\mathfrak{p}_3$. Le dernier cas est impossible car $2\mathcal{O}_K = \mathfrak{p}_2\mathfrak{q}_2 \supset \mathfrak{p}_2\mathfrak{q}_2\mathfrak{p}_3$, mais 2 ne divise pas α. Donc $\alpha\mathcal{O}_K = \mathfrak{p}_2^2\mathfrak{p}_3$ et $\mathfrak{p}_3 \sim \mathfrak{p}_2^{-2}$. Il s'ensuit que $\mathcal{C}_K$ est engendré par la classe de $\mathfrak{p}_2$.

(*ii*) La norme de $\alpha + 1$ est 14, donc $(\alpha+1)\mathcal{O}_K$ a dans sa décomposition un idéal de norme 7 que nous n'avons pas à considérer.

(*iii*) La norme de $\alpha + 2$ est 18, si bien que $(\alpha+2)\mathcal{O}_K$ a dans sa décomposition des idéaux premiers de norme 2 et 3. Comme $\alpha + 2 \in \mathfrak{p}_2$ et $\alpha + 2 = (\alpha - 1) + 3 \in \mathfrak{q}_3$, il vient $(\alpha+2)\mathcal{O}_K = \mathfrak{p}_2\mathfrak{p}_3\mathfrak{q}_3$ ou $(\alpha+2)\mathcal{O}_K = \mathfrak{p}_2\mathfrak{q}_3^2$. Le dernier cas est impossible car $\mathfrak{p}_3\mathfrak{q}_3 = 3\mathcal{O}_K$ ne divise pas $(\alpha+2)\mathcal{O}_K$. Donc $(\alpha+2)\mathcal{O}_K = \mathfrak{p}_2\mathfrak{q}_3^2$, puis

$$\mathfrak{p}_2 \sim \mathfrak{q}_3^{-2} \sim \mathfrak{p}_3^2 \sim \mathfrak{p}_2^{-4}$$

et finalement $\mathfrak{p}_2^5 \sim \mathcal{O}_K$.

L'idéal $\mathfrak{p}_2$ n'est pas principal. En effet, sinon soit β un générateur de $\mathfrak{p}_2$ avec $\beta = \dfrac{b + c\sqrt{-47}}{2}$. On aurait $\mathrm{N}_{K/\mathbb{Q}}(\beta) = 2$, mais l'équation $b^2 + 47c^2 = 8$ n'a clairement pas de solutions entières. Donc $\mathfrak{p}_2 \nsim \mathcal{O}_K$, et $\mathcal{C}_K$ est cyclique d'ordre 5, engendré par $\mathfrak{p}_2$.

4.26 Exemple. — Soit α une racine de $X^3 + 2X + 1$ et $K = \mathbb{Q}(\alpha)$. D'après l'exemple 1.43, $\mathcal{O}_K = \mathbb{Z}[\alpha]$ et le discriminant de K est -59. Il n'est pas difficile de voir que le polynôme $X^3 + 2X + 1$

ne possède qu'une seule racine réelle, donc $r_1 = r_2 = 1$. On trouve $\mu_K \approx 2,17$ si bien qu'il suffit de considérer la factorisation de $2\mathcal{O}_K$. Or d'après l'exempe 3.28,

$$2\mathcal{O}_K = (2, \alpha + 1)(2, \alpha^2 + \alpha + 1).$$

Donc les deux seuls idéaux premiers à analyser sont $\mathfrak{p}_1 = (2, \alpha + 1)$ et $\mathfrak{p}_2 = (2, \alpha^2 + \alpha + 1)$. Il est clair que $(\alpha + 1)\mathcal{O}_K \subset (2, \alpha + 1)$. Réciproquement, en observant que le polynôme (minimal) de $\alpha + 1$ est

$$X^3 - 3X^2 + 5X - 2$$

on voit que $2 \in (\alpha + 1)\mathcal{O}_K$, ce qui montre que $\mathfrak{p}_1 = (\alpha + 1)$, donc $\mathfrak{p}_1$ est principal. Par suite $\mathfrak{p}_1 \sim \mathcal{O}_K$, et comme $\mathcal{O}_K \sim \mathfrak{p}_1\mathfrak{p}_2$, il vient $\mathfrak{p}_2 \sim \mathcal{O}_K$, c'est-à-dire que $\mathfrak{p}_2$ est également principal. Ici $\mathcal{C}_K$ est réduit à la classe de $\mathcal{O}_K$ et $\mathcal{O}_K$ est principal.

4.5 Exemples des corps cyclotomiques

4.27 Exemple. — Soit $K = \mathbb{Q}(\xi_5)$. Le discriminant de K est 5^3 (proposition 1.58) et $r_2 = 2$, donc la constante de Minkowski vaut

$$\mu_K = \left(\frac{4}{\pi}\right)^2 \frac{4!}{4^4}\sqrt{125} \approx 1,70.$$

Il en résulte que $\mathcal{O}_K = \mathbb{Z}[\xi_5]$ est principal.

4.28 Exemple. — Soit $K = \mathbb{Q}(\xi_7)$. Le discriminant de K est -7^5 (proposition 1.58) et $r_2 = 3$ et la constante de Minkowski vaut

$$\mu_K = \left(\frac{4}{\pi}\right)^3 \frac{6!}{6^6}\sqrt{7^5} \approx 4,13.$$

Donc chaque classe d'idéaux contient un idéal de norme au plus 4. Soit $\mathfrak{a}$ un tel idéal, avec $\mathfrak{a} \neq \mathcal{O}_K$. Puisque les seuls facteurs premiers possible de $\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a})$ sont 2 et 3, chaque idéal premier facteur de $\mathfrak{a}$ est au-dessus de 2 ou 3. On utilise maintenant la proposition 3.34.

L'ordre de 2 dans $(\mathbb{Z}/7\mathbb{Z})^\times$ est 3 donc les idéaux de $\mathcal{O}_K$ au-dessus de 2 ont un degré d'inertie égal à 3. En particulier leur norme est $2^3 = 8$; il ne peuvent donc pas apparaître en facteur dans $\mathfrak{a}$. L'ordre de 3 dans $(\mathbb{Z}/7\mathbb{Z})^\times$ est 6, donc $3\mathcal{O}_K$ est premier et sa norme est 3^6, il ne peut donc pas non plus figurer dans les facteurs de $\mathfrak{a}$. Il en résulte que $\mathcal{O}_K$ est principal.

Voici un exemple un peu plus compliqué.

4.29 Proposition. — *L'anneau $\mathbb{Z}[\xi_{23}]$ n'est pas principal.*

Preuve. — Posons $K = \mathbb{Q}(\sqrt{-23})$, $L = \mathbb{Q}(\xi_{23})$ et $\alpha = \dfrac{1 + \sqrt{-23}}{2}$. D'après la proposition 3.37, on a $K \subset L$. Dans K, l'idéal $2\mathcal{O}_K$ se décompose en $(2, \alpha)(2, \alpha + 1)$ par le théorème 3.26. Posons $\mathfrak{p} = (2, \alpha)$. Soit $\mathfrak{P}$ un idéal de $\mathcal{O}_L$ au-dessus de $\mathfrak{p}$. Montrons que $\mathfrak{P}$ n'est pas principal. On a

$$\mathrm{N}_{L/K}(\mathfrak{P}) = \mathfrak{p}^{f(\mathfrak{P}/p)}.$$

Le sous-groupe d'ordre 2 de $\mathrm{Gal}(L/\mathbb{Q})$ est distingué, donc l'extension L/K est galoisienne de degré 11, donc d'après le théorème 3.21, $f(\mathfrak{P}/p)$ divise 11. Donc $f(\mathfrak{P}/p) = 1$ ou 11. D'après le lemme 3.32, l'idéal $\mathfrak{p} = (2, \alpha)$ n'est pas principal dans $\mathcal{O}_K$. Dans le chapitre suivant, on montrera que $h_K = 3$, d'où la principalité de $\mathfrak{p}^3$, ainsi $\mathfrak{p}^{f(\mathfrak{P}/p)}$ n'est pas principal. Mais d'après la proposition 3.25, l'idéal $\mathfrak{P}$ ne peut être principal car sinon sa norme sur K le serait, ce qui n'est pas le cas. ∎

La recherche exhaustive des corps cyclotomiques a occupé notamment Siegel, Montgomery et Uchida. En 1972, Masley résout la question dans thèse [Mas76-1]. Comme pour tout m impair on a $\mathbb{Q}(\xi_{2m}) = \mathbb{Q}(\xi_m)$, on écarte le cas $m \equiv 2 \bmod 4$.

4.30 Théorème (Masley, 1972). — *Soit m un entier qui n'est pas congru à 2 modulo 4. Alors l'anneau des entiers de $\mathbb{Q}(\xi_m)$ est principal si et seulement si*

$$m \in \{3, 4, 5, 7, 8, 9, 11, 12, 13, 15, 16, 17, 19, 20, 21, 24, 25, 27, 28, 32, 33, 35, 36, 40, 44, 45, 48, 60, 84\}.$$

Le premier corps cyclotomique dont le groupe des classes d'idéaux n'est pas trivial est $\mathbb{Q}(\xi_{23})$, son nombre de classes est 3.

En 1975 il publie un article de deux pages sur la détermination des corps de cyclotomiques de nombre de classes égal à 2 [Mas75] et en 1976, il détermine tous les corps cyclotomiques de nombre de classes inférieur ou égal à 10 (voir [Mas76-2]).

4.31 Théorème (Masley, 1976). — *Soit m un entier qui n'est pas congru à 2 modulo 4. Toutes les valeurs de m pour lesquelles le nombre de classes h_m de $\mathbb{Q}(\xi_m)$ est h_m avec $2 \leqslant h_m \leqslant 10$ sont les suivantes*

h_m	2	3	4	5	6	7	8	9	10
m	39	23	120	51	*aucun*	63	29	31	55
	56	52		80			68	57	
		72						96	

Chapitre 5

Corps quadratiques imaginaires

Soit $K = \mathbb{Q}(\sqrt{d})$ avec $d < 0$ sans facteurs carrés un corps quadratique imaginaire. Nous poserons

$$\alpha = \begin{cases} \sqrt{d} & \text{si } d \equiv 2, 3 \bmod (4)\,; \\ \dfrac{1+\sqrt{d}}{2} & \text{si } d \equiv 1 \bmod (4), \end{cases}$$

si bien que $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Soit $\mathfrak{a}$ un idéal de $\mathcal{O}_K$, et a un rationnel appartenant à $\mathfrak{a}$. Alors $a\mathcal{O}_K \subset \mathfrak{a} \subset \mathcal{O}_K$, donc $\mathfrak{a}$ est un $\mathbb{Z}$-module libre de rang de 2. Ce sont donc des réseaux de $\mathbb{C}$ (en identifiant $\mathbb{C}$ à $\mathbb{R}^2$), on parlera de réseaux complexes ; leur étude fait l'objet de 5.1. Nous verrons ensuite comment le calcul dans les réseaux d'un invariant bien choisi permet de déterminer le groupe des classes d'idéaux de K.

5.1 Réseaux complexes, étude de $\mathbf{SL}_2(\mathbb{Z})$

5.1 Définition (Réseaux complexes homothétiques). — *Deux réseaux Λ_1 et Λ_2 pour lesquels il existe $\alpha \in \mathbb{C}^*$ tel que $\Lambda_1 = \alpha\Lambda_2$ sont dits homothétiques.*

Deux idéaux $\mathfrak{a}$ et $\mathfrak{b}$ apprtiennent à la même classe si et seulement s'il existe $\gamma \in K^*$ tel que $\gamma\mathfrak{a} = \mathfrak{b}$, donc, selon cette définition , si et seulement s'ils sont homothétiques.

Soit $\Lambda \subset \mathbb{C}$ un $\mathbb{Z}$-module libre de rang 2 qui contient une $\mathbb{R}$-base de $\mathbb{C}$. On peut écrire

$$\Lambda = \{a\lambda_1 + b\lambda_2 \,|\, a, b \in \mathbb{Z}\}$$

pour des $\lambda_1, \lambda_2 \in \Lambda$. La condition que Λ est libre de rang 2 implique que le quotient λ_1/λ_2 n'appartient pas à $\mathbb{Q}$, et la condition qu'il contient une base $\mathbb{R}$-base de $\mathbb{C}$ montre que ce quotient n'appartient pas à $\mathbb{R}$. Nous allons donner une méthode pour vérifier si deux réseaux complexes sont homothétiques.

Choisissons une $\mathbb{Z}$-base λ_1, λ_2 de Λ comme ci-dessus. On supposera que toutes les bases sont telles que $\Im(\lambda_1/\lambda_2) > 0$. Ceci est possible car d'une part nécessairement $\Im(\lambda_1/\lambda_2) \neq 0$ puisque ce quotient n'appartient pas à $\mathbb{R}$ et d'autre part si $\Im(\lambda_1/\lambda_2) < 0$, il suffit d'intervertir le rôle de λ_1 et λ_2. Notons $\mathfrak{H} = \{z \in \mathbb{C} \,|\, \Im z > 0\}$ le demi-plan supérieur. On définit

$$\mathrm{j}(\lambda_1, \lambda_2) = \frac{\lambda_1}{\lambda_2} \in \mathfrak{H}.$$

Notons que pour tout $\alpha \in \mathbb{C}^*$,

$$\mathrm{j}(\alpha\lambda_1, \alpha\lambda_2) = \mathrm{j}(\lambda_1, \lambda_2),$$

ce qui suggère que $\mathfrak{j}$ est un bon objet pour classifier les réseaux à homothétie près.

Malheureusement $\mathfrak{j}(\lambda_1, \lambda_2)$ dépend aussi de la base λ_1, λ_2. Nous devons donc enlever la dépendance en la base pour classifier les réseaux à homothétie près. Voyons comment $\mathfrak{j}$ dépend du choix de la base. On sait que les autres bases de Λ sont données par

$$\lambda_1' = a\lambda_1 + b\lambda_2 \quad \text{et} \quad \lambda_2' = c\lambda_1 + d\lambda_2$$

où

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}).$$

Comme ci-dessus on veut se restreindre aux bases λ_1', λ_2' de Λ telles que $\Im(\lambda_1'/\lambda_2') > 0$. Il est facile de vérifier que les matrices préservant cette condition sont celles de $\mathrm{SL}_2(\mathbb{Z})$. En effet

$$\Im\left(\frac{\lambda_1'}{\lambda_2'}\right) = \Im\left(\frac{a\frac{\lambda_1}{\lambda_2} + b}{c\frac{\lambda_1}{\lambda_2} + d}\right) = \Im\left(\frac{\left(a\frac{\lambda_1}{\lambda_2} + b\right)\left(a\frac{\overline{\lambda_1}}{\overline{\lambda_2}} + b\right)}{\left|c\frac{\lambda_1}{\lambda_2} + d\right|^2}\right) = \frac{ad - bc}{\left|c\frac{\lambda_1}{\lambda_2} + d\right|^2}\Im\left(\frac{\lambda_1}{\lambda_2}\right).$$

Ainsi $\Im\left(\frac{\lambda_1'}{\lambda_2'}\right)$ et $\Im\left(\frac{\lambda_1}{\lambda_2}\right)$ sont positifs si et seulement si $ad - bc > 0$ (donc si $ab - dc = 1$).

Ces calculs suggèrent de considérer l'action de $\mathrm{SL}_2(\mathbb{Z})$ sur $\mathfrak{H}$ par

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \frac{az + b}{cz + d}.$$

Le calcul ci-dessus montre que pour $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$,

$$\Im(gz) = \Im\left(\frac{az + b}{cz + d}\right) = \frac{\Im(z)}{|cz + d|^2}.$$

Cette action est telle que si λ_1, λ_2 et λ_1', λ_2' sont deux bases correctement ordonnées, alors $\mathfrak{j}(\lambda_1, \lambda_2)$ et $\mathfrak{j}(\lambda_1', \lambda_2')$ appartiennent à la même orbite de $\mathfrak{H}$.

Maintenant, il nous reste à déterminer un ensemble dont chaque élément appartient à une unique orbite de $\mathfrak{H}$.

5.2 Définition (Groupe modulaire). — *On appelle groupe modulaire le groupe $SL_2(\mathbb{Z})/\{\pm Id\}$ noté G dans la suite.*

Soit $\mathfrak{H} = \{z \in \mathbb{C},\, \Im(z) > 0\}$. Le groupe $\mathrm{SL}_2(\mathbb{Z})$ agit sur $\mathfrak{H}$ par $gz = \frac{az + b}{cz + d}$ où g est la matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ de G. On a en effet $\Im(gz) = \frac{\Im(z)}{|cz + d|^2}$. Comme $-\mathrm{Id}$ agit trivialement, on en déduit une action de G sur $\mathfrak{H}$.

Posons

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{et} \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

On a $S(z) = -1/z$ et $T(z) = z + 1$. Notons enfin $D = \{z \in \mathbb{C}\,,\, |\,z| \geqslant 1, |\,\Re(z)| \leqslant 1/2\}$.

5.3 Lemme. — *(a) Pour tout $z \in \mathfrak{H}$, il existe $g \in G$ tel que $gz \in D$.*
(b) Supposons que deux points distincts z et z' de D soient dans la même orbite. Alors soit $\Re(z) = \pm 1/2$ et $z = z' \pm 1$, soit $|z| = 1$ et $z' = -1/z$.
(c) Soit $z \in D$ et soit $I(z) = \{g \in G, gz = z\}$ le stabilisateur de z dans G. On a $I(z) = \{Id\}$ sauf dans les trois cas suivants.
$z = i$, auquel cas $I(z)$ est le groupe d'ordre 2 engendré par S ;
$z = j = \exp(2i\pi/3)$, auquel cas $I(z)$ est le groupe d'ordre 3 engendré par ST ;
$z = -\overline{j}$, auquel cas $I(z)$ est le groupe d'ordre 3 engendré par TS.

Preuve. — (a) Soit $z \in \mathfrak{H}$ et $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$. On a $\Im(gz) = \dfrac{\Im(z)}{|cz+d|^2}$. Comme c et d sont entiers, le nombre de couples (c,d) tels que $|cz+d|$ soit inférieur à un nombre donné est fini, comme le montre l'égalité $|c|\Im(z) = |\Im(cz+d)|$. On en conclut qu'il existe $g \in G$ tel que $\Im(gz)$ soit maximal. Il existe d'autre part un entier n tel que $T^n gz$ ait une partie réelle comprise entre $-1/2$ et $1/2$. L'élément $z' = T^n gz$ appartient à D ; pour voir cela, il suffit de montrer que $|z'| \geqslant 1$. Si l'on avait $|z'| < 1$, l'élément $S(z') = -1/z'$ serait tel que

$$\Im\left(-\frac{1}{z'}\right) = \frac{\Im(z')}{|z'|^2} > \Im(z'),$$

ce qui contredit le choix de g. L'élément $g' = T^n g$ répond à la question.

(b) et (c) Soit $z \in D$ et $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ tel que $gz \in D$. Quitte à remplacer (z,g) par (gz, g^{-1}), on peut supposer que $\Im(gz) \geqslant \Im(z)$, c'est-à-dire $|\,cz+d| \leqslant 1$. Or $2\Re(z) \leqslant 1$, donc

$$1 \geqslant |cz+d|^2 = c^2|z|^2 + 2cd\Re(z) + d^2 \geqslant c^2 - |cd| + d^2 = \left(|d| - \frac{1}{2}|c|\right)^2 + \frac{3}{4}c^2 \geqslant \frac{3}{4}c^2 \quad \bigstar$$

et finalement $c \in \{-1, 0, 1\}$.

(i) Si $c = 0$, on a $d = \pm 1$ et g est une translation par $\pm b$. Comme $\Re(z)$ et $\Re(gz)$ sont tous les deux dans compris entre $-1/2$ et $1/2$, cela entraîne, soit $b = 0$ et $g = \mathrm{Id}$, soit $b = \pm 1$, auquel cas l'un des nombres $\Re(z)$ et $\Re(gz)$ doit être égal à $-1/2$ et l'autre à $1/2$.

(ii) Supposons $c = 1$. Il vient en remplaçant dans $\bigstar$

$$1 \geqslant 1 - |d| + d^2$$

d'où $|d|(|d|-1) \leqslant 0$ et enfin $d \in \{-1, 0, 1\}$.

Si $d = 1$, c'est que $|z|^2 + 2\Re(z) \leqslant 0$, d'où $|z| = 1$ et $\Re(z) = -1/2$, d'où $z = j$. On trouve alors $a - b = 1$ et $gj = a - 1/(1+j) = a + j$. Comme $-1/2 \leqslant \Re(gz) \leqslant 1/2$, on a $a = 0$ ou 1 puisque $\Re(j) = -1/2$.
De même si $d = -1$ et $z - \overline{j}$ puis $a = 0$ ou $a = -1$.

Le cas $d = 0$ donne $|z| \leqslant 1$, d'où $|z| = 1$; d'autre part puisque $ad - bc = 1$, on a $b = -1$, d'où $gz = a - 1/z = a - \overline{z}$. Mais $\Re(gz) = a - \Re(z)$ est entre $-1/2$ et $1/2$, donc si $\Re(z) \neq \pm 1/2$, on a $a = 0$, si $\Re(z) = 1/2$ on a $z = -\overline{j}$ et on peut prendre $a = 0$ ou 1 et enfin si $\Re(z) = -1/2$, on a $z = j$ avec $a = 0$ ou -1.

(iii) Le cas $c = -1$ se ramène à celui de $c = 1$ en changeant les signes de a, b, c, d (ce qui ne change pas g considéré comme élément de G).

Dans les cas (ii) et (iii), on a bien $gz = -\overline{z} = -1/z$. ∎

5.4 Corollaire. — *Les matrices S et T engendrent G.*

Preuve. — Appelons H le sous-groupe de G engendré par S et T. Il faut montrer que $G = H$. Soit donc $g \in G$. Choisissons un point z_0 intérieur à D (par exemple $z_0 = 2i$), et soit $z = gz_0$. Par le lemme, il existe $g' \in G$ tel que $g'z \in D$. Les points z_0 et $g'z = g'gz_0$ sont dans la même orbite sous l'action de $\mathrm{SL}_2(\mathbb{Z})$ et l'un d'eux est intérieur à D. D'après le lemme il en résulte que ces points sont confondus et que $gg' = \mathrm{Id}$ donc $g \in H$. L'inclusion opposée est claire. ∎

5.5 Corollaire. — *Soit*

$$\begin{aligned} Y \;=\; & \left\{ z \in \mathbb{C}, \Im(z) > 0, -\frac{1}{2} < \Re(z) < \frac{1}{2}, |z| > 1 \right\} \cup \\ & \left\{ z \in \mathbb{C}, |z| = 1, 0 \leqslant \Re(z) < \frac{1}{2} \right\} \cup \left\{ z \in \mathbb{C}, \Re(z) = \frac{1}{2}, \Im(z) \geqslant \frac{\sqrt{3}}{2} \right\}. \end{aligned}$$

Alors Y contient un et un seul élément de chaque orbite de $\mathfrak{H}$ sous l'action de G.

Preuve. — D'après le lemme, D contient au moins un point de chacune des orbites, et l'intérieur Δ de D ne contient que des éléments distincs de chaque orbite de $\mathfrak{H}$. Soit $z, z' \in D$ dans la même orbite. Si $|\Re(z)| = |\Re(z')| = 1/2$, un et un seul des deux éléments z et z' est situé sur la demi-droite $\left\{ z \in \mathbb{C}, \Re(z) = \frac{1}{2}, \Im(z) \geqslant \frac{\sqrt{3}}{2} \right\}$. Si $|z| = |z'| = 1$ avec $|\Re(z)| \neq \frac{1}{2}$ et $|\Re(z')| \neq \frac{1}{2}$ (le cas d'égalité a déjà été vu sinon), en remarquant que $-1/z$ est le symétrique de z par rapport à l'axe des ordonnées, il vient que l'arc de cercle $\left\{ z \in \mathbb{C}, |z| = 1, 0 \leqslant \Re(z) < \frac{1}{2} \right\}$ ne contient qu'un seul des deux points z et z', d'où le corollaire puisque l'intérieur de D n'est autre que $\left\{ z \in \mathbb{C}, \Im(z) > 0, -\frac{1}{2} < \Re(z) < \frac{1}{2}, |z| > 1 \right\}$. ∎

Ces résultats nous donne un algorithme pour déterminer la classe d'homothétie d'un réseau complexe Λ de base λ_1, λ_2. Commençons par calculer $\mathrm{j} = \mathrm{j}(\Lambda) = \lambda_1/\lambda_2$. On veut appliquer à j les matrices S et T pour le ramener dans Y. Si $\Im(j) < 0$, on remplace j par $1/\mathrm{j}$ et on recommence (cela revient à échanger les éléments de base). Si j est dans Y, on a fini. Sinon on ajoute un entier m tel que

$$-\frac{1}{2} < \Re(\mathrm{j} + m) \leqslant \frac{1}{2},$$

ce qui revient à appliquer m fois T. Si $\mathrm{j} + m \in Y$, on a fini. Sinon, on remplae $\mathrm{j} + m$ par $-\dfrac{1}{\mathrm{j} + m}$ et on recommance. Le corollaire 5.4 assure que l'algorithme ramène dans Y en un nombre fini de fois.

5.6 Exemple. — Soit $\Lambda = 5\mathbb{Z} + (1+i)\mathbb{Z}$. On calcule

$$\mathrm{j}(\Lambda) = \frac{5}{1+i} = \frac{5}{2} - \frac{5}{2}i,$$

donc on le remplace par

$$\frac{1}{j(\Lambda)} = \frac{1}{5} + \frac{1}{5}i \in \mathfrak{H}.$$

Ce nombre n'est pas dans Y car son module vaut $2/5 < 1$. Puisque sa partie réelle est déjà entre $-1/2$ et $1/2$, on remplace $1/\mathrm{j}(\Lambda)$ par son image par S,

$$S\left(\frac{1}{j(\Lambda)}\right) = -\mathrm{j}(\Lambda) = -\frac{5}{2} + \frac{5}{2}i$$

En ajoutant 3 à cet élément, on obtient

$$\frac{1}{2}+\frac{5}{2}i$$

qui appartient bien à Y.

Supposons que nous voulions utiliser la base $23+3i = 4(5)+3(1+i)$ et $17+2i = 3(5)+2(1+i)$ de Λ. On calcule

$$\mathfrak{j}(\Lambda) = \frac{23+3i}{17+2i} = \frac{397}{293}+\frac{5}{293}i.$$

En soustrayant 1, il vient $\frac{104}{293}+\frac{5}{293}i$, dont le module est strictement inférieur à 1. Son image par S est

$$-\frac{104}{37}+\frac{5}{37}i$$

d'où en ajoutant 3,

$$\frac{7}{37}+\frac{5}{37}i,$$

nombre dont le module est encore strictement inférieur à 1. En appliquant S,

$$-\frac{7}{2}+\frac{5}{2}i$$

et enfin en ajoutant 4,

$$\frac{1}{2}+\frac{5}{2}i \in Y,$$

comme précédemment.

Pour tirer pleinement profit des réseaux complexes, il nous faut être capables, étant donné un idéal $\mathfrak{a} = (a_1, a_2)$, de trouver une $\mathbb{Z}$-base $\mathfrak{a}$. La méthode consiste à utiliser l'algorithme de Gauss. On sait que a_1, a_2 est un système $\mathbb{Z}[\alpha]$-générateur de $\mathfrak{a}$, donc $a_1, a_1\alpha, a_2, a_2\alpha$ est un système $\mathbb{Z}$-générateur de $\mathfrak{a}$. Ecrivons chacun de ces éléments dans la base $1, \alpha$ de $\mathcal{O}_K$. Par l'algorithme d'élimination de Gauss, il nous restera deux vecteurs qui formeront une $\mathbb{Z}$-base.

5.7 Exemple. — Soit $K = \mathbb{Q}(\sqrt{-5})$ et $\mathfrak{a} = (10, \alpha+5)$, où $\alpha = \sqrt{-5}$. Alors $10, 10\alpha, 5+\alpha$ et $(5+\alpha)\alpha = -5+5\alpha$ est un système $\mathbb{Z}$-générateur de $\mathfrak{a}$. On applique l'algorithme d'élimination de Gauss à la matrice

$$\begin{pmatrix} 10 & 0 & 5 & -5 \\ 0 & 10 & 1 & 5 \end{pmatrix}.$$

En ajoutant -5 fois la troisième colonne à la dernière, il vient

$$\begin{pmatrix} 10 & 0 & 5 & -30 \\ 0 & 10 & 1 & 0 \end{pmatrix}.$$

En ajoutant 3 fois la première colonne à la dernière, on élimine la dernière colonne. Enfin en ôtant 10 fois la troisième colonne à la seconde, on a

$$\begin{pmatrix} 10 & -50 & 5 \\ 0 & 0 & 1 \end{pmatrix}.$$

Finalement, en ajoutant 5 fois la première colonne à la seconde, la seconde colonne disparaît. L'idéal $\mathfrak{a}$ est donc engendré sur $\mathbb{Z}$ par 10 et $\alpha+5$.

Voici une proposition bien utile pour éviter de nombreux calculs (rappelons que K est un corps quadratique).

5.8 Proposition. — *Soit p un premier rationnel qui se décompose ou qui se ramifie dans K et soit $\mathfrak{p} = (p, \alpha + m)$ un idéal au-dessus de p. Alors p et $\alpha + m$ est une $\mathbb{Z}$-base du réseau $\mathfrak{p}$.*

Preuve. — L'idéal $(p, \alpha + m)$ admet pour système $\mathbb{Z}[\alpha]$-générateur $p, \alpha + m$, et par conséquent $p, p\alpha, \alpha + m, \alpha^2 + m\alpha$ comme système $\mathbb{Z}$-générateur. Il suffit de montrer que $p\alpha$ et $\alpha^2 + m\alpha$ s'expriment comme combinaisons $\mathbb{Z}$-linéaires de p et $\alpha + m$.

Sans hypothèse sur la classe de d mod (4), on a

$$p\alpha = -m(p) + p(\alpha + m)$$

Pour décomposer $\alpha^2 + m\alpha$, il faut envisager deux cas.

Suppsons d'abord que $d \equiv 2, 3 \bmod (4)$. Alors $-m$ est racine de $X^2 - d$ mod (p), donc p divise $m^2 - d$. On a aussi $\alpha^2 + m\alpha = d + m\alpha$, donc on peut écrire

$$d + m\alpha = \frac{d - m^2}{p}(p) + m(\alpha + m).$$

Suppsons maintenant que $d \equiv 1 \bmod (4)$. Alors $-m$ est racine de $X^2 - X + \dfrac{1-d}{4}$ mod (p), donc p divise $m^2 + m + \dfrac{1-d}{4}$. On a $\alpha^2 = \alpha - \dfrac{1-d}{4}$, donc $\alpha^2 + m\alpha = (m+1)\alpha - \dfrac{1-d}{4}$, et on peut écrire

$$-\frac{1-d}{4} + (m+1)\alpha = \frac{m^2 + m + \frac{1-d}{4}}{p}(p) + (m+1)(\alpha + m),$$

d'où le résultat. ∎

5.2 Calculs de groupes de classes d'idéaux

Dans le cas des corps quadratiques imaginaires, la constante de Minkowski prend une forme très simple

$$\mu_K = \begin{cases} \dfrac{4}{\pi}\sqrt{-d} & \text{si } d \equiv 2, 3 \bmod (4) \\ \dfrac{2}{\pi}\sqrt{-d} & \text{si } d \equiv 1 \bmod (4). \end{cases}$$

Rappelons que d'après 4.4, l'ensemble P_0 des idéaux au-dessus des p rationnels premiers, avec $p \leqslant \mu_K$, contient des générateurs de $\mathcal{C}_K$. La question est maintenant de déterminer lesquels de ces générateurs sont égaux, et quelles relations ils satisfont entre eux.

Si pour $\mathfrak{p}, \mathfrak{q} \in P_0$, on a $\mathfrak{j}(\mathfrak{p}) = \mathfrak{j}(\mathfrak{q})$, on sait que ces réseaux complexes sont homothétiques, c'est-à-dire qu'il existe $\gamma \in \mathbb{C}^*$ tel que $\mathfrak{p} = \gamma\mathfrak{q}$. Mais bien sûr $\gamma \in K^*$; en effet soit α un élement de $\mathfrak{a}$, alors $\gamma\alpha$ appartient à $\mathfrak{b}$, appelons β cet élément. Il vient $\gamma = \beta/\alpha \in K^*$, et donc $\mathfrak{p} \sim \mathfrak{q}$. Ainsi $\mathfrak{p}$ et $\mathfrak{q}$ sont égaux dans $\mathcal{C}_K$, et seul un des idéaux $\mathfrak{p}$ et $\mathfrak{q}$ doit être inclus dans la liste des générateurs de $\mathcal{C}_K$ (on élimine les répétitions). Soit P_1 un ensemble contenant un élément de P_0 pour chaque valeur de $\mathfrak{j}$ obtenue ; P_1 engendre toujours $\mathcal{C}_K$ et ses éléments sont distincts dans $\mathcal{C}_K$.

Enfin on peut déterminer la table de multiplication de $\mathcal{C}_K$. Tout d'abord on connaît l'inverse de chaque élément de $\mathfrak{p} \in P_1$ puisqu'il existe $\mathfrak{p}' \in P_0$ tel que $\mathfrak{p}\mathfrak{p}' = (p)$ est principal. Si $\mathfrak{p}$ et $\mathfrak{q}$ sont deux deux idéaux premiers qui ne sont pas inverses, on détermine une base du réseau $\mathfrak{p}\mathfrak{q}$ et on calcule $\mathfrak{j}(\mathfrak{p}\mathfrak{q}) \in Y$. Si cette quantité égale l'un des $\mathfrak{j}(\mathfrak{a})$ pour $\mathfrak{a} \in P_1$, c'est que $\mathfrak{p}\mathfrak{q}$ et $\mathfrak{a}$ sont égaux dans $\mathcal{C}_K$. Sinon on obtient un nouvel élément qu'on ajoute à la table. On continue ainsi jusqu'à ce que tous les produits aient été déterminés. Très souvent le nombre de calculs est réduit en utilisant des relations déjà établies dans les calculs précédents.

5.9 Exemple. — Soit $K = \mathbb{Q}(\sqrt{-14})$. On a $\mu_K \approx 4,76$, donc les seuls idéaux à considérer sont $2\mathcal{O}_K$ et $3\mathcal{O}_K$. Un calcul montre que

$$2\mathcal{O}_K = (2, \sqrt{-14})^2 \quad \text{et} \quad 3\mathcal{O}_K = (3, \sqrt{-14}+1)(3, \sqrt{-14}+2).$$

Soit $\mathfrak{a}_1 = \mathcal{O}_K$, $\mathfrak{a}_2 = (2, \sqrt{-14})$, $\mathfrak{a}_3 = (3, \sqrt{-14}+1)$ et $(3, \sqrt{-14}+2)$.

On va calculer $\mathfrak{j}$ pour chacun de ses idéaux. On a

$$\mathfrak{j}(\mathfrak{a}_1) = \sqrt{14}i.$$

Par la proposition 5.8 on voit que 2 et $\sqrt{-14}$ constituent une base du réseau $\mathfrak{a}_2$, on trouve

$$\mathfrak{j}(\mathfrak{a}_2) = \frac{\sqrt{14}}{2}i.$$

De même

$$\mathfrak{j}(\mathfrak{a}_3) = \frac{1}{3} + \frac{\sqrt{14}}{3}i \quad \text{et} \quad \mathfrak{j}(\mathfrak{a}_3') = -\frac{1}{3} + \frac{\sqrt{14}}{3}i.$$

Donc ces trois générateurs sont distincts dans $\mathcal{C}_K$ et $h_K = 4$.

Déterminons maintenant la table de $\mathcal{C}_K$. On a déjà la table partielle suivante

	$\mathfrak{a}_1$	$\mathfrak{a}_2$	$\mathfrak{a}_3$	$\mathfrak{a}_3'$
$\mathfrak{a}_1$	$\mathfrak{a}_1$	$\mathfrak{a}_2$	$\mathfrak{a}_3$	$\mathfrak{a}_3'$
$\mathfrak{a}_2$	$\mathfrak{a}_2$	$\mathfrak{a}_1$		
$\mathfrak{a}_3$	$\mathfrak{a}_3$			$\mathfrak{a}_1$
$\mathfrak{a}_3'$	$\mathfrak{a}_3'$		$\mathfrak{a}_1$	

On calcule

$$\mathfrak{a}_2\mathfrak{a}_3 = (2, \alpha)(3, \alpha+1) = (6, 2\alpha+2, 3\alpha, \alpha^2+\alpha) = (6, 2\alpha+2, 3\alpha, \alpha-14) = (6, \alpha+4).$$

Soit $\mathfrak{a}$ cet idéal. L'algorithme d'élimination de Gauss montre que 6 et $\alpha+4$ sont une base du réseau $\mathfrak{a}$. On trouve

$$\mathfrak{j}(\mathfrak{a}) = -\frac{1}{3} + \frac{\sqrt{14}}{3}i,$$

donc $\mathfrak{a}_2\mathfrak{a}_3 \sim \mathfrak{a}_3'$. Ceci nous permet de calculer $\mathfrak{a}_3'^2 \sim \mathfrak{a}_2\mathfrak{a}_3\mathfrak{a}_3' \sim \mathfrak{a}_2$ puis $\mathfrak{a}_2\mathfrak{a}_3' \sim \mathfrak{a}_2^2\mathfrak{a}_3 \sim \mathfrak{a}_3$ et $\mathfrak{a}_3^2 \sim \mathfrak{a}_2\mathfrak{a}_3'\mathfrak{a}_3 \sim \mathfrak{a}_2$. La table de multiplication de $\mathcal{C}_K$ est donc

	$\mathfrak{a}_1$	$\mathfrak{a}_2$	$\mathfrak{a}_3$	$\mathfrak{a}_3'$
$\mathfrak{a}_1$	$\mathfrak{a}_1$	$\mathfrak{a}_2$	$\mathfrak{a}_3$	$\mathfrak{a}_3'$
$\mathfrak{a}_2$	$\mathfrak{a}_2$	$\mathfrak{a}_1$	$\mathfrak{a}_3'$	$\mathfrak{a}_3$
$\mathfrak{a}_3$	$\mathfrak{a}_3$	$\mathfrak{a}_3'$	$\mathfrak{a}_2$	$\mathfrak{a}_1$
$\mathfrak{a}_3'$	$\mathfrak{a}_3'$	$\mathfrak{a}_3$	$\mathfrak{a}_1$	$\mathfrak{a}_2$

Par conséquent $\mathcal{C}_K \simeq \mathbb{Z}/4\mathbb{Z}$.

5.10 Exemple. — Soit $K = \mathbb{Q}(\sqrt{-119})$ et $\alpha = \dfrac{1+\sqrt{-119}}{2}$, si bien que $\alpha^2 = \alpha - 30$. La constante de Minkowski est $\mu_K \approx 6,94$ de sorte que nous devons considérons les premiers 2, 3 et 5. On trouve

$$2\mathcal{O}_K = (2, \alpha)(2, \alpha+1), \quad 3\mathcal{O}_K = (3, \alpha)(3, \alpha+2) \quad \text{et} \quad 5\mathcal{O}_K = (5, \alpha)(5, \alpha+4).$$

Soit $a_1 = \mathcal{O}_K, \mathfrak{a}_2 = (2, \alpha), \mathfrak{a}_2' = (2, \alpha+1), \mathfrak{a}_3 = (3, \alpha), \mathfrak{a}_3' = (3, \alpha+2), \mathfrak{a}_5 = (5, \alpha)$ et $\mathfrak{a}_5' = (5, \alpha+4)$. On trouve $\mathfrak{j}(\mathfrak{a}_1) = \dfrac{1}{2} + \dfrac{\sqrt{119}}{2}i$ et

$$\mathfrak{j}(\mathfrak{a}_2) = \frac{1}{4} + \frac{\sqrt{119}}{4}i, \qquad \mathfrak{j}(\mathfrak{a}_3) = \frac{1}{6} + \frac{\sqrt{119}}{6}i, \qquad \mathfrak{j}(\mathfrak{a}_5) = \frac{1}{10} + \frac{\sqrt{119}}{10}i$$
$$\mathfrak{j}(\mathfrak{a}_2') = -\frac{1}{4} + \frac{\sqrt{119}}{4}i, \qquad \mathfrak{j}(\mathfrak{a}_3') = -\frac{1}{6} + \frac{\sqrt{119}}{6}i, \qquad \mathfrak{j}(\mathfrak{a}_5') = -\frac{1}{10} + \frac{\sqrt{119}}{10}i.$$

On commence par calculer les puissances de $\mathfrak{a}_2$. On trouve

$$\mathfrak{a}_2^2 = (4, 2\alpha, \alpha^2) = (4, 2\alpha, \alpha - 30) = (4, \alpha + 2).$$

Soit $\mathfrak{a}_4$ cet idéal. On vérifie facilement que $4, \alpha + 2$ et

$$\mathfrak{j}(\mathfrak{a}_4) = -\frac{3}{8} + \frac{\sqrt{119}}{8}i.$$

Ensuite on a

$$\mathfrak{a}_2^3 = \mathfrak{a}_2\mathfrak{a}_4 = (2, \alpha)(4, \alpha + 2) = (8, 4\alpha, 2\alpha + 4, \alpha^2 + 2\alpha) = (8, 4\alpha, 2\alpha + 4, 3\alpha - 30) = (8, \alpha + 6).$$

Soit $\mathfrak{a}_8$ cet idéal. Il a pour base en tant que réseau $8, \alpha + 6$; par suite

$$\mathfrak{j}(\mathfrak{a}_8) = \frac{3}{8} + \frac{\sqrt{119}}{8}i.$$

Puis

$$\mathfrak{a}_2^4 = \mathfrak{a}_2\mathfrak{a}_8 = (2, \alpha)(8, \alpha+6) = (16, 2\alpha+12, 8\alpha, \alpha^2+6\alpha) = (16, 2\alpha+12, 8\alpha, 7\alpha-30) = (16, \alpha-2).$$

Soit $\mathfrak{a}_{16}$ ce réseau dont une base est $16, \alpha - 2$. On a

$$\mathfrak{j}(\mathfrak{a}_{16}) = -\frac{1}{4} + \frac{\sqrt{119}}{4}i$$

donc $\mathfrak{a}_2^4 \sim \mathfrak{a}_2'$ puis $\mathfrak{a}_2^5 \sim \mathfrak{a}_1$. On a donc trouvé un sous-groupe cyclique d'ordre 5 de $\mathcal{C}_K$.

Calculons maintenant les puissances de $\mathfrak{a}_3$. On a

$$\mathfrak{a}_3^2 = (9, 3\alpha, \alpha - 30) = (9, \alpha + 6);$$

ce réseau a pour base $9, \alpha + 6$ et son invariant $\mathfrak{j}$ est

$$-\frac{3}{8} + \frac{\sqrt{119}}{8}i,$$

donc $\mathfrak{a}_3^2 \sim \mathfrak{a}_4$. On en déduit immédiatement les puissances paires de $\mathfrak{a}_3$ en calculant dans le groupe cyclique engendré par $\mathfrak{a}_2$. On a $\mathfrak{a}_3^4 \sim \mathfrak{a}_4^2 \sim \mathfrak{a}_2'$, $\mathfrak{a}_3^6 \sim \mathfrak{a}_4^3 \sim \mathfrak{a}_2$, $\mathfrak{a}_3^8 \sim \mathfrak{a}_4^4 \sim \mathfrak{a}_8$ et $\mathfrak{a}_3^{10} \sim \mathfrak{a}_4^5 \sim \mathfrak{a}_1$. Pour calculer les puissances impaires de $\mathfrak{a}_3$ on va multiplier les puissances paires de $\mathfrak{a}_3$ par $\mathfrak{a}_3$. On trouve

$$\mathfrak{a}_3^3 \sim \mathfrak{a}_3\mathfrak{a}_4 = (3, \alpha)(4, \alpha + 2) = (12, 3\alpha + 6, 4\alpha, \alpha^2 + 2\alpha) = (12, 3\alpha + 6, 4\alpha, 3\alpha - 30) = (12, \alpha + 6).$$

Une base de ce réseau est $12, \alpha + 6$ et son invariant $\mathfrak{j}$ est

$$\frac{1}{10} + \frac{\sqrt{119}}{10}i,$$

donc $\mathfrak{a}_3^3 \sim \mathfrak{a}_5$. Puisque $\mathfrak{a}_3$ a pour ordre 10 et $\mathfrak{a}_5^{-1} \sim \mathfrak{a}_5'$, on a $\mathfrak{a}_3^7 \sim \mathfrak{a}_5'$. Puisque on a aussi $\mathfrak{a}_3^9 \sim \mathfrak{a}_3'$, chaque générateur est une puissance de $\mathfrak{a}_3$. Donc $\mathcal{C}_K$ est cyclique d'ordre 10 engendré par $\mathfrak{a}_3$.

5.3 Formes quadratiques et nombre de classes

5.3.1 Formes quadratiques binaires à coefficients entiers

Une forme quadratique binaire à coefficients entiers est une fonction de la forme

$$\varphi(x,y) = ax^2 + bxy + cy^2, \quad (a,b,c) \in \mathbb{Z}.$$

Le forme φ sera notée (a,b,c). Le discriminant de la forme (a,b,c) est $\mathrm{D} = b^2 - 4ac$; elle est définie positive si $\mathrm{D} < 0$ et $a > 0$. Dans ce cas on aussi $c > 0$ et $\varphi(x,y) > 0$ si $(x,y) \neq (0,0)$.

On dira que l'entier n est représentable par la forme (a,b,c) s'il existe $(x,y) \in \mathbb{Z}$ tels que $n = ax^2 + bxy + c$.

Soit $f : \mathbb{Z}^2 \longmapsto \mathbb{Z}^2$ une application. Elle est dite *unimodulaire* si son déterminant vaut 1. En notant $f(x,y) = (px+qy, rx+sy)$, cela se traduit par $ps - qr = 1$. En particulier f est inversible.

Les exemples les plus simples de transformations unimodulaires sont

$$f_1(x,y) = (y,-x) \quad ; \quad f_2(x,y) = (x+y,y) \quad \text{et} \quad f_3(x,y) = (x-y,y).$$

Si, dans $\varphi(x,y) = ax^2 + bxy + cy^2$, on remplace x par $px' + qy'$ et y par $rx' + sy'$, on obtient une nouvelle forme quadratique $\varphi'(x',y') = a'x'^2 + b'x'y' + c'y'^2$ avec

$$\left\{ \begin{array}{l} a' = ap^2 + bpr + cr^2 = \varphi(p,r) \\ b' = 2apq + b(ps+qr) + 2crs \\ c' = aq^2 + bqs + cs^2 = \varphi(q,s). \end{array} \right. \tag{5.1}$$

5.11 Définition. — *Deux formes quadratiques φ et φ' sont dites équivalentes s'il existe une transformation unimodulaire f telle que $\varphi \circ f = \varphi'$. On notera $\varphi \sim \varphi'$.*

Par exemple en utilisant f_1, f_2 et f_3, on a les transformations suivantes.

(**T1**) $(a,b,c) \sim (c,-b,a)$;

(**T2**) $(a,b,c) \sim (a,b+2a,a+b+c)$;

(**T3**) $(a,b,c) \sim (a,b-2a,a-b+c)$.

5.12 Proposition. — *La relation $\sim$ est une relation d'équivalence qui conserve le discriminant.*

Preuve. — Posons $M = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$ et $X = \begin{pmatrix} x \\ y \end{pmatrix}$. On a $\varphi(X) = X^t M X$ ou X^t désigne la transposée de X. Soit U une matrice unimodulaire et $Y = UX$ le changement de variables correspondant. Alors $\varphi'(Y) = Y^t M' X$ avec $M' = U^t M U$. Ainsi φ et φ' sont équivalentes si et seulement si leurs matrices sont liées par la relation $M' = U^t M U$ où U est unimodulaire. La relation est

(*i*) réflexive car $M = \mathrm{Id}_2^t M \mathrm{Id}_2$;

(*ii*) symétrique car $M' = U^t M U \Longleftrightarrow M = (U^{-1})^t M' U^{-1}$ et U^{-1} est unimodulaire;

(*iii*) transitive car $M' = U^t M U$ et $M'' = V^t M V$ implique $M'' = (UV)^t M (UV)$ et UV est unimodulaire car $\det(UV) = \det(U)\det(V) = 1$.

Enfin si $M' = U^t M U$, on a $\det(M') = \det(M)$, donc D = D' car $\mathrm{D} = -4\det(M)$ par un calcul immédiat. ∎

5.13 Remarque. — Soit φ une forme définie positive; en rangeant les valeurs $v_0 = 0 < v_1 \leqslant v_2 \leqslant v_3 \leqslant \ldots$ de le forme φ dans l'ordre croissant (chaque valeur figurant autant de fois qu'elle est atteinte), nous voyons que deux formes définies positives équivalentes ont la même suite v_n. En particulier, elles représentent les mêmes entiers.

5.14 Théorème. — *Toute forme quadratique définie positive est équivalente à une forme (a, b, c) vérifiant*

$$-a < b \leqslant a < c \quad ou \quad 0 \leqslant b \leqslant a = c. \tag{5.2}$$

Preuve. — La transformation (T1) échange a et c en laissant $|b|$ inchangé, et les transformations (T2) et (T3) diminuent $|b|$ en laissant a inchangé. En appliquant alternativement ces transformations, on voit que toute forme définie positive est équivalente à une forme (a_0, b_0, c_0) avec $-a_0 \leqslant b_0 \leqslant a_0 \leqslant c_0$. Si $b_0 = -a_0$, la transformation (T2) montre que $(a_0, b_0, c_0) \sim (a_1, b_1, c_1)$, avec $-a_1 < b_1 \leqslant a_1 \leqslant c_1$, car alors $c_1 = c_0$. Si $a_1 = c_1$, la transformation (T1) permet de remplacer b_1 par $-b_1$. ∎

5.15 Exemple. — Réduisons la forme $(10, 34, 29)$; on a

$$(10, 34, 29) \overset{T3}{\sim} (10, 14, 5) \overset{T3}{\sim} (10, -6, 1) \overset{T1}{\sim} (1, 6, 10) \overset{T3}{\sim} (1, 4, 5) \overset{T3}{\sim} (1, 2, 2) \overset{T3}{\sim} (1, 0, 1)$$

où on a indiqué les transformations à appliquer.

5.16 Théorème. — *Deux formes quadratiques définies positives réduites sont non équivalentes.*

Preuve. — Soit $\varphi = (a, b, c)$ une forme quadratique définie positive réduite, donc $|b| \leqslant a \leqslant c$. Si $|x| \geqslant |y| \geqslant 1$, on a

$$\varphi(x, y) \geqslant |x|(a|x| - |by|) + cy^2 \geqslant |x|(a - |b|) + cy^2 \geqslant a - b + c.$$

Par symétrie, cette inégalité est vraie si $(x, y) \neq (0, 0)$. Donc les premières valeurs de φ sont

$$v_0 = 0,\ v_1 = a,\ v_2 = a,\ v_3 = c,\ v_4 = c \text{ et } v_5 = a - |b| + c$$

atteintes respectivement pour $(x, y) = (0, 0), (1, 0), (-1, 0), (0, 1), (0, -1)$ et $(1, 1)$.

Si $\varphi' = (a', b', c')$, réduite, est équivalente à φ, elle a même suite de valeurs, donc $a' = a$, $c' = c$ et $a' - |b'| + c = a - |b| + c$ d'où $|b'| = |b|$. Il reste à montrer $b' = b$. Distinguons plusieurs cas et utilisons (5.2).

(*i*) Si $b = a$, on a $b \geqslant 0$, donc $|b'| = a$ et puisque φ' est réduite,

$$-a' = -a < b' \leqslant a' = a \Longrightarrow b' = a = b.$$

(*ii*) Si $a = c$, alors $a' = c'$ donc $b \geqslant 0$ et $b' \geqslant 0$, d'où $b = b'$.

(*iii*) En vertu de (5.2), il reste le cas $-a < b < a < c$. Notons $x = px' + qy'$ et $y = rx' + sy'$ avec $ps - qr = 1$ la transformation unimodulaire qui tranforme φ et φ'. Le première équation de (5.1) s'écrit

$$a' = a = \varphi(p, r) = v_1 = v_2 < v_3.$$

Donc $p = \pm 1, r = 0$; par suite $ps = 1$. La deuxième relation de (5.1) entraîne $b' \equiv b \bmod (2a)$. Mais $-a < b < a$ et $-a < b' \leqslant a$, donc $-2a < b - b' \leqslant 0$ et $b = b'$. ∎

5.17 Théorème. — *Il n'existe qu'un nombre fini de classes d'équivalences de formes quadratiques de discriminants $D < 0$ donné. Ce nombre, noté h_D est égal au nombre de solution $(a, b, c) \in \mathbb{N}^* \times \mathbb{Z} \times \mathbb{N}^*$ du système d'équation*

$$\begin{cases} b^2 - 4ac = D \\ a \leqslant \sqrt{-D/3} \\ -a < b \leqslant a < c \quad ou \quad 0 \leqslant b \leqslant a = c. \end{cases}$$

Preuve. — Toute forme étant équivalente à une forme réduite et les formes réduites étant non équivalentes entre elles, le nombre de classe d'équivalence de forme de discriminant D est donc le nombre de formes réduites $\varphi = (a, b, c)$ de discriminant D.

On a alors $b^2 - 4ac = \mathrm{D}$. Par les formules (5.2),

$$|b| \leqslant a \text{ et } |b| \leqslant c \Longrightarrow b^2 \leqslant ac,$$

d'où $-3ac \geqslant \mathrm{D}$ puis $ac \leqslant -\mathrm{D}/3$. Mais $0 \leqslant a \leqslant c$, donc $a \leqslant \sqrt{-\mathrm{D}/3}$ et a ne peut prendre qu'un nombre fini de valeurs ; il en est de même de b puisque $|b| \leqslant a$, et de c puisque $b^2 - 4ac = \mathrm{D}$. ∎

Donnons trois exemples.

5.18 Exemple. — Prenons $\mathrm{D} = -20$. Alors $a \leqslant \sqrt{20/3}$ montre que $a = 1$ ou $a = 2$.

(*i*) Supposons $a = 1$. Alors $-1 < b \leqslant 1$ ou $0 \leqslant b \leqslant 1$, donc $b = 0$ ou $b = 1$. Si $b = 0$, on a $-20 = b^2 - 4ac = -4c$, donc $c = 5$. Le cas $b = 1$ est impossible car 4 ne divise pas 21.

(*ii*) Supposons $a = 2$. On obtient $b = 0, \pm 1$ ou 2. Alors c vérifie respectivement $-8c = -20$, $1 - 8c = -20$ ou $4 - 8c = -20$; seule la dernière équation convient ; ainsi $c = 3, b = 2$.

Il n'existe donc que deux formes réduites de discriminant -20, et $h_{-20} = 2$.

5.19 Exemple. — Prenons $\mathrm{D} = -163$. Alors $a \leqslant \sqrt{163/3}$ montre que $a = 1, 2, 3, 4, 5, 6$ ou 7 et les valeurs possibles de b sont $0, \pm 1, \pm 2, \pm 3, \pm 5, \pm 6$ et 7 avec $b^2 - 4ac = -163$ et $|b| \leqslant a$.

(*i*) Pour tout a, le cas $b = 0$ ne peut se produire puisque 163 est impair.

(*ii*) Le cas $b = \pm 1$ mène à $4ac = 164 = 4 \times 41$; il ne peut se produire que si $a = 1$ et dans ce cas $b = 1$ et $c = 41$;

(*iii*) le cas $b = \pm 2$ mène à $4ac = 167$ qui est premier ;

(*iv*) le cas $b = \pm 3$ mène à $4ac = 172 = 4 \times 43$, incompatible avec $a \geqslant 3$;

(*v*) le cas $b = \pm 4$ mène à $4ac = 173$ qui premier ;

(*vi*) le cas $b = \pm 5$ mène à $4ac = 188 = 4 \times 47$, incompatible avec $a \geqslant 5$;

(*vii*) le cas $b = \pm 6$ mène à $4ac = 199$ qui est premier ;

(*viii*) le cas $b \pm 7$ mène à $4ac = 212 = 4 \times 53$, incompatible avec $a \geqslant 7$.

Par conséquent il n'existe qu'une seule forme quadratique réduite de discriminant -163, c'est $(1, 1, 41)$.

La valeur -163 est remarquable, on verra d'ailleurs plus loin que c'est la plus petite valeur possible de D telle que $h_{\mathrm{D}} = 1$. Prenons maintenant une valeur de D qui, à l'inverse, fournit beaucoup de formes quadratiques réduites.

5.20 Exemple. — Prenons $\mathrm{D} = -47$. Alors $a \leqslant \sqrt{47/3}$ montre que $a = 1, 2, 3$ ou 4 et les valeurs possibles de b sont $0, \pm 1, \pm 2, \pm 3$ et 4 avec $b^2 - 4ac = -47$ et $|b| \leqslant a$.

(*i*) Pour tout a, le cas $b = 0$ ne peut se produire puisque 47 est impair.

(*ii*) Le cas $b = \pm 1$ mène à $ac = 12$. Si $a = 1$, alors $c = 12$, puis $b = 1$. Si $a = 2$, on a $c = 6$ et $b = \pm 1$. Si $a = 3$, on a $c = 4$ et $b = \pm 1$. Pour les autres valeurs de a qui divisent 12, on a $a > c$, impossible.

(*iii*) le cas $b = \pm 2$ mène à $4ac = 51$ qui est premier ;

(*iv*) le cas $b = \pm 3$ mène à $4ac = 56 = 4 \times 14$, incompatible avec $3 \leqslant a \leqslant 4$;

(*v*) le cas $b = \pm 4$ mène à $4ac = 63$ qui est impair.

Il existe donc cinq formes quadratiques réduites de discriminant -47, ce sont $(1, 1, 12)$, $(2, \pm 1, 6)$ et $(3, \pm 1, 4)$.

5.3.2 Nombre de classes

Nous allons maintenant utiliser les formes quadratiques à coefficients entiers pour calculer le nombre de classes d'un corps quadratique imaginaire. L'objet de cette section est de démontrer le théorème suivant.

5.21 Théorème. — *Soit $K = \mathbb{Q}(\sqrt{d})$, $d < 0$ et sans facteur carré un corps quadratique imaginaire. Alors le nombre de classes de $\mathcal{O}_K$ est égal au nombre de classes de formes quadratiques définies positives de discriminant D_K.*

La première étape est de construire une application de l'ensemble des classes d'idéaux de $\mathcal{O}_K$ dans l'ensemble des classes d'équivalence des formes quadratiques de discriminant D.

5.22 Lemme. — *Soit $\mathfrak{a}$ un idéal de $\mathcal{O}_K$. Il existe une base de $\mathfrak{a}$ en tant que $\mathbb{Z}$-module de la forme $(\alpha, \theta\alpha)$ avec $\alpha \in \mathcal{O}_K$ et $\theta \in K$ tel que $\Im(\theta) > 0$.*

Preuve. — La preuve n'est pas sans rappeler la construction de $\mathfrak{j}$ page 52. Soit (α, β) une base $\mathfrak{a}$ en tant que $\mathbb{Z}$-module. Quitte à invertir α et β, on peut supposer $\Im(\alpha/\beta) > 0$ (α/β est n'est pas réel car sinon α et β seraient liés sur $\mathbb{R}$). Le nombre $\theta = \beta/\alpha \in K$ convient. ∎

Soit $\mathfrak{a}$ un idéal de $\mathcal{O}_K$, et $(\alpha, \theta\alpha)$ une base comme dans le lemme. Considérons la forme quadratique

$$Q_{\mathfrak{a}}(x, y) = (\alpha x + \theta\alpha y)(\overline{\alpha} + \overline{\theta\alpha} y) = px^2 + qxy + ry^2.$$

On a $p = \alpha\overline{\alpha} = \mathrm{N}_{K/\mathbb{Q}}(\alpha)$, $r = \mathrm{N}_{K/\mathbb{Q}}(\theta\alpha)$ et $q = \alpha\overline{\theta\alpha} + \overline{\alpha}\theta\alpha = \mathrm{Tr}_{K/\mathbb{Q}}(\alpha\theta\alpha)$, et comme α et $\theta\alpha$ sont dans $\mathcal{O}_K$, il vient $p, q, r \in \mathbb{Z}$.

Le discriminant de cette forme quadratique est

$$q^2 - 4pr = (\alpha\overline{\alpha\theta} + \overline{\alpha}\theta\alpha)^2 - 4(\alpha\overline{\alpha})(\theta\alpha)\overline{\theta\alpha} = (\alpha\overline{\alpha\theta} - \overline{\alpha}\theta\alpha)^2 = \left| \begin{array}{cc} \alpha & \overline{\alpha} \\ \theta\alpha & \overline{\theta\alpha} \end{array} \right|^2 = \mathrm{D}_{\mathfrak{a}} = (\mathrm{N}_K(\mathfrak{a}))^2 \mathrm{D}_K,$$

la dernière égalité résultant du corollaire 1.46.

Comme $\alpha\mathcal{O}_K \subset \mathfrak{a}$, on a $\mathrm{N}_K(\mathfrak{a}) | \mathrm{N}_{K/\mathbb{Q}}(\alpha) = p$ et de même $\mathrm{N}_K(\mathfrak{a}) | r$. D'après le calcul ci-dessus, on en déduit que q^2 est divisible par $(\mathrm{N}_K(\mathfrak{a}))^2$, donc $\mathrm{N}_K(\mathfrak{a}) | q$. On pose alors

$$a = \frac{p}{\mathrm{N}_K(\mathfrak{a})}, \quad b = \frac{q}{\mathrm{N}_K(\mathfrak{a})} \quad \text{et} \quad c = \frac{r}{\mathrm{N}_K(\mathfrak{a})} \tag{5.3}$$

et

$$R_{\mathfrak{a}}(x, y) = ax^2 + bxy + c.$$

Le discriminant de R est $b^2 - 4ac = \dfrac{q^2 - 4pr}{(\mathrm{N}_K(\mathfrak{a}))^2} = \mathrm{D}_K$.

5.23 Lemme. — *L'application*

$$\Psi : \mathfrak{a} \longmapsto R_{\mathfrak{a}}(x, y)$$

définit une application de l'ensemble des classes d'idéaux de $\mathcal{O}_K$ dans l'ensemble des classes d'équivalence des formes quadratiques de discriminant D_K.

Preuve. — Soit $\mathfrak{a}_1$ et $\mathfrak{a}_2$ deux idéaux de $\mathcal{O}_K$ équivalents de base respective $(\alpha_1, \theta_1\alpha_1)$ et $(\alpha_2, \theta_2\alpha_2)$ comme dans le lemme 5.22. Puisque $\mathfrak{a}_1 \sim \mathfrak{a}_2$, il existe $\gamma \in K$ tel que $\mathfrak{a}_1 = (\gamma)\mathfrak{a}_2$, donc en écrivant $\gamma = \gamma_1/\gamma_2$, il vient $\gamma_1\mathfrak{a}_1 = \gamma_2\mathfrak{a}_2$. Par suite il existe $s, t, u, v \in \mathbb{Z}$ tels que

$$\left\{ \begin{array}{rcl} \gamma_1\alpha_1 & = & \gamma_2(s\alpha_2 + t\theta_2\alpha_2) \\ \gamma_1\theta_1\alpha_1 & = & \gamma_2(u\alpha_2 + v\theta_2\alpha_2). \end{array} \right. \tag{5.4}$$

De même il existe $s', t', u', v' \in \mathbb{Z}$ tels que

$$\left\{ \begin{array}{rcl} \gamma_2\alpha_2 & = & \gamma_1(s'\alpha_1 + t'\theta_1\alpha_1) \\ \gamma_2\theta_2\alpha_2 & = & \gamma_1(u'\alpha_1 + v'\theta_1\alpha_1). \end{array} \right. \tag{5.5}$$

Donc $\begin{pmatrix} s & t \\ u & v \end{pmatrix} \begin{pmatrix} s' & t' \\ u' & v' \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, d'où en prenant les déterminants $(sv-ut)(s'v'-u't') = 1$, donc $sv - ut = \pm 1$. Mais en divisant entre elles les équations de (5.4),

$$\theta_1 = \frac{u + v\theta_2}{s + t\theta_2} = \frac{(u + v\theta_2)(s + t\overline{\theta_2})}{|s + t\theta_2|^2} = \frac{1}{|s + t\theta_2|^2}\,(us + vt|\theta_2|^2 + sv\theta_2 + ut\overline{\theta_2}). \tag{5.6}$$

donc

$$\Im(\theta_1) = \frac{sv - ut}{|s + t\theta_2|^2}\,\Im(\theta_2).$$

Or $\Im(\theta_1) > 0$ et $\Im(\theta_2) > 0$, donc $sv - ut = 1$.

Montrons maintenant que les formes quadratiques $R_{\mathfrak{a}_1} = (a_1, b_1, c_1)$ et $R_{\mathfrak{a}_2} = (a_2, b_2, c_2)$ sont équivalentes. La substitution $X = sx + uy$ et $Y = tx + vy$ conduit à

$$\begin{array}{rcl} a_2X^2 + b_2XY + c_2Y^2 & = & a_2(X + \theta_2 Y)(X + \overline{\theta_2}Y) \\ & = & a_2[(s + t\theta_2)x + (u + v\theta_2)y][(s + t\overline{\theta_2})x + (u + v\overline{\theta_2})y]. \end{array}$$

Mais d'après la première égalité de (5.6), on a $u + v\theta_2 = \theta_1(s + t\theta_2)$, et en conjuguant $u + v\overline{\theta_2} = \theta_1(s + t\overline{\theta_2})$, donc en remplaçant,

$$a_2X^2 + b_2XY + c_2Y^2 = a_2|s + t\theta_2|^2(x + \theta_1 y)(x + \overline{\theta_1}y)$$

Or d'après (5.3) et la définition de la norme,

$$a_2X^2 + b_2XY + c_2Y^2 = \frac{\mathrm{N}_{K/\mathbb{Q}}(\alpha_2)}{\mathrm{N}_K(\mathfrak{a}_2)}\mathrm{N}_{K/\mathbb{Q}}(s + t\theta_2)(x + \theta_1 y)(x + \overline{\theta_1}y).$$

En prenant la norme par rapport à K dans la première ligne de 5.4,

$$\mathrm{N}_{K/\mathbb{Q}}(\gamma_1)\mathrm{N}_{K/\mathbb{Q}}(\alpha_1) = \mathrm{N}_{K/\mathbb{Q}}(\gamma_2)\mathrm{N}_{K/\mathbb{Q}}(\alpha_2)\mathrm{N}_{K/\mathbb{Q}}(s + t\theta_2)$$

donc

$$a_2X^2 + b_2XY + c_2Y^2 = \frac{\mathrm{N}_{K/\mathbb{Q}}(\gamma_1)\mathrm{N}_{K/\mathbb{Q}}(\alpha_1)}{\mathrm{N}_{K/\mathbb{Q}}(\gamma_2)\mathrm{N}_K(\mathfrak{a}_2)}(x + \theta_1 y)(x + \overline{\theta_1}y).$$

Prenons la norme de l'égalité $\gamma_1\mathfrak{a}_1 = \gamma_2\mathfrak{a}_2$ et remplaçons ; on obtient

$$a_2X^2 + b_2XY + c_2Y^2 = \frac{\mathrm{N}_{K/\mathbb{Q}}(\alpha_1)}{\mathrm{N}_K(\mathfrak{a}_1)}(x + \theta_1 y)(x + \overline{\theta_1}y).$$

D'où enfin, par définition

$$a_2X^2 + b_2XY + c_2Y^2 = a_1(x + \theta_1 y)(x + \overline{\theta_1}y) = a_1x^2 + b_1xy + c_1y^2.$$

ce qui montre que les formes quadratiques $R_{\mathfrak{a}_1}$ et $R_{\mathfrak{a}_2}$ sont équivalentes et prouve le lemme. ∎

Preuve (du théorème 5.21). — Il suffit de montrer que Ψ est une bijection.

(i) **Surjectivité de Ψ.** Soit $R(x,y) = ax^2 + bxy + c$ une forme quadratique définie positive de discriminant D_K. Posons $\theta = \dfrac{b + \sqrt{\mathrm{D}_K}}{2a}$ de sorte que $R(x,y) = a(x+\theta y)(x+\overline{\theta}y)$. On a $\theta \in K$ et $\theta \in \mathcal{O}_K$ car $a\theta^2 + b\theta + c \Longrightarrow (a\theta)^2 + b(a\theta) + ca = 0$. Ainsi $\mathfrak{a} = a\mathbb{Z} + \theta a\mathbb{Z}$ est un idéal de $\mathcal{O}_K$. Son discriminant vaut

$$\mathrm{D}_{\mathfrak{a}} = \begin{vmatrix} a & a \\ \theta a & \overline{\theta} a \end{vmatrix}^2 = a^4(\overline{\theta} - \theta)^2 = a^2 \mathrm{D}_K.$$

On en déduit $\mathrm{N}_K(\mathfrak{a}) = a$ puisque $a > 0$. La forme quadratique $Q_{\mathfrak{a}}$ associée à $\mathfrak{a}$ est donc

$$Q_{\mathfrak{a}}(x,y) = (ax + a\theta y)(ax + a\overline{\theta}y) = aR(x,y),$$

d'où $R(x,y) = \dfrac{Q_{\mathfrak{a}}(x,y)}{\mathrm{N}_K(\mathfrak{a})} = R_{\mathfrak{a}}(x,y)$, et Ψ est surjective.

(ii) **Injectivité de Ψ.** Soit $\mathfrak{a}_1$ et $\mathfrak{a}_2$ deux idéaux tels que $R_{\mathfrak{a}_1} = R_{\mathfrak{a}_2}$ et montrons que $\mathfrak{a}_1 \sim \mathfrak{a}_2$. Soit $(\alpha_1, \theta_1\alpha_1)$ et $(\alpha_2, \theta_2\alpha_2)$ des bases respectives de $\mathfrak{a}_1$ et $\mathfrak{a}_2$ comme dans le lemme 5.22 de sorte que $R_{\mathfrak{a}_1}(x,y) = a_1x^2 + b_1xy + c_1y^2 = a_1(x+\theta_1 y)(x+\overline{\theta_1}y)$ et $R_{\mathfrak{a}_2}(X,Y) = a_2(X+\theta_1 Y)(X+\overline{\theta_1}Y)$ soient équivalentes. Il existe donc $s,t,u,v \in \mathbb{Z}$ avec $sv - ut = 1$ et tels que la substitution $X = sx + uy, Y = tx + vy$ transforme $R_{\mathfrak{a}_2}$ en $R_{\mathfrak{a}_1}$. Il vient

$$\begin{aligned} R_{\mathfrak{a}_2}(sx+uy, tx+vy) &= a_2[(s+t\theta_2)x + (u+v\theta_2)y][(s+t\overline{\theta_2})x + (u+v\overline{\theta_2})y] \\ &= a_2 N_{K/\mathbb{Q}}(s+t\theta_2)\left(x + \frac{u+v\theta_2}{s+t\theta_2}\,y\right)\left(x + \frac{u+v\overline{\theta_2}}{s+t\overline{\theta_2}y}\right) = a_1(x+\theta_1 y)(x+\overline{\theta_1}y). \end{aligned}$$

D'où en identifiant

$$\theta_1 = \frac{u+v\theta_2}{s+t\theta_2} \tag{5.7}$$

A priori on pourrait avoir $\theta_1 = \dfrac{u+v\overline{\theta_2}}{s+t\overline{\theta_2}}$, mais ceci est impossible car $\Im(\theta_1) > 0$, $\Im(\theta_2) > 0$ et $sv - ut = 1$.
Choisissons $\gamma_1, \gamma_2 \in \mathcal{O}_K$ de façon à satisfaire la première équation de (5.4), par exemple $\gamma_1 = \alpha_2(s+t\theta_2)$ et $\gamma_2 = \alpha_1$. On a donc $\gamma_1\alpha_1 = \gamma_2(s\alpha_2 + t\theta_2\alpha_2)$ et par (5.7),

$$\theta_1\gamma_1\alpha_1 = \theta_1\gamma_2\alpha_2(s+t\theta_2) = \gamma_2\alpha_2(u+v\theta_2)$$

donc la deuxième équation de (5.4) est satisfaite, donc le système (5.4) est satisfait pour ces valeurs γ_1, γ_2 ; ceci exprime que $\gamma_1\mathfrak{a}_1 \subset \gamma_2\mathfrak{a}_2$. Or ce système s'inverse en (5.5) avec $s', t', u', v' \in \mathbb{Z}$ car $sv - ut = 1$. On a donc aussi $\gamma_1\mathfrak{a}_1 \supset \gamma_2\mathfrak{a}_2$, et finalement $\mathfrak{a}_1 \sim \mathfrak{a}_2$. ∎

5.24 Exemple. — Prenons $K = \mathbb{Q}(\sqrt{-5})$. Le discriminant du corps vaut -20, donc d'après l'exemple 5.18, le groupe $\mathcal{C}_K$ est de cardinal 2, ce que l'on savait déjà par l'exemple 4.24.

5.25 Exemple. — Prenons $K = \mathbb{Q}(\sqrt{-163})$. Le discriminant du corps vaut -163, donc d'après l'exemple 5.19, le groupe $\mathcal{C}_K$ est de cardinal 1, c'est-à-dire que $\mathcal{O}_K$ est principal. D'après le théorème de Stark, qui est loin d'être trivial, -163 est la plus petite valeur d telle que $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ est principal.

Pour terminer cette section sur le calcul du nombre de classes d'un corps quadratique imaginaire, voici un théorème dont la démonstration est loin d'être triviale, voir [Rib01]. On note Q^+ le nombre de résidus quadratiques mod (p) appartenant à l'intervalle $\left[1, \dfrac{p-1}{2}\right]$ et Q^- le nombre de non-résidus quadratiques mod (p) du même intervalle.

5.26 Théorème. — *Soit $p \neq -3$ un nombre premier négatif avec $p \equiv 1 \bmod (4)$ et soit $K = \mathbb{Q}(\sqrt{d})$. Si $p \equiv 1 \bmod (8)$, alors $h_K = Q^+ - Q^-$ et si $p \equiv 5 \bmod (8)$, alors $h_K = \dfrac{Q^+ - Q^-}{3}$.*

5.27 Exemple. — Prenons $K = \mathbb{Q}(\sqrt{-23})$. Les résidus quadratiques modulo 23 appartenant à l'intervalle $[1, 11]$ sont $1, 2, 3, 4, 6, 8$ et 9, tandis que $5, 7, 10$ et 11 sont non-résidus quadratiques. Ainsi $h_K = 7 - 4 = 3$.

5.4 Corps quadratiques imaginaires principaux

La recherche des corps quadratiques imaginaires principaux a occupé de nombreux mathématiciens. La réponse complète fut apportée en 1967 par Stark. Nous démontrons une version très affaiblie de ce théorème.

5.28 Lemme. — *Soit $d \leqslant -15$ un entier sans facteurs carrés, $d \equiv 1 \bmod (4)$ et $K = \mathbb{Q}(\sqrt{d})$. Alors $\mathcal{O}_K$ est principal si et seulement si tout nombre premier $p \leqslant \mu_K$ est inerte dans K.*

Preuve. — Soit $\mathfrak{a}$ un idéal de $\mathcal{O}_K$. Il existe un idéal premier $\mathfrak{p}$ tel que $\mathfrak{p} \sim \mathfrak{a}$ et $\mathrm{N}_K(\mathfrak{p}) \leqslant \mu_K$. Pour un nombre premier $p \leqslant \lambda$, l'idéal $\mathfrak{p}$ est au-dessus de (p). Comme p est inerte, $p\mathcal{O}_K$ est principal, donc $\mathfrak{p}$, puis $\mathfrak{a}$ aussi. Ainsi tout idéal de $\mathcal{O}_K$ est principal.

Réciproquement supposons que l'un des nombres premiers $p \leqslant \mu_K$ ne soit pas inerte. D'après le théorème 3.26 et la proposition 3.30, $p\mathcal{O}_K$ admet un facteur premier de la forme $(p, \alpha + \beta)$ avec $\beta \in \mathbb{Z}$. Comme $\mu_K = \dfrac{2}{\pi}\sqrt{-d} < \sqrt{-d}$, on a $p^2 \leqslant -d$ et donc le lemme 3.32 s'applique et montre que cet idéal n'est pas principal. ∎

5.29 Proposition. — *Soit $d < 0$ un entier sans facteurs carrés et $K = \mathbb{Q}(\sqrt{d})$. Si l'anneau $\mathcal{O}_K$ est principal, alors $d = -1, -2, -7$ ou $d \equiv 5 \bmod (8)$ et d est premier.*

Preuve. — (i) Supposons $d \equiv 2, 3 \bmod (4)$. D'après la proposition 3.30, l'idéal $2\mathcal{O}_K$ se factorise en idéaux premiers $2\mathcal{O}_K = \mathfrak{p}^2$ avec $\mathfrak{p} = (2, \alpha)$ ou $\mathfrak{p} = (2, \alpha + 1)$, avec $\alpha = \sqrt{d}$. On a $\mathrm{N}_K(\mathfrak{p}) = 2$ et si $\gamma = x + y\alpha$, $x, y \in \mathbb{Z}$ engendre $\mathfrak{p}$, sa norme vaut aussi 2. Or dans $\mathcal{O}_K$,

$$\mathrm{N}_{K/\mathbb{Q}}(\gamma) = \mathrm{N}_{K/\mathbb{Q}}(x + y\alpha) = x^2 - dy^2.$$

Cette équation en nombres entiers n'a de solutions non nulles que si $d = -1$ ou -2.

(ii) Supposons $d \equiv 1 \bmod (8)$ et posons $\alpha = \dfrac{1 + \sqrt{d}}{2}$. L'idéal $2\mathcal{O}_K$ se factorise en $2\mathcal{O}_K = (2, \alpha)(2, \alpha + 1)$. Posons $\mathfrak{p} = (2, \alpha)$. Cet idéal est premier et $\mathrm{N}_K(\mathfrak{p}) = 2$. Si $\gamma = x + y\alpha$, $x, y \in \mathbb{Z}$ engendre $\mathfrak{p}$, sa norme vaut aussi 2. On a

$$\mathrm{N}_{K/\mathbb{Q}}(\gamma) = \mathrm{N}_{K/\mathbb{Q}}(x + y\alpha) = \left(x + \frac{y}{2}\right)^2 + y^2\frac{|d|}{4} \geqslant \frac{1}{4} + \frac{|d|}{4} \quad \text{si } y \neq 0.$$

Pour $d \leqslant -8$, on a $\mathrm{N}_{K/\mathbb{Q}}(\gamma) > 2$. Si $y = 0$, c'est que $\gamma \in \mathbb{Z}$; or $\alpha \in \mathfrak{p}$ donc il existe $x, y \in \mathbb{Z}$ tels que $\gamma(x + y\alpha) = \alpha$, d'où $\gamma = \pm 1$, ce qui est impossible car $\mathfrak{p}$ est premier. Ainsi dans ce cas, la seule valeur possible est $d = -7$.

(*iii*) Supposons maintenant $d \equiv 5 \bmod (8)$. Si $d \leqslant -15$ et d non premier, écrivons $-d = qr$ avec $q \geqslant 3$ le plus petit facteur premier de $-d$. Puisque q divise d, la proposition 3.30 montre que q se ramifie sur K. Comme $q^2 \leqslant -d$, le lemme 3.32 montre que $\mathcal{O}_K$ n'est pas principal. Si $d > -15$, c'est que $d = -3$ ou $d = -11$, et ces deux nombres sont bien premiers. ∎

Il est facile de vérifier que pour $d = -163, -67, -43, -19, -11, -7, -3, -2$ et -1 l'anneau $\mathcal{O}_K$ est principal, c'est ce que nous allons faire ci-dessous. En 1934, Heilbronn et Linfoot démontrèrent qu'il n'existe qu'au plus une autre valeur de d telle que $\mathcal{O}_K$ est principal, et en 1966 Stark prouve que si cette valeur de d existe, elle vérifie $d > -\exp(2,2 \times 10^7)$. L'année suivante, il publie un article de 28 pages montrant que cette valeur n'existe pas ([Sta67]) et prouve ainsi le théorème suivant.

5.30 Théorème (Stark, 1967). — *L'anneau des entiers de $\mathbb{Q}(\sqrt{d})$ avec $d < 0$ est principal si, et seulement si, $d = -163, -67, -43, -19, -11, -7, -3, -2$ ou -1.*

La démonstration de ce théorème utilise les formes binaires quadratiques introduites précédemment. Elle consiste par des méthodes analytiques à montrer que $d \geqslant -200$. Il reste alors à vérifier à la main que les seules valeurs de d qui font de $\mathcal{O}_K$ un anneau principal sont celles annoncées, c'est l'objet de la proposition suivante.

5.31 Proposition. — *Soit $K = \mathbb{Q}(\sqrt{d})$ avec $-200 \leqslant d \leqslant -1$ et d sans facteurs carrés. Alors $\mathcal{O}_K$ est principal si et seulement si $d = -163, -67, -43, -19, -11, -7, -3, -2$ ou -1.*

Preuve. — Par la proposition 5.29, si $\mathcal{O}_K$ est principal, nécessairement $d = -1$, -2 -7 ou ($d \equiv 5 \bmod (8)$ et d premier).

On note μ_d pour $\mu_{\mathbb{Q}(\sqrt{-d})}$. On a $\mu_1 \approx 1,27$, $\mu_2 \approx 1,80$ et $\mu_7 \approx 1,68$ donc les valeurs $-1, -2, -7$ de d conviennent.

Les valeurs restantes de d vérifient $d \equiv 5 \bmod (8)$, donc d'après la proposition 3.30, on sait déjà que 2 est inerte. De plus $\mu_d = \dfrac{2}{\pi}\sqrt{-d}$, d'où les calculs suivants

$$(i)\ \mu_d < 3 \iff d \geqslant -22, \qquad (ii)\ \mu_d < 5 \iff d \geqslant -61,$$
$$(iii)\ \mu_d < 7 \iff d \geqslant -120, \qquad (iv)\ \mu_d < 9 \iff d \geqslant -199.$$

(*i*) Les valeurs $d = -3, -11, -19$ conviennent car $\mu_d < 3$.

Supposons maintenant $d \leqslant -22$. D'après le lemme 5.28, il est nécessaire que 3 soit inerte dans K, c'est-à-dire que d soit un non-résidu quadratique modulo 3. Il en résulte $d \equiv 2 \bmod (3)$, d'où $d \equiv 5 \bmod (24)$. Ainsi $d = -43, -67, -139$ ou -163. D'où la discussion qui suit selon les trois cas restants et en utilisant le symbole de Legendre.

(*ii*) La valeur $d = -43$ convient car $\mu_{43} < 5$.

(*iii*) $\left(\dfrac{-67}{5}\right) = \left(\dfrac{3}{5}\right) = -1$, donc $d = -67$ convient.

(*iv*) On a $\left(\dfrac{-163}{3}\right) = \left(\dfrac{2}{3}\right) = -1$, $\left(\dfrac{-163}{5}\right) = \left(\dfrac{2}{5}\right) = -1$ et $\left(\dfrac{-163}{7}\right) = \left(\dfrac{5}{7}\right) = -1$, donc $\mathcal{O}_K$ est principal pour $d = -163$.

Pour $d = -139$, on a $\left(\dfrac{-139}{5}\right) = \left(\dfrac{1}{5}\right) = 1$ et 5 n'est pas inerte. Donc le lemme 5.28 montre que $\mathcal{O}_K$ n'est pas principal. On pouvait aussi constater que $x^2 + xy + 35y^2$ et $5x^2 + xy + 7y^2$ sont deux formes quadratiques réduites de discriminant -139 non équivalentes. ∎

5.5 Application aux équations diophantiennes

Un des intérêts de la factorialité des anneaux d'entiers (ce qui est équivalent à être principal dans ce cas) est la résolution d'équation diophantiennes. Voyons d'abord deux lemmes très simples.

5.32 Lemme. — *Soit K un corps de nombres et m un entier premier avec h_K. Si $\mathfrak{a}$ est un idéal de $\mathcal{O}_K$ et si $\mathfrak{a}^m$ est principal, alors $\mathfrak{a}$ est principal.*

Preuve. — Par hypothèse dans $\mathcal{C}_K$, on a $\mathfrak{a}^m \sim \mathcal{O}_K$. Puisque h_K est l'ordre de $\mathcal{C}_K$, on a aussi $\mathfrak{a}^{h_K} \sim \mathcal{O}_K$. Par le théorème de Bezout, il existe des entiers r et s tels que $mr + h_K s = 1$. Donc

$$\mathfrak{a} = \mathfrak{a}^{mr+h_K s} \sim (\mathfrak{a}^m)^r (\mathfrak{a}^{h_K})^s \sim \mathcal{O}_K^r \mathcal{O}_K^s \sim \mathcal{O}_K$$

et $\mathfrak{a}$ est principal. ∎

5.33 Définition (Idéaux étrangers). — *Soit $\mathfrak{a}_1$ et $\mathfrak{a}_2$ deux idéaux de $\mathcal{O}_K$. On dit que ces idéaux sont étrangers si $\mathfrak{a}_1 + \mathfrak{a}_2 = \mathcal{O}_K$.*

Si $\mathfrak{a}_1$ et $\mathfrak{a}_2$ sont étrangers, il n'y a pas d'idéaux premiers $\mathfrak{p}$ tels que $\mathfrak{a}_1 \subset \mathfrak{p}$ et $\mathfrak{a}_2 \subset \mathfrak{p}$ car sinon $\mathfrak{a}_1 + \mathfrak{a}_2 \subset \mathfrak{p}$, et donc il n'y a pas d'idéaux premiers communs aux factorisations en idéaux premiers de $\mathfrak{a}_1$ et $\mathfrak{a}_2$.

5.34 Lemme. — *Soit K un corps de nombres et $\mathfrak{a}_1, \mathfrak{a}_2$ des idéaux étrangers. Supposons qu'il existe un idéal $\mathfrak{b}$ et un entier m tels que $\mathfrak{a}_1\mathfrak{a}_2 = \mathfrak{b}^m$. Alors il existe deux idéaux $\mathfrak{b}_1$ et $\mathfrak{b}_2$ tels que $\mathfrak{a}_1 = \mathfrak{b}_1^m$ et $\mathfrak{a}_2 = \mathfrak{b}_2^m$.*

Preuve. — Ecrivons les décompositions en produit d'idéaux premiers de $\mathfrak{a}_1$, $\mathfrak{a}_2$ et $\mathfrak{b}$:

$$\mathfrak{a}_1 = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_p^{e_p} \quad \mathfrak{a}_2 = \mathfrak{q}_1^{f_1} \dots \mathfrak{q}_q^{f_q} \quad \text{et} \quad \mathfrak{b} = \mathfrak{r}_1^{g_1} \dots \mathfrak{r}_r^{g_r}$$

Comme $\mathfrak{a}_1$ et $\mathfrak{a}_2$ sont premiers entre eux, on a

$$\mathfrak{a}_1\mathfrak{a}_2 = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_p^{e_p} \mathfrak{p}_1^{f_1} \dots \mathfrak{p}_q^{f_q} = \mathfrak{r}_1^{mg_1} \dots \mathfrak{r}_r^{mg_r}.$$

On déduit que $r = p + q$ et que m divise les e_i et les f_j. Donc $\mathfrak{a}_1$ et $\mathfrak{a}_2$ s'écrivent bien sous forme de puissance m-ième d'un idéal. ∎

5.5.1 Equation de Mordell $y^2 = x^3 + d$

5.35 Théorème. — *Soit $d \leqslant -1$ sans facteurs carrés, avec $d \equiv 2, 3 \bmod (4)$. Supposons que le nombre de classe de $\mathbb{Z}[\sqrt{d}]$ n'est pas divisible par 3. Alors l'équation $y^2 = x^3 + d$ admet des solutions en nombres entiers si et seulement si $d = \pm 1 - 3a^2, a \in \mathbb{N}^*$ et dans ce cas les solutions sont $x = a^2 - d, y = \pm a(a^2 + 3d)$.*

Preuve. — Remarquons d'abord que x et y sont premiers entre eux ; en effet si p divise x et y, alors p^2 divise d, ce qui est contraire à l'hypothèse. De plus x est impair car sinon on aurait $y^2 \equiv d \bmod (4)$, alors que les seuls carrés modulo 4 sont 0 et 1.
Ecrivons l'équation sous la forme $(y + \sqrt{d})(y - \sqrt{d}) = x^3$ et passons aux idéaux dans $\mathcal{O}_K$ (pour alléger l'écriture, on notera $\langle \alpha \rangle$ l'idéal engendré par α dans $\mathcal{O}_K$ et non $\alpha\mathcal{O}_K$),

$$\langle y + \sqrt{d} \rangle \langle y - \sqrt{d} \rangle = \langle x \rangle^3.$$

Soit $\mathfrak{p}$ un idéal premier divisant $\langle y+\sqrt{d}\rangle$ et $\langle y-\sqrt{d}\rangle$. Alors $y+\sqrt{d}\in\mathfrak{p}$ et $y-\sqrt{d}\in\mathfrak{p}$, d'où $2y\in\mathfrak{p}$, donc $\mathfrak{p}|\langle 2y\rangle$ et également $\mathfrak{p}|\langle x\rangle$ car il intervient dans la factorisation en idéaux premiers de $\langle x\rangle^3$. En prenant les normes, il vient que $\mathrm{N}(\mathfrak{p})|\mathrm{N}(\langle 2y\rangle)=4y^2$ et $\mathrm{N}(\mathfrak{p})|\mathrm{N}(\langle x\rangle)=x^2$. Puisque x est impair, $\mathrm{N}(\mathfrak{p})$ est impair, donc $\mathrm{N}(\mathfrak{p})|y^2$. Or $\mathrm{N}(\mathfrak{p})\neq 1$ car $\mathfrak{p}$ est premier, donc x et y ont un facteur en commun, contradiction. Ainsi $\langle y+\sqrt{d}\rangle$ et $\langle y-\sqrt{d}\rangle$ sont étrangers et d'après le lemme 5.34, il existe un idéal $\mathfrak{a}$ de $\mathcal{O}_K$ tel que

$$\langle y+\sqrt{d}\rangle=\mathfrak{a}^3.$$

Comme $\mathfrak{a}^3$ est principal et que 3 ne divise pas h_K, le lemme 5.32 montre que $\mathfrak{a}$ est principal. Comme $d\equiv 2,3 \bmod 4$, on a $\mathcal{O}_K=\mathbb{Z}[\sqrt{d}]$ et donc il existe donc $a,b\in\mathbb{Z}$ tel que $\mathfrak{a}=\langle a+b\sqrt{d}\rangle$ d'où $\langle y+\sqrt{d}\rangle=\langle a+b\sqrt{d}\rangle^3$. Il existe donc une unité ε de $\mathcal{O}_K$ telle que

$$y+\sqrt{d}=\varepsilon(a+b\sqrt{k})^3.$$

Or les seules unités de $\mathcal{O}_K$ sont ± 1 (proposition 1.54). Comme $(1,\sqrt{d})$ forme une base de $\mathcal{O}_K$, il vient

$$y=\pm a(a^2+3db^2)\quad\text{et}\quad 1=\pm b(3a^2+db^2).$$

De la deuxième équation, on tire $b=\pm 1$ et $d=\pm 1-3a^2$. D'où $y=\pm a(a^2+3d)$ et en reportant dans l'équation $y^2=x^3+d$ de départ

$$x^3=a^6+6a^4d+9a^2d^2-d.$$

Or $(d+3a^2)^2=1$, donc $d=d^3+6a^2d^2+9a^4d$ et en reportant

$$x^3=a^6-3a^4d+3a^2d^2-d^3.$$

D'où $x=a^2-d$. ∎

5.5.2 L'équation de Fermat $x^3+y^3=z^3$

C'est en 1994 que Andrew Wiles parvint à montrer que l'équation de Fermat $x^n+y^n=z^n$ n'a pas de solutions entières non triviales pour $n\geqslant 3$. Les solutions de l'équation dans le cas $n=2$ étaient connues depuis fort longtemps sous le nom de triplets pythagoriciens. Kummer avait réussi à démontrer ce résultat pour certaines valeurs de n. On trouvera dans [Duv98] le cas $n=5$. Outre la factorialité de l'anneau des entiers de $\mathbb{Q}(\xi_5)$, la démonstration utilise la connaissance de ses unités. Dans le cas $n=3$ que nous présentons ici, la question des unités est plus simple.

5.36 Lemme. — *Tout élément de l'anneau $\mathbb{Z}[\omega]$ des entiers de $\mathbb{Q}(\sqrt{-3})$ peut être associé à un élément de $\mathbb{Z}[\sqrt{-3}]$, c'est-à-dire que pour tout $x\in\mathbb{Z}[\omega]$, il existe $\varepsilon\in\mathbb{Z}[\omega]^\times$ tel que $\varepsilon x\in\mathbb{Z}[\sqrt{-3}]$.*

Preuve. — Soit $x=\dfrac{\alpha+\beta\sqrt{-3}}{2}\in\mathbb{Z}[\omega]$ avec $\alpha,\beta\in\mathbb{Z}$. Si α,β sont pairs, il n'y a rien à montrer car $x\in\mathbb{Z}[\sqrt{-3}]$. Supposons α et β impairs et envisageons quatre cas.

(*i*) $\alpha\equiv 1 \bmod (4)$ et $\beta\equiv 1 \bmod (4)$. On a

$$x\omega^2=\frac{\alpha+\beta\sqrt{-3}}{2}\times\frac{-1+\sqrt{-3}}{2}=\frac{-\alpha-3\beta+(\alpha-\beta)\sqrt{-3}}{4}\in\mathbb{Z}[\sqrt{-3}]$$

(*ii*) $\alpha\equiv 1 \bmod (4)$ et $\beta\equiv -1 \bmod (4)$. On a

$$x\omega=\frac{\alpha+\beta\sqrt{-3}}{2}\times\frac{1+\sqrt{-3}}{2}=\frac{\alpha-3\beta+(\alpha+\beta)\sqrt{-3}}{4}\in\mathbb{Z}[\sqrt{-3}]$$

(*iii*) $\alpha \equiv -1 \bmod (4)$ et $\beta \equiv 1 \bmod (4)$. On a

$$x\omega^4 = \frac{\alpha+\beta\sqrt{-3}}{2} \times \frac{-1-\sqrt{-3}}{2} = \frac{3\beta-\alpha-(\alpha+\beta)\sqrt{-3}}{4} \in \mathbb{Z}[\sqrt{-3}]$$

(*vi*) $\alpha \equiv -1 \bmod (4)$ et $\beta \equiv -1 \bmod (4)$. On a

$$x\omega^5 = \frac{\alpha+\beta\sqrt{-3}}{2} \times \frac{1-\sqrt{-3}}{2} = \frac{\alpha+3\beta+(\beta-\alpha)\sqrt{-3}}{4} \in \mathbb{Z}[\sqrt{-3}]$$

5.37 Théorème. — *L'équation $x^3+y^3=z^3$ n'a pas de solutions en entiers relatifs x, y, z non nuls.*

Preuve. — Soit x, y, z des entiers relatifs avec $x^3+y^3+z^3=0$ et $(x,y,z) \neq (0,0,0)$. On peut supposer x, y, z premiers entre eux quitte à simplifier par leur PGCD. Les entiers x, y, z ne sont donc pas tous les trois pairs. Il est impossible que tous les trois soient impairs ou que deux d'entre eux soient pairs et le troisième soit impair (la somme serait impaire), donc quitte les permuter, on peut supposer x, z impairs et y pair. Choisissons une solution telle que $|y|$ soit minimal, et posons $x=a+b$ et $z=a-b$; alors a et b sont premiers entre eux (sinon x et z, donc x, y et z auraient un diviseur commun) et de parité différente (car x et z sont impairs). Il vient

$$2a(a^2+3b^2) = -y^3.$$

Puisque a et b sont de parités différentes, a^2+3b^2 est impair et comme y est pair, c'est que 8 divise $2a$ et tout diviseur commun à $2a$ et a^2+3b^2 est impair, donc divise a, donc divise $3b^2$. Comme a et b sont premiers entre eux, il en résulte $\mathrm{PGCD}(2a, a^2+3b^2) = 1$ ou 3. Envisageons les deux cas.

(*i*) $\mathrm{PGCD}(2a, a^2+3b^2) = 1$. De $2a(a^2+3b^2) = -y^3$, on en déduit qu'il existe $r, s \in \mathbb{Z}$ tels que $2a = r^3$ et $a^2+3b^2 = s^3$, avec s impair. On factorise dans l'anneau factoriel $\mathcal{O}_K$ des entiers de $K = \mathbb{Q}(\sqrt{-3})$. Il vient

$$(a+b\sqrt{-3})(a-b\sqrt{-3}) = s^3.$$

Soit p qui divise $a+b\sqrt{-3}$ et $a-b\sqrt{-3}$, il divise leur somme $2a$ et leur différence $2ib\sqrt{3}$. En prenant les normes $\mathrm{N}_{K/\mathbb{Q}}(p)|4a^2$ et $\mathrm{N}_{K/\mathbb{Q}}(p)|12b^2$. Or $\mathrm{N}_{K/\mathbb{Q}}(p)$ est impair car il divise a^2+3b^2, donc $\mathrm{N}_{K/\mathbb{Q}}(p)|a^2$ et $\mathrm{N}_{K/\mathbb{Q}}(p)|a^2+3b^2$, d'où $\mathrm{N}_{K/\mathbb{Q}}(p) = 1$ et $p \in A^\times$ car a et a^2+3b^2 sont premiers entre eux. Ainsi les idéaux $\langle a+b\sqrt{-3}\rangle$ et $\langle a+b\sqrt{-3}\rangle$ sont premiers entre eux et d'après le lemme 5.34, il existe $\langle t'\rangle$ tel que $\langle a+b\sqrt{-3}\rangle = \langle t'\rangle^3$, d'où l'existence de $\epsilon \in \mathcal{O}_K^\times$ tel que $a+b\sqrt{-3} = \epsilon t$. Mais toutes les unités de $\mathcal{O}_K$ sont des cubes (propositon 1.54), donc on peut écrire $a+b\sqrt{-3} = t^3$ avec $t \in \mathcal{O}_K$.

D'après le lemme 5.36, il existe $\varepsilon \in \mathcal{O}_K$ tel que $\varepsilon t \in \mathbb{Z}[\sqrt{-3}]$. Puisque ε est une racine sixième de l'unité de $\mathbb{C}$, on a $\varepsilon^{-3} = \pm 1$, donc $a+b\sqrt{-3} = \varepsilon^{-3}(\varepsilon t)^3 = (\pm\varepsilon t)^3$. Par suite il existe $u, v \in \mathbb{Z}$ tels que $a+b\sqrt{-3} = (u+v\sqrt{-3})^3$, et en développant

$$a = u(u+3v)(u-3v) \quad \text{et} \quad b = 3v(u-v)(u+v).$$

Comme b est impair, $v, u-v$ et $u+v$ sont impairs, donc u est pair. Comme a et b sont premiers entre eux, u et $3v$ le sont aussi, donc également $2u$ et $3v$ puisque $3v$ est impair. Puisque $2a = r^3$, il vient

$$r^3 = 2u(u+3v)(u-3v).$$

Comme $2u, u+3v$ et $u-3v$ sont premiers entre eux deux à deux, il existe $l, m, n \in \mathbb{Z}$ tels que $2u = l^3$, $u+3v = m^3$ et $u-3v = n^3$. Par addition, $m^3 + n^3 = l^3$ avec l pair et l, m, n premiers entre eux. De plus

$$|y^3| = |2a(a^2+3b^2)| = |l^3(u^2-9v^2)(a^2+3b^2)| \geqslant 3|l^2| > |l^3|$$

donc $0 < |l| < |y|$, ce qui contredit la minimalité de $|y|$.

(ii) PGCD$(2a, a^2+3b^2) = 3$. Posons $a = 3c$. On a que b et c sont de parités différentes et premiers entre eux. L'équation $2a(a^2+3b^2) = -y^3$ s'écrit

$$18c(3c^2+b^2) = -y^3.$$

Soit d un diviseur premier de $18c$ et $3c^2+b^2$. On a $d \neq 2$ car b et c sont de parités différentes ; on a aussi $d \neq 3$ car 3 ne divise pas b sinon 3 diviserait a et b. Enfin si $d|c$, on a $d|b$ donc $d = 1$. Ceci prouve que $18c$ et $3c^2+b^2$ sont premiers entre eux, donc par unicité de la factorisation dans $\mathbb{Z}$, on a $18c = r^3$ et $3c^2+b^2 = s^3$ avec s impair.

En procédant comme dans (i), on obtient

$$b = u(u+3v)(u-3v) \quad \text{et} \quad c = 3v(u-v)(u+v)$$

avec u impair, v pair, u et v premiers entre eux. Puisque $18c = r^3$, il vient $r^3 = 54v(u-v)(u+v)$ et r étant un multiple de 3, en écrivant $r = 3r'$, on a $r'^3 = 2v(u-v)(u+v)$. Les nombres $2v, u-v, u+v$ sont premiers entre eux deux à deux, donc il exitste $l, m, n \in \mathbb{Z}$ tels que $l^2 = 2v, m^3 = u-v$, $n^3 = u+v$ d'où en ajoutant $l^3+m^3+(-n)^3 = 0$ avec l pair. Enfin

$$|y^3| = |18c(3c^2+b^2)| = |27l^3(u^2-v^2)(3c^2+b^2)| \geqslant 27|l^3| > |l^3|,$$

ce qui contredit encore la minimalité de $|y|$. ∎

Chapitre 6

Anneaux d'entiers euclidiens

6.1 Généralités

Rappelons la définition d'un anneau euclidien.

6.1 Définition. — *Un anneau intègre A est dit euclidien s'il existe une application (appelée stathme) $\Psi : A \longrightarrow \mathbb{N}$ telle que si $a, b \in A$, avec $b \neq 0$, il existe $q, r \in A$ tel que $a = bq + r$ avec $\Psi(r) < \Psi(b)$.*

On montre facilement qu'un anneau euclidien est principal. Etant donné un anneau euclidien et un stathme Ψ, il est intéressant de construire un stathme vérifiant des conditions plus fortes.

6.2 Proposition. — *Soit A un anneau euclidien. Il existe un stathme φ satisfaisant les propriétés suivantes.*

(i) 0 est l'unique élément où φ s'annule ;

(ii) pour x, y non nuls de A, on a $\varphi(x) \leqslant \varphi(xy)$ avec égalité si et seulement si y est inversible ;

(iii) x est inversible si et seulement si $\varphi(x) = 1$.

Preuve. — (i) Soit Ψ un stathme. Pour $b \neq 0$, on écrit $1 = bq + r$ avec $\Psi(r) < \Psi(b)$, et Ψ n'est pas minimal en b. Donc 0 est le seul élément en lequel Ψ est minimal. En remplaçant Ψ par $\Psi_1 = \Psi - \Psi(0)$, le stathme Ψ_1 s'annule en 0 et seulement en 0.

(ii) Pour tout a, on pose $\Psi_2(a) = \inf\{\Psi_1(a\xi),\, \xi \neq 0\}$. Clairement $\Psi_2 \leqslant \Psi_1$ et Ψ_2 ne s'annule qu'en 0. Montrons qu'il existe une division euclidienne pour Ψ_2. Soit a et $b \neq 0$. Il existe x tel que $\Psi_2(b) = \Psi_1(bx)$. Faisons la division euclidienne de a par bx pour Ψ_1 :

$$a = bxq + r \quad \text{avec} \quad \Psi_1(r) < \Psi_2(bx).$$

Alors $\Psi_2(r) \leqslant \Psi_1(r) < \Psi_1(bx) = \Psi_2(b)$, donc r est le reste d'une division euclidienne de a par b pour Ψ_2 qui est donc bien un stathme euclidien.
Pour x, y non nuls de A, on a

$$\Psi_2(xy) = \inf_{\xi \neq 0} \Psi_1(xy\xi) \geqslant \inf_{\eta \neq 0} \Psi_1(x\eta) = \Psi_2(x).$$

Supposons $\Psi_2(xy) = \Psi_2(x)$. En faisant la division de x par xy pour Ψ_2, on a $x = xyq + r$ et $\Psi_2(r) < \Psi_2(xy) = \Psi_2(x)$; Si $r \neq 0$, on aurait l'inégalité $\Psi_2(x(1 - yq)) \geqslant \Psi_2(x)$ qui est fausse. Donc $r = 0$, $yq = 1$ et y est inversible.

(iii) Comme 1 divise tout élément nul x de A, on a $\Psi_2(1) \leqslant \Psi_2(x)$, l'égalité ayant lieu si et seulement si 1 et x sont associés, c'est-à-dire si et seulement si x est inversible.

Finalement en posant $\varphi(0) = 0$ et $\varphi(x) = \Psi_2(x) - \Psi_2(1) + 1$ pour $x \neq 0$, ce stathme satisfait les conditions souhaitées. ∎

Voici un lemme qui permet de construire des stathmes sur des anneaux d'entiers.

6.3 Lemme. — *Soit K un corps de nombres φ une application $\mathcal{O}_K \longrightarrow \mathbb{N}$ multiplicative sur $\mathcal{O}_K$, c'est-à-dire vérifiant*

$$\forall z, z' \in \mathcal{O}_K,\ \varphi(zz') = \varphi(z)\varphi(z').$$

Alors l'application φ se prolonge en une fonction multiplicative sur K, et φ est un stathme sur $\mathcal{O}_K$ si et seulement si pour tout $z \in K$, il existe $\gamma \in \mathcal{O}_K$ tel que $\varphi(z-\gamma) < 1$.

Preuve. — Rappelons que le corps des fractions de $\mathcal{O}_K$ est K. Soit $z = \alpha/\beta \in K$ avec $\alpha, \beta \in \mathcal{O}_K$. En posant

$$\varphi(z) = \frac{\varphi(\alpha)}{\varphi(\beta)}\,\varphi(1),$$

on voit que cette définition prolonge de façon multplicative φ à K.

Supposons $\mathcal{O}_K$ euclidien pour φ et soit $z = \alpha/\beta \in K$, avec $\alpha, \beta \in \mathcal{O}_K$. Il existe $q, r \in \mathcal{O}_K$ tels que $\alpha = \beta q + r$ avec $\varphi(r) < \varphi(\beta)$, donc $\varphi\left(\dfrac{\alpha}{\beta} - q\right) = \varphi\left(\dfrac{r}{\beta}\right) < 1$.

Réciproquement, soit $\alpha, \beta \in \mathcal{O}_K$, avec $\beta \neq 0$. Il existe $\gamma \in \mathcal{O}_K$ tel que $\varphi\left(\dfrac{\alpha}{\beta} - \gamma\right) < 1$, d'où avec $r = \alpha - \beta\gamma$, $\varphi(r) < \varphi(\beta)$ et $\mathcal{O}_K$ est euclidien pour φ. ∎

6.2 Corps quadratiques euclidiens

Soit d un entier sans facteur carré et $K = \mathbb{Q}(\sqrt{d})$. On se demande si l'application $z \mapsto |\mathrm{N}_{K/\mathbb{Q}}(z)|$ est un stathme euclidien. Puisqu'elle est multiplicative, le lemme 6.3 se reformule ainsi.

6.4 Lemme. — *L'application $|\mathrm{N}_{K/\mathbb{Q}}|$ est un stathme euclidien sur $\mathcal{O}_K$ si et seulement si pour tout $z \in K$, il existe $\gamma \in \mathcal{O}_K$ tel que $|\mathrm{N}_{K/\mathbb{Q}}(z-\gamma)| < 1$.*

En 1893, Dedekind montre que $\mathbb{Q}(\sqrt{d})$ est euclidien pour la norme pour $d = -1$, -2, -3, -7, -11, 2, 3, 5 et 13. En 1927, Dickson affirme que la liste des corps quadratiques euclidiens pour la norme est complète. Perron, en 1932, constate qu'en réalité l'argument de Dickson n'est valable que pour les corps quadratiques imaginaires. Dans les trente années qui suivent, les corps quadratiques euclidiens pour la norme sont complètement caractérisés ; les valeurs à rajouter à la liste précédente sont

$$d = 6, 7, 11, 17, 19, 21, 29, 33, 37, 41, 57 \text{ et } 73.$$

Cependant il existe des anneaux d'entiers quadratiques qui sont euclidiens pour un stathme différent de la norme. C'est notamment le cas pour $d = 69$ et 14. Ce sont des résultats récents démontré par Clark en 1993 et Harper en 2000 respectivement. Nous en reparlerons dans l'ouverture page 78.

6.2.1 Cas imaginaire

Dans le cas $d < 0$, le fait de disposer d'une interprétation géométrique de la norme permet de trouver très facilement les valeurs de d rendant $\mathcal{O}_K$ euclidien pour la norme.

6.5 Proposition. — *Soit $d < 0$ un entier sans facteurs carrés. Alors*

(i) pour $d \equiv 2, 3 \bmod (4)$, l'anneau est $\mathcal{O}_K$ est euclidien pour la norme si et seulement si $d = -1$ ou $d = -2$;

(ii) pour $d \equiv 1 \bmod (4)$, l'anneau est $\mathcal{O}_K$ est euclidien pour la norme si et seulement si $d = -3, -7$ ou $d = -11$.

Preuve. — Dans les deux cas, il nous faut chercher un des points les plus éloignés d'un point du réseau. Cette distance ne pourra pas excèder 1 d'après le lemme 6.4.
(*i*) Si $d \equiv 2, 3 \bmod (4)$, les mailles du réseaux sont des rectangles de côté 1 et $\sqrt{-d}$. Chaque point de $\mathbb{Q}(\sqrt{d})$ appartient un de ces rectangles, et le point le plus éloigné des sommets est le centre, à distance $\frac{1}{2}\sqrt{1-d}$ des sommets. D'après le lemme, $\mathcal{O}_K$ est euclidien si et seulement si $\frac{1}{2}\sqrt{1-d} < 1$, d'où $d > -3$.
(*ii*) Si $d \equiv 1 \bmod (4)$, les mailles du réseaux sont des losanges dont les diagonales mesurent 1 et $\sqrt{-d}$. Considérons l'un des deux triangles isocèles de base 1 composant ce losange. En traçant les arcs de cercle de rayon 1 centré en les extrémités de la base, on obtient un point m sur la hauteur relative à la base, à distance $\frac{\sqrt{3}}{2}$ de la base. Le point m est à distance 1 des extrémités de la base et à distance $A = \frac{\sqrt{-d}}{2} - \frac{\sqrt{3}}{2}$ du troisième sommet. L'anneau $\mathcal{O}_K$ est euclidien si et seulement si $A < 1$, soit si et seulement si $d > -7 - 4\sqrt{3} \approx -13,92$. ∎

Cependant comme signalé ci-dessus, il se pourrait que $\mathcal{O}_K$ soit euclidien pour un stathme différent de $\mathrm{N}_{K/\mathbb{Q}}$. Dans le cas $d < 0$, il n'en est rien, c'est-à-dire que $\mathcal{O}_K$ est euclidien si et seulement s'il est euclidien pour la norme. Pour cela il faut dégager des propriétés intrinsèques aux anneaux euclidiens, c'est l'objet du lemme suivant.

6.6 Lemme. — *Soit A un anneau euclidien de stathme φ. Il existe des éléments premiers p tel que le morphisme de groupe multiplicatif $A^\times \to (A/(p))^\times$ induit par la surjection canonique $A \twoheadrightarrow A/(p)$ soit surjectif.*

Preuve. — Soit φ un stathme euclidien vérifiant les conditions de la proposition 6.2. Soit $m = \inf\{n \in \mathbb{N} \,|\, \exists x \in A,\, \varphi(x) = n \geqslant 2\}$. Les diviseurs de p tel que $\varphi(p) = m$ les éléments inversibles et les associés de p. Ces éléments p sont donc premiers. Soit $a \notin (p)$ et $\overline{a} \in (A/(p))^\times$ sa classe mod (p). Il existe q, r tels que $a = pq + r$ avec $\varphi(r) < \varphi(p) = m$. Comme $a \notin (p)$, on a $r \neq 0$, et donc $\varphi(r) = 1$ et $r \in A^\times$. Comme $\overline{a} = \overline{r}$, l'élément $\overline{a}$ a un antécédant dans $A^\times$. ∎

On déduit alors du théorème de Stark le théorème suivant.

6.7 Théorème. — *L'anneau des entiers de $\mathbb{Q}(\sqrt{d})$ avec $d < 0$ est euclidien si, et seulement si, $d = -11, -7, -3, -2$ et -1.*

Preuve. — Seuls les cas $d = -19, -43, -67, -163$ sont à envisager. Comme $d \equiv 5 \bmod 8$, l'anneau des entiers est $\mathbb{Z}[\alpha]$ avec $\alpha = \frac{1+\sqrt{d}}{2}$, racine de $g(X) = X^2 - X + \frac{1-d}{4} = 0$. Comme $A^\times = \{-1, 1\}$ est de cardinal 2, si $\mathcal{O}_K$ est euclidien, il existe p premier tel que $\mathrm{Card}(A/(p))$ est 2 ou 3. Dans le corps $A/(p)$, le polynôme $g(X)$ doit être scindé.
(*i*) Si $A/(p) \simeq \mathbb{F}_2$, ceci exige que $\frac{1-d}{4}$ soit pair (car $X^2 + X = X(X+1)$ et $X^2 + X + 1$ est irréductible modulo 2), c'est-à-dire $d \equiv 1 \bmod (8)$, ce qui n'est pas possible ;
(*ii*) Si $A/(p) \simeq \mathbb{F}_3$, comme $X^2 - X = X(X-1)$, $X^2 - X + 1 = (X-2)^2$ et $X^2 - X + 2$ est irréductible modulo 3, il faut que $\frac{1-d}{4} \equiv 0, 1 \bmod (3)$, d'où $d \equiv 0, 1 \bmod (3)$, ce qui est exclu. ∎

6.2.2 Cas réel

Formulons sous forme de théorème les faits évoqués en introduction de cette section.

6.8 Théorème. — *L'anneau des entiers de $\mathbb{Q}(\sqrt{d})$ avec $d > 0$ est euclidien pour la norme si et seulement si $d = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57$ ou 73.*

Nous allons nous contenter de vérifier que $\mathcal{O}_K$ est euclidien pour $d = 2, 3, 5$ et 13. Pour ceux qui n'aiment pas la géométrie, on redémontre les cas $d = -11, -7, -3, -2$ et -1 déjà abordés dans le paragraphe précédents sans efforts supplémentaires ; on aurait tort de s'en priver !

6.9 Proposition. — *L'anneau $\mathcal{O}_K$ des entiers de $K = \mathbb{Q}(\sqrt{d})$ est euclidien pour $d = -11$, -7, -3, -2, -1, 2, 3, 5 et 13.*

Preuve. — Supposons d'abord $d = -2, -1, 2$ ou 3. Alors $d \equiv 2$ ou $3 \bmod (4)$. Dans ces cas, $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$. Soit $a, b \in \mathcal{O}_K$, avec $b \neq 0$; alors $a/b = x + y\sqrt{d}$ avec $x, y \in \mathbb{Q}$. Soient α et β les entiers les plus proches de x et y respectivement ; ainsi $|x - \alpha| \leqslant 1/2$ et $|y - \beta| \leqslant 1/2$. Posons $q = \alpha + \beta\sqrt{d}$ et $r = a - bq$. On a $a = b(x + y\sqrt{d})$, donc $r = b((x - \alpha) + (y - \beta)\sqrt{d})$ et

$$\mathrm{N}_{K/\mathbb{Q}}(r) = \mathrm{N}_{K/\mathbb{Q}}((x - \alpha)^2 - d(y - \beta)^2).$$

Si $|d| \leqslant 2$, il vient

$$|(x - \alpha)^2 - d(y - \beta)^2| \leqslant (x - \alpha)^2 + |d|(y - \beta)^2 \leqslant \frac{3}{4}.$$

Si $d = 3$,

$$|(x - \alpha)^2 - 3(y - \beta)^2| \leqslant \max\{(x - \alpha)^2, 3(y - \beta)^2\} \leqslant \frac{3}{4}.$$

Dans les deux cas, $|\mathrm{N}_{K/\mathbb{Q}}(r)| < |\mathrm{N}_{K/\mathbb{Q}}(b)|$ et $\mathcal{O}_K$ est euclidien.

Si $d = -11, -7, -3, 5$ ou 13, on a $d \equiv 1 \bmod (4)$, et $\mathcal{O}_K = \mathbb{Z}[(1 + \sqrt{d})/2]$. Soit de nouveau $a, b \in \mathcal{O}_K$ avec $a/b = x + y\sqrt{d}$ et $x, y \in \mathbb{Q}$. Soit β l'entier le plus proche de $2y$; alors $|\beta/2 - y| \leqslant 1/4$. Soit α l'entier de même parité que β le plus proche de $2x$. On a donc $|\alpha - 2x| \leqslant 1$, donc

$$r = b\left[\left(x - \frac{\alpha}{2}\right) + \left(y - \frac{\beta}{2}\right)\sqrt{d}\right] \quad \text{et} \quad \mathrm{N}_{K/\mathbb{Q}}(r) = \mathrm{N}_{K/\mathbb{Q}}(b)\left[\left(x - \frac{\alpha}{2}\right)^2 - d\left(y - \frac{\beta}{2}\right)^2\right].$$

Pour $|d| \leqslant 11$, on a

$$\left|\left(x - \frac{\alpha}{2}\right)^2 - d\left(y - \frac{\beta}{2}\right)^2\right| \leqslant \frac{1}{4} + \frac{11}{16} < 1.$$

Si $d = 13$,

$$\left|\left(x - \frac{\alpha}{2}\right)^2 - 13\left(y - \frac{\beta}{2}\right)^2\right| \leqslant \frac{13}{16} < 1$$

et la proposition est démontrée. ∎

6.3 Corps cyclotomiques euclidiens

On a vu que $\mathbb{Z}[\xi_3] = \mathbb{Z}[\sqrt{3}]$ est euclidien. En revanche il est plus difficile de voir que $\mathbb{Z}[\xi_5]$ est euclidien.

6.10 Proposition. — *$\mathbb{Z}[\xi_5]$ est euclidien pour la norme.*

Preuve. — Posons $K = \mathbb{Q}(\xi_5)$ et prenons $\xi_5 = \exp(2i\pi/5)$ comme racine cinquième de l'unité. Pour alléger les notations on écrira $\xi = \xi_5$.
Soit $P(X) = a_0 + a_1 + X + a_2X^2 + a_3X^3 \in \mathbb{Q}[X]$ et $\alpha = P(\xi) \in \mathbb{Q}(\xi)$. Les quatre $\mathbb{Q}$-isomorphismes de K sont définis par $\sigma_i(\xi) = \xi^i$ pour $1 \leqslant i \leqslant 4$, donc

$$\mathrm{N}_{K/\mathbb{Q}}(\alpha) = P(\xi)P(\overline{\xi})P(\xi^2)P(\overline{\xi}^2) \geqslant 0.$$

Or

$$P(\xi)P(\overline{\xi}) = (a_0^1 + a_1^2 + a_2^2 + a_3^2) + (a_0a_1 + a_1a_2 + a_2a_3)(\xi + \overline{\xi}) + (a_0a_2 + a_1a_3 + a_0a_3)(\xi^2 + \overline{\xi}^2).$$

Comme

$$\xi + \overline{\xi} = \xi + \xi^4 = 2\cos\left(\frac{2\pi}{5}\right) = \frac{-1+\sqrt{5}}{2} \quad \text{et} \quad \xi^2 + \overline{\xi}^2 = \xi^2 + \xi^3 = 2\cos\left(\frac{4\pi}{5}\right) = \frac{-1-\sqrt{5}}{2},$$

il vient

$$P(\xi)P(\overline{\xi}) = \sum_{i=0}^{3} a_i^2 - \frac{1}{2}\sum_{0\leqslant i<j\leqslant 3} a_ia_j + B\sqrt{5}, \quad B \in \mathbb{Q}.$$

Mais

$$\sum_{0\leqslant i<j\leqslant 3} a_ia_j = \frac{1}{2}\left(\left(\sum_{i=0}^{3} a_i\right)^2 - \sum_{i=0}^{3} a_i^2\right),$$

d'où finalement $P(\xi)P(\overline{\xi}) = A + B\sqrt{5}$ avec

$$A = \frac{5}{4}\sum_{i=0}^{3} a_i^2 - \frac{1}{4}\left(\sum_{i=0}^{3} a_i\right)^2 \in \mathbb{Q}.$$

Quand on remplace ξ par ξ^2 on intervertit le rôle de $\cos(2\pi/5)$ et $\cos(4\pi)/5$ dans les calculs qui viennent d'être faits, donc $P(\xi^2)P(\overline{\xi}^2) = A - B\sqrt{5}$ et $\mathrm{N}_{K/\mathbb{Q}}(\alpha) = A^2 - 5B^2$.

Soit $b_i = a_i - [a_i]$ pour $0 \leqslant i \leqslant 3$ et $b_4 = 0$ (où $[a_i]$ désigne la partie entière de a_i). On a $b_i \in [0,1[$ pour tout i. Si on divise en cinq parties égales l'intervalle $[0,1]$, on voit qu'il existe $i \neq j$ tels que $|b_i - b_j| \leqslant 1/5$, c'est-à-dire il existe $i \neq j$ et un entier C tel que $|a_i - a_j - C| \leqslant 1/5$. Or on a

$$\begin{cases} \alpha\xi &= -a_3 + (a_0 - a_3)\xi + (a_1 - a_3)\xi^2 + (a_2 - a_3)\xi^3 \\ \alpha\xi^2 &= (a_3 - a_2) - a_2\xi + (a_0 - a_2)\xi^2 + (a_1 - a_2)\xi^3 \\ \alpha\xi^3 &= (a_2 - a_1) + (a_3 - a_1)\xi - a_1\xi^2 + (a_0 - a_1)\xi^3 \\ \alpha\xi^4 &= (a_1 - a_0) + (a_2 - a_0)\xi + (a_3 - a_0)\xi^2 - a_0\xi^3 \end{cases}$$

donc il existe $1 \leqslant q \leqslant 4$ tel que $\alpha\xi^q = A_0 + A_1\xi + A_2\xi^2 + A_3\xi^3$ et que pour l'un des A_j, il existe $B_j \in \mathbb{Z}$ vérifiant $|A_j - B_j| \leqslant 1/5$. Pour les trois autres A_i, il existe $B_i \in \mathbb{Z}$ tel que $|A_i - B_i| \leqslant 1/2$. Ainsi il existe $1 \leqslant q \leqslant 4$ et $\beta = \sum_{i=0}^{3} B_i\xi^i \in \mathbb{Z}[\xi]$ tels que $\alpha\xi^q - \beta = \sum_{i=0}^{3} c_i\xi^i$ avec

$$\sum_{i=0}^{3} c_i^2 \leqslant \frac{1}{25} + 3\,\frac{1}{4} = 0,79 \quad \text{et} \quad \left|\sum_{i=0}^{3} c_i\right| \leqslant \frac{1}{5} + 3\,\frac{1}{2} = 1,7.$$

Alors $\mathrm{N}_{K/\mathbb{Q}}(\alpha\xi^q - \beta) = A^2 - 5B^2 \leqslant A^2$ avec

$$-\frac{1}{4}\left(\sum_{i=0}^{3} c_i\right)^2 \leqslant A \leqslant \frac{5}{4}\sum_{i=0}^{3} c_i^2,$$

d'où $-0,7225 \leqslant A \leqslant 0,9875$. Ainsi $A^2 < 1$ et $\mathrm{N}_{K/\mathbb{Q}}(\alpha\xi^q - \beta) < 1$. Or $\mathrm{N}_{K/\mathbb{Q}}(\xi^{-q}) = 1$, donc

$$\mathrm{N}_{K/\mathbb{Q}}(\alpha - \beta\xi^{-q}) = \mathrm{N}_{K/\mathbb{Q}}(\xi^{-q})\mathrm{N}_{K/\mathbb{Q}}(\alpha\xi^q - \beta) < 1.$$

On a donc montré que pour tout $\alpha \in K$, il existe $\gamma \in \mathcal{O}_K$ tel que $\mathrm{N}_{K/\mathbb{Q}}(\alpha - \gamma) < 1$, ce qui d'après le lemme 6.3 montre que $\mathcal{O}_K$ est euclidien pour la norme. ∎

Lenstra a prouvé en 1975 que $\mathbb{Z}[\xi_m]$ est euclidien pour la norme si $\varphi(m) \leqslant 10$ et $m \neq 16, 24$. En 1977, Ojala a montré que $\mathbb{Z}[\xi_{16}]$ est euclidien pour la norme, et Lenstra a fait de même pour $\mathbb{Z}[\xi_{24}]$ l'année suivante. En 2004, Harper a démontré que $\mathbb{Z}[\xi_m]$ est euclidien si et seulement s'il est principal. Dans un article de 1979, Lenstra prouve que $\mathbb{Z}[\xi_{32}]$ n'est pas euclidien pour la norme. On a donc là un exemple d'anneau d'entiers cyclotomiques euclidien, mais pas euclidien pour la norme ; c'est la seule valeur de m connue de Harper au moment où il écrit son article pour laquelle ce phénomène se produit. Les autres valeurs de m pour lesquelles on ne sait rien sont 13, 17, 19, 21, 25, 27, 28 et les valeurs $m \geqslant 33$ donnée par le théorème 4.30 de Masley. On reparlera de ces problèmes dans l'ouverture page 78.

Chapitre 7

Quelques résultats complémentaires

Finissons par quelques résultat sur la détermination des corps de nombres principaux et euclidiens. En 1994, Yamamura termine la classification des corps de nombres imaginaires c'est-à-dire ceux pour lesquels $r_1 = 0$ avec les notations de 4.2.3. Dans son article [Yam94], il énonce le théorème suivant.

7.1 Théorème (Yamamura, 1994). — *Il existe exactement 172 corps de nombres abéliens imaginaires principaux. Parmi eux, il y a 29 corps cyclotomiques, 49 corps cycliques et 88 corps sont maximaux pour l'inclusion.*

Les degrés de ces corps sont 2 (ceux du théorème 5.30), 4, 6, 8, 10, 12, 14, 16, 18, 20 et 24. A titre d'exemple, il n'existe que 3 corps de nombres principaux de degré 10, ce sont $\mathbb{Q}(\xi_{11}), \mathbb{Q}(\sqrt{-1}, \cos(2\pi/11))$ et $\mathbb{Q}(\sqrt{-3}, \cos(2\pi/11))$. Ceux de degré 24 sont

$$\mathbb{Q}(\xi_{35}),\ \mathbb{Q}(\xi_{45}),\ \mathbb{Q}(\xi_{21}, \sqrt{5}), \mathbb{Q}(\xi_{84})\ \text{ et }\ \mathbb{Q}(\xi_{15}, \cos(2\pi/7)).$$

La liste des corps cyclotomiques a été vue au théorème 4.31.

Dans le cas où $r_1 > 0$ la question reste aujourd'hui très ouverte. On ne sait même si le nombre de valeur de $d > 0$ pour lesquelles $\mathbb{Q}(\sqrt{d})$ est principal est fini ou pas...

Dans un article fondamental écrit en 1971, Pierre Samuel soulevait plusieurs questions à propos des anneaux euclidiens, la plus célèbre étant $\mathbb{Z}[\sqrt{14}]$ est-il euclidien ? Il est bien connu que cet anneau n'est pas euclidien pour la norme ; Samuel demande donc si l'anneau ne pourrait pas être euclidien pour un autre stathme. Weinberger a montré en 1973 le résultat suivant.

7.2 Théorème (Weinberger, 1973). — *Soit K un corps de nombres principal. Supposons que $\mathcal{O}_K$ a une infinité d'unités. Supposons que l'hypothèse de Riemann généralisée soit vraie. Alors $\mathcal{O}_K$ est euclidien.*

L'anneau $\mathbb{Z}[\sqrt{14}]$ vérifiant ces conditions, il serait hypothétiquement euclidien pour un stathme différent de la norme.

Dans une série d'articles écrits dans les années 1980, Rajiv Gupta, Kumar Murty et Ram Murty ont élaboré de nouvelles techniques pour l'étude des anneaux euclidiens dans le but d'éviter l'utilisation de l'hypothèse de Riemann généralisée avancée par Weinberger. Les premiers exemples d'anneaux euclidiens pour un stathme différent de la norme ont été donné par ces mathématiciens, mais leurs résulats ne s'appliquaient pas aux anneaux d'entiers. Le premier exemple d'un tel

anneau d'entiers a été donné en 1992 par David Clark dans sa thèse, puis en 1993 il en donne un beaucoup plus simple, à savoir $\mathcal{O}_{\mathbb{Q}(\sqrt{69})}$. Peu après il montre avec Ram Murty que $\mathbb{Z}[\sqrt{14}, 1/p]$ est euclidien pour le nombre premier $p = 1298852237$, sans recourir à l'hypothèse de Riemann généralisée. Dans sa thèse, Malcolm Harper montre en 2000 que le résultat de Clark et de Ram Murty s'applique à tout nombre premier p. Plus tard, par un emploi ingénieux de la méthode du crible, il a éliminé l'emploi du nombre premier auxiliaire et a établi la conjecture de Samuel sur $\mathbb{Z}[\sqrt{14}]$.

En 2004 dans [Har04-1], Harper présente des catégories de corps de nombres réel ($r_2 = 0$) tel que $\mathcal{O}_K$ soit euclidien si et seulement s'il est principal. Il obtient les corollaires suivants.

7.3 Théorème (Harper, 2004). — *Soit K un corps de nombres réel de discriminant inférieur à 500. Alors $\mathcal{O}_K$ est euclidien si et seulement s'il est principal.*

7.4 Théorème (Harper, 2004). — *Soit $m \geqslant 3$ un entier. Alors $\mathbb{Z}[\xi_m]$ est euclidien si et seulement s'il est principal.*

Concerant la preuve du second théorème, ses travaux ne s'appliquent que si $\varphi(m) \geqslant 8$. Pour les valeurs de m telles que $\varphi(m) \leqslant 7$, il s'appuie sur des résultats antérieurs mentionnés à la fin de la section 6.3.

Citons enfin un résultat de Harper et Murty (voir [Har04-2]).

7.5 Théorème (Harper et Murty, 2004). — *Soit $K/\mathbb{Q}$ une extension galoisienne de degré fini > 8. Alors $\mathcal{O}_K$ est euclidien si et seulement s'il est principal.*

Bibliographie

Articles

[Har04-1] Harper, M., $\mathbb{Z}[\sqrt{14}]$ *is euclidean*. Canad. J. Math. Vol. 56, No 1, pp. 50-70, 2004.

[Har04-2] Harper, M. et Murty, R., *Euclidean rings of algebraic integers*. Canad. J. Math. Vol. 56, No 1, pp. 71-76, 2004.

[Sta67] Stark, H. M., *A complete determination of the complex quadratic fields of class-number one*. Mich. Math. J. 14, pp. 1-27, 1967.

[Mas75] J. M. Masley, *Solution of the class number two problem for cyclotomic fields*. Inventiones Math. Vol. 25, 1975.

[Mas76-1] J. M. Masley et H. L. Montgomery, *Cyclotomic fields with unique factorization*. J. reine angew. Math., 28.6/287, pp. 248-256, 1976.

[Mas76-2] J. M. Masley, *Solution of small class number problems in cyclotomic fields*. Compositio mathematica, Vol. 33, No. 2, pp. 179-186, 1976.

[Yam94] Yamamura, K. *The determination of the imaginary abelian number fields with class-number one*. Mathematics of Computation, Vol. 62, No. 206, pp. 899-921, 1994.

Ouvrages

[Duv98] Duverney, D., *Théorie des nombres*. Dunod, 1998.

[Gob01] Goblot, R., *Algèbre commutative*. Dunod, 2001.

[Goz97] Gozard, Y., *Théorie de Galois*. Ellipses, 1997.

[Gra04] Gras, G. et M.-N., *Algèbre fondamentale, Arithmétique*. Ellipses, 2004.

[Per96] Perrin, D., *Cours d'algèbre*. Ellipses, 1996.

[Rib01] Ribenboim, P., *Classical theory of algebraic numbers*. Springer, 2001.

[Sam71] Samuel, P., *Théorie algébrique des nombres*. Hermann, 1971.

[Was97] Washington, L., *Introduction to cyclotomic fields*. Springer, 1997.

Polycopié

[Wes] Weston, T. *Algebraic number theory*. Disponible sur internet.