# Autour du douzième problème de Hilbert

Kéva Bruno Djambaé
Encadré par D. Kohel, Professeur des Universités
(Aix-Marseille Université)

Du 15 Avril au 15 Juin 2022

**Résumé**

Ce mémoire a été réalisé au sein de l'équipe Arithmétique et Théorie de l'Information (ATI) à l'Institut de Mathématiques de Marseille (I2M) au cours de mon Master 2-Recherche qui avait pour thématique le « Programme de Langlands ». Encadré par Dr. D.Kohel, Professeur des Universités, l'axe principal du stage était la généralisation du théorème de Kronecker-Weber.

Nous avons donc découpé en trois chapitres ce mémoire. Au cours du premier, nous établissons le théorème de Kronecker-Weber. Le deuxième s'intéresse à la généralisation dans le cas des corps quadratiques imaginaires. Ensuite, si les deux premières parties étaient majoritairement algébriques, le troisième chapitre est à l'intersection entre l'algèbre et la géométrie. Nous généraliserons nos connaissances acquises lors du deuxième chapitre grâce à la notion de courbe elliptique.
Enfin, dans le dernier, nous expliciterons les analogies possibles pour les extensions abéliennes du corps des rationnels et celles d'un corps quadratique imaginaire.

## Sommaire

## Remerciements

Je souhaiterais adresser ma gratitude envers David Kohel, qui m'a encadré pour ce stage de master 2. Il a su m'aiguiller malgré un sujet très vaste, ses conseils et ses relectures furent déterminante dans mon travail et ma compréhension du problème.

# 0 Introduction et Avant-Propos

## Avant-propos

Ce document est un mémoire résultant du stage de recherche de deux mois effectué à l'Institut Mathématiques de Marseille (I2M) encadré par le Dr. D.Kohel, Professeur des Universités, au sein de l'équipe Arithmétique et Théorie de l'Information (ATI), une composante du groupe scientifique Arithmétique, Géométrie, Logique et Représentations (AGLR). Nous avions pour axe de recherche le douzième problème de Hilbert.

Ce dernier consiste en la généralisation du théorème de Kronecker-Weber à tout corps de nombres. Bien entendu, la question étant encore ouverte, nous nous sommes restreint au cas des corps quadratiques. Cela nous a permis d'entrevoir un large spectre de l'algèbre et de la géométrie. Nous avons essayé de concentrer dans ce texte toutes les notions et objets rencontrés lors du stage. En résulte un aspect légèrement abscon car chaque notion mériterait de s'y intéresser exclusivement. Nous avons donc choisi de découper cet écrit en quatres chapitres.

La démonstration du théorème de Kronecker-Weber nous occupera lors du chapitre I. Il est divisé en trois sections. La première s'intéresse aux extensions cyclotomiques où nous évoquerons la ramification et les anneaux d'entiers de telles extensions. La deuxième est un rappel succint de la théorie du corps de classes (locale et globale). Nous concluons par une troisième consacrée à la démonstration du théorème de Kronecker-Weber où nous proposons deux approches pour arriver à nos fins.

Le chapitre II s'intéresse donc à la généralisation de ce théorème et se décompose en deux sous-chapitres, le premier portant sur la notion d'ordre et d'anneau du corps de classe, le second sur les notion de fonctions elliptiques et la fonction $j$. La quatrième section s'intéresse à la notion d'ordre dans un corps quadratique $K$ imaginaire (sur $\mathbb{Q}$). Nous la relierons aux notions de formes quadratiques et d'idéaux (premiers). La cinquième section introduit l'anneau du corps de classes qui (comme son nom l'indique) est fortement lié aux extensions abéliennes. Ce sera aussi l'occasion d'en caractériser certaines. La sixième section permet d'entrevoir les apports de la géométrie à notre raisonnement. Nous commencerons par étudier les notions de réseaux et de fonctions elliptiques dans le plan complexe $\mathbb{C}$ pour introduire un objet central : la fonction $j$. La septième section est une étude de la fonction $j$. On établit que le $j$-invariant d'un réseau $\Lambda$ de $\mathbb{C}$ est un nombre algébrique. La huitième section conclut notre étude du côté de l'algèbre. En établissant que le $j$-invariant est un entier algébrique. Nous pourrons enfin généraliser le théorème de Kronecker-Weber au cas des corps quadratiques imaginaires.

Le chapitre III porte sur les liens avec la géométrie. La neuvième section crée le lien entre les courbes elliptiques et la notion de fonction elliptique, permettant ainsi d'utiliser l'éventail d'outils que nous avons précédemment évoqué. La dizième section est dédiée à la découverte des corps de fonctions, un objet assez proche de ce que nous connaissons en théorie algébrique des nombres permettant aisément beaucoup d'analogies.

Le (court) chapitre IV conclut notre investigation. Nous mettons en lumière l'analogie pour la classification des extensions abéliennes entre les situations sur $\mathbb{Q}$ et sur $K$ un corps quadratique imaginaire.

Ce document comporte aussi plusieurs annexes.
La première établit le fait que tout groupe de Galois d'une extension de corps de nombres est un groupe profini et sa réciproque. Cela nous est utile dans le chapitre portant sur le théorème Kronecker-Weber. La deuxième annexe se consacre exclusivement à un résultat de géométrie algébrique, le théorème de Riemann-Roch. Ce dernier nous offre une ouverture pour généraliser notre cadre de travail.

### Rétrospective historique

Se réfèrer à l'article [9] de Schappacher pour plus de détails.

## Première partie

# Théorème de Kronecker-Weber

Ce premier chapitre est découpé en trois parties distinctes. Nous débutons par une étude générale des extensions cyclotomiques afin de mieux appréhender les corps dans lesquels nous travaillons. Ensuite, nous en profitons pour évoquer la théorie du corps de classe, théorie primordiale dans notre mémoire. Nous ferons un rappel de la théorie locale et globale. Nous profiterons établirons aussi la théorie de Kummer. Enfin, dans la troisième section, nous démontrerons le théorème de Kronecker-Weber de deux manières.
La plupart des résultats sont issus de [8] et [13].

## 1 Extensions cyclotomiques

Avant de nous atteler à la démonstration du théorème de Kronecker-Weber, nous présentons lors de cette partie les extensions cyclotomiques. En effet, une fois le théorème établi, toute extension abélienne de $\mathbb{Q}$ pourra être vu comme une sous-extension d'une extension cyclotomique et ce sont des extensions relativement bien connues.

### 1.1 Introduction aux corps cyclotomiques

On commence par définir récursivement les polynômes cyclotomiques :

**Théorème 1.1.** *[Définition des polynômes cyclotomiques]*
*Il existe une suite unique de polynômes $(\Phi_n)_{n\geq 0}$ à coefficients dans $\mathbb{Q}$ tel que :*

- *on ait $\Phi_1 = X - 1$.*
- *pour tout entier $n > 0$, $X^n - 1 = \prod_{d|n} \Phi_d(X)$.*

*De plus, chacun des $\Phi_n \in \mathbb{Z}[X]$ est unitaire de degré $\varphi(n)$ et les $(\Phi_n)_{n\geq 0}$ sont premiers entre eux deux à deux.*

*Démonstration.* Unicité
Soient $\Phi_n$ et $\Psi_n$ deux suites satisfaisant les conditions requises du théorème. Par récurrence, on montre :

$$\text{Pour tout } n \in \mathbb{N},\ \Phi_n = \Psi_n. \tag{1}$$

Pour $n = 1$, avec le premier item on a $\Psi_1 = \Phi_1 = X - 1$ donc c'est vérifié.
Soit $n > 1$ entier tel que l'égalité (1) pour tout entier $m < n$. Avec le

deuxième item, on peut affirmer pour tout $d$ divisant $n$ que :

$$\prod_{d|n} \Phi_d = \prod_{d|n} \Psi_d = X^n - 1.$$

Donc $\Phi_d = \Psi_d$ par hypothèse de récurrence. Comme $X^n - 1 \neq 0$ et que $\mathbb{Q}[X]$ est un anneau intègre, on peut conclure que $\Phi_n = \Psi_n$.

Existence

Nous allons construire récursivement les $\Phi_n$. Tout d'abord, on a $\Phi_1 = X - 1$ qui est un polynôme unitaire, à coefficients dans $\mathbb{Z}$ et on a $\varphi(1) = 1$.
Supposons avoir construit $(\Phi_i)_{1 \leq i \leq n-1}$ tel que pour tout $m < n$ entier, on ait $X^m - 1 = \prod_{d|m} \Phi_d(X)$ où chaque $\Phi_i \in \mathbb{Z}[X]$ est unitaire de degré $\varphi(n)$ tel que les $\Phi_i$ soient premiers entre eux deux à deux.

Soit $d < n$ un entier tel que $d|n$, on voit que $X^d - 1$ divise $X^n - 1$ donc $\Phi_d$ divise $X^n - 1$. Ainsi, on a :

$$\prod_{d|n, d \neq n} \Phi_d \text{ divise } X^n - 1.$$

Comme ce sont deux polynôme unitaire à coefficient dans $\mathbb{Z}$. On définit $\Phi_n$ comme étant ce quotient. Par construction, on a pour tout $m \leq n$, $X^m - 1 = \prod_{d|m} \Phi_d(X)$.

Il nous reste à vérifier que $\varphi(n) = \deg(\Phi_n)$ et pour tout $i < n$, $\Phi_i$ et $\Phi_n$ sont premiers entre eux.

Commençons par le degré, comme $X^n - 1 = \prod_{d|n} \Phi_d(X)$, on a, par hypothèse de récurrence :

$$\text{Pour tout } d < n, \ \deg \Phi_d = \varphi(d) \text{ donc on a } n = \deg \Phi_n + \sum_{d|n, d \neq n} \varphi(d).$$

Or $n = \sum_{d|n} \varphi(d)$ donc on a $\deg(\Phi_n) = \varphi(n)$.

Maintenant, montrons que si $\delta < n, \delta | n$ alors $\Phi_n$ et $\Phi_d$ sont premiers entre eux.

Soit $L$ le corps de décomposition de $X^n - 1 = \prod_{d|n} \Phi_d(X)$ est un produit de polynôme scindé à racines simples dans L donc ils n'ont aucune racine commune ainsi ils sont premiers entre eux.

Ensuite, montrons que si $d < n$ et $d|n$, alors $\text{pgcd}(\Phi_n, X^d - 1) = 1$.
Comme $X^d - 1 = \prod_{\delta|d} \Phi_\delta(X)$ mais si $\delta | d$ alors sait que $\delta$ est un diviseur strict de $n$. Le paragraphe précédent nous permet affirmer que $\Phi_n$ et $\Phi_d$ sont

premiers entre eux donc $\text{pgcd}(\Phi_n, X^d - 1) = 1$.

Pour conclure, soit $i < n$ un entier. Supposons que $P = \text{pgcd}(\Phi_n, \phi_i)$ et $d = \text{pgcd}(i, n)$. Comme $P$ divise $\Phi_n$ (resp. $\Phi_i$), on a $P$ divise $X^n - 1$ (resp. $X^i - 1$). Donc $P$ divise le $\text{pgcd}(X^n - 1, X^i - 1) = X^d - 1$. Comme $i < n$, $d$ divise $n$ et $d < n$ et que $\phi_n$ est premier avec $X^d - 1$ alors $P = 1$ car ils sont multiples. □

On montre maintenant l'irréductibilité des polynômes cyclotomiques $(\Phi_n)$ sur $\mathbb{Q}$.

**Théorème 1.2.** *Pour tout entier $n$ non nul, $\Phi_n(X) \in \mathbb{Z}[X]$ est irréductible sur $\mathbb{Q}[X]$.*

*Démonstration.* On a déjà établit que $\Phi_n$ était à coefficients entiers avec le théorème 1.1.
Cette preuve va se découper en deux étapes :

- $\Phi_n$ est le polynôme minimal des racines primitives.
- $\Phi_n$ est un polynôme minimal.

Etape 1.
Soit $\zeta \in \mu_n$ et $P$ son polynôme minimal dans $\mathbb{Q}$. $P|(X^n - 1)$, donc il existe $Q \in \mathbb{Q}[X]$ tel que $X^n - 1 = PQ$, avec ce qui précède on peut affirmer $Q \in \mathbb{Z}[X]$. Soit $p$ un nombre premier ne divisant pas $n$ et $u$ une racine de P. Notre but est de montrer que $P(u^p) = 0$.

Comme $P|(X^n - 1)$ on a $u^n - 1 = 0$ donc $0 = (u^p)^n - 1 = P(u^p)Q(u^p)$.
Par l'absurde, si $P(u^p) \neq 0$ alors $Q(u^p) = 0$ mais comme $u$ est une racine de $P$, unitaire et irréductible sur $\mathbb{Q}$ donc $P$ est le polynôme minimal de $u$.
Ainsi, comme $Q(u^p) = 0$ on a $P|Q(X^p)$ et $Q(X^p) = P(X)R(X), R \in \mathbb{Z}[X]$.
En réduisant modulo $p$, on obtient $\overline{Q}(X^p) = \overline{Q}(X)^p = \overline{P}(X)\overline{R}(X)$.
Si $T \in \mathbb{F}_p[X]$ est un facteur irréductible de $\overline{P}$ alors $T|\overline{Q}^p$ donc $T|\overline{Q}$ et du fait que $T|\overline{P}$ on a $T^2|\overline{PQ} = (X^n - 1)$.
Ainsi, $X^n - 1$ possède une racine double dans une clôture algébrique de $\mathbb{F}_p$.
Mais, $1 = \dfrac{X}{n}(nX^{n-1}) - (X^n - 1)$ grâce au théorème de Bezout, on obtient donc une contradiction.

Etape 2.
Soit $\alpha$ une racine de $P$ tel que pour tout $p$ premier non diviseur de $n$, $x^p$ est une racine de $P$. Il suit par élévations successives à des puissances premières que $\forall k \in \mathbb{N}$, $\text{pgcd}(k, n) = 1$ donc $\alpha^k$ est une racine de $P$ donc toutes les racines $n$-primitives sont des racines de $P$. Donc $\Phi_n|P$ or $\Phi_n(\alpha) = 0$ donc $P|\Phi_n$. Ces deux polynômes étant unitaires, on a $\Phi_n = P$ est irréductible dans $\mathbb{Q}[X]$. □

**Corollaire 1.3.** *Soit $\zeta_n$ une racine primitive n-ième de l'unité. Alors, en posant $K = \mathbb{Q}(\zeta_n)$, $K/\mathbb{Q}$ est une extension abélienne et $G = \mathrm{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$.*

*Démonstration.* Pour tout $n \in \mathbb{N}$, $\phi_n$ est le polynôme minimal de $\zeta_n$ sur $\mathbb{Q}[X]$, c'est un polynôme scindé à racines simples et tout les conjugués de $\zeta_n$ sont des puissances de $\zeta_n$. On peut donc affirmer que $K/\mathbb{Q}$ est normale. Elle est séparable car on est en caractéristique 0. Donc $K/\mathbb{Q}$ est une extension galoisienne. Grâce à la théorie de Galois, on a :

$$\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times| = \deg(\Phi_n) = [K : \mathbb{Q}] = |G|.$$

En notant $(\sigma_i)_{1\leq i\leq \varphi(n)} : \zeta_n \longmapsto \sigma_i(\zeta_n) = (\zeta_n)^i$ les éléments de G on a un isomorphisme $G = \mathrm{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$ par l'application :
$k \in (\mathbb{Z}/n\mathbb{Z})^\times \longmapsto \sigma_k \in G$. □

**Remarque 1.4.** *Ainsi, si $K = \mathbb{Q}(\zeta_n)$ alors $\mathcal{O}_K$ est un $\mathbb{Z}$-module libre de rang $n = |Gal(K/\mathbb{Q})|$. De plus, on sait que $\Phi_n$ est un polynôme à coefficients entiers irréductible sur $\mathbb{Q}$.*

## 1.2 Anneaux d'entiers d'un corps cyclotomique

On va maintenant s'intéresser plus particulièrement à l'anneau des entiers. Soient $n \geq 3$ un entier, $\zeta = \zeta_n = e^{\frac{2i\pi}{n}}$, $K = \mathbb{Q}(\zeta)$. On commence par un petit lemme :

**Lemme 1.5.** *On a $p = \prod^m_{\substack{k=1 \\ pgcd(p,k)=1}} (1 - \zeta^k)$*

*Démonstration.*

Soit $P(X) = \dfrac{X^{p^r} - 1}{X^{p^{r-1}} - 1} = 1 + X^{p^{r-1}} + X^{2p^{r-1}} + \cdots + X^{(p-1)p^{r-1}}$ et $p = P(1)$.

De plus, pour tout $p$ premier ne divisant pas $k$ $\zeta^k$ est une racine de $P$ car c'est une racine de $X^{p^r} - 1$ mais pas une racine de $X^{p^{r-1}} - 1$. Ainsi, on a :

$$P(X) = \prod_{\substack{k=1 \\ pgcd(p,k)=1}}^{m} (X - \zeta^k)$$

et avec X=1 on obtient le résultat. □

**Proposition 1.6.** *On a* $\mathrm{Disc}(\zeta_n) | n^{\varphi(n)}$

*Démonstration.* Soit $\Phi_n$ le polynôme minimal de $\zeta_n$.
Alors $X^n - 1 = \Phi_n(X)Q(X), Q \in \mathbb{Z}[X]$. En dérivant et en évaluant en $\zeta_n$, on a $n = \zeta_n \Phi'_n(\zeta_n)Q(\zeta_n)$.

Comme $\mathrm{Disc}(\zeta) = \prod_{r\neq s}(\zeta_r - \zeta_s)^2 = (-1)^{\frac{n(n-1)}{2}} N_{K/\mathbb{Q}}(\Phi'_n(\zeta))$ avec $(\zeta_r)$ les conjugués de $\zeta$. En passant aux normes, on a donc :

$$n^{\varphi(n)} = \mathrm{Disc}(\zeta) N_{K/\mathbb{Q}}(\zeta Q(\zeta)) \text{ avec } N_{K/\mathbb{Q}}(\zeta Q(\alpha)) \in \mathbb{Z}$$

car $Q \in \mathbb{Z}[X]$ et $\zeta$ est un entier algébrique d'où le résultat. □

**Théorème 1.7.** *L'anneau des entiers de $K$ est $\mathcal{O}_K = \mathbb{Z}[\zeta]$.*

*Démonstration.* La preuve va se décomposer en deux parties :

- pour $n \in \mathbb{N}$.
- si $n = p^r$ avec $p$ premier.

Etape 1
Commençons par le cas simple, on suppose $n \in \mathbb{N}$ quelconque. On suppose le théorème prouvé si $n$ est une puissance de premiers.
On procède, par récurrence, sur le nombre de facteurs premiers de $n$.

Si $n$ est une puissance de premier, c'est admis pour l'instant.
Sinon, supposons $n = n_1 n_2$ avec $n_1, n_2 \in \mathbb{N}^*$ et $n_1$ et $n_2$ premiers entre eux.
On a par hypothèse de récurrence $\zeta_{n_1} = e^{\frac{2i\pi}{n_1}}$, $\zeta_{n_2} = e^{\frac{2i\pi}{n_2}}$, $K_1 = \mathbb{Q}(\zeta_{n_1})$, $K_2 = \mathbb{Q}(\zeta_{n_2})$.
Grâce au fait que $\mathrm{pgcd}(n_1, n_2) = 1$ on a $[K_1K_2 : \mathbb{Q}] = [K_1 : \mathbb{Q}][K_2 : \mathbb{Q}]$.
En vertu du théorème de Bezout, il existe $u, v \in \mathbb{Z}$ tel que $um_1 + vm_2 = 1$.
En posant $\zeta = \zeta_1^u \zeta_2^v$, grâce à la proposition 1.6 on a :

$$\mathcal{O}_K = \mathcal{O}_{K_1}\mathcal{O}_{K_2} = \mathbb{Z}[\zeta_{n_1}]\mathbb{Z}[\zeta_{n_2}] = \mathbb{Z}[\zeta_n]$$

Etape 2
Maintenant, supposons $n = p^r$ avec $p$ premier.
On a $\mathbb{Q}(\zeta) = \mathbb{Q}(1-\zeta)$ et pour tout $x \in \mathcal{O}_K$, on a

$$x = \frac{\sum_{0\leq k\leq n-1} m_k(1-\zeta)^{k-1}}{d} \text{ avec } n = \varphi(p^r), m_i \in \mathbb{Z}, d = \mathrm{Disc}(\zeta) = \mathrm{Disc}(1-\zeta)$$

car :
$\mathrm{Disc}(\zeta) = \prod_{r\neq s}(\zeta_r - \zeta_s)^2 = \prod((1-\zeta_r) - (1-\zeta_s))^2 = \mathrm{Disc}(1-\zeta)$ avec $(\zeta_r)$ conjugués de $\zeta$. Cela implique aussi que les $(1-\zeta_r)$ sont les conjugués de $(1-\zeta)$. Avec la proposition 1.6, on peut affirmer que $d$ est une puissance de $p$.

Montrons que $\mathcal{O}_K = \mathbb{Z}[1-\zeta] = \mathbb{Z}[\zeta]$. Par l'absurde, supposons $\mathcal{O}_K \neq \mathbb{Z}[1-\zeta]$ alors il existe $x = \dfrac{\sum_{j=0}^{n-1} m_j(1-\zeta)^j}{p^k} \neq 0$ pour lequel aucun des $m_j$ n'est divisible par $p^k = d$. Considérons alors le premier indice $i$ pour lequel la

valuation $v_i$ de $m_i$ en $p$ est minimale (pour tout $j$, $p^{v_i}|m_j$ et $p^{v_{i+1}}$ ne divise pas $m_j$) et on pose $\beta = p^{k-v_i-1}x - \sum_{j<i} \frac{m_j 1-\zeta)^{j-1}}{p^{v_i+1}}$.
Par définition de $i$, les $\frac{m_j(1-\zeta)^{j-1}}{p^{v_i+1}}$ sont des entiers donc $\beta \in O_K$.
Donc pour $p$ ne divisant pas $m_j$, on a :

$$\beta = \frac{m_i(1-\zeta)^{i-1} + m_{i+1}(1-\zeta)^i + \cdots + m_n(1-\zeta)^{n-1}}{p}.$$

Or d'après le lemme 1.5 $\frac{P}{(1-\zeta)^n} \in \mathbb{Z}[\zeta]$ car $(1-\zeta)|(1-\zeta^k)$ dans $\mathbb{Z}[\zeta]$ et on a $\varphi(n) = n$ tels facteurs donc $\frac{P}{(1-\zeta)^i} \in \mathbb{Z}[\zeta]$ d'où :

$$\frac{\beta p}{(1-ß)^i} = \frac{m_i}{1-\zeta} + m_j(1-\zeta)^{j-1} \in O_K.$$

Dans ce nombre tout les termes d'indices supérieur à $i$ sont dans $\mathcal{O}_K$ donc $\frac{m_i}{1-\zeta} \in \mathcal{O}_K$. Donc $N_{K/\mathbb{Q}}(1-\zeta)$ divise $N_{K/\mathbb{Q}}(m_i)$ mais cela est impossible car $N_{K/\mathbb{Q}} = m_i^n$ et le lemme 1.5 montre que $N_{K/\mathbb{Q}}(1-\zeta) = p$. □

## 1.3 Ramification dans un corps cyclotomique

On rappelle que $\zeta_n = \zeta = e^{\frac{2i\pi}{n}}$. On choisit $n = p^k m$ un entier tel que $\text{pgcd}(p, m) = 1$. On pose $\alpha = \zeta^m$ et $\beta = \zeta^{p^k}$. On commence par un premier lemme :

**Lemme 1.8.** *Si $p$ est premier alors son indice de ramification dans $\mathbb{Q}(\zeta_{p^k})$ est $\varphi(p^k) = e$.*

*Démonstration.* Dans $\mathbb{Q}(\alpha)$, on sait que :

$$p = \prod_{1\leq i\leq p^k, \text{pgcd}(p,i)=1} (1-\alpha^i).$$

Or si $p$ ne divise pas $i$, alors, en écrivant, $1 = ui + vp$ on a :
$\frac{1-\alpha}{(1-\alpha)^i} = \sum_{j=0}^{u-1}(\alpha^i)^j \in \mathbb{Z}[\alpha]$ et son inverse est aussi un entier donc c'est une unité.
On peut donc écrire $p = \prod_{\text{pgcd}(p,i)=1}^{i=1} {}^{p^k} u_i(1-\alpha) = u(1-\alpha)^{\varphi(p^k)}$, où $u$ est une unité. Donc $p$ est une puissance $\varphi(k)$-ième de l'idéal $(1-\alpha)$ comme $\varphi(p^k) = [\mathbb{Q}(\alpha) : \mathbb{Q}]$. On a donc une factorisation en termes d'idéaux premiers de $(p)$. □

On peut donc étudier la décomposition des premiers dans un corps cyclotomique :

**Théorème 1.9.** *Soit* $\zeta = e^{\frac{2i\pi}{n}}, K = \mathbb{Q}(\zeta)$ *et* $p$ *premier. On écrit* $n = p^k m$ *avec* $\text{pgcd}(p, m) = 1$. *Alors,*

- *L'indice de ramification de* $p$ *est* $\varphi(p^k) = e$.
- *Le degré d'inertie* $f$ *est l'ordre (multiplicatif) de* $p \mod m$.

*Démonstration.* Le résultat découle immédiatement de la décomposition de $p$ dans $\mathbb{Q}(\alpha)$ et $\mathbb{Q}(\beta)$ en prenant l'extension composée.
Le premier item découle du lemme 1.8 et de la remarque ci-dessus.

Dans $\mathbb{Q}(\beta)$, calculons le degré d'inertie $f$.
On sait que $p$ est non ramifiée dans $\mathbb{Q}(\beta)$ si et seulement si $p$ ne divise pas le discriminant $\mathcal{O}_{\mathbb{Q}(\beta)}$. En effet, grâce au théorème 1.7, on a $\mathcal{O}_{\mathbb{Q}(\beta)} = \mathbb{Z}[\beta]$ et grâce à la proposition 1.6 on a $\text{Disc}(\mathbb{Z}[\beta]) = \text{Disc}(\beta) | n^{\varphi(n)}$. Comme $\text{pgcd}(p, m) = 1$ on peut affirmer que $p$ est non ramifié dans $\mathbb{Q}(\beta)$. On peut donc écrire $p\mathbb{Z}[\beta] = p_1 \dots p_r$ et $rf = \varphi(n)$.

Montrons que $p^f \equiv 1 \mod m$.
Grâce au corollaire 1.3, l'ordre de $p$ est celui de $\sigma_p$. Soit $P$ un idéal au dessus de $p$, par définition $f = [\mathbb{Z}[\beta]/P : \mathbb{Z}/p\mathbb{Z}]$ engendré par le Frobenius $\gamma : x \longmapsto x^p$. Montrons que l'ordre de $\gamma$ et $\sigma_p$ sont égaux.
D'un côté, on a pour tout $k \in \mathbb{Z}, \sigma_p^k = id$ si et seulement si $\beta^{p^k} = \beta$ si et seulement si $p^k \equiv 1 \mod m$. De l'autre, on a $\gamma^k = id$ si et seulement si $\beta^{p^k} \equiv \beta \mod p$.

Soit $l \in \{1, \dots, m\}$ tel que $p^k \equiv l \mod m$, $\beta^{p^k} = \beta^l \equiv \beta \mod P$.
Donc $\beta^{l-1} \equiv 1 \mod P$ car $\beta$ est une unité.
Or, on sait que $(1-\beta)\dots(1-\beta^{n-1}) = n$ (en prenant la dérivée de $X^n$-1 en 1). De ce fait, la condition $\text{pgcd}(m, p) = 1$ impose $l = 1$.
Ainsi, pour tout $k \in \mathbb{Z}$, $\beta^{p^k} \equiv \beta \mod p$ si et seulement si $p^k \equiv 1 \mod m$.
De tout cela découle, $\sigma_p^k = id$ si et seulement si $\gamma^k = id$ donc :

$$\text{ordre}(\gamma) = \text{ordre}(\sigma_p) = f.$$

Maintenant, on se place dans $K$. Considérons des premiers $\mathfrak{P}_1, \dots, \mathfrak{P}_r$ au dessus de $P_1 \dots P_r$ respectivement. Alors, chaque $\mathfrak{P}_i$ est au dessus de $p$ donc $(1-\alpha)$. De ce fait, $p\mathbb{Z}[\alpha] = (1-\alpha)^{\varphi(k)}$. On a donc :

- $e(\mathfrak{P}_i | p) \geq e(1-\alpha | p) = \varphi(p^k)$.
- $f($
  $mathfrakP_i | p) \geq f(P_i | p) = f$ or $rf = \varphi(n)$.

Donc $\varphi(p^k) rf = \varphi(n)$ et les inégalités sont des égalités. Enfin, les $\mathfrak{P}_i$ sont les seuls premiers au dessus de $p$ et on a le résultat. □

# 2 Théorie du corps de classes

Nous faisons un rappel succint de la théorie du corps de classes. Nous en profitons pour l'évoquer dans le cas local puis global. Dans le second cas nous essayons de présenter le point de vue historique (par les idéaux) et du point de vue moderne (point de vue adélique).

## 2.1 Théorie du corps de classes locale

Dans cette partie, nous allons énoncer la théorie locale du corps de classes. Nous renvoyons à [3] et [10] pour les démonstrations. On supposera que $L/K$ est une extension galoisienne abélienne de corps locaux de groupe de Galois $G$.

**Définition 2.1.** *Soit $H \subset K^*$ un sous-groupe, $H$ est un groupe de normes s'il existe $L/K$ une extension abélienne finie telle que $H = N_{L/K}(L^*)$.*

**Définition 2.2.** *On appelle groupe résiduel des normes (ou de cohomologie d'ordre 0) $H^0(\mathrm{Gal}(L/K); L^*)$, le groupe quotient $K^*/N_{L/K}(L^*)$.*

**Définition 2.3.** *Une application $f : G \to L^*$ est un 1-cocycle si pour tout $\sigma, \tau \in G$, $f(\sigma\tau) = f(\sigma).\sigma f(\tau)$. L'ensemble des 1-cocycle est un groupe abélien $Z^1(G, L^*)$.*
*On notera $B^1(G, L^*) = \{f_a \in Z^1(G, L^*), f_a(\sigma) = \frac{\sigma(a)}{a}\}$ le groupe des 1-cobords.*

**Remarque 2.4.** *On pourrait aussi adopter une notation exponentielle en posant $\sigma(f(\tau)) = f(\tau)^\sigma$, alors on aurait $f(\sigma\tau) = f(\sigma).f(\tau)^\sigma$.*

**Définition 2.5.** *On notera $H^1(G, L^*) = Z^1(G; L^*)/B^1(G; L^*)$ le premier groupe de cohomologie.*

Nous serons dans un cas qui respecte l'axiome du corps de classes :

**Théorème 2.6** (Axiome du corps de classes)**.** *Si $L/K$ est une extension cyclique finie d'un corps local alors $\#H^0(\mathrm{Gal}(L/K); L^*) = [L : K]$ et $\#H^1(\mathrm{Gal}(L/K); L^*) = 1$*

*Démonstration.* Voir [3]. □

**Théorème 2.7** (Loi de réciprocité locale)**.** *Pour toute extension galoisienne $L/K$ d'un corps local $K$, on a l'isomorphisme canonique : $r_{L/K}$ : $Gal(L/K)^{ab} \to K^*/N_{L/K}L^*$ où $Gal(L/K)^{ab}$ est le groupe de galois de l'extension abélienne maximale.*

*Démonstration.* Voir [3]. □

**Théorème 2.8** (de Correspondance ou d'Existence)**.** *L'application $L \mapsto \mathcal{N}_L = N_{L/K}L^*$ est une correspondance bijective entre les extensions abéliennes finies $L$ d'un corps local $K$ et les sous-groupes d'indices finis de $K^*$. De plus, on a $L_2 \subset L_1$ si et seulement si $\mathcal{N}_{L_2} \subset \mathcal{N}_{L_1}$.*

*Démonstration.* Voir [3]. □

**Proposition 2.9** (Caractérisation des groupes de normes)**.** *Un sous-groupe de $K^*$ est un groupe de normes si et seulement s'il est fermé et d'indice fini.*

*Démonstration.* Voir [3]. □

## 2.2 Théorie de Kummer

La théorie de Kummer donne une description de extensions abéliennes d'un corps contenant suffisamment de racines de l'unité.
Soit $K$ un corps de nombres contenant le groupe $\mu_n$ des racines $n$-ième de l'unité où $n \in \mathbb{N}^*$ et $n$ est premier à la caractéristique de $K$ (si elle est positive).

**Définition 2.10.** *Une extension de Kummer est une extension de la forme $L = K(\sqrt[n]{\Delta})$ avec $\Delta \subset K^*$ un sous-groupe contenant $K^{*n}$ le groupe des puissances $n$-ième.*

On en profite pour faire un rappel :

**Définition 2.11.** *Soit $G$ un groupe.*
*L'ensemble $\{n \in \mathbb{Z}$ tel que pour tout $x \in G, x^n = 1\}$ est un sous-groupe de $(\mathbb{Z}, +)$ donc il existe un unique générateur $k \in \mathbb{N}$.*
*L'élement $k$ sera nommé exposant de $G$.*

**Remarque 2.12.** *La caractéristique d'un corps est l'exposant de son groupe additif.*

Une extensions de Kummer $L/K$ est abélienne d'exposant $n$ si et seulement si son groupe de Galois $G = \mathrm{Gal}(L/K)$ est abélien et pour tout $\sigma \in G$, $\sigma^n = 1$. En fait, pour chaque $a \in \Delta$, la sous-extension $K(\sqrt[n]{a})/K$ est cyclique de degré divisant $n$ donc la restriction de $\sigma^n$ à $K(\sqrt[n]{\Delta})$ est 1 donc $\sigma^n = 1$. Réciproquement, on a :

**Proposition 2.13.** *Si $L/K$ est abélienne d'exposant $n$ alors $L = K(\sqrt[n]{\Delta})$ avec $\Delta = L^{*n} \bigcap K^*$*

*Démonstration.* On a $K(\sqrt[n]{\Delta}) \subset L$.
De l'autre côté, $L/K$ est le compositum de ses sous-extensions cycliques. Plus précisément, $L/K$ est le compositum de ses sous-extensions finies $L'/K$ et le groupe fini abélien $\mathrm{Gal}(L'/K)$ est un produit direct de groupe cyclique où chaque terme du produit peut être vu comme le groupe de Galois d'une sous-extensions cycliques de $L'/K$. Donc, $L'/K$ est le compositum de ses sous-extensions cycliques.

Maintenant, soit $M/K$ une sous-extension cyclique de $L/K$.
Alors, le groupe $\mathrm{Gal}(M/K)$ est d'ordre divisant $n$ donc $M = K(\sqrt[n]{a})$ avec $a \in K^* \cap L^{*n}$. Donc $M \subset K(\sqrt[n]{\Delta})$ et de plus, $L \subset K(\sqrt[n]{\Delta})$. □

On énonce un résultat classique :

**Théorème 2.14.** *(90 d'Hilbert)*
*Soit $L/K$ une extension galoisienne finie de groupe de Galois $G$. Alors le groupe multiplicatif $L^*$ est un $G$-module et $H^1(G, L^*) = \{1\}$.*
*En particulier, si $G$ est cyclique et $\sigma$ un générateur de $G$ alors $\forall a \in L^*$ tel que $N_{L/K}(a) = 1$ on a $a = \frac{\sigma(b)}{b}, b \in L^*$.*

*Démonstration.* Commençons par un lemme :

**Lemme 2.15** (Lemme de Dedekind)**.** *Soit $G$ un groupe, $K$ un corps et $(\sigma_i)_{1 \leq i \leq n}$ des homomorphismes distincts de $G$ dans $K^*$.*
*Alors les $\sigma_1, \ldots, \sigma_n$ sont linéairement indépendants sur $K$.*

*Démonstration du lemme.* Par l'absurde, supposons qu'il existe des éléments $z_1, \ldots, z_n \in K$ non tous nuls tel que $\sum_{i=1}^n z_i \sigma_i = 0$. Choissions une relation de dépendance minimale (pour le nombre de $i$ tel que $z_i \neq 0$).
Quitte à renuméroter, on peut supposer que $\sum_{i=1}^q z_i \sigma_i = 0$ est cette relation. On a $q \geq 2$ car les $\sigma_i$ sont non tous nuls. De plus, pour tout $g, h \in G$, on a :

$$0 = \sum z_i \sigma_i(gh) - \sigma_1(h)(\sum z_i \sigma_i(g)) \quad = \sum_{2 \leq i \leq q} z_i(\sigma_i(h) - \sigma_1(h))\sigma_i(g)$$

Cela étant vrai pour tout $g$ et $q$ étant minimum, on a en particulier $z_2(\sigma_2(h) - \sigma_1(h)) = 0$. Par minimalité, $z_2 \neq 0$ donc $\sigma_1(h) = \sigma_2(h)$ pour tout $h$, on obtient donc une contradiction. □

Soit $f : G \to L^*$ un 1-cocycle. Pour $c \in L^*$, on pose $\alpha = \sum_{\sigma \in G} f(\sigma)\sigma c$. Grâce au lemme 2.15, on peut choisir $c \in L^*$ tel que $\alpha \neq 0$.
Pour $\tau \in G$, $\tau\alpha = \sum_\sigma \tau f(\sigma)(\tau\sigma c) = \sum_\sigma f(\tau)^{-1} f(\tau\sigma)(\tau\sigma c) = f(\tau)^{-1}\alpha$ donc $f(\tau) = \frac{\tau\alpha^{-1}}{\alpha^{-1}}$. De plus, $f \in B^1(G, L^*)$ donc $H^1(G, L^*) = \{1\}$.

Maintenant si $G =< \sigma >$ est cyclique, grâce au fait que si $G$ est fini et cyclique alors $H^1(G, L^*) = \{1\}$ alors $\forall a \in L^*$ tel que $N_{L/K}(a) = 1$, on a $a = \frac{\sigma(b)}{b}, b \in L^*$. □

On va maintenant énoncer le théorème central pour la théorie de Kummer :

**Théorème 2.16.** *Les extensions de Kummer $L/K$ sont en bijection avec les sous-groupes $\Delta$ de $K^*$ contenant $K^{*n}$.*
*Si $L = K(\sqrt[n]{\Delta})$ alors $\Delta = L^{*n} \cap K^*$ et on un a un isomorphisme* $\mathrm{Hom}(Gal(L/K), \mu_n) \cong \Delta/K^{*n}$.
*Un élement $a \bmod K^{*n} \in \Delta/K^{*n}$ est associé au caractère*

$$\begin{array}{rccc} \chi_a : \mathrm{Gal}(L/K) & \longrightarrow & \mu_n \\ \sigma & \longmapsto & \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}} \end{array}$$

**Remarque 2.17.**

- *La composée de deux extensions de Kummer (d'exposant $n$) est encore une extension de Kummer.*
- *Toutes les extensions de Kummer d'exposant $n$ sont contenues dans l'extension de Kummer maximale $\tilde{K} = K(\sqrt[n]{K^*})$ d'exposant $n$ et on a* $\mathrm{Hom}(Gal(\tilde{K}/K), \mu_n) \cong K^*/K^{*n}$.

*Démonstration.* Soit $L/K$ une extension de Kummer alors $L = K(\sqrt[n]{\Delta})$ en vertu de la proposition précédente. On peut ainsi définir le morphisme

$$\begin{array}{rcl} \Delta & \longrightarrow & \mathrm{Hom}(\mathrm{Gal}(L/K), \mu_n) \\ a & \longmapsto & \chi_a. \end{array} \quad \text{avec} \quad \begin{array}{rcl} \chi_a : \mathrm{Gal}(L/K) & \longrightarrow & \mu_n \\ \sigma & \longmapsto & \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}} \end{array} .$$

Le noyau de cette application est $K^{*n}$ car

$$\begin{aligned} \chi_a = 1 \text{ si et seulement si } \sigma(\sqrt[n]{a}) &= \sqrt[n]{a}, \text{ pour tout } \sigma \in Gal(L/K) \\ \text{si et seulement si } \sqrt[n]{a} &\in K^* \\ \text{si et seulement si } a &\in K^{*n} \end{aligned}$$

On obtient un morphisme injectif $\Delta/K^{*n} \to \mathrm{Hom}(\mathrm{Gal}(L/K), \mu_n)$. Grâce au théorème 2.14, il existe $b \in L^*$ tel que $\chi(\sigma) = \frac{\sigma b}{b}$, pour tout $\sigma$ dans $\mathrm{Gal}(L/K)$.

On a pour tout $\sigma \in \mathrm{Gal}(L/K), \sigma(b^n) = (\sigma b)^n = \chi(\sigma)^n b^n = b^n$ on voit donc que $b^n = a \in K^* \cap L^{*n} = \Delta$ donc $\chi = \chi_a$.

Si $\Delta$ est n'importe quel groupe entre $K^*$ et $K^{*n}$ et si on pose $L = K(\sqrt[n]{\Delta})$ alors on a nécessairement $\Delta = L^{*n} \bigcap K^*$.
En effet, soit $\Delta' = L^{*n} \cap K^*$, on voit que $\Delta'/K^{*n} \cong Hom(Gal(L/K), \mu_n)$.
Le sous-groupe $\Delta/K^{*n}$ est associé au sous-groupe $\mathrm{Hom}(Gal(L/K)/H, \mu_n)$ inclus dans $\mathrm{Hom}(Gal(L/K), \mu_n)$ avec $H = \{\sigma \in \mathrm{Gal}(L/K)$ tel que $\chi_a(\sigma) = \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}, \forall a \in \Delta\}$.

Comme $\sigma(\sqrt[n]{a}) = \chi_a(\sigma)\sqrt[n]{a}$ on voit que $H$ fixe les élements de $\sqrt[n]{\Delta}$.
Du fait que L est engendré par $\sqrt[n]{\Delta}$ on a $H = 1$ et on a :

$$\mathrm{Hom}(\mathrm{Gal}(L/K)/H, \mu_n) = \mathrm{Hom}(\mathrm{Gal}(L/K), \mu_n) \text{ donc } \Delta/K^{*n} = \Delta'/K^{*n}.$$

En conclusion, $\Delta = \Delta'$ prouvant ainsi notre théorème. □

## 2.3 Théorie globale avec les idéaux

On rappelle la théorie globale du corps de classe. Pour cela, on suit ici le déroulement du chapitre VIII de [2] et pour les démonstrations manquantes nous renvoyons à [3].

**Proposition 2.18.** *Soient $L/K$ une extension galoisienne de corps de nombres, $\mathfrak{p}$ un idéal premier non ramifié de $L$. Si $\mathfrak{P}|\mathfrak{p}$ alors il existe un unique élément $\sigma \in \mathrm{Gal}(L/K)$ tel que :*
*Pour tout $\alpha \in \mathcal{O}_L$, $\sigma(\alpha) \equiv \alpha^{N(p)} \mod \mathfrak{P}$ avec $N(\mathfrak{p}) = |\mathcal{O}_K/\mathfrak{p}|$.*

**Définition 2.19.** *Cet unique élément $\sigma \in \mathrm{Gal}(L/K)$, qui est unique, s'appelle le symbole d'Artin. On le notera $\left(\frac{L/K}{\mathfrak{P}}\right)$ avec $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$.*

*Démonstration.*
Soient $D_{\mathfrak{P}}$ le groupe de décomposition et $I_{\mathfrak{P}}$ le groupe d'inertie pour $\mathfrak{P}$. On rappelle que si $\sigma \in D_{\mathfrak{P}}$, il induit $\tilde{\sigma} \in \tilde{G}$ avec $\tilde{G} = \mathrm{Gal}(\mathcal{O}_L/\mathfrak{P}/\mathcal{O}_K/\mathfrak{p})$ or si $\mathfrak{p}$ est non ramifié dans $L$, on sait que l'indice de ramification $e_{\mathfrak{P}|\mathfrak{p}}$ de $p$ est égal au cardinal du groupe d'inertie (ici 1). De plus, $|D_{\mathfrak{P}}| = e_{\mathfrak{P}|\mathfrak{p}} f_{\mathfrak{P}|\mathfrak{p}}$.
On a donc un isomorphisme $D_{\mathfrak{P}} \cong \tilde{G}$. Mais si $q = |\mathcal{O}_K/\mathfrak{p}|$ alors $\tilde{G}$ est cyclique. Il admet un générateur canonique qui est donné par l'automorphisme de Frobenius.
Ainsi, il existe un unique $\sigma \in D_{\mathfrak{P}}$ est envoyé sur l'élément de Frobenius. Or $q$ est la norme de $p$ par définition, alors $\sigma$ satisfait $\sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \mod \mathfrak{P}$. □

Dans le cas d'une extension abélienne le symbole d'Artin ne dépend que de $p$. Cela nous permet de définir :

**Définition 2.20.** *On définit l'application d'Artin :*
$\left(\frac{L/K}{\cdot}\right) : I_K \to \mathrm{Gal}(L/K)$
$\mathfrak{a} = \prod_{i=1}^r \mathfrak{p}_i^{r_i} \in I_K \mapsto \left(\frac{L/K}{\mathfrak{a}}\right) = \prod_{i=1}^r \left(\frac{L/K}{\mathfrak{p}_i}\right)^{r_i}$

**Définition 2.21.** *Soit $K$ un coprs de nombres, on appelle module $\mathfrak{m}$ dans $K$ le produit formel $\mathfrak{m} = \prod_p p^{n_p}$ sur toutes les places $p$, finies ou infinies, de $K$ où :*

- *$n_p \geq 0$ pour un nombre fini de places.*
- *$n_p = 0$ si $p$ est une place infinie et complexe.*
- *$n_p \leq 1$ si $p$ est une place réelle et infinie.*

*On pourra toujours écrire $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ avec $\mathfrak{m}_0$ un idéal de $\mathcal{O}_K$ et $\mathfrak{m}_\infty$ est un produit distinct de place réelle et infinie.*

**Remarque 2.22.** *Si $K$ est un corps quadratique purement imaginaire, on pourra voir un module comme un idéal de $\mathcal{O}_K$.*

**Définition 2.23.** *Soit $\mathfrak{m}$ un module de $K$. On note $I_K(\mathfrak{m})$ le groupe des idéaux fractionnaires de $\mathcal{O}_K$ premiers avec $\mathfrak{m}$ (donc avec $\mathfrak{m}_0$).*
*Le sous-groupe $P_{K,1}(\mathfrak{m}) \subset I_K(\mathfrak{m})$ d'indice fini est engendré par les idéaux principaux de $\alpha\mathcal{O}_K, \alpha \in \mathcal{O}_K$ satisfaisant $\alpha \equiv 1 \mod \mathfrak{m}_0$ et si $\sigma|\mathfrak{m}_\infty$ alors $\sigma(\alpha) > 0$.*

**Définition 2.24.** *Un sous-groupe $H \subset I_K(\mathfrak{m})$ est un sous-groupe de congruence pour $\mathfrak{m}$ s'il satisfait $P_{K,1}(\mathfrak{m}) \subset H \subset I_K(\mathfrak{m})$.*

**Remarque 2.25.** *Le quotient $I_K(\mathfrak{m})/H$ s'appelle groupe des classes d'idéaux généralisés pour $\mathfrak{m}$.*

Soit $\mathfrak{m}$ un module divisible par tous les premiers ramifiés d'une extension abélienne $K \subset L$. Prenons $\mathfrak{p}$ un premier ne divisant pas $\mathfrak{m}$, on peut définir comme précédemment le symbole d'Artin $(\frac{L/K}{\mathfrak{p}})$ et l'application d'Artin $\left(\frac{L/K}{\cdot}\right)_\mathfrak{m} : I_K(\mathfrak{m}) \to \mathrm{Gal}(L/K)$ pour $K \subset L$ et $\mathfrak{m}$.

**Théorème 2.26.** *Soit $L/K$ une extension abélienne et soit $\mathfrak{m}$ un module divisible par tous les premiers de $K$, finis ou infinis, se ramifiant dans $L$. Alors, on a :*

- *$\left(\frac{L/K}{\cdot}\right)_\mathfrak{m}$ est surjective.*
- *Si tout les exposants des premiers finis divisant $\mathfrak{m}$ sont assez grand, alors $\mathrm{Ker}\left(\frac{L/K}{\cdot}\right)_\mathfrak{m}$ est un sous-groupe de congruence pour $\mathfrak{m}$.*

*Et par conséquent, on a l'isomorphisme $I_K(\mathfrak{m})/\mathrm{Ker}\left(\frac{L/K}{\cdot}\right)_\mathfrak{m} \to \mathrm{Gal}(L/K)$ montrant que $\mathrm{Gal}(L/K)$ est un groupe de classe d'idéaux généralisé pour le module $\mathfrak{m}$.*

*Démonstration.* Voir [3]. □

**Théorème 2.27.** *Soit $L/K$ une extension abélienne. Alors il existe un module $\mathfrak{f} = \mathfrak{f}(L/K)$ tel que :*

- *Un premier de $K$, fini ou infini se ramifie dans $L$ si et seulement s'il divise $\mathfrak{f}$.*
- *Soit $\mathfrak{m}$ un module divisible par tous les premiers de $K$ se ramifiant dans $L$.*
  *Alors, $\mathrm{Ker}\left(\frac{L/K}{\cdot}\right)_{\mathfrak{m}}$ est un sous-groupe de congruence pour $\mathfrak{m}$ si et seulement si $\mathfrak{f}|\mathfrak{m}$.*

*Démonstration.* Voir [3]. □

**Définition 2.28.** *Le module $\mathfrak{f}(L/K)$ du théorème 2.27 est le conducteur de $L/K$.*

**Théorème 2.29.** *Soit $\mathfrak{m}$ un module de $K$ et soit $H$ un sous-groupe de congruence pour $\mathfrak{m}$.*
*Alors, il existe une unique extension abélienne $L$ de $K$ pour laquelle tous les premiers ramifiés divisent $\mathfrak{m}$ tel que si $\left(\frac{L/K}{\cdot}\right)_{\mathfrak{m}}$ est l'application d'Artin pour $L/K$ alors $H = \mathrm{Ker}\left(\frac{L/K}{\cdot}\right)_{\mathfrak{m}}$.*

*Démonstration.* Voir [3]. □

**Corollaire 2.30.** *Soit $L$ et $M$ des extensions abéliennes de $K$.*
*Alors $L \subset M$ si et seulement s'il existe $\mathfrak{m}$ un module divisible par tous les premiers de $K$ se ramifiant dans $L$ ou $M$ tel que $P_{K,1}(\mathfrak{m}) \subset \mathrm{Ker}\left(\frac{L/K}{\cdot}\right)_{\mathfrak{m}} \subset \mathrm{Ker}\left(\frac{M/K}{\cdot}\right)_{\mathfrak{m}}$*

*Démonstration.* Supposons $L \subset M$ et $r : \mathrm{Gal}(M/K) \to \mathrm{Gal}(L/K)$ application de restriction. Grâce au théorème 2.26, on sait qu'il existe $\mathfrak{m}$ pour lequel $\left(\frac{M/K}{\cdot}\right)_{\mathfrak{m}}$ et $\left(\frac{L/K}{\cdot}\right)_{\mathfrak{m}}$ sont des sous-groupes de congruence pour $\mathfrak{m}$.
On a $r \circ \left(\frac{M/K}{\cdot}\right)_{\mathfrak{m}} = \left(\frac{L/K}{\cdot}\right)_{\mathfrak{m}}$ donc $\mathrm{Ker}\left(\frac{M/K}{\cdot}\right)_{\mathfrak{m}} \subset \mathrm{Ker}\left(\frac{L/K}{\cdot}\right)_{\mathfrak{m}}$.

Réciproquement, supposons que $P_{K,1}(\mathfrak{m}) \subset \mathrm{Ker}\left(\frac{M/K}{\cdot}\right)_{\mathfrak{m}} \subset \mathrm{Ker}\left(\frac{L/K}{\cdot}\right)_{\mathfrak{m}}$. Alors, sous $\left(\frac{M/K}{\cdot}\right)_{\mathfrak{m}}$, le sous-groupe $\mathrm{Ker}\left(\frac{L/K}{\cdot}\right)_{\mathfrak{m}} \subset I_K(\mathfrak{m})$ s'envoie sur un sous-groupe $H \subset \mathrm{Gal}(M/K)$. Grâce à la théorie de Galois, $H$ correspond à un corps intermédiaire $K \subset \tilde{L} \subset M$. En appliquant le début pour $\tilde{L} \subset M$, on obtient $\mathrm{Ker}\left(\frac{\tilde{L}/K}{\cdot}\right)_{\mathfrak{m}} = \mathrm{Ker}\left(\frac{L/K}{\cdot}\right)_{\mathfrak{m}}$. Grâce à l'unicité du théorème 2.29, on conclut $L = \tilde{L} \subset M$. □

Pour finir, on peut maintenant définir $L$ le corps de classe de $K$.
En appliquant le théorème 2.29 au module $\mathfrak{m} = 1$, on a $P_K = P_{K,1}(\mathfrak{m}) \subset I_K$.
Il existe une unique extension abélienne $L$ de $K$ non ramifiée car $\mathfrak{m} = 1$ tel que l'application d'Artin induit un isomorphisme :
$C(\mathcal{O}_K) = I_K/P_K \to \mathrm{Gal}(L/K)$.

**Définition 2.31.** *L'extension $L$ est le corps de classe de $K$.*

On définit enfin le corps de classe de rayon pour le module $\mathfrak{m}$ :

**Définition 2.32.** *Pour $K$ un corps de nombre (grâce au théorème 2.29) il existe une extension abélienne $K_\mathfrak{m}$ de $K$ tel que $P_{K,1}(\mathfrak{m}) \subset \mathrm{Ker}\left(\frac{K_\mathfrak{m}/K}{\cdot}\right)_\mathfrak{m}$.*
*$K_\mathfrak{m}$ est le corps de classe de rayon de $K$ pour le module $\mathfrak{m}$.*
*Pour $\mathfrak{m} = 1$, $K_\mathfrak{m}$ est le corps de classe de Hilbert de $K$. On rappelle que c'est l'extension abélienne non ramifié maximale de $K$.*

## 2.4 Théorie globale avec les adèles

Soit $L/K$ une extension finie, on a l'application norme $N_{L/K} : L^* \to K^*$ qui s'étend aux idéaux (fractionnaires) $N_{L/K} : I_L \to I_K$. Si $L/K$ est une extension abélienne et $\mathfrak{m}$ un module pour lequel $P_{K,1}(\mathfrak{m}) \subset \mathrm{Ker}\left(\frac{L/K}{\cdot}\right)_\mathfrak{m}$, le théorème 2.26 établit :

$$\mathrm{Ker}\left(\frac{L/K}{\cdot}\right)_\mathfrak{m} = N_{L/K}(I_L(\mathfrak{m}))P_{K,1}(\mathfrak{m})$$

On rappelle la définition du groupe d'idèles :

**Définition 2.33.** *Soit $K$ un corps de nombres, on appelle groupe des idèles de $K$, noté $\mathbb{I}_K$, le produit restreint $\mathbb{I}_K = \prod_p K_p^*$ avec $p$ premier et $K_p$ la complétion de $K$.*
*Le produit est restreint car pour $(x_p) \in \mathbb{I}_K$, on a un nombre fini de $p$ tel que $x_p \in \mathcal{O}_{K_p}$.*
*$\mathbb{I}_K$ est un groupe localement profini et le groupe multiplicatif $K^*$ s'injecte naturellement dans $\mathbb{I}_K$ comme groupe discret.*

On introduit l'analogue du groupe des classes pour des idèles.

**Définition 2.34.** *On appelle groupe des classes d'idèles le groupe*
$C_K = \mathbb{I}_K/K^*$

On reformule la théorie du corps de classes en termes d'idèles. Grâce à l'application d'Artin $\left(\frac{L/K}{\cdot}\right) : C_K \to \mathrm{Gal}(L/K)$ est surjective et continue. De plus, $\mathrm{Ker}\left(\frac{L/K}{\cdot}\right)$ est un sous-groupe fermé d'indice fini de $C_K$.
On a donc une correspondance $1-1$ entre les extensions abéliennes finies de $K$ et les sous-groupes fermés d'indice fini.
Ainsi, on peut étendre la norme aux groupes de classes d'idèles

$N_{L/K} : C_L \to C_K$ et le noyau de $\left(\frac{L/K}{\cdot}\right) : C_K \to \mathrm{Gal}(L/K)$ est $N_{L/K}(C_L)$. De plus, les sous-groupes de $C_K$ qui sont fermés et d'indice finis correspondent exactement aux groupes de normes.

# 3 Théorème de Kronecker-Weber

Nous proposons ici deux démonstrations pour établir le théorème de Kronecker-Weber. On commencera par une preuve utilisant des arguments locaux pour arriver à théorie locale. La seconde utilisera des arguements globaux et invoquera les corps de classe de rayon, ce qui sera plus conforme à nos raisonnements quand nous introduirons la multiplication complexe. La principale référence de cette partie est [3].

Nous nous intéressons au résultat suivant qui s'énonçait historiquement :

**Théorème 3.1.** *Soit $K/\mathbb{Q}$ une extension abélienne finie alors on a pour un certain $n \in \mathbb{N}$ $K \subset \mathbb{Q}(\zeta_n)$.*

On renvoie à l'annexe 11 pour les définitions et les notions topologiques. En posant $\mathbb{Q}^{ab}$ l'extension abélienne maximale, on peut le reformuler :

**Théorème 3.2** (Kronecker-Weber global)**.** *On a $\mathbb{Q}^{ab} = \bigcup_{n\in\mathbb{N}^*} \mathbb{Q}(\zeta_n)$.*
*Ainsi, on a $\mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q}) \simeq \hat{\mathbb{Z}}^* = \varprojlim(\mathbb{Z}/n\mathbb{Z})^*$.*

Dans l'annexe 11, on montre que si $\overline{\mathbb{Q}}$ est une clôture algébrique de $\mathbb{Q}$, alors $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ est isomorphe à $\varprojlim \mathrm{Gal}(K/\mathbb{Q})$ où $K$ parcourt les extensions galoisiennes finies de $\mathbb{Q}$. En se restreignant au cas abélien et grâce au corollaire 1.3, en montrant la version historique du théorème de Kronecker-Weber, on aura le théorème 3.2.

## 3.1 Une démonstration de Kronecker-Weber par la théorie locale

### 3.1.1 Préliminaires

On commence par deux résultats basiques en théorie algébrique des nombres :

**Proposition 3.3.** *Soit $A$ un anneau de Dedekind de corps de fraction $K$. Soit $L/K$ une extension finie et séparable. Notons $B$ la clôture intégrale de $A$ dans $L$.*
*Les idéaux premiers de $A$ qui se ramifient dans $B$ coïncident avec les idéaux premiers de $A$ qui divisent le discriminant $d = \mathrm{Disc}(L/K)$.*
*En particulier, il n'y a qu'un nombre fini d'idéaux premiers de $A$ qui sont ramifiés dans $B$.*

*Démonstration.* Soit $A$ un anneau de Dedekind. En vertu du théorème de Dedekind sur la décomposotion en produit d'idéaux premiers et grâce au fait que si $\mathfrak{P}$ un idéal premier de $A$, en notant $\mathcal{D}_{B/A}$ l'idéal engendré par les discriminants des systèmes formés par les bases de $L$ sur $K$ qui seraient dans $B$. On appelle cet idéal le discriminant de $B$ sur $A$ et on sait que

$\mathcal{D}_{B/A}A_{(\mathfrak{P})} = \mathcal{D}_{B_{(\mathfrak{P})}/A_{(\mathfrak{P})}}$ avec $A_{(\mathfrak{P})}$ le localisé de $A$ en $\mathfrak{P}$. Il suffit donc de vérifier localement la proposition.
Supposons que $A$ soit un anneau de valuation discrète et notons $\mathfrak{P}$ l'idéal maximal de $A$. $A$ est principal donc $B$ est libre sur $A$.

Supposons qu'il existe $P$ un idéal maximal de $B$ ramifié. Il existe $x \in B - \mathfrak{P}B$ et $n > 1$ tel que $x^n \in \mathfrak{P}B$. La classe de $\overline{x}$ de $x$ dans $B/\mathfrak{P}B$ est un élément non nul. On sait que $B/\mathfrak{P}B$ est un $A/\mathfrak{P}$-espace vectoriel.
Complétons $\overline{x}$ en une base $(\overline{x} = \overline{x_1}, \ldots, \overline{x_n})$ de $B/\mathfrak{P}$. C'est un réprésentant $(x_1 = x, x_2, \ldots, x_n)$ de cette base dans $B^n$ donc une base de $B$ comme $A$-module.
Pour cela on identifie $B \cong A^n$ et on remarque que la réduction modulo $\mathfrak{P}$ de $\det(x_1, \ldots, x_n)$ dans la base canonique de $A^n$ est non nulle donc ce déterminant est inversible.
Soit $x_0 \in B$, comme $B$ est un $A$-module libre, la trace de l'endomorphisme de $B/\mathfrak{P}B$, $y \longmapsto x_0 y$. est l'image dans $A/\mathfrak{P}$ de la trace de l'endormorphisme de $B$ donné par $y \longmapsto x_0 y$.
On a $(x_1 x_i)^n \in \mathfrak{P}$ pour tout $i$. L'endomorphisme de $B/\mathfrak{P}B$ donné par $y \mapsto y(\overline{x_1} x_i)$ est donc nilpotent. De ce fait, sa trace est nulle. Ainsi, le déterminant $\det(Tr(x_i x_j))$ est dans $\mathfrak{P}$ donc $\mathcal{D}_{B/A} \subset \mathfrak{P}$.

Réciproquement, supposons que tout idéal premier de $B$ divisant $\mathfrak{P}$ soit non ramifié. On a un isomorphisme de $A$-modules :
$B/\mathfrak{P}B \cong \bigoplus_{i=1}^{n} B/P_i$ où $(P_i)$ sont les idéaux premiers de $B$ divisant $\mathfrak{P}$. Soient $(\alpha_i)_{1 \leq i \leq n}$ des bases des $A/\mathfrak{P}$-espaces vectoriels $(B/P_i)_{1 \leq i \leq n}$. Elles définissent grâce à l'isomorphisme ci-dessus une base $\alpha$ de $B/\mathfrak{P}B$.
Dans cette base, la matrice de l'endomorphisme de $B/\mathfrak{P} \to B/\mathfrak{P}, y \mapsto x_0 y$ est une matrice par blocs ($x_0 \in B$). Le discriminant du système formé par la base $\alpha$ est donc le produit des discriminants $\mathcal{D}_{\rangle}$ des systèmes formés par les $\alpha_i$. Chacun de ces discriminants est non nul car les extensions des corps résiduels sont séparables. Leur produit est donc non nul.
La base $\alpha$ est la réduction modulo $\mathfrak{P}$ d'une base de $B$ sur $A$. La réduction modulo $\mathfrak{P}$ du discriminant du système formé par cette base est donc égal au discriminant du système formé par la base $\alpha$. Ce dernier discriminant est non nul. Le discriminant de $B/A$ n'est donc pas contenu dans $\mathfrak{P}$ achevant ainsi la démonstration. □

On établit un lemme global sur la ramification :

**Lemme 3.4.** *Si $F/\mathbb{Q}$ est une extension avec aucune place ramifiée finie alors $F = \mathbb{Q}$*

*Démonstration.*
On admet l'existence d'un idéal entier de norme $\frac{n!}{n^n}(\frac{4}{\pi})^{r_2}\sqrt{|d_F|}$ si on a posé $n = [F : \mathbb{Q}]$ et $d_F$ la valeur absolue du discriminant et $r_2 \leq \frac{n}{2}$ le nombre de

places complexes. Cette quantité est supérieure (ou égale) à 1 donc

$$\sqrt{d_F} \geq \frac{n^n}{n!}(\frac{\pi}{4})^{r_2} \geq \frac{n^n}{n!}(\frac{n}{4})^{\frac{n}{2}} = b_n$$

Comme $b_2 > 1$ et $\frac{b_{n+1}}{b_n} = (1+\frac{1}{n})^n\sqrt{\frac{\pi}{4}} \geq 2\sqrt{\frac{\pi}{4}} > 1$

Si $n \geq 2$, on a $d_F > 1$, grâce à la proposition 3.3 il existe donc $p|d_F$ si et seulement si $p$ se ramifie donc $[F : \mathbb{Q}] = 1$. □

Soit $K$ un corps local de corps résiduel fini que l'on notera $k_K$ , $\mathfrak{m}_K$ son idéal maximal et $\pi$ une uniformisante. Notons $U_K^{(n)} = 1 + \mathfrak{m}_K^n$, la caractéristique du corps résiduel sera $p$ et $q$ son cardinal. On supposera, de plus, que la valuation $v_K$ est normalisée i.e $v_K(K^*) = \mathbb{Z}$.

**Proposition 3.5.** *On a la décomposition $K^* = (\pi) \times \mu_{q-1} \times U_K^{(1)}$ avec $\mu_{q-1}$ le groupe des racines primitives $(q-1)-$ième de l'unité.*
*De plus, on a la chaîne $\cdots \subset U_K^{(2)} \subset U_K^{(1)} \subset U_K$ tel que $U_K/U_K^{(1)} \simeq k_K^*$ et $U_K^{(n)}/U_K^{(n+1)} \simeq k_K$*

*Démonstration.* Si $a \in K^*$, $a$ possède une décomposition unique en $a = \prod v_K(a)u, u \in U_K$. Le groupe $U_K$ contient le groupe $\mu_{q-1}$ car le lemme d'Hensel permet d'affirmer que le polynôme $X^{q-1} - 1 = 0$ est scindé sur $K$. Le morphisme $U_K \to k_K^*, u \mapsto u \mod \mathfrak{m}_K$ envoie bijectivement $\mu_{q-1}$ sur $k_K^*$. Il est de noyau $U_K^{(1)}$. Ceci montre que $U_K = \mu_{q-1} \times U_K^{(1)}$ et $U_K/U_K^{(1)} \cong k_K^*$. De plus, on a un homomorphisme surjectif :

$$U_K^{(n)} \to k_K, (1 + a\pi^n) \mapsto a \mod \mathfrak{m}_K$$

dont le noyau est $U_K^{(n+1)}$ donc $U_K^{(n)}/U_K^{(n+1)} \cong k_K$. □

**Proposition 3.6.** *Si $K$ est une extension finie de $\mathbb{Q}_p$, si $e = v_K(p)$ et si $n > \frac{e}{p-1}$ alors les séries entières $\exp(x) = \sum_{n\in\mathbb{N}} \frac{x^n}{n!}$ et $\log(1-x) = \sum_{k=1}^{+\infty}(-1)^{k+1}\frac{x^k}{k!}$ donnent des isomorphismes (et des homémorphismes) réciproques :* $\exp : \mathfrak{m}_K^n \to U_K^{(n)}$ *et* $\log : U_K^{(n)} \to m_K^n$

*Démonstration.* Soit $v = v_K$. On pose pour $x \in K, |x| = q^{-\frac{1}{[K:\mathbb{Q}_p]}v_K(x)}$ rappelle que $q = \mathrm{card}(k_K)$.
Soit $x \in K$ tel que $v(x) > \frac{e}{p-1}$ si et seulement si $|x| < p^{-\frac{1}{p-1}}$.
Si $p^r \leq v < p^{r+1}$ et $v \geq 2$ alors :

$$\begin{aligned}\log_p|\frac{x^v}{v}| - \log_p|x| =& (v-1)\log_p|x| - \log_p|v| \\ &< -\frac{v-1}{p-1} - r < 0.\end{aligned}$$

Ceci montre que $\frac{x^v}{v} \to 0$ si $v \to +\infty$ et $|\frac{x^v}{v}| < |x|$.
Donc la série $\log(1+x)$ converge et vérifie $v(\log(1+x)) = v(x)$.
Ainsi, si $n > \frac{e}{p-1}$ alors log envoie $U_K^{(n)}$ sur $\mathfrak{m}_K^n$.

D'un autre côté, considérons maintenant les termes $|\frac{x^v}{v}|$. En écrivant $v = \sum_{0 \leq k \leq r} a_k p^k$ avec pour tout $0 \leq i \leq r$, $0 \leq a_i \leq p-1$.
Pour considérer la série exponentielle, on va montrer que :

$$val_p(v!) = \frac{E(v - (a_0 + \cdots + a_r))}{p-1} \text{ avec } E(.) \text{ la partie entière.}$$

En effet, $E(\frac{v}{p}) = a_1 + \cdots + a_r p^{r-1}$ et $E(\frac{v}{p^2}) = a_2 + \cdots + a_r p^{r-2}$, $E(\frac{v}{p^r}) = a_r$.
Il y a $E(\frac{v}{p})$ élements de $1, 2, \ldots, v$ divisible par $p^i$. En effet, cela est direct vu qu'un tel nombre est de la forme $\alpha p^i \leq v$. On en déduit que :

$$\begin{aligned} val_p(v!) &= E(\frac{v}{p}) + \cdots + E(\frac{v}{p^r}) \\ &= a_1 + (p-1)a_2 + \cdots + (p^r + \cdots + 1)a_r. \end{aligned}$$

De ce fait, on a :

$$\begin{aligned} \text{donc } (p-1)val_p(v!) =& (p-1)a_1 + (p^2-1)a_2 + \cdots + (p^r-1)a_r \\ =& v - (a_0 + \cdots + a_r) \end{aligned}$$

Ceci prouvant le résultat.

Maintenant pour $v(x) > \frac{e}{p-1}$ si et seulement si $|x| < p^{\frac{1}{p-1}}$ et si $v \geq 2$, on a :

$$\begin{aligned} \log_p |\frac{x^v}{v!}| =& v \log_p |x| - \log_p |v!| \\ <& v(\log_p |x| + \frac{1}{p-1}) \end{aligned}$$

et ainsi,

$$\begin{aligned} \log_p |\frac{x^v}{v!}| - \log_p |x| &= (v-1) \log_p |x| - \log_p |v!| \\ &\leq -\frac{v-1}{p-1} - \frac{1}{p-1}(v - (a_0 + \cdots + a_r)) \\ &\leq 0 \end{aligned}$$

Ceci implique que $\frac{x^v}{v!}$ tend vers 0 quand $v \to +\infty$ et pour $v \leq 2, |\frac{x^v}{v!}| < |x|$.
Donc la série exponentielle $\exp(x)$ converge et $v(\exp(x) - 1) = v(x)$.
Ainsi, si $n > \frac{e}{p-1}$ alors exp envoie $\mathfrak{m}_K^n$ sur $U_K^{(n)}$.

De plus, pour $|x|, |y| < p^{-\frac{1}{p-1}}$, on a $\exp(\log(1+x)) = 1 + x$.

$$\begin{aligned}\text{Et } \exp(\log(1+x)) &= 1+x,\\ \log(\exp(x)) &= x,\\ \exp(x+y) &= \exp(x)\times\exp(y) \text{ et}\\ \log((1+x)(1+y)) &= \log(1+x)+\log(1+y).\end{aligned}$$

Ce sont des égalités de séries formelles et toutes ces séries convergent. □

### 3.1.2 Le cas local implique le cas global

**Proposition 3.7.** *Soit $\zeta$ une racine primitive $p^n$-ième de l'unité et soit $K=\mathbb{Q}_p$ et $L=\mathbb{Q}_p(\zeta)$. Alors*

- *$L/K$ est totalement ramifiée de degré $p^{n-1}(p-1)$.*
- *$\lambda=\zeta-1$ est un élément premier de $L$ et $N_{L/K}(-\lambda)=p$.*

*Démonstration.* Tout d'abord, le polynôme cyclotomique $\Phi_n(X)=\frac{X^{p^n}}{X^{p^{n-1}}}=X^{p^{n-1}(p-1)}+\cdots+X^{p^{n-1}}+1$ est irréductible sur $\mathbb{Q}$. On sait que c'est le polynôme minimal de $\zeta$.
De ce fait, $[L:K]=p^{n-1}(p-1)$ et $\Phi_n(X)=\prod_{\sigma\in\mathrm{Gal}(L/K)}(X-\zeta^\sigma)$.

Pour $X=1$, on a $p=\prod_\sigma(1-\zeta^\sigma)=N_{L/K}(1-\zeta^\sigma)$ mais $v_L(1-\zeta^\sigma)=v_L(1-\zeta)$ car $\sigma$ est une isométrie. On a :

$$v_L(1-\zeta)=\frac{v_L(p)}{[L:K]}=\frac{1}{[L:K]}.$$

Donc $L/K$ est une extension totalement ramifiée et $(1-\zeta)$ est premier. □

**Remarque 3.8.** *Le premier item aurait pu se déduire du théorème 1.9 et le deuxième item du lemme 1.5. On choisit ici de respecter la structure du texte original.*

**Théorème 3.9.** *Le groupe de normes de $\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q}_p$ est le groupe $(p)\times U^{(n)}_{\mathbb{Q}_p}$ avec $\mu_{p^n}$ le groupe des racines primitives $p^n$-ième de l'unité.*

*Démonstration.* On pose $K=\mathbb{Q}_p$ et $L=\mathbb{Q}_p(\mu_{p^n})$. Grâce à la proposition 3.5, l'application $a\in\mathfrak{m}_K\longmapsto p^{(s-1)}(p-1)a\in\mathfrak{m}_K^s$ est un isomorphisme.

Grâce à la proposition 3.6, on sait que exp est un isomorphisme pour $\mathfrak{m}_K^v\to U_K^{(v)}$ pour $v\geq 1$ si $p\neq 2$ et $v\geq 2$ si $p=2$.

Comme exp envoie l'application $(a\mapsto p^{s-1}(p-1)a)$ sur l'application $(x\mapsto xp^{s-1(p-1)})$. On en déduit :

- pour $p \neq 2$, on a $(U_K^{(1)})^{p^{n-1}(p-1)} = U_K^{(n)}$.
- pour $p = 2$, si $n > 1$, on a $(U_K^{(2)})^{2^{n-1}} = U_K^{(n)}$ .

Ceci montre que $U_K^{(n)} \subset N_{L/K}L^*$ pour $p \neq 2$.

Pour $p = 2$, le cas $n = 1$ est trivial sinon on remarque que :
$U_K^{(2)} = U_K^{(3)} \cup 5U_K^{(3)} = (U_K^{(2)})^2 \cup 5(U_K^{(2)})^2$. En effet, un nombre congru à 1 mod 4 est soit congru à 1 mod 8 soit congru à 5 mod 8. On a alors, par une récurrence directe, que :
$U_K^{(n)} = (U_K^{(2)})^{2^{n-1}} \cup 5(U_K^{(2)})^{2^{n-1}}$. On a aussi directement que :
$5^{2^{n-2}} = N_{L/K}(2+i)$ donc $U_K^{(n)} \subset N_{L/K}L^*$ pour $p = 2$.

Avec la proposition 3.7, on en déduit que $(p) \times U_K^{(n)} \subset N_{L/K}L^*$. Ces deux derniers groupes étant d'indices $p^{n-1}(p-1)$ dans $K^*$ (par définition ou grâce à la proposition précédente) on en déduit l'égalité $N_{L/K}L^* = (p) \times U_K^{(n)}$. □

Le théorème 2.29 dans le cas local, nous permet de conclure de conclure :

**Corollaire 3.10** (Version locale du théorème 3.2)**.** *Toute extension abélienne finie $L/\mathbb{Q}_p$ est contenue dans un corps $\mathbb{Q}_p(\zeta)$ avec $\zeta$ une racine de l'unité.*

*Démonstration.* On a $(p^f) \times U_{\mathbb{Q}_p}^{(n)} \subset N_{L/\mathbb{Q}_p}L^*$ pour un certain $f$ et un certain $n$. Ainsi, grâce au théorème 2.29 on sait que L est contenu dans un corps de classe $M$ du groupe $(p^f) \times U_{\mathbb{Q}_p}^{(n)} = ((p^f) \times U_{\mathbb{Q}_p}) \cap ((p)) \times U_{\mathbb{Q}_p}^{(n)})$. Le même théorème (et le théorème 1.9) nous dit que $M$ est la composée du corps de classe de $(p^f) \times U_{\mathbb{Q}_p}$ qui est une extension non ramifiée de degré $f$ et le corps de classes de $\mathbb{Q}_p(\mu_{p^n})$ de $(p) \times U_{\mathbb{Q}_p}^{(n)}$.
Donc $M$ est engendré par les $(p^f-1)p^n-$ièmes racines de l'unité. En d'autres termes, $L \subset L(\zeta)$. □

On peut donc maintenant déduire le théorème de Kronecker-Weber :

*Démonstration du théorème 3.2.* Soit $S$ l'ensemble des nombres premiers se ramifiant dans $K$. Grâce à la proposition 3.3 on sait que $S$ est fini. Notons $K_p$ le complété de $K$ par rapport à une extension de $v_p$. Comme $K/\mathbb{Q}$ est abélienne, l'extension $K_p/\mathbb{Q}_p$ est abélienne. En vertu du corollaire 3.10, on a
$K_p \subset \mathbb{Q}_p(\mu_{n_p}), \mu_{n_p}$ une racine primitive de l'unité, pour un certain $n_p$.

Soit $e_p = v_p(n_p)$ et soit $n = \prod_{p \in S} p^{e_p}$. Montrons que $K \subset \mathbb{Q}(\mu_n)$.
Soit $M = K(\mu_n)$ alors $M/\mathbb{Q}$ est une extension abélienne et si $p$ se ramifie dans $M/\mathbb{Q}$ alors $p$ se ramifie dans $K/\mathbb{Q}$.
Aussi, si $M_p$ est le complété de $M$ pour une extension de $v_p$ alors :

$M_p = K_p(\mu_n) \subset \mathbb{Q}_p(\mu_{p^{e_p}n'}) = \mathbb{Q}_p(\mu_{p^{e_p}})\mathbb{Q}_p(\mu_{n'})$ avec $\text{pgcd}(n', p) = 1$.

On a $[\mathbb{Q}_p(\mu_{n'}) : \mathbb{Q}_p] = 1$ grâce au lemme 3.4. Le groupe d'inertie $I_p$ de $M_p/\mathbb{Q}_p$ est isomorphe au groupe de Galois $\text{Gal}(M_p/\mathbb{Q}_p)$ car comme $p$ divise $\varphi(p^{e_p})$ (l'ordre du groupe $\text{Gal}(M_p/\mathbb{Q}_p)$), avec $\varphi$ l'indicatrice d'Euler donc $p$ est totalement ramifiée.

Soit $I \subset \text{Gal}(M/\mathbb{Q})$, le groupe engendré par tout les $I_p$ avec $p$ ramifié dans $K$. Le corps, non ramifié, fixé par $I$ sur $\mathbb{Q}$ est donc égal à $\mathbb{Q}$. Par le théorème de correspondance de Galois, $I = \text{Gal}(M/\mathbb{Q})$.

D'un autre côté, on a :

$$\#I \leq \prod_{p \in S} \#I_p = \prod_{p \in S} \varphi(p^{e_p}) = \varphi(n) = [\mathbb{Q}(\mu_n) : \mathbb{Q}]$$

De l'autre, $[M : \mathbb{Q}] = [\mathbb{Q}(\mu_n) : \mathbb{Q}]$. On a ainsi $M = \mathbb{Q}(\mu_n)$ i.e $K \subset \mathbb{Q}(\mu_n)$.
Le théorème de Kronecker-Weber est démontré. □

## 3.2 Démonstration par des arguments globaux

Nous proposons maintenant de démontrer le fait suivant qui généralise le théorème 3.2 :

**Théorème 3.11.** *Soient $n \in \mathbb{N}^*$, $p_\infty$ la place infinie de $\mathbb{Q}$ et $\mathfrak{n}$ le module $\mathfrak{n} = mp_\infty$. Alors le corps de classe de rayon de $\mathbb{Q}$ pour le module $\mathfrak{n}$ , est $\mathbb{Q}^{\mathfrak{n}} = \mathbb{Q}(\mu_n)$ le $n$-ième corps cyclotomique.*

*Démonstration.* Soit $n = \prod_{p \neq p_\infty} p^{n_p}$ alors $I_{\mathbb{Q}}(\mathfrak{n}) = \prod_{p \neq p_\infty} U_p^{n_p} \times \mathbb{R}_+$ le groupe des idèles de $\mathbb{Q}$ premier avec $\mathfrak{n}$. On pose aussi $N$ la norme entre $\mathbb{Q}^{\mathfrak{n}}/\mathbb{Q}$
Soit $n = n'p^{n_p}$ alors par le théorème 3.9, on a $U_p^{n_p}$ contenu dans le groupe de norme de $\mathbb{Q}_p(\mu_{p^{n_p}})/\mathbb{Q}_p$ et dans le groupe de norme de l'extension non ramifiée $\mathbb{Q}_p(\mu_{n'})$.
On admet maintenant le lemme suivant :

**Lemme 3.12.** *Si $L/K$ une extension abélienne de corps de nombres, on a :*

$$I_K/N_{L/K}I_L = \bigoplus_p K_p^*/N_{L_{\mathfrak{P}}/K_p}L_{\mathfrak{P}}^* \text{ où } \mathfrak{P}|p.$$

**Remarque 3.13.** *Ainsi, toute idèle $\alpha \in I_K$ est la norme d'une idèle de $L$ si et seulement si toute composante locale $\alpha_p$ est la norme d'un élément de $L_{\mathfrak{P}}^*$. i.e Une idèle est une norme globale si et seulement si c'est une norme locale pour chaque coordonnée.*

Ainsi, toute idèle de $I_{\mathbb{Q}}(\mathfrak{n})$ est la norme d'une idèle de $\mathbb{Q}(\mu_n)$ montrant ainsi que $C_{\mathbb{Q}}(\mathfrak{n}) \subset N(C_{\mathbb{Q}(\mu_n)})$.

D'un autre côté, on a :

$$\begin{aligned}[C_{\mathbb{Q}} : C_{\mathbb{Q}}(\mathfrak{n})] &= [C_{\mathbb{Q}} : C_{\mathbb{Q}}(1)][C_{\mathbb{Q}}(1) : C_{\mathbb{Q}}(\mathfrak{n})] \\ &= [I_{\mathbb{Q}}(1)\mathbb{Q}^* : I_{\mathbb{Q}}(\mathfrak{n})\mathbb{Q}^*] \\ &= [I_{\mathbb{Q}}(1) : I_{\mathbb{Q}}(\mathfrak{n})]/[I_{\mathbb{Q}}(1) \cap \mathbb{Q}^* : I_{\mathbb{Q}}(\mathfrak{n}) \cap \mathbb{Q}^*]\end{aligned}$$

Maintenant, $I_{\mathbb{Q}}(1) = \prod_{p \neq p\infty} U_p \times \mathbb{R}^*$ et $I_{\mathbb{Q}}(\mathfrak{n}) = \prod_{p \neq p_\infty} U_p^{n_p} \times \mathbb{R}_+$ donc $I_{\mathbb{Q}}(1) \cap \mathbb{Q}^* = \{-1, +1\}$ et $I_{\mathbb{Q}}(\mathfrak{n}) \cap \mathbb{Q}^* = \{1\}$. On obtient donc (en posant $\varphi$ la fonction d'Euler ) :

$$\begin{aligned}[C_{\mathbb{Q}} : C_{\mathbb{Q}}(\mathfrak{n})] &= \frac{1}{2} \prod_{p \neq p_\infty} [U_p : U_p^{n_p}][\mathbb{R}^* : \mathbb{R}_+] \\ &= \prod_{p \neq p\infty} \varphi(p^{n_p}) \\ &= \varphi(n)\end{aligned}$$

Donc $[C_{\mathbb{Q}} : C_{\mathbb{Q}}(\mathfrak{n})] = [\mathbb{Q}(\mu_n) : \mathbb{Q}] = [C\mathbb{Q} : N(C_{\mathbb{Q}(\mu_n)})]$.
D'où $C_{\mathbb{Q}}(\mathfrak{n}) = N(C_{\mathbb{Q}(\mu_m)})$ et le théorème est prouvé. □

## Deuxième partie

# Généralisation et multiplication complexe

Ce deuxième chapitre est le début du travail de généralisation du théorème 3.2 au cas des corps quadratiques imaginaires. Nous proposons cinq sections pour y parvenir.
Dans le première, nous introduisons la notion d'ordre et nous la relions à des notions algébriques bien connues (formes quadratiques, idéaux, conducteurs). La deuxième consiste à lier la notion d'ordre à la théorie du corps de classes grâce aux anneaux du corps de classes. Cela nous permettra d'avoir une première approche des extensions abéliennes d'un corps quadratique (imaginaire) $K$. La troisième section crée un lien entre l'analyse complexe et la théorie algébrique des nombres. La connexion entre les fonctions elliptiques, les réseaux et les ordres y est mise en lumière. La quatrième est une étude de la fonction $j$. Cet invariant d'un réseau du plan complexe est un nombre algébrique. La dernière section établit que le $j$-invariant d'un réseau est un entier algébrique. Le résultat final de cette section permet de déterminer le corps de classe de rayon $n\mathcal{O}_K$ de $K$ ($n \in \mathbb{N}$).

## 4 Ordres dans un corps quadratique

Nous nous intéressons ici à une notion généralisant la notion d'idéal dans un corps quadratique imaginaire. Nous proposons une étude systématique pour en dégager les propriétés générales. L'ouvrage de Cox [2] fut d'une grande aide, nous avons aussi eu besoin de celui de Lang [5] pour compléter certaines preuves.

### 4.1 Rappels sur les formes quadratiques

Dans cette partie, nous en profitons pour faire des rappels au sujet des formes quadratiques que l'on se contentera de rappeler sans démonstration. On introduit quelques définitions et propriétés basiques au sujet des formes quadratiques :

**Définition 4.1** (Formes quadratiques)**.**
*La forme quadratique binaire* $f(x, y) = ax^2 + bxy + cy^2$ *est primitive si* $\text{pgcd}(a, b, c) = 1$.

**Définition 4.2.** *Un entier $m$ est représenté par $f(x,y)$ si $m = f(x,y)$ a une solution.*
*L'entier $m$ est primitivement représenté si une solution existe et que* $\text{pgcd}(x,y) = 1$.

On définit l'action de $\text{GL}_2(\mathbb{Z})$ sur l'ensemble des formes quadratiques binaires par :
Pour $\gamma = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \text{GL}_2(\mathbb{Z})$ et $f(x,y)$ une forme quadratique, on a :
$\gamma.f(x,y) = f(px+qy, rx+sy)$

**Définition 4.3.** *Les fonctions $f(x,y)$ et $g(x,y)$ sont équivalentes (resp. primitivement équivalente) s'il existe $\gamma = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \text{GL}_2(\mathbb{Z})$ (resp. $\text{SL}_2(\mathbb{Z})$) et $f(x,y) = \gamma.g(x,y) = g(px+qy, rx+sy)$.*

On définit maintenant la notion de discriminant d'une forme quadratique binaire :

**Définition 4.4** (Discriminant)**.**
*Pour $f(x,y) = ax^2 + bxy + cy^2$, le nombre $D = b^2 - 4ac$ est le discriminant et on a la propriété :*

$$4af(x,y) = (2ax+by)^2 - Dy^2$$

Si $D > 0$ alors $f(x,y)$ représente des entiers positifs comme négatifs.
Si $D < 0$ alors $f(x,y)$ représente des entiers positifs ou négatifs, cela dépend uniquement du signe de $a$. On a $D \equiv 0 \mod 4$ ou $D \equiv 1 \mod 4$ en fonction de la parité de $b$.

**Lemme 4.5.** *Soit $D$ un entier congru à 0,1 modulo 4 et $m$ un entier impaire premier avec $D$. Alors $m$ est primitivement représenté par une forme quadratique de discriminant $D$ si et seulement si $D$ est un résidu quadratique modulo $m$.*

*Démonstration.* La forme $f(x,y)$ représente primitivement $m$ si et seulement si $f(x,y)$ est primitivement équivalent à la forme $mx^2 + bxy + cy^2, b, c \in \mathbb{Z}$ et $ps - qr = 1$. Alors, $D = b^2 - 4mc \equiv b^2 \mod m$.

Réciproquement, supposons $D \equiv b^2 \mod m$. Comme $m$ est impair, on peut donc supposer que $D$ et $b$ ont même parité alors $D$ est congru à 0 ou 1 mod 4 donc $D \equiv b^2 \mod 4m$ i.e $D = b^2 - 4mc$.
Alors, $mx^2 + bxy + cy^2$ représente $m$ proprement. De plus, son discriminant est $D$ et $\text{pgcd}(m,b,c) = 1$. □

**Définition 4.6.** *Une forme quadratique (binaire) $ax^2 + bxy + cy^2$ définie positive est réduite si $|b| \leq a \leq c$ et $b \geq 0$ si $a = c$ ou $|b| = a$.*

**Proposition 4.7.** *Toute forme quadratique (binaire) définie positive est primitivement équivalente à une forme quadratique (binaire) réduite.*

*Démonstration.* Voir [2]. □

**Définition 4.8.** *Soit $D$ un entier négatif non nul.*
*On dit que $D$ est un discriminant (d'une forme binaire sur $\mathbb{Z}$) si $D$ est congru à 0 ou 1 modulo 4.*

**Théorème 4.9.** *Soit $D$ un discriminant.*
*Alors le nombre $h(D)$ de classes de formes quadratiques primitive définies positives de discriminant $D$ est fini.*
*De plus, $h(D)$ est égal au nombre de formes quadratiques réduites de discriminant $D$.*

*Démonstration.* Voir [2]. □

**Définition 4.10.** *Soit $D$ un discriminant.*
*L'ensemble $C(D)$ désigne les classes primitives des forme quadratique (binaire) primitives définies positives de discriminant $D$.*

**Remarque 4.11.** *On appelera $C(D)$ le groupe des classes des forme quadratique (binaire) primitives.*

**Théorème 4.12.** *$C(D)$ est un groupe abélien d'ordre $h(D)$.*

*Démonstration.* Voir [2]. □

## 4.2 Notion d'ordre

### 4.2.1 Premières définitions

On fixe $K$ un corps quadratique imaginaire de discriminant $d_K$.

**Définition 4.13.** *Un ordre $\mathcal{O}$ d'un corps quadratique $K$ est un sous-ensemble $\mathcal{O} \subset K$ tel que :*

- *$\mathcal{O}$ est un sous-anneau de $K$ contenant 1.*
- *$\mathcal{O}$ est un $\mathbb{Z}$-module de type fini.*
- *$\mathcal{O}$ contient une $\mathbb{Q}$-base de $K$.*

**Remarque 4.14.** *Les deux derniers items permettent d'affirmer que $\mathcal{O}$ est un $\mathbb{Z}$-module libre de rang 2 sans torsion. Le troisième item permet d'affirmer que $K$ est le corps de fraction de $\mathcal{O}$.*

**Remarque 4.15.** *L'anneau des entiers $\mathcal{O}_K$ est un ordre de $K$ et pour tout ordre $\mathcal{O}$, on a $\mathcal{O} \subset \mathcal{O}_K$.*

**Définition 4.16.** *Si $\mathcal{O}$ est un ordre de $K$ et on pose $f = [\mathcal{O}_K : \mathcal{O}]$, $f$ est le conducteur de $\mathcal{O}$.*

Si $w_K$ est une uniformisante de $\mathcal{O}_K$, on a $\omega_K = \dfrac{d_K + \sqrt{d_K}}{2}$.
Ainsi, on a $\mathcal{O}_K = [1, \omega_K]$.

**Lemme 4.17.** *Si $f$ est le conducteur de $\mathcal{O}$ alors $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K = [1, f\omega_K]$.*

*Démonstration.* Comme $\mathcal{O}$ et $\mathcal{O}_K$ sont des $\mathbb{Z}$-modules libres de rang 2 ainsi $[\mathcal{O}_K : \mathcal{O}] < \infty$. Posons $f = [\mathcal{O}_K : \mathcal{O}]$, on a $f\mathcal{O}_K \subset \mathcal{O}$ et $\mathbb{Z} + f\mathcal{O}_K \subset \mathcal{O}$. De ce fait, $[1, f\omega_K]$ est d'indice fini dans $\mathcal{O}_K = [1, \omega_K]$ donc $[1, f\omega_K] = \mathbb{Z} + f\mathcal{O}_K$ prouvant le lemme. □

**Définition 4.18.** *Soit $\sigma \mapsto \sigma'$ un automorphisme non trivial de $K$, supposons $\mathcal{O} = [\alpha, \beta]$. On appellera discriminant de $\mathcal{O}$, le nombre*
$D = \left(\det \begin{pmatrix} \alpha & \beta \\ \alpha' & \beta' \end{pmatrix}\right)^2$ *qui est indépendant de la base choisie.*
*Dans le cas où $\mathcal{O} = [1, f\omega_K]$, on a $D = f^2 d_K$*

**Remarque 4.19.** *Avec les hypothèses de la définition, on note que $D$ est congru à 0 ou* $1 \mod 4$. *Ainsi, $K = \mathbb{Q}(\sqrt{D})$ et $D$ détermine $\mathcal{O}$.*

### 4.2.2 Idéaux et ordres

Si $\mathfrak{a}$ est un idéal non nul de $\mathcal{O}$ alors le quotient $\mathcal{O}/a$ est fini.

**Définition 4.20.** *On définit la norme de $\mathfrak{a}$ par $N(a) = |\mathcal{O}/a|$.*

Par définition d'un ordre $\mathcal{O}$, on peut affirmer que $\mathcal{O}$ est noethérien donc tout idéal premier non nul de $\mathcal{O}$ est maximal. Ceci équivaut au fait que $f$ le conducteur de $\mathcal{O}$ soit plus grand que 1.
Ainsi, comme $\mathcal{O}$ n'est pas intégralement clos dans $K$ ceci montre que $\mathcal{O}$ n'est pas un anneau de Dedekind. Cela implique que les idéaux de $\mathcal{O}$ n'ont pas de décomposition unique (à l'ordre près des facteurs).

**Définition 4.21.** *Un idéal $\mathfrak{a}$ de $\mathcal{O}$ est propre si $\mathcal{O} = \{\beta \in K | \beta a \subset a\}$.*

**Remarque 4.22.**

- *On a toujours $\mathcal{O} \subset \{\beta \in K | \beta a \subset a\}$.*
- *Les idéaux principaux sont toujours propres pour l'ordre maximal tout les idéaux sont propres.*

On étend cette terminologie aux idéaux fractionnaires i.e un sous-ensemble de $K$ qui est un $\mathcal{O}$-module non nul de type fini. On continue par caractériser les idéaux fractionnaires propres de $\mathcal{O}$ :

**Proposition 4.23.** *Soit $\mathfrak{a}$ un idéal fractionnaire de $\mathcal{O}$. On a que $\mathfrak{a}$ idéal propre si et seulement si $\mathfrak{a}$ est inversible.*

*Démonstration.* Supposons $\mathfrak{a}$ un idéal inversible alors il existe $\mathfrak{b}$ un idéal de $\mathcal{O}$ tel que $\mathfrak{ab} = O$.
Maintenant, si $\beta \in K$ et $\beta\mathfrak{a} \subset \mathfrak{a}$ alors on a $\beta\mathcal{O} = \beta(\mathfrak{ab}) = (\beta\mathfrak{a})b \subset \mathfrak{ab} = O$ donc $\beta \in \mathcal{O}$ donc $\mathfrak{a}$ est propre.
Pour prouver la réciproque, on commence par démontrer le lemme ci-dessous :

**Lemme 4.24.** *Soit $K = \mathbb{Q}(\tau)$ un corps quadratique et soit $ax^2 + bx + c$ le polynôme minimal de $\tau$ avec $a, b, c$ des entiers premiers entre eux deux à deux. Alors $[1, \tau]$ est un idéal fractionnaire pour l'ordre de $[1, a\tau]$ de $K$.*

*Démonstration du lemme.* Comme $a\tau$ est un entier algébrique alors $[1, a\tau]$ est un ordre.
Pour $\beta \in K$, notons $\beta[1, \tau] \subset [1, \tau]$ si et seulement si $\beta.1 \in [1, \tau]$ et $\beta.\tau \in [1\tau]$.
De $\beta.1 \in [1, \tau]$ on en déduit $\beta = m + n\tau, m, n \in \mathbb{Z}$.
De $\beta.\tau \in [1\tau]$, remarquons que :

$$\begin{aligned}\beta\tau &= m\tau + n\tau^2 \\ &= m\tau + \frac{n}{a}(-b\tau - c) \\ &= \frac{-cn}{a} + (\frac{-bn}{a} + m)\tau.\end{aligned}$$

Or $\text{pgcd}(a, b, c) = 1$ on a donc $\beta\tau \in [1, \tau]$ si et seulement si $a|n$.
Ainsi, $\{\beta \in K | \beta[1, \tau] \subset [1, \tau]\} = [1, a\tau]$ □

Maintenant, prouvons la réciproque.
Tout d'abord, remarquons que pour tout $\mathfrak{a}$ $\mathbb{Z}$-module de rang 2, on a $\mathfrak{a} = [\alpha, \beta]$ pour $\alpha, \beta \in K$. Alors $\mathfrak{a} = \alpha[1, \tau]$ avec $\tau = \dfrac{\beta}{\alpha}$ alors le lemme précédent implique que $\mathcal{O} = [1, \alpha\tau]$.
Notons $\beta \to \beta'$ l'automorphisme non trivial de $K$. Comme $\tau'$ est l'autre racine de $ax^2 + bx + c$ le lemme précédent montre que $\mathfrak{a}' = \alpha'[1, \tau]$ est un idéal fractionnaire pour $[1, a\tau] = [1, a\tau'] = \mathcal{O}$.
On affirme que $\mathfrak{a}\mathfrak{a}' = \dfrac{N(\alpha)}{a}\mathcal{O}$.
Notons que $\tau + \tau' = \dfrac{-b}{a}$ et $\tau\tau' = \dfrac{c}{a}$, on a :

$$\begin{aligned}a\mathfrak{a}\mathfrak{a}' &= a\alpha\alpha'[1, \tau][1, \tau'] \\ &= N(\alpha)[a, a\tau, a\tau', a\tau\tau'] \\ &= N(\alpha)[a, a\tau, -b, c] \\ &= N(\alpha)\mathcal{O}\end{aligned}$$

La dernière égalité découlait du fait que $\text{pgcd}(a,b,c) = 1$ et elle implique que $\mathfrak{a}\mathfrak{a}' = \dfrac{N(\alpha)}{a}\mathcal{O}$. □

Pour un ordre $\mathcal{O}$, on notera $I(\mathcal{O})$ l'ensemble des idéaux propres de $\mathcal{O}$.
La dernière proposition de fait que $I(\mathcal{O})$ est un groupe multiplicatif. Les idéaux principaux de $\mathcal{O}$ forment un sous-groupe de $P(\mathcal{O}) \subset I(\mathcal{O})$.

**Définition 4.25.** *Le groupe des classes d'idéaux de $\mathcal{O}$ est le quotient $C(\mathcal{O}) = I(\mathcal{O})/P(\mathcal{O})$.*

On peut ainsi montrer le théorème suivant :

**Théorème 4.26.** *Soit $m$ un entier, $\mathcal{O}$ un ordre de $K$. On a la suite exacte :*

$$1 \to (\mathcal{O}_K/m\mathcal{O}_K)^*/\mathcal{O}_K^*\mathbb{Z}/m\mathbb{Z} \to C(\mathcal{O}) \to C(\mathcal{O}_K) \to 1$$

*Démonstration.* Voir [2]. □

### 4.2.3 Ordres et formes quadratiques

Dans cette section on va expliciter le lien entre le groupe des classes d'idéaux de $\mathcal{O}$ et le groupe des classes de discriminant $D$.

**Théorème 4.27.** *Soit $\mathcal{O}$ un ordre de discriminant $D$ dans un corps quadratique imaginaire $K$.*

- *i) Si $f(x,y) = ax^2 + bxy + cy^2$ est une forme positive définie positive de discriminant $D$ alors $[a, (-b + \frac{\sqrt{D}}{2})]$ est un idéal propre de $\mathcal{O}$.*
- *ii) L'application envoyant $f(x,y)$ sur $[a, (-b + \frac{\sqrt{D}}{2})]$ induit un isomorphisme entre $C(D)$ et $C(\mathcal{O})$. Donc l'ordre de $C(\mathcal{O}) = h(D)$.*
- *iii) Un entier positif $m$ est représenté par la forme $f(x,y)$ si et seulement si $m$ est la norme $N(\mathfrak{a})$ d'un idéal $\mathfrak{a}$ correspondant à la classe d'idéal dans $C(\mathcal{O})$.*

*Démonstration.* On commence par démontrer un lemme qui nous sera utile pour établir le i).

**Lemme 4.28.** *Soit $K = \mathbb{Q}(\tau)$ un corps quadratique où $ax^2+bx+c$ désignera le polynôme de $\tau$ où $a, b, c$ sont premiers entre eux. Alors $[1, \tau]$ est un idéal fractionnaire propre pour l'ordre $[1, \alpha\tau]$ de $K$.*

*Démonstration.* Tout d'abord, $[1, a\tau]$ est un ordre car $a\tau$ est un entier algébrique. Alors pour $\beta \in K$, notons $\beta[1,\tau] \subset [1,\tau]$ si et seulement si $\begin{cases} \beta.a \in [1,\tau] \\ \beta.\tau \in [1,\tau] \end{cases}$ si et seulement si $\begin{cases} \beta = m + n\tau, mn \in \mathbb{Z} \\ \beta\tau = m\tau + n\tau^2 \end{cases}$

Or $\beta\tau = m\tau + \frac{n}{a}(-b\tau - c) = \frac{-cn}{a} + (\frac{-bn}{a} + m)\tau$ donc comme $\text{pgcd}(a,b,c) = 1$, on peut affirmer que $\beta\tau \in [1,\tau]$ si et seulement si $a|m$.
Il en découle que $\{\beta \in K, \beta[1,\tau] \subset [1,\tau]\} = [1, a\tau]$. □

- i) Soit $f(x,y) = ax^2 + bxy + cy^2$ une forme primitive définie positive de discriminant $D < 0$.
  Les racines de $f(x,1) = ax^2 + bx + c$ sont complexes.
  On pose $\mathbb{H} = \{z = x + iy \in \mathbb{C} | y > 0\}$ on a qu'il existe un unique $\tau \in \mathbb{H}$ tel que $f(\tau, 1) = 0$ donc $\tau$ est une racine de $f(x,y)$.
  Comme $a > 0$, il suit que $\tau = \frac{-b + \sqrt{D}}{2a}$ donc $[a, \frac{-b+\sqrt{D}}{2}] = [a, a\tau]$ $= a[1,\tau]$ donc $\tau \in K$. Grâce au dernier lemme, on peut affirmer que $[1,\tau]$ est un idéal propre.
  Si $f$ est le conducteur de $\mathcal{O}$ alors $D^2 = f^2 d_K$ et on a :

$$\begin{aligned} a\tau &= \frac{-b + \sqrt{D}}{2} \\ &= \frac{-b + f\sqrt{d_K}}{2} \\ &= \frac{-b + fd_K}{2} + f(\frac{d_K + \sqrt{d_K}}{2}) \\ &= \frac{-b + fd_K}{2} + fw_k \end{aligned}$$

  Mais, $D = b^2 - 4ac$, $fd_K$ et $b$ sont de même parité donc $\frac{b + fd_K}{2} \in \mathbb{Z}$.
  Ainsi, on a $[1, a\tau] = [1, f\omega_K]$ donc $[1, a\tau] = \mathcal{O}$ donc $a[1,\tau]$ est un idéal propre de $\mathcal{O}$.

- ii) Soit $f(x,y)$ et $g(x,y)$ des formes de discriminant $D$ et soit $\tau$ et $\tau'$ leurs racines respectives. On va montrer les équivalences suivantes :

$$\text{Les formes } f(x,y) \text{ et } g(x,y) \text{ sont proprement équivalentes} \quad (2)$$

$$\text{si et seulement si } \tau' = \frac{p\tau + q}{r\tau + s}, \begin{pmatrix} r & q \\ r & s \end{pmatrix} \in SL_2(\mathbb{Z}) \quad (3)$$

$$\text{si et seulement si } \begin{cases} [1,\tau] = \lambda[1,\tau'] \\ \lambda \in K^* \end{cases} \quad (4)$$

  Supposons que $f(x,y) = g(px + qy, rx + sy)$ avec $\begin{pmatrix} r & q \\ r & s \end{pmatrix} \in SL_2(\mathbb{Z})$.
  Alors, on a :

$$\begin{aligned} 0 = f(\tau, 1) &= g\left(p\tau + q, r\tau + s\right) \\ &= (r\tau + t)^2 g\left(\frac{p\tau + q}{r\tau + s}, 1\right) \end{aligned}$$

donc $g\left(\frac{p\tau+q}{r\tau+s},1\right)=0$. On a $\Im\left(\frac{p\tau+q}{r\tau+s}\right)=det\begin{pmatrix}r&q\\r&s\end{pmatrix}|r\tau+s|^{-2}Im(\tau)$ impliquant $\frac{p\tau+q}{r\tau+s}\in\mathbb{H}$ donc $\tau'=\frac{p\tau+q}{r\tau+s}$ par unicité de la racine $\tau'$.
Réciproquement, si $\tau'=\frac{p\tau+q}{r\tau+s}$ alors $f(x,y)$ et $g(px+qy,rx+sy)$ ont les mêmes racines et celles-ci sont égales prouvant ainsi la première équivalence.
Ensuite, si $\tau'=\frac{p\tau+q}{r\tau+s}$ posons $\lambda=r\tau+s\in K^*$. Alors :

$$\begin{aligned}\lambda[1,\tau']&=(r\tau+s)[1,\frac{p\tau+q}{r\tau+s}]\\&=[r\tau+s,p\tau+q]\\&=[1,\tau]\end{aligned}$$

car $\begin{pmatrix}r&q\\r&s\end{pmatrix}\in SL_2(\mathbb{Z})$.

Réciproquement, si $\lambda[1,\tau']=[1,\tau],\lambda\in K^*$ alors $[1,\tau]=[\lambda,\lambda\tau']$ donc $\lambda\tau'=p\tau+q$ donc $\lambda=r\tau+s$ pour $\begin{pmatrix}r&q\\r&s\end{pmatrix}\in GL_2(\mathbb{Z})$. Ainsi, $\tau'=\frac{p\tau+q}{r\tau+s}$ or $Im(\frac{p\tau+q}{r\tau+s})=det\begin{pmatrix}p&q\\r&s\end{pmatrix}|r\tau+s|^{-2}Im(\tau)$.
De ce fait, on peut affirmer que $\begin{pmatrix}p&q\\r&s\end{pmatrix}\in SL_2(\mathbb{Z})$ car $\tau,\tau'\in\mathbb{H}$ complétant ainsi la preuve des équivalences de (2).

En utilisant (2) l'application $f(x,y)\mapsto a[1,\tau]$ induit une injection $C(D)\to C(\mathcal{O})$. Pour montrer que cette application est surjective, soit $\mathfrak{a}$ un idéal fractionnaire de $\mathcal{O}$. On peut écrire $\mathfrak{a}=[\alpha,\beta],\alpha,\beta\in K$ (en échangeant les rôles de $\alpha$ et $\beta$ si nécessaire).
On peut donc supposer $\tau=\frac{\beta}{\alpha}\in\mathbb{H}$. Soit $ax^2+bx+c$ le polynôme minimal de $\tau$. On peut supposer $\text{pgcd}(a,b,c)=1$ et $a>0$.
Alors $f(x,y)=ax^2+bxy+cy^2$ est une forme quadratique définie positive de discriminant $D$ et $f(x,y)$ s'envoie sur $a[1,\tau]\in\mathfrak{a}=[\alpha,\beta]=\alpha[1,\tau]$ dans $C(\mathcal{O})$ prouvant la surjectivité.
On a donc un une bijection d'ensemble entre $C(D)$ et $C(\mathcal{O})$. On admet que la structure de groupe est préservée.

- iii) On admet le lemme suivant qui permet d'affimer que $(\mathfrak{a})^{-1}=\overline{\mathfrak{a}}$ :

**Lemme 4.29.** *Soit $\mathcal{O}$ un ordre quadatique imaginaire. Alors :*

- *Pour $\alpha \in \mathcal{O}, \alpha \neq 0, N(\alpha\mathcal{O}) = N(\alpha)$.*
- *Pour des idéaux propres $\mathfrak{a}$ et $\mathfrak{b}$, on a $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$*
- *Pour un idéal propre $\mathfrak{a}$ alors $\mathfrak{a}\overline{\mathfrak{a}} = N(\mathfrak{a})\mathcal{O}$.*

*Démonstration.* Voir [2] pour la démonstration. □

Maintenant, si $m$ est représenté par $f(x, y)$ alors $m = d^2a$ avec $a$ qui est proprement représenté par $f(x, y)$.
On peut supposer $f(x, y) = ax^2 + bxy + cy^2$. Alors $f(x, y)$ est envoyé sur $\mathfrak{a} = a[1, \tau]$ donc $N(\mathfrak{a}) = a$.
Donc on a $N(d\mathfrak{a}) = d^2a = m$ donc $m$ est la norme de l'idéal de la classe de $\mathfrak{a}$.

Réciproquement, supposons $N(\mathfrak{a}) = m$, on sait que $\mathfrak{a} = a[1, \tau]$ où $Im(\tau) > 0$ et $\begin{cases} a\tau^2 + b\tau + c = 0 \\ \text{pgcd}(a, b, c) = 1, a > 0 \end{cases}$
Alors, $f(x, y) = ax^2 + bxy + cy^2$ est envoyé sur la classe de $\mathfrak{a}$. Il reste à montrer que $f(x, y)$ représente $m$.
Comme $N(\mathfrak{a}) = \dfrac{N(\alpha)}{a}$ on a donc $m = N(\mathfrak{a}) = \dfrac{N(\alpha)}{a}$.
Or $\alpha[1, \tau] = \mathfrak{a} \subset \mathcal{O} = [1, a\tau]$ donc $\begin{cases} \alpha = p + qa\tau \\ \alpha\tau = r + sa\tau, (p, q, r, s) \in \mathbb{Z} \end{cases}$
Alors, $(p + qa\tau)\tau = r + sa\tau$ et comme $a\tau^2 = -b\tau - c$ on a $p = as + bq$.
Donc :

$$\begin{aligned} m = \frac{N(\alpha)}{a} &= \frac{1}{a}(p^2 - bqp + acq^2) \\ &= \frac{1}{a}((as + bq)^2 - b(as + bq)q + acq^2) \\ &= \frac{1}{a}(a^2s^2 + absq + acq^2) \\ &= as^2 + bsq + cq^2 \\ &= f(s, q) \end{aligned}$$

□

Avec le iii) du théorème précédent, on obtient le corollaire suivant :

**Corollaire 4.30.** *Pour $m \in \mathbb{Z}, m \neq 0$ alors toute classe d'idéal dans $C(\mathcal{O})$ contient un idéal propre de $\mathcal{O}$ dont la norme est première avec $m$.*

### 4.2.4 Idéaux premiers et conducteurs

Soit $\mathcal{O}$ un ordre dans un corps quadratique de conducteur $f$.

**Définition 4.31.** *Un idéal non nul $\mathfrak{a}$ est premier à $f$ si $\mathfrak{a} + f\mathcal{O} = \mathcal{O}$.*

On commence par un lemme :

**Lemme 4.32.**
- *Tout idéal $\mathfrak{a}$ de $\mathcal{O}$ est premier avec $f$ si et seulement si sa norme $N(\mathfrak{a})$ est première avec $f$.*
- *Tout idéal de $\mathcal{O}$ premier avec $f$ est propre.*

*Démonstration.* Pour le premier item. Soit $m_f : \mathcal{O}/\mathfrak{a} \to \mathcal{O}/\mathfrak{a}$ la multiplication par $f$. Alors on a :

$$\begin{aligned} \mathfrak{a} + f\mathcal{O} = \mathcal{O} &\text{ si et seulement si } m_f \text{ est surjective.} \\ &\text{si et seulement si } m_f \text{ est un isomorphisme.} \end{aligned}$$

Par le théorème de structure des groupes abéliens finis, $m_f$ est un isomorphisme si et seulement si $\text{pgcd}(f, N(\mathfrak{a})) = 1$ prouvant le premier item.
Pour le second, soit $\beta \in K$ tel que $\beta\mathfrak{a} \subset \mathfrak{a}$ alors $\beta \in O_K$ et on a :

$$\begin{aligned} \beta\mathcal{O} &= \beta(\mathfrak{a} + f\mathcal{O}) \\ &= \beta\mathfrak{a} + \beta f\mathcal{O}c\mathfrak{a} + f\mathcal{O}_K \end{aligned}$$

donc $f\mathcal{O}_K \subset \mathcal{O}$ montrant $f\mathcal{O} \subset \mathcal{O}$.
Alors, $\beta \in \mathcal{O}$ montrant que $\mathfrak{a}$ est un idéal propre. □

On peut donc affirmer que les idéaux de $\mathcal{O}$ premiers avec $f$ appartiennent à $I(\mathcal{O})$ et sont fermés sous la multiplication car $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$ sont aussi premiers avec $f$.
On notera $I(\mathcal{O}, f) \subset I(\mathcal{O})$ le sous-groupe engendré et $P(\mathcal{O}, f)$ celui des idéaux principaux $\alpha\mathcal{O}, \alpha \in \mathcal{O}$ et la norme de $N(\alpha)$ est première avec $f$.
On peut donc décrire le groupe des classes $C(\mathcal{O})$ en fonction de $I(\mathcal{O}, f)$ et $P(\mathcal{O}, f)$.

**Proposition 4.33.** *L'inclusion $I(\mathcal{O}, f) \subset I(\mathcal{O})$ induit un isomorphisme : $I(\mathcal{O}, f)/P(\mathcal{O}, f) \simeq I(\mathcal{O})/P(\mathcal{O}) \simeq C(\mathcal{O})$*

*Démonstration.* L'application $I(\mathcal{O}, f) \to C(\mathcal{O})$ est surjective, son noyau est $I(\mathcal{O}, f) \cap P(\mathcal{O})$ contient $P(\mathcal{O}, f)$ mais l'inclusion $P(\mathcal{O}) \cap I(\mathcal{O}, f) \subset P(\mathcal{O}, f)$ doit être prouvé :
Un élement de $I(\mathcal{O}, f) \cap P(\mathcal{O})$ est un idéal fractionnaire $\alpha\mathcal{O} = \mathfrak{ab}^{-1}$ où $\alpha \in K$ et $\mathfrak{a}, \mathfrak{b}$ sont deux idéaux de $\mathcal{O}$ premiers avec $f$.
Soit $\mathfrak{m} = N(\mathfrak{b})$ alors $\mathfrak{m}\mathcal{O} = N(\mathfrak{b})\mathcal{O} = \mathfrak{b}\overline{\mathfrak{b}}$ donc $\mathfrak{mb}^{-1} = \mathfrak{b}$.
Donc $\mathfrak{m}\alpha\mathcal{O} = \mathfrak{amb}^{-1} = \mathfrak{a}\overline{\mathfrak{b}} \subset \mathcal{O}$ prouvant $\mathfrak{m}\alpha\mathcal{O} \in P(\mathcal{O}, f)$.
Alors $\alpha\mathcal{O} = \mathfrak{m}\alpha\mathcal{O}(\mathfrak{m}\mathcal{O})^{-1} \in P(\mathcal{O}, f)$. □

Pour tout ordre $\mathcal{O}$, les idéaux premiers au conducteur se relient facilement aux idéaux de l'ordre maximal $\mathcal{O}_K$.

**Définition 4.34.** *Pour un entier positif $m$, un idéal $\mathfrak{a}$ de $\mathcal{O}_K$ premier à $\mathfrak{m}$ est de la forme $\mathfrak{a} + \mathfrak{m}\mathcal{O}_K = \mathcal{O}_K$.*

Cela revient à considérer $\text{pgcd}(N(\mathfrak{a}), \mathfrak{m}) = 1$. On a donc un sous-groupe $I_K(\mathfrak{m}) \subset I_K$ engendré par les idéaux de $O_K$ premiers à $\mathfrak{m}$

**Proposition 4.35.** *Soit $\mathcal{O}$ un ordre de conducteur $f$ dans $K$ un corps quadratique imaginaire.*

- *i) Si $\mathfrak{a}$ est un idéal de $\mathcal{O}_K$ premier avec $f$ alors $\mathfrak{a} \cup \mathcal{O}$ est un idéal de $\mathcal{O}$ premier avec $f$ de même norme.*
- *ii) Si $\mathfrak{a}$ est un idéal de $\mathcal{O}$ premier avec $f$ alors $\mathfrak{a}O_K$ est un idéal de $\mathcal{O}_K$ premier avec $f$ de même norme.*
- *iii) L'application $\mathfrak{a} \mapsto \mathfrak{a} \cap \mathcal{O}$ induit un isomorphisme $I_K(f) \simeq I(\mathcal{O}, f)$ et son inverse est donné par $\mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_K$*

*Démonstration.* i) Soit $\mathfrak{a}$ un idéal de $\mathcal{O}_K$ premier avec $f$. Comme $\mathcal{O}/\mathfrak{a} \cap \mathcal{O}$ s'injecte dans $\mathcal{O}_K/\mathfrak{a}$ et $N(\mathfrak{a})$ est premier avec $f$ donc sa norme est $N(\mathfrak{a} \cap \mathcal{O})$ montrant que $\mathfrak{a} \cap \mathcal{O}$ est premier avec $f$.
Pour la norme, considérons l'application naturelle $\mathcal{O}/\mathfrak{a} \cap \mathcal{O} \to \mathcal{O}_K/\mathfrak{a}$.
Elle est injective et comme $\mathfrak{a}$ est premier avec $f$ on peut affirmer que la multiplication par $f$ induit un isomorphisme de $O_K/\mathfrak{a}$. Mais comme $f\mathcal{O}_K \subset \mathcal{O}$ on a la surjectivité. Cela prouve l'égalité des normes donc i).

ii) Soit $\mathfrak{a}$ un idéal de $\mathcal{O}$ premier avec $f$.
Comme $\mathfrak{a}\mathcal{O}_K + f\mathcal{O}_K = (\mathfrak{a} + f\mathcal{O})\mathcal{O}_K = \mathcal{O}_K$. On voit donc que $\mathfrak{a}\mathcal{O}_K$ est premier avec $f$ et on a déjà prouvé l'égalité des normes.

iii) On affirme que :

- a)$\mathfrak{a}\mathcal{O}_K \cap \mathcal{O} = \mathfrak{a}$ quand $\mathfrak{a}$ est un idéal de $\mathcal{O}$ premier avec $f$.
- b)$(\mathfrak{a}\mathcal{O}) \cap \mathcal{O}_K = \mathfrak{a}$ quand $\mathfrak{a}$ est un idéal de $\mathcal{O}_K$ premier avec $f$.

Pour a) on a :

$$\begin{aligned}\mathfrak{a}\mathcal{O}_K \cap \mathcal{O} &= (\mathfrak{a}\mathcal{O}_K \cap \mathcal{O})\mathcal{O} \\ &= (\mathfrak{a}\mathcal{O}_K \cap \mathcal{O})(\mathfrak{a} + f\mathcal{O}) \\ &\subset \mathfrak{a} + f(\mathfrak{a}\mathcal{O}_K \cap \mathcal{O}) \\ &\subset \mathfrak{a} + \mathfrak{a}.f\mathcal{O}_K\end{aligned}$$

Or $f\mathcal{O}_K \subset \mathcal{O}$ montrant ainsi que $\mathfrak{a}\mathcal{O}_K \cap \mathcal{O} \subset \mathfrak{a}$, l'autre inclusion étant évidente.

Pour le b), on affirme $\mathfrak{a} = \mathfrak{a}\mathcal{O} = \mathfrak{a}(\mathfrak{a} \cap \mathcal{O} + f\mathcal{O}) \subset (\mathfrak{a} \cap \mathcal{O})\mathcal{O}_K + f\mathfrak{a}$.
Toutefois, $f\mathfrak{a} \subset f\mathcal{O}_K \subset \mathcal{O}$ donc $f\mathfrak{a} \subset \mathfrak{a} \cap \mathcal{O} \subset (\mathfrak{a} \cap \mathcal{O})\mathcal{O}_K$ et $\mathfrak{a} \subset (\mathfrak{a} \cap \mathcal{O})\mathcal{O}_K$ suit. L'autre inclusion étant évidetnte on a fini la preuve de l'affirmation.

On remarque que l'affirmation et le i) implique l'égalité des normes au sens de ii). De l'affirmation, on obtient une bijection entre le monoïdes des idéaux de $\mathcal{O}$ et ceux de $\mathcal{O}_K$ premiers avec $f$. Comme $\mathfrak{a} \mapsto \mathfrak{a} \cap \mathcal{O}$ préserve la multiplication alors on a un isomorphsime $I_K(f) \simeq I(\mathcal{O}, f)$. L'inverse étant multiplicative, on a $(\mathfrak{ab})\mathcal{O}_K = \mathfrak{a}\mathcal{O}_K.\mathfrak{b}\mathcal{O}_K$ on peut conclure. □

Pour conclure cette partie, on établir que tout idéal premier avec $f$ possède une décomposition unique comme produit d'idéaux premiers de $\mathcal{O}$ premiers avec $f$. Décrivons le groupe des classe $C(\mathcal{O})$ en fonction de l'ordre maximal :

**Proposition 4.36.** *Soit $\mathcal{O}$ un ordre de conducteur $f$ dans un corps quadratique imaginaire $K$. Alors, on a les isomorphismes naturels :*

*$C(\mathcal{O}) \simeq I(\mathcal{O}, f)/P(\mathcal{O}, f) \simeq I_K(f)/P_{K,\mathbb{Z}}(f)$ où $P_{K,\mathbb{Z}}(f)$ est le sous-groupe de $I_K(f)$ engendré par les idéaux principaux de la forme $\alpha\mathcal{O}_K$ vérifiant :*
*$\alpha \equiv a \mod f\mathcal{O}_K$ pour $a$ un entier premier avec $f$.*

*Démonstration.* On a le premier isomorphisme grâce à a la proposition 4.33. Pour le second, remarquons $\mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_K$ induit un isomorphisme $I(\mathcal{O}, f) \simeq I_K(f)$ grâce à la proposition 4.35. Sous cet isomorphisme $P(\mathcal{O}, f) \subset I(\mathcal{O}, f)$ est envoyé sur un sous-groupe $\subset I_K(f)$. On est donc ramené à montrer que $\tilde{P} = P_{K,\mathbb{Z}}(f)$. Tout d'abord, on montre que :

$$\begin{aligned}&\text{Pour tout } \alpha \in \mathcal{O}_K,\ \alpha \equiv a \mod f\mathcal{O}_K, a \in \mathbb{Z},\ \gcd(a, f) = 1\\ &\quad\text{si et seulement si } \alpha \in \mathcal{O},\ \gcd(N(\alpha), f) = 1.\end{aligned}$$

On peut supposer que $\alpha \equiv a \mod f\mathcal{O}_K$ avec $a \in \mathbb{Z}$ et $\gcd(a, f) = 1$ alors $N(\alpha) \equiv a^2 \mod f$ donc $\gcd(N(\alpha), f) = \gcd(a^2, f) = 1$.
Supposons $\alpha \equiv a \mod f\mathcal{O}_K$ où $a \in \mathbb{Z}$, $\gcd(a, f) = 1$.
Alors $N(\alpha) \equiv a^2 \mod f$ donc $\gcd(N(\alpha), f) = \gcd(a^2, f) = 1$.
Or $f\mathcal{O}_K \subset \mathcal{O}$ donc $\alpha \in \mathcal{O}$.

Réciproquement, soit $\alpha \in \mathcal{O} = [1, fw_K]$ ayant une norme première avec $f$. Alors $\alpha \equiv a \mod f\mathcal{O}_K$ pour un certain $a \in \mathbb{Z}$. Mais $\gcd(N(\alpha), f) = 1$ et $N(\alpha) \equiv a^2 \mod f$ donc $\gcd(a, f) = 1$ montre l'équivalence.
Enfin, on sait que $P(\mathcal{O}, f)$ est engendré par des idéaux $\alpha\mathcal{O}, \alpha \in \mathcal{O}$ et $\gcd(N(\alpha), f) = 1$ et grâce à l'équivalence cela implique $\tilde{P} = P_K(\mathcal{O}, f)$ □

# 5 Anneaux du corps de classes

Ici on va relier la théorie du corps de classe avec la notion d'ordre dans le cas des corps quadratiques. Ce travail algébrique préliminaire est une étape pour réussir à atteindre notre objectif. La principale référence pour cette section est [2] même si [4] peut être aussi utile par moments.

## 5.1 Premières définitions

Soient $K$ un corps de nombres et un idéal $\mathfrak{m}$ de $\mathcal{O}_K$ vu comme un module de $I_K(\mathfrak{m})$ et $P_{K,1}(\mathfrak{m})$. On se limitera ici au cas où $K$ est un corps imaginaire quadratique. On aura donc que $\mathfrak{m}$ est un idéal principal $\alpha\mathcal{O}_K$ et on aura $I_K(\mathfrak{m})$ et $P_{K,1}(\mathfrak{m})$. Soit $\mathcal{O}$ un ordre de conducteur $f$.
D'un autre côté, on a : $C(\mathcal{O}) \simeq I_K(f)/P_{K,\mathbb{Z}}(f)$.
De l'autre côté, $P_{K,1}(f) \subset P_{K,\mathbb{Z}}(f) \subset I_K(f)$. Ainsi, $C(\mathcal{O})$ est un groupe de classes d'idéaux de $K$ pour le module $f\mathcal{O}_K$. Grâce au théorème 2.29, cela détermine une unique extension abélienne $L$ de $K$.

**Définition 5.1.** *On désigne par $L$ l'anneau du corps de classe de l'ordre $\mathcal{O}$.*

**Proposition 5.2.**
- *L'application d'Artin nous fournit donne :* $C(\mathcal{O}) \simeq I_K(f)/P_{K,\mathbb{Z}}(f) \simeq \mathrm{Gal}(L/K)$.
- *Tous les premiers de $K$ ramifié dans $L$ divise $f\mathcal{O}_k$.*
- $[L : K] = h(\mathcal{O})$.

**Remarque 5.3.** *Pour l'ordre maximal $\mathcal{O}_K$ son anneau de corps de classe est le corps de classe de Hilbert de $K$.*

**Proposition 5.4.** *Soit $L$ l'anneau du corps de classe d'un ordre $\mathcal{O}$ dans un corps quadratique imaginaire $K$. Alors, $L$ est une extension galoisienne de $\mathbb{Q}$ et on a $\mathrm{Gal}(L/\mathbb{Q}) \simeq \mathrm{Gal}(L/K) \rtimes (\mathbb{Z}/2\mathbb{Z})$ où l'élément non trivial de $\mathbb{Z}/2\mathbb{Z}$ agit sur $\mathrm{Gal}(L/K)$ en envoyant $\sigma$ sur son inverse $\sigma^{-1}$.*

*Démonstration.* Tout d'abord, montrons $\tau(L) = L$ où $\tau$ est la conjugaison complexe.
Soit $\mathfrak{m}$ désignant le module $f\mathcal{O}_K$ et remarquons $\tau(\mathfrak{m}) = \mathfrak{m}$. On rappelle que $\left(\frac{L/K}{\cdot}\right)_{\mathfrak{m}}$ est l'application d'Artin. Comme $\mathrm{Ker}\left(\frac{L/K}{\cdot}\right)_{\mathfrak{m}} = P_{K,\mathbb{Z}}(f)$ un calcul facile montre que :

$$\begin{aligned}\mathrm{Ker}\left(\frac{L/K}{\cdot}\right)_{\mathfrak{m}} &= \tau(\mathrm{Ker}\left(\frac{L/K}{\cdot}\right)_{\mathfrak{m}}) \\ &= \tau(P_{K,\mathbb{Z}}(f)) \\ &= P_{K,\mathbb{Z}}(f)\end{aligned}$$

Donc $\mathrm{Ker}\left(\frac{\tau(L)/K}{\cdot}\right)_{\mathfrak{m}} = \mathrm{Ker}\left(\frac{L/K}{\cdot}\right)_{\mathfrak{m}}$. Alors, $\tau(L) = L$ grâce au théorème 2.29. De ce fait, $L/\mathbb{Q}$ est galoisienne et on a la suite exacte :

$$1 \to \mathrm{Gal}(L/K) \to \mathrm{Gal}(L/\mathbb{Q}) \to \mathrm{Gal}(K/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \to 1$$

Comme $\tau \in \mathrm{Gal}(L/\mathbb{Q})$, on a $\mathrm{Gal}(L/K) \rtimes (\mathbb{Z}/2\mathbb{Z})$ où l'élément non trivial de $\mathbb{Z}/2\mathbb{Z}$ agit par conjugaison par $\tau$.
Pour un premier $\mathfrak{p}$ de $K$, on a :

$$\begin{aligned}\tau\left(\frac{L/K}{\mathfrak{p}}\right)\tau^{-1} &= \left(\frac{L/K}{\tau(\mathfrak{p})}\right)\\ &= \left(\frac{L/K}{\overline{\mathfrak{p}}}\right)\end{aligned}$$

Sous l'isomorphisme $I_K(f)/P_{K,\mathbb{Z}}(f) \simeq \mathrm{Gal}(L/K)$ la conjugaison par $\tau$ dans $\mathrm{Gal}(L/K)$ correspond à l'action usuelle de $\tau$ sur $I_K(f)$.
Mais si $\mathfrak{a}$ est un idéal de $I_K(f)$ alors $\mathfrak{a}\overline{\mathfrak{a}} = N(\mathfrak{a})O_K \in P_{K,\mathbb{Z}}(f)$. □

## 5.2 Extensions diédrales généralisées

Soient $K$ un corps quadratique imaginaire de discriminant $d_K$, $L/K$ une extension (galoisienne) abélienne. Comme la conjugaison complexe $\tau$ est un automorphisme de $L$, on a $\mathrm{Gal}(L/\mathbb{Q}) \simeq \mathrm{Gal}(L/K) \rtimes \mathbb{Z}/2\mathbb{Z}$ où l'élément non trivial de $\mathbb{Z}/2\mathbb{Z}$ agit sur $\mathrm{Gal}(L/K)$ par conjugaison par $\tau$.

**Définition 5.5.** *Une extension abélienne $L/K$ est une extension diédrale généralisée de $\mathbb{Q}$ si l'action de son groupe de Galois envoie tout élémént de $\mathrm{Gal}(L/K)$ sur son inverse.*

Avec la proposition 5.4, on a montré tout anneau de corps de classe $L$ est une extension diédrale généralisée sur $\mathbb{Q}$.

**Théorème 5.6.** *Soit $K$ un corps quadratique imaginaire.*
*Alors une extension abélienne $L$ de $K$ est une extension diédrale généralisée si et seulement $L$ est contenu dans un anneau du corps de classe de $K$.*

*Démonstration.* Tout d'abord, on sait qu'une extension de $K$ contenu dans un anneau du corps de classe de $K$ est une extension diédrale généralisée.

Réciproquement, fixons $L/K$ abélienne diédrale généralisée sur $\mathbb{Q}$.
Par la loi de réciprocité d'Artin, il existe un idéal $\mathfrak{m}$ et un sous-groupe $P_{K,1}(\mathfrak{m}) \subset H \subset I_K(\mathfrak{m})$ tel que l'application d'Artin induit un isomorphisme $I_K(\mathfrak{m})/H \xrightarrow{\sim} \mathrm{Gal}(L/K)$.
On a vu que si $\mathfrak{m}$ est assez grand, on peut supposer $\mathfrak{m} = fO_K$ pour un $f$ entier. On peut supposer $d_k | f$.
Pour prouver le théorème, il suffit de montrer que $P_{K,\mathbb{Z}}(f) \subset H$ cela impliquant que $L$ appartient à l'anneau du corps de classe pour l'ordre de

conducteur $f$ dans $\mathcal{O}_K$.
De la définition de $P_{K,\mathbb{Z}}(f)$, on doit prouver la propriété suivante :

$$c \in \mathbb{Z}, c \wedge f = 1, u \equiv c \mod f \implies u\mathcal{O}_K \in H \tag{5}$$

On utilise le fait que $P_{K,1}(f\mathcal{O}_K) \subset H$ : si $\alpha, \beta \in \mathcal{O}_K$ sont premiers avec $f$ alors on affirme que :

$$\alpha \equiv \beta \mod f\mathcal{O}_K \text{ donc } (\alpha\mathcal{O}_K \in H \text{ si et seulement si } \beta\mathcal{O}_K \in H) \tag{6}$$

Pour prouver cela, prenons $\gamma \in \mathcal{O}_K$ tel que $\alpha\gamma \equiv 1 \mod f\mathcal{O}_K$) alors $\beta\gamma \equiv 1 \mod f\mathcal{O}_K$ est vraie donc on a $\alpha\gamma\mathcal{O}_K, \beta\gamma\mathcal{O}_K \in P_{K,1}(f\mathcal{O}_K) \subset H$ donc l'affirmation suit.
Alors, on a (5) si et seulement si $c \in \mathbb{Z}, c \wedge f = 1$ donc $c\mathcal{O}_K \in H$.
Pour voir le lien entre (5) et le fait que $L$ que soit une extension diédrale généralisé sur $\mathbb{Q}$, prenons l'isomorphisme $I_K(\mathfrak{m})/H \xrightarrow{\sim} \mathrm{Gal}(L/K)$, on sait que la conjugaison par $\tau$ sous $\mathrm{Gal}(L/K)$ correspond à l'action usuelle de $\tau$ sur $I_K(f)$. Alors le fait que $L$ soit une extension diédrale généralisé sur $\mathbb{Q}$ signifie que pour tout $\mathfrak{a} \in I_K(f)$ la classe de $\overline{a}$ est donnée par l'inverse de $\mathfrak{a}$ dans $I_K(f)/H$ donc $\mathfrak{a}\overline{\mathfrak{a}} \in H$. Comme $\mathfrak{a}\overline{\mathfrak{a}} = N(\mathfrak{a})O_K$, on a :

$$\forall \mathfrak{a} \in I_K(f), N(\mathfrak{a})O_K \in H \tag{7}$$

On est amené à montrer que (7) implique (5).
Notons qu'il suffit de prouver (5) quand $c$ est un premier $p$ ne divisant par $f$. Rappelons que $d_K | f$ donc $p$ ne divise pas $d_K$ si et seulement si $p$ est non ramifiée

- $p$ est décomposé alors $p = N(\mathfrak{p})$ où $\mathfrak{p}$ est un facteur premier de $p\mathcal{O}_K$. Alors, grâce à (7), on a $p\mathcal{O}_K = N(\mathfrak{p})O_K \in H$ comme voulu.

- Sinon, $\left(\frac{d_k}{p}\right) = -1$. Soit $q$ un premier tel que $q \equiv -p \mod f$ grâce au théorème de Dirichlet. On affirme que $q$ se décompose totalement dans ce cas.
  On sait que $\left(\frac{d_k}{\cdot}\right)$ induit un morphisme bien défini :
  $\chi : (\mathbb{Z}/d_K\mathbb{Z})^* \to \{\pm 1\}$ et comme $d_K < 0$, on sait que $\chi([-1]) = -1$.
  Or $d_K | f$, on a $q \equiv -p \mod d_K$) et donc $\left(\frac{d_K}{p}\right) = \chi([q]) = \chi([-p])$.
  Donc, on a :

$$\begin{aligned}\left(\frac{d_K}{q}\right) &= \chi([-1])\chi([p]) \\ &= -\left(\frac{d_K}{p}\right) \\ &= 1\end{aligned}$$

Donc $q$ se décompose totalement, cela implique que $q\mathcal{O}_K \in H$ et donc $q \equiv -p \mod f\mathcal{O}_K$. Cela implique que $q\mathcal{O}_K \in H$ et donc $q \equiv -p \mod f\mathcal{O}_K$) et (6) implique que $p\mathcal{O}_K = (-p)\mathcal{O}_K \in H$ prouvant (5).

□

On a donc une caractérisation de certaines extensions abéliennes d'un corps quadratique imaginaire, notre but final étant généraliser le théorème de Kronecker-Weber au cas des corps quadratiques imaginaires.

## 5.3 Un exemple de lien entre la ramification et l'anneau du corps de classe

On conclut ce chapitre par un exemple qui nous sera utile dans une démonstration plus tard :

**Théorème 5.7.** *Soient $n > 0$ un entier et $L$ l'anneau du corps de classe de $\mathbb{Z}[\sqrt{-n}]$ dans le corps quadratique imaginaire $K = \mathbb{Q}(\sqrt{-n})$. Si $p$ est un premier impaire ne divisant pas $n$ alors :*

$$p = x^2 + ny \text{ si et seulement si } p \text{ se décompose totlament dans } L.$$

*Démonstration.* Soit $\mathcal{O} = \mathbb{Z}[\sqrt{-n}]$, son discriminant est $-4n = f^2 d_K$, $f$ étant le conducteur de $\mathcal{O}$. Soit $p$ un premier impair ne divisant pas $n$. Alors $p$ ne divise pas $f^2 d_K$ impliquant que $p$ n'est pas ramifié dans $K$. Notre but est de montrer les équivalences suivantes :

$$\begin{aligned}
p = x^2 + ny^2 &\iff p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}},\ \mathfrak{p} \neq \overline{\mathfrak{p}} \text{ et } \overline{\mathfrak{p}} = \alpha\mathcal{O}_K, \alpha \in \mathcal{O} \\
&\iff p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}},\ \mathfrak{p} \neq \overline{\mathfrak{p}} \text{ et } \mathfrak{p} \in P_{K,\mathbb{Z}}(f) \\
&\iff p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}},\ \mathfrak{p} \neq \overline{\mathfrak{p}} \text{ et } \left(\frac{L/K}{\mathfrak{p}}\right) = 1 \\
&\iff p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}},\ \mathfrak{p} \neq \overline{\mathfrak{p}} \text{ et } \mathfrak{p} \text{ se décompose totalement dans } L \\
&\iff p \text{ se décompose totalement dans } L.
\end{aligned}$$

Pour la première équivalence, supposons $p = x^2 + ny^2 = (x + \sqrt{-n}y)(x - \sqrt{-n}y)$. Si on pose $\mathfrak{p} = (x + \sqrt{-n}y)\mathcal{O}_K$ alors $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$ est la factorisation en facteurs premiers de $p\mathcal{O}_K$ dans $\mathcal{O}_K$. De plus, $x + \sqrt{-n}y \in \mathcal{O}$ et $\mathfrak{p} \neq \overline{\mathfrak{p}}$ car $\mathfrak{p}$ est non ramifié dans $K$.
Réciproquement, si $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$ où $\mathfrak{p} = (x + \sqrt{-n}y)\mathcal{O}_K$, on a $p = x^2 + ny^2$.

Comme $p$ ne divise pas $f$, la deuxième équivalence découle de la proposition 4.36.

Pour les deux suivantes, l'isomorphisme $\mathrm{Gal}(L/K) \simeq I_K(f)/P_{K,\mathbb{Z}}(f)$ nous montre, par l'application d'Artin que $\mathfrak{p} \in P_{K,\mathbb{Z}}(f)$ si et seulement si $\left(\frac{L/K}{\mathfrak{p}}\right)$

si et seulement si $\mathfrak{p}$ se décompose totalement dans $L$.

Pour la dernière équivalence, la propostion 5.4 montre que $L/\mathbb{Q}$ est galoisienne donc $p$ se ramifie totalement dans $L$. □

# 6 Réseaux et fonctions elliptiques

Notre but est maintenant d'établir que le $j$-invariant d'un réseau $\Lambda$ de $\mathbb{C}$ est un entier algébrique. Pour cela, on commence à faire un pas vers la géométrie grâce à l'analyse complexe. Nous allons introduire dans le plan complexe, par ordre d'apparition, la notion de réseaux puis de fonction elliptiques pour pouvoir définir la notion de $j$-invariant. Les références pour cette section sont [2] et [6].

## 6.1 Réseaux et fonctions elliptiques

On commence par définir quelques objets basiques. Tout d'abord la notion de réseaux qui va devenir rapidement incontournable pour notre propos :

**Définition 6.1.** *Un sous-ensemble $\Lambda \subset \mathbb{C}$ est un réseau de $\mathbb{C}$ si c'est un sous-groupe additif engendré par deux nombres complexes $\omega_1$ et $\omega_2$ tel que $(w_1, w_2)$ soit une famille $\mathbb{R}$-libre. On écrira $\Lambda = [\omega_1, \omega_2]$.*

Introduisons un peu d'analyse complexe dans notre raisonnement. Cela nous permettra de mieux comprendre la notion de réseau (et plus tard de courbes elliptiques) :

**Définition 6.2.** *Soit $\Lambda$ un réseau de $\mathbb{C}$, une fonction $f$ définie sur $\mathbb{C}$, excepté aux singularités isolées, est elliptique pour $\Lambda$ si elle vérifie :*

- *$f$ est méromorphe sur $\mathbb{C}$.*
- *Pour tout $\omega \in \Lambda$, et $z \in \mathbb{C} \setminus \Lambda$, $f(z+\omega) = f(z)$.*

*Le deuxième item est équivalent à :*
*Si $\Lambda = [\omega_1, \omega_2]$, pour tout $z \in \mathbb{C} \setminus \Lambda$, on a $f(z+\omega_1) = f(z+\omega_2) = f(z)$.*

Intéressons nous à une fonction elliptique, la $\wp$-fonction de Weierstrass :

**Définition 6.3.** *Pour un réseau $\Lambda$, et pour $z \in \mathbb{C}\setminus\Lambda$,on définit la $\wp$-fonction de Weierstrass par :*

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{\omega\in\Lambda,\omega\neq 0} \left( \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

*Quand il n'y aura aucune ambiguité sur le réseau $\Lambda$ on notera $\wp_\Lambda(z) = \wp(z)$*

Nous caractérisons maintenant les propriétés des $\wp$-fonction de Weierstrass :

**Théorème 6.4.**

- *$\wp_L$ est une fonction elliptique.*
  *De plus, les singularités sont les points de $\Lambda$ et ce sont des pôles d'ordre deux.*
- *En posant $g_2(\Lambda) = 60\sum_{\omega\in\Lambda,\omega\neq 0}\frac{1}{\omega^4}$ et $g_2(\Lambda) = 140\sum_{\omega\in\Lambda,\omega\neq 0}\frac{1}{\omega^6}$ on a :*

$$(\wp'_\Lambda(z))^2 = 4\wp_\Lambda(z) - g_2(\Lambda)\wp_\Lambda(z) - g_3(\Lambda).$$

- *Pour $z,\omega \notin \Lambda$ tel que $z+\omega \notin \Lambda$ on a la loi additive :*

$$\wp_\Lambda(z+\omega) = -\wp_\Lambda(z) - \wp_\Lambda(\omega) - \frac{1}{4}\left(\frac{\wp'_\Lambda(z) - \wp'_\Lambda(\omega)}{\wp_\Lambda(z) - \wp_\Lambda(\omega)}\right)^2$$

*Démonstration.* Premier item

On commence par établir un lemme :

**Lemme 6.5.** *Pour $r > 2$, la série $G_r(\Lambda) = \sum_{\omega\in\Lambda,\omega\neq 0}\frac{1}{\omega^2}$ converge absolument.*

*Démonstration du lemme.* Si $\Lambda = [\omega_1, \omega_2]$, on doit montrer que :

$$\sum_{\omega\in\Lambda,\omega\neq 0}\frac{1}{|\omega|^r} = \sum_{(m,n)\in(\mathbb{N}^*)^2}\frac{1}{|m\omega_1 + n\omega_2|^r} \text{ converge}$$

Posons, $M = \min\{|x\omega_1 + y\omega_2| \text{ tel que } x^2 + y^2 = 1\}$.
Alors, pour tout $x, y \in \mathbb{R}, |x\omega_1 + y\omega_2| \leq M\sqrt{x^2+y^2}$.
Donc, on obtient :

$$\sum_{(m,n)\in(\mathbb{N}^*)^2}\frac{1}{|m\omega_1 + n\omega_2|^r} \leq \frac{1}{M^r}\sum_{(m,n)\in(\mathbb{N}^*)^2}\frac{1}{(m^2+n^2)^{\frac{r}{2}}}$$

En comparant la somme de droite à l'intégrale $\int\int_{x^2+y^2\geq 1}\frac{1}{(x^2+y^2)^{\frac{r}{2}}}dxdy$ on conclut que la somme converge quand $r > 2$. □

Maintenant, montrons que $\wp_\Lambda$ est holomorphe sur $\mathbb{C} - \Lambda$.

Si $\Omega \subset \mathbb{C}$ compact tel que $\Omega \cap \Lambda = \emptyset$, il sufit de montrer que la somme ci-dessous converge absolument et uniformément sur $\Omega$ :

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{\omega\in\Lambda,\omega\neq 0}\left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right)$$

Soit $R \in \mathbb{R}$ tel que pour tout $z \in \Omega, |z| \leq R$.
Supposons maintenant que $z \in \Omega$ et $\omega \in \Lambda$ tel que $|\omega| \leq 2R$.
Alors $|z - \omega| \geq \frac{1}{2}|\omega|$ et on voit que :

$$\begin{aligned} |\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}| &\leq |\frac{z(2\omega - z)}{\omega^2(z-\omega)^2}| \\ &\leq \frac{R(2|\omega| + \frac{1}{2}|\omega|)}{|\omega|^2(\frac{1}{2}|\omega|)} = \frac{10R}{|\omega|^3} \end{aligned}$$

Comme $|\omega| \geq 2R$ pour un nombre fini d'élément de $\Lambda$, on a grâce au lemme 6.5 que cette somme converge absolument et uniformément sur $\Omega$.
Ainsi, $\wp$ est holomorphe sur $\mathbb{C} \setminus \Lambda$ et possède un pôle d'ordre 2 en l'origine.
Comme $(-z-\omega)^2 = (z-(-\omega))^2$, l'identité $\wp_L(-z) = \wp_L(z)$ montre que $\wp_L$ est une fonction paire qui converge absolument.

Attelons nous à la périodicité maintenant. Cela est un peu plus astucieux. On commence par dériver une première fois :

$$\wp'_\Lambda(z) = -2 \sum_{\omega \in \Lambda} \frac{1}{(z-\omega)^3}$$

Cette série converge absolument et on voit que $\wp'_\Lambda$ est elliptique pour $\Lambda$.
Maintenant, supposons que $\Lambda = [\omega_1, \omega_2]$, les fonctions $\wp_\Lambda(z)$ et $\wp_\Lambda(z + \omega_i)$ ont la même dérivée car $\wp'_\Lambda$ est périodique.
Ainsi, on a $\wp_\Lambda(z) = \wp(z + \omega_i) + C$. En évaluant en $-\frac{\omega_i}{2} \notin \Lambda$, on a :

$$\begin{aligned} \wp_\Lambda(\frac{-\omega_i}{2}) &= \wp_\Lambda(\frac{-\omega_i}{2} + \omega_i) + C \\ &= \wp_\Lambda(\frac{-\omega_i}{2}) + C \end{aligned}$$

Comme $\wp_\Lambda$ est paire, on a $C = 0$ et la périodicité est établie. De ce fait, les pôles de $\wp_\Lambda$ seront d'ordre 2 et se sont des points de $\Lambda$.

Deuxième item
On va calculer la série de Laurent de $\wp_\Lambda$ en l'origine.

**Lemme 6.6.** *Au voisinage de l'origine, on a :*

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{n \leq 1} (2n+1) G_{2n+2}(\Lambda) z^{2n}.$$

*Démonstration du lemme.* Pour $|x| < 1$, on a :

$$\frac{1}{(1-x^2)} = 1 + \sum_{n\geq 1}(n+1)x^n.$$

Donc si $|x| < \omega$, on peut poser $x = \dfrac{z}{\omega}$ et on a :

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \sum_{n\geq 1}\frac{n+1}{\omega^{n+2}}z^n.$$

En sommant pour tout $\omega \in \Lambda, \omega \neq 0$, on a grâce à la convergence absolue :

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{n\geq 1}(n+1)G_{n+2}(\Lambda)z^n.$$

On obtient l'identité désirée en notant que $\wp_\Lambda$ est une fonction paire. De ce fait, les coefficients impairs sont nuls et on peut conclure. □

De ce lemme on obtient par un calcul simple :

$$\begin{aligned}
\wp'_\Lambda &= \frac{-2}{z^3} + \sum_{n\leq 1} 2n(2n+1)G_{2n+2}(\Lambda)z^{2n-1} \\
\wp^3_\Lambda &= \frac{1}{z^6} + \frac{9G_4(\Lambda)}{z^2} + 15G_6(\Lambda) + \dots \\
(\wp'_\Lambda)^2 &= \frac{4}{z^6} - \frac{24G_4(\Lambda)}{z^2} - 80G_6(\Lambda) + \dots
\end{aligned}$$

Maintenant, considérons la fonction elliptique :

$$F(z) = \wp'_\Lambda(z)^2 - 4\wp(z) + 60G_4(\Lambda)\wp(z) + 140G_6(\Lambda)$$

On voit que $F$ s'annule pour $z = 0$ et par périodicité, elle est nulle sur $\Lambda$. Cependant, elle est holomorphe sur $\mathbb{C} - \Lambda$ donc $F$ est entière. Par le théorème de Liouville, elle est constante donc identiquement nulle.
Or $g_2(\Lambda) = 60G_4(\Lambda)$ et $g_3(\Lambda) = 140G_6(\Lambda)$, le deuxième item est établi.

Troisième item
Encore une fois, on commence par établir un lemme :

**Lemme 6.7.** *Si $z, \omega \notin \Lambda$, $\wp_\Lambda(z) = \wp_\Lambda(\omega)$ si et seulement si $z = \pm\omega \mod \Lambda$.*

*Démonstration du lemme.* Supposons $z = \pm\omega \mod \Lambda$, comme $\wp_L$ est paire, on a l'égalité.

Réciproquement, supposons que $\Lambda = [\omega_1, \omega_2]$ et fixons un nombre $-1 < \delta < 0$.
Soient $\mathbb{P} = \{s\omega_1 + t\omega_2 : \delta \leq s, t \leq \delta + 1\}$ un parallélogramme et $\Gamma$ l'ensemble-limite orienté dans le sens des aiguilles d'une montre. Notons que tout nombre complexe est congru modulo $\Lambda$ à un nombre dans $\mathbb{P}$.
Fixons $\omega$ et considérons $f(z) = \wp_\Lambda(z) - \wp_\Lambda(\omega)$. En ajustant $\delta$, on peut s'assurer que $f$ ni de zéro ni de pôle dans $\Gamma$. Alors, en notant, avec multiplicité, $Z$(resp. $P$) le nombre de zéros (resp. pôles), on a :

$$\frac{1}{2\pi i}\int_\Gamma \frac{f'(z)}{f(z)}dz = Z - P$$

Comme $\dfrac{f'(z)}{f(z)}$ est périodique, l'intégrale s'annule sur les bords de $\Gamma$ et $\int_\Gamma \dfrac{f'(z)}{f(z)}dz = 0$ montrant $Z = P$.
P est facile à calculer. Par définition de $\mathbb{P}$, 0 est le pôle de $f$ dans $\mathbb{P}$.
De plus, il est double donc $Z = P = 2$.
On a deux cas à considérer :

- Si Si $\omega \not\equiv -\omega \mod \Lambda$ alors $\omega$ et $-\omega$ sont deux points distincts de $\mathbb{P}$ et ce sont deux zéros de $f$ du fait que $Z = 2$. Ils sont donc de multiplicité 1.

- Si $\omega \equiv -\omega \mod \Lambda$ alors $2\omega \in \Lambda$ et comme $\wp'_\Lambda$ est une fonction impaire on obtient :

$$\begin{aligned}\wp'_\Lambda(\omega) &= \wp'_\Lambda(\omega - 2\omega)\\ &= \wp'_\Lambda(-\omega)\\ &= -\wp'_\Lambda(\omega)\end{aligned}$$

  Donc $\wp'_\Lambda(\omega) = 0$. Ainsi modulo $\Lambda$, $\omega$ fournit un zéro de $f$ d'ordre au moins 2 dans $\mathbb{P}$ comme $Z = 2$ on peut conclure.

□

Grâce à la démonstration du lemme 6.7 on a obtenu :

**Corollaire 6.8.** *Si $\omega \notin \Lambda, \wp'(\omega) = 0$ si et seulement si $2\omega \in \Lambda$.*

Etablissons le troisième item. On fixe $\omega \notin \Lambda$ et on considère la fonction elliptique :

$$G(z) = \wp_\Lambda(z+\omega) + \wp_\Lambda(z) + \wp_\Lambda(\omega) - \frac{1}{4}\left(\frac{\wp'_\Lambda(z) - \wp'_\Lambda(\omega)}{\wp_\Lambda(z) - \wp_\Lambda(\omega)}\right)^2$$

$G$ est une fonction holomorphe sur $\mathbb{C}$ qui s'annule en l'origine. Le théorème de Liouville implique donc que $G$ est identiquement nulle.
Avec le lemme 6.7, les possibles singularités de $G$ proviennent de trois endroits :

- $\Lambda$
- $\Lambda + \{\omega\}$
- $\Lambda - \{\omega\}$

Par périodicité, il suffira de considérer $G(0)$, $G(\omega)$ et $G(-\omega)$.
Pour $G(0)$.
Le développement en série de Laurent de $\wp_L$ et $\wp_l'$ nous donnent :

$$\begin{aligned}\frac{1}{4}\left(\frac{\wp'_\Lambda(z)-\wp'_\Lambda(\omega)}{\wp_\Lambda(z)-\wp_\Lambda(\omega)}\right)^2 &= \frac{1}{4}\left(\frac{-\frac{2}{z^3}-\wp'_\Lambda(z)+\dots}{\frac{1}{z^2}-\wp_\Lambda(z)+\dots}\right)^2 \\ &= \frac{1}{z^2}+2\wp_\Lambda(w)+\dots\end{aligned}$$

Ainsi, $G(z) = \wp_\Lambda(z+\omega)+\wp_\Lambda(\omega)+\frac{1}{z^2}+\dots-\frac{1}{z^2}-2\wp_\Lambda(\omega)-\dots$ donc $G(0)=0$.

Supposons $2\omega \notin \Lambda$, avec la règle de l'Hospital, on obtient :

$$G(\omega) = \wp(2\omega)+2\wp(\omega)-\frac{1}{4}\left(\frac{\wp''(\omega)}{\wp'(\omega)}\right)^2.$$

Comme $2\omega \notin \Lambda$, le corollaire 6.8 montre que $\wp(\omega) \neq 0$ et $G(\omega)$ est défini.
On est ramené à considérer $G(-\omega)$.
On calcule la série de Laurent pour $z = -\omega$ :

$$\begin{aligned}\wp(z+\omega) &= \frac{1}{(z+\omega)^2}+\dots \\ \wp(z) = \wp(-\omega)+\wp'(-\omega)(z+\omega)+\dots &= \wp(\omega)-\wp'(\omega)(z+\omega)+\dots\end{aligned}$$

où $+\dots$ réfère aux puissances supérieurs de $z+\omega$. Comme $\wp'(\omega) \neq 0$, ces formules nous permettent de montrer que $G(-\omega)$ est définie en utilisant le fait que $\wp$ est une fonction paire.
Donc $G$ est holomorphe et s'annule en 0 donc $G$ est nulle partout.

Il reste a considérer le cas $2\omega \in \Lambda$. Considérons $(\omega_n)_{n\in\mathbb{N}}$ tel que $\omega_n$ converge vers $\omega$ et pour tout $n \in \mathbb{N}$, $2\omega_n \notin \Lambda$.
Donc ce qui précéde s'applique pour chaque terme de la suite, en utilisant le prolongement analytique. □

## 6.2 $j$-invariant d'un réseau

On définit la relation d'équivalence entre deux réseaux :

**Définition 6.9.** *Deux réseaux $\Lambda, \Lambda'$ de $\mathbb{C}$ sont homothétique s'il existe $\lambda \in \mathbb{C}^*$ tel que $\Lambda' = \lambda\Lambda$.*

**Remarque 6.10.** *Si $f$ est une fonction elliptique pour $\Lambda$ alors $f(\lambda^{-1}.)$ est une fonction elliptique pour $\lambda\Lambda$ et on a $\wp_{\lambda\Lambda}(\lambda.) = \lambda^2\wp_\Lambda(.)$*

On va introduire la notion de $j$-invariant pour pouvoir classifier les réseaux. Avec le théorème 6.4, on a l'existence de deux constantes dans l'équation différentielle vérifié par la $\wp$-fonction de Weierstrass $g_2$ et $g_3$ qui ne dépendent que du réseau $\Lambda$.

**Définition 6.11.** *Pour un réseau $\Lambda$, on pose $\Delta(\Lambda) = g_2(\Lambda)^2 - 27g_3(\Lambda)^2$.*

Notons que $\Delta(\Lambda)$ est relié au discriminant de l'équation $x^3 - g_2(\Lambda)x - g_3(\Lambda)$. En notant $(e_1, e_2, e_3)$ les racines de ce polynôme on obtient :
$\Delta(\Lambda) = 16(e_1 - e_2)^2(e_1 - e_3)^2(e_2 - e_3)^2$.

**Proposition 6.12.** *Si $\Lambda$ est un réseau alors $\Delta(\Lambda) \neq 0$.*

*Démonstration.* Si $\omega \notin \Lambda$ et $2\omega \in \Lambda$ alors $\wp'_\Lambda(\omega) = 0$.
Ainsi, on a $0 = \wp'_\Lambda(\omega)^2 = 4\wp_\Lambda(\omega)^3 - g_2(\Lambda)\wp_\Lambda(\omega) - g_3(\Lambda)$. Donc $\wp_\Lambda(\omega)$ est une racine de $4x^3 - g_2(\Lambda)x - g_3(\Lambda)$.
Si $\Lambda = [\omega_1, \omega_2]$ ce processus fournit trois racines
$\wp_\Lambda(\frac{\omega_1}{2})$, $\wp_\Lambda(\frac{\omega_2}{2})$ et $\wp_\Lambda(\frac{\omega_1+\omega_2}{2})$. Elles sont distinctes pour deux raisons :

- Si $x, y \notin \Lambda$ alors $x \equiv \pm y \mod \Lambda$ si et seulement si $\wp_\Lambda(x) = \wp_\Lambda(y)$.
- $\pm\frac{\omega_1}{2}$, $\pm\frac{\omega_2}{2}$ et $\pm\frac{\omega_1+\omega_2}{2}$ sont distinctes modulo $\Lambda$.

Alors les racines de $4x^3 - g_2(\Lambda)x - g_3(\Lambda)$ sont simples donc $\Delta(\Lambda) \neq 0$. □

On peut maintenant définir le nombre $j(\Lambda)$ :

**Définition 6.13.** *On définit le $j$-invariant d'un réseau $\Lambda$ par :*

$$\begin{aligned} j(\Lambda) &= 1728\frac{g_2(\Lambda)^3}{\Delta(\Lambda)} \\ &= 1728\frac{g_2(\Lambda)^3}{g_2(\Lambda)^3 - 27g_3(\Lambda)} \end{aligned}$$

**Remarque 6.14.** *Si $\Lambda$ est un réseau alors $\Delta(\Lambda) \neq 0$ donc $j(\Lambda)$ est toujours défini.*

On caractérise son intérêt :

**Théorème 6.15.** *Pour $\Lambda, \Lambda'$ deux réseaux de $\mathbb{C}$ on a :*
*$j(\Lambda) = j(\Lambda')$ si et seulement s'il existe $\lambda \in \mathbb{C}, \Lambda' = \lambda\Lambda$.*

*Démonstration.* Si $\lambda \in \mathbb{C}$, non nul, tel que $\Lambda' = \lambda\Lambda$ alors la définition de $g_2(\Lambda)$ et $g_3(\Lambda)$ implique que $g_2(\lambda\Lambda) = \lambda^{-4}g_2(\Lambda)$ et $g_3(\lambda\Lambda) = \lambda^{-6}g_3(\Lambda)$.
Donc $j(\lambda\Lambda) = j(\Lambda)$.

Réciproquement, supposons que $\Lambda$ et $\Lambda'$ sont des réseaux tels que $j(\Lambda) = j(\Lambda')$. On affirme qu'il existe $\lambda \in \mathbb{C}$ tel que $g_2(\Lambda') = \lambda^{-4}g_2(\Lambda)$ et $g_3(\Lambda') = \lambda^{-6}g_3(\Lambda)$.
Quand $g_2(\Lambda') \neq 0$ et $g_3(\Lambda') \neq 0$ on peut choisir un nombre $\lambda$ tel que $\lambda^4 = \dfrac{g_2(\Lambda)}{g_2(\Lambda')}$.
Comme $j(\Lambda) = j(\Lambda')$ on a $\lambda^{12} = \left(\dfrac{g_3(\Lambda)}{g_3(\Lambda')}\right)^2$ donc $\lambda^6 = \pm\dfrac{g_3(\Lambda)}{g_3(\Lambda')}$.
En remplaçant $\lambda$ par $i\lambda$ si nécessaire, on peut supposer que le signe est $+$ et l'affirmation suit.

Avec la remarque 6.14, on a $g_2(\Lambda') = 0$ ou $g_3(\Lambda') = 0$ mais les deux ne peuvent pas l'être simultanément.
Si $g_2(\Lambda') = 0$, on a $j(\Lambda) = j(\Lambda') = 0$ donc pour $\lambda = 0$ on a les égalités voulues.
Si $g_3(\Lambda') = 0$, on a $j(\Lambda) = j(\Lambda') = 1$ donc pour $\lambda = 1$ on a les égalités voulues.

Pour exploiter l'affirmation on aura besoin du lemme :

**Lemme 6.16.** *On rappelle qu'au voisinage de 0, on a :*

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{n\geq 1}(2n+1)G_{2n+2}(\Lambda)z^{2n}.$$

*Alors, pour $n \geq 1$, le coefficient $(2n+1)G_{2n+2}(\Lambda)$ de $z2n$ est un polynôme de $\mathbb{Q}[X]$ indépendant de $\Lambda$ en $g_2(\Lambda)$ et $g_3(\Lambda)$.*

*Démonstration du lemme.* Par simplicité, on notera $a_n = (2n+1)G_{2n+2}(\Lambda)$.
Tout d'abord, on a en dérivant :

$$\wp'_\Lambda(z)^2 = 4\wp_\Lambda(z)^3 - g_2(\Lambda)\wp_\Lambda(z) - g_3(\Lambda).$$
$$\wp''_\Lambda(z) = 6\wp_\Lambda(z)^2 - \frac{1}{2}g_2(\Lambda)$$

En appliquant le développement en série de Laurent et en comparant les coefficients de $z^{2n-2}$, on voit que pour $n \geq 3$ on obtient :

$$2n(2n-1)a_n = 6(2a_n + \sum_{1 \leq i \leq n-2} a_i a_{n-1-i}).$$

$$\text{Donc } (2n+3)(n-2)a_n = 3 \sum_{1 \leq i \leq n-2} a_i a_{n-1-i}.$$

Comme $\begin{cases} g_2(\Lambda) = 60G_4(\Lambda) = 20a_1 \\ g_3(\Lambda) = 140G_6(\Lambda) = 28a_2. \end{cases}$
Par une récurrence directe, on montre que $a_n$ est polynômiale à coefficients rationnels en $g_2(\Lambda)$ et $g_3(\Lambda)$ prouvant ainsi le lemme. □

Maintenant, supposons que $\Lambda$ et $\Lambda'$ sont des réseaux comme dans l'affirmation pour une certaine constante $\lambda$. Montrons que $\Lambda' = \lambda\Lambda$.
Comme on a $\begin{cases} g_2(\Lambda') = \lambda^{-4} g_2(\Lambda) \\ g_3(\Lambda') = \lambda^{-6} g_3(\Lambda) \end{cases}$ on obtient donc $\begin{cases} g_2(\Lambda') = g_2(\lambda\Lambda) \\ g_3(\Lambda') = g_3(\lambda\Lambda) \end{cases}$
Donc grâce au lemme 6.16 on peut conclure que $\wp_{\lambda\Lambda}$ et $\wp_{\Lambda'}$ ont la même série de Laurent au voisinagine de 0 donc $\wp_{\Lambda'} = \wp_{\lambda\Lambda}$ sur $\mathbb{C}$.
Comme l'ensemble des pôles de $\wp_\Lambda$ est le réseau, le théorème est établit. □

On finit cette section par définir la fonction $j$ associé aux $j$-invariants.

**Définition 6.17.** *On rappelle que* $\mathbb{H} = \{z \in \mathbb{C}, z = x + iy/y > 0\}$.
*On peut définir une fonction* $j : \tau \in \mathbb{H} \longmapsto j([1, \tau])$.

# 7 La fonction $j$

Dans cette section, on établit le fait que $j$-invariant d'un réseau est un nombre algébrique. Cela sera l'occasion de faire une brève étude de la fonction $j$. La référence pour cette section est [2].

## 7.1 Le $j$-invariant d'un réseau est un nombre algébrique

Nous allons maintenant introduire la notion de multiplication complexe pour établir que je $j$-invariant d'un réseau est un nombre algébrique.

Pour un ordre $\mathcal{O}$ dans un corps quadratique imaginaire $K$ et $\mathfrak{a}$ un idéal fractionnaire propre de $\mathcal{O}$, on a $\mathfrak{a} = [\alpha, \beta]$ avec $\alpha, \beta \in K$.
On considéra $K$ comme un sous-ensemble de $\mathbb{C}$ et comme $K$ est un corps quadratique imaginaire, on sait que $(\alpha, \beta)$ est une famille $\mathbb{R}$-libre.
Donc $\mathfrak{a}$ est un réseau de $\mathbb{C}$ alors nous pouvons définir

**Définition 7.1.** *On appelle $j(\mathfrak{a})$ le module singulier.*

On commence par établir une propriété des fonction utile des fonctions elliptiques :

**Proposition 7.2.** *Le corps des fonctions elliptiques paires (par rapport à $\Lambda = [\omega_1, \omega_2]$) est $\mathbb{C}(\wp(z))$.*

Avant de prouver la proposition, on établit un lemme :

**Lemme 7.3.** *Soit $f$ une fonction elliptique paire (par rapport à $\Lambda$) ayant un zéro(resp. un pôle) d'ordre $m$ en $u$. Alors $f$ a un zéro (resp. un pôle) d'ordre $m$ en $-u$ car $f^{(k)}(u) = (-1)^k f^{(k)}(-u)$.*
*En outre, si $u \equiv -u \mod \Lambda$ alors $f$ a un zéro (resp. un pôle) d'ordre paire en $u$.*

*Démonstration.* Tout d'abord, notons que $u \equiv -u \mod \Lambda$ si et seulement si $2u \equiv 0 \mod \Lambda$. Sur le tore $\mathbb{C}/\Lambda$, on a exactement quatres représentants $0, \frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_1+\omega_2}{2}$ dans un parallélogramme périodique
i.e pour $\alpha \in \mathbb{C}$, l'ensemble $\{\alpha + t_1\omega_1 + t_2\omega_2 \mid 0 \leq t_i \leq 1,\ i \in \{1, 2\}\}$.
Du fait que $f$ est paire alors $f'$ est impaire.
Or comme $u \equiv -u \mod \Lambda$ et $f'$ est périodique, on peut affirmer que
$f'(u) = 0$ donc $f$ possède un zéro d'ordre au moins deux.
Si $u \not\equiv 0 \mod \Lambda$ alors la fonction $g(z) = \wp(z) - \wp(u)$ a un zéro d'ordre au moins deux grâce au lemme 6.7. Donc $\frac{f}{g}$ est une fonction paire, elliptique et holomorphe en $u$.
Si $u \equiv 0 \mod \Lambda$ alors on pose $g = \frac{1}{\wp}$ et en argumentant de manière similaire, on obtient que $f$ possède un zéro d'ordre paire en $u$.

- Si $\frac{f(u)}{g(u)} \neq 0$ alors $f$ a un zéro d'ordre deux en $u$.

- Si $\frac{f(u)}{g(u)} = 0$ alors $\frac{f}{g}$ a un zéro d'ordre au moins deux en $u$ et on peut répéter l'argument précédent.

□

*Démonstration (de la proposition 7.2).*
Soit $(u_i)_{1\leq i\leq r}$ une famille de points contenant un réprésentant de chaque classe $(u, -u)(\mod \Lambda)$ où $f$ possède un zéro ou un pôle et la classe de $\Lambda$.
Si $2u_i \not\equiv 0 \mod \Lambda$, on pose $m_i$ est l'ordre de $u_i$ pour $f$.
Si $2u_i \equiv 0 \mod \Lambda$, on pose $m_i$ désignera la moitié l'ordre de $u_i$ pour $f$.

Avec le lemme 7.3, pour $a \in \mathbb{C}$, $a \not\equiv 0 \mod \Lambda$, la fonction $\wp(z) - \wp(a)$ possède un zéro d'ordre deux en $a$ si et seulement si $2a \equiv 0 \mod \Lambda$. Sinon, cette fonction possède deux zéros d'ordre un distincts en $a$ et $-a$.
Donc pour tout $z \not\equiv 0 \mod \Lambda$, la fonction $\prod_{1\leq i\leq r}(\wp(z) - \wp(u_i))^{m_i}$ possède des zéros de même ordre que $f$ en $z$. Comme $\sum m_i = 0$, cela est aussi vrai en 0. Ainsi, ce produit est une fonction elliptique sans zéro ni pôle, donc elle est constante établissant la proposition. □

**Remarque 7.4.** *On peut généraliser facilement le résulat et montrer que le corps des fonctions elliptiques par rapport à $\Lambda$ est engendré par $\wp$ et $\wp'$.*

Maintenant, on va réaliser une première approche de la notion de multiplication complexe au travers des fonctions elliptiques. Nous la généraliserons, plus tard, aux courbes elliptiques :

**Théorème 7.5.** *Soit $\Lambda$ un réseau de $\mathbb{C}$ et on notera $\wp = \wp_L$ la $\wp$-fonction de Weierstrass associé à $\Lambda$. Alors, pour tout $\alpha \in \mathbb{C} \setminus \mathbb{Z}$ et $z \in \mathbb{C}$, les conditions suivantes sont équivalentes :*

- *i) $\wp(\alpha.) : z \in \mathbb{C} \mapsto \wp(\alpha z)$ est une fonction rationnelle en $\wp(z)$.*
- *ii) $\alpha\Lambda \subset \Lambda$.*
- *iii) Il existe un ordre $\mathcal{O}$ de $K$ tel que $\alpha \in \mathcal{O}$ et $\Lambda$ est homothétique à un idéal propre de $\mathcal{O}$*

*De plus, si l'une des conditions est satisfaite on a :*

$$\wp(\alpha z) = \frac{A(\wp(z))}{B(\wp(z))}$$

*et où $A, B$ sont deux polynômes tel que :*

$$\begin{aligned}\deg(A) &= \deg(B) + 1 \\ &= [\Lambda : \alpha\Lambda] \\ &= N(\alpha)\end{aligned}$$

Avant d'entamer la démonstration de ce théorème, grâce au troisième item c'est l'occasion de définir une nouvelle notion :

**Définition 7.6.** *$\mathcal{O}$ est l'anneau de multiplication complexe du réseau $\Lambda$.*

*Démonstration.* i) implique ii)
Si $\wp(\alpha z)$ est rationnelle en $\wp(z)$ alors il existe $A, B$ deux polynômes tel que :

$$B(\wp(z))\wp(\alpha z) = A(\wp(z)) \tag{8}$$

Or, $\wp(z)$ comme $\wp(\alpha z)$ ont toutes deux un pôle double en l'origine. De ce fait, on a :

$$\deg(A) = \deg(B) + 1 \tag{9}$$

Maintenant, soit $\omega \in \Lambda$ grâce à (8) et (9) on peut affirmer que $\wp(\alpha.)$ possède un pôle en $\omega$ montrant que $\wp$ possède un pôle en $\alpha\omega$. Donc $\alpha\Lambda \subset \Lambda$.

ii) implique i)
Si $\alpha\Lambda \subset \Lambda$, il suit que $\wp(\alpha.)$ est méromorphe et possède $\Lambda$ comme réseau de période. De plus, remarquons que $\wp(\alpha.)$ est paire car $\wp$ l'est.
La proposition 7.2 permet de conclure.

ii) implique iii)
Supposons $\alpha\Lambda \subset \Lambda$, en remplaçant $\Lambda$ par $\lambda\Lambda$ pour un $\lambda$ qui convient, on peut supposer que $\tau \in \mathbb{C} \setminus \mathbb{R}$, $\Lambda = [1, \tau]$.
Alors, $\alpha\Lambda \subset \Lambda$ signifie que $\alpha = a + b\tau$ et $\alpha\tau = c + d\tau$ pour des entiers $a, b, c, d$.
On obtient donc $\tau = \dfrac{c + d\tau}{a + b\tau}$ nous fournissant ainsi l'équation quadratique $b\tau^2 + (a - d)\tau - c = 0$.
Mais $\tau \notin \mathbb{R}$, on a $b \neq 0$ et $K = \mathbb{Q}(\tau)$ est un corps quadratique imaginaire. Ainsi, il découle que $\mathcal{O} = \{\beta \in K \mid \beta\Lambda \subset \Lambda\}$ est un ordre de $K$ pour lequel $\Lambda$ est un idéal propre de $\mathcal{O}$ et comme $\alpha \in \mathcal{O}$ on a fini.

iii) implique ii) est trivial.

Pour la dernière partie du théorème, supposons que :

$$\wp(\alpha z) = \frac{A(\wp(z))}{B(\wp(z))}$$

Comme $\deg(A) = \deg(B) + 1$, en admettant $N(\alpha) = [l : \alpha\Lambda]$ on est ramené à montrer que $\deg(A) = [\Lambda : \alpha\Lambda]$.

Fixons $z \in \mathbb{C}$ tel que $2z \in \frac{1}{\alpha}\Lambda$ et considérons le polynôme $A(x) - \wp(\alpha z)B(x)$.

Ce polynôme est de même degré que $A$ et $z$ peut être choisi car les racines sont distinctes. Alors, on prend $\Lambda \subset \frac{1}{\alpha}\Lambda$ et soit $\{w_i\}$ un ensemble de représentants de $\Lambda$ dans $\frac{1}{\alpha}\Lambda$. On a besoin d'un dernier lemme pour conclure. On affirme que :

**Lemme 7.7.** *Les $\wp(z+w_i)$ sont distints et fournissent toutes les racines de $A(x) - \wp(\alpha z)B(x)$.*

*Démonstration du lemme.* Commençons par montrer que les $\wp(z+w_i)$ sont distints. Par l'absurde, on a pour certain $i \neq j$, $\wp(z+w_i) = \wp(z+w_j)$.
Alors, on a $z + w_i \equiv \pm(z+w_j) \mod \Lambda$.

- Si $z + w_i \equiv z + w_j \mod \Lambda$ on a $w_i \equiv w_j \mod \Lambda$ aboutissant à une contradiction.
- Sinon, $2z \equiv w_j - w_i \mod \Lambda$ et on aboutit à une contradiction car $2z \notin \frac{1}{\alpha}\Lambda$.

Montrant donc que les $\wp(z+w_i)$ sont distincts.

De $\wp(\alpha z) = \dfrac{A(\wp(z))}{B(\wp(z))}$ on obtient :
$A(\wp(z+w_i)) = \wp(\alpha(z+w_i))B(\wp(z+w_i))$.
Cela montre que $\wp(z+w_i)$ sont les racines de $A(x) - \wp(\alpha z)B(x)$.
Il ne reste qu'à montrer qu'on les a toutes.

Soit $u$ une autre racine. Notons que $B(u) \neq 0$ car si $B(u) = 0$ alors $A(u) = 0$ ce qui est impossible car $A, B$ sont premiers entre eux.
Pour un certain $w \in \mathbb{C}$, on a $u = \wp(w)$.
Ainsi, $\wp(\alpha z) = \dfrac{A(u)}{B(u)} = \dfrac{A(\wp(w))}{B(\wp(w))} = \wp(\alpha w)$.
On obtient donc $\alpha w \equiv \pm \alpha z \mod \Lambda$. En changeant $w$ pour $-w$ si nécessaire, on peut supposer $w \equiv z \mod \frac{1}{\alpha}\Lambda$.
Cela montre que pour un certain $i$, $w \equiv z + w_i \mod \Lambda$ donc on voit
$u = \wp(w) = \wp(z+w_i)$ est une des racines connues prouvant ainsi le lemme. □

Cela implique que :

$$\deg(A) = \left[\frac{1}{\alpha}\Lambda : \Lambda\right] = [\Lambda : \alpha\Lambda].$$

suffisant à prouver le théorème. □

**Remarque 7.8.** *Ce théorème montre que si une fonction elliptique a une multiplication par un certain $\alpha \in \mathbb{C} \setminus \mathbb{R}$ alors elle a une multiplication pour un ordre $\mathcal{O}$ dans un corps quadratique imaginaire.*

**Remarque 7.9.** *Le nom de multiplication complexe provient du fait que les éléments de $\mathcal{O} \setminus \mathbb{Z}$ sont purement imaginaires.*

On en profite pour établir une nouvelle correspondance :

**Corollaire 7.10.** *Pour $\mathcal{O}$ un ordre dans $K$ un corps quadratique imaginaire. On a une correspondance $1-1$ entre le groupe des classes $C(\mathcal{O})$ et les classes d'homothéhie de réseaux de $\mathbb{C}$ qui ont $\mathcal{O}$ pour anneau de multiplication complexe.*

*Démonstration.* Fixons un ordre $\mathcal{O}$ dans un corps quadratique imaginaire $K$ et considérons un réseau $\Lambda$ où $\mathcal{O}$ est l'anneau de multiplication complexe. Le théorème 7.5 permet d'affirmer que $\Lambda$ est un idéal fractionnaire propre de $\mathcal{O}$.

Réciproquement, tout idéal fractionnaire propre de $\mathcal{O}$ est un réseau avec $\mathcal{O}$ comme anneau de multiplication complexe.
De plus, deux idéaux fractionnaires propres sont homothétiques comme réseau si et seulement s'ils déterminent la même classe dans le groupe des classes d'idéaux $C(\mathcal{O})$.
En effet, si $\Lambda$ et $\Lambda'$ sont deux idéaux fractionnaires propres qui appartiennent à la même classe dans $C(\mathcal{O})$ alors il existe $\gamma \in \mathcal{O}$ tel que $\Lambda' = \gamma\Lambda$ ce qui permet de conclure.
Si $\Lambda$ et $\Lambda'$ sont deux réseaux homothétiques, alors avec le théorème 7.5, on sait que $\Lambda$ et $\Lambda'$ sont homothétique à deux idéaux propres de $\mathcal{O}$. En combinant cela avec notre hypothèse de départ, on peut conclure que $\Lambda$ et $\Lambda'$ appartiennent à la même classe dans $C(\mathcal{O})$. □

Pour conclure cette section, on établit le fait que le $j$-invariant d'un réseau est un nombre algébrique sur $\mathbb{Q}$ :

**Théorème 7.11.** *Si $\mathcal{O}$ est un ordre d'un corps quadratique imaginaire $K$ et $\mathfrak{a}$ un idéal fractionnaire propre de $\mathcal{O}$.*
*Alors, $j(\mathfrak{a})$ est un nombre algébrique sur $\mathbb{Q}$ de degré au plus $h(\mathcal{O})$.*

*Démonstration.* On sait que la série de Laurent de $\wp$ peut s'écrire :

$$\wp(z) = \frac{1}{z^2} + \sum_{n \geq 1} a_n(g_2, g_3) z^{2n}.$$

où $a_n(g_2, g_3)$ est un polynôme en $g_2, g_3$ à coefficients rationnels. On écrira désormais $\wp(z, g_2, g_3)$ pour montrer cette relation.

Pour tout $\alpha \in \mathcal{O}$, $\wp(\alpha z)$ est une fonction rationnelle en $\wp(z)$. On a donc :

$$\wp(\alpha z, g_2, g_3) = \frac{A(\wp(z, g_2, g_3))}{B(\wp(z, g_2, g_3))}. \tag{10}$$

On a la série de Laurent $\wp(\alpha z, g_2, g_3) = \dfrac{1}{\alpha^2 z^2} + \sum_{n\geq 1} a_n(g_2, g_3)\alpha^{2n} z^{2n}$ qui peut être vu comme l'identité dans le corps $\mathbb{C}((z))$ des séries méromorphes de Laurent. On rappelle que $\mathbb{C}((z))$ est le corps de fonction de l'anneau des séries formelles de $\mathbb{C}[[z]]$.
Si $\sigma$ est un automorphisme de $\mathbb{C}$, alors $\sigma$ induit un automorphisme sur $\mathbb{C}((z))$ qui agit sur les coefficients en appliquant $\sigma$ à (10) et en posant $A^\sigma$ (resp. $B^\sigma$) le polynôme obtenu en appliquant $\sigma$ aux coefficients de $A$ (resp. B) :

$$\wp(\sigma(\alpha)z, \sigma(g_2), \sigma(g_3)) = \frac{A^\sigma(\wp(\sigma(z), \sigma(g_2), \sigma(g_3))}{B^\sigma(\wp(\sigma(z), \sigma(g_2), \sigma(g_3))}.$$

Aussi, comme $g_2^3 - 27g_3^2 \neq 0$ on a $\sigma(g_2)^3 - 27\sigma(g_3)^2 \neq 0$.
On montrera plus tard que cela assure que $\Lambda$ soit un réseau tel que $\begin{cases} g_2(\Lambda) = \sigma(g_2) \\ g_3(\Lambda) = \sigma(g_3) \end{cases}$ Ainsi, les séries formelles de Laurent $(\wp(\sigma(z), \sigma(g_2), \sigma(g_3))$ est la série de Laurent de la $\wp$-fonction de Weierstrass donc $\wp_\Lambda$ a une multiplication complexe pour $\sigma(\alpha)$.
Cela est vrai pour tout $\alpha \in \mathcal{O}$ donc si $\mathcal{O}'$ est l'anneau de toute les mulplications complexes, nous avons prouvé que $\mathcal{O} = \sigma(\mathcal{O}) \subset \mathcal{O}'$.
Si on travaille avec $\sigma^{-1}$ en interchangeant $\mathfrak{a}$ et $\Lambda$, les arguments ci-dessus montrent $\mathcal{O}' \subset \mathcal{O}$ et donc que $\mathcal{O}$ est l'anneau de toutes les multiplications complexes entre $\mathfrak{a}$ et $\Lambda$.

Maintenant, considérons les $j$-invariants. Les formules pour $g_2(\Lambda)$ et $g_3(\Lambda)$ montrent que $j(\Lambda) = \sigma(j(\mathfrak{a}))$. Comme $\Lambda$ a $\mathcal{O}$ pour anneau de multiplication complexe, la correspondance entre $C(\mathcal{O})$ et les classes d'homothéties qui ont $\mathcal{O}$ pour anneau de multiplication complexe.
On a donc $h(\mathcal{O})$ possibilités pour $j(\Lambda)$ et au plus $\sigma(j(\mathfrak{a}))$ possibilités. Du fait que $\sigma$ est arbitraire, il suit que $j(\mathfrak{a})$ doit être un nombre algébrique et son polynôme minimal sur $\mathbb{Q}$ est d'ordre au plus $h(\mathcal{O})$. □

Soit $\mathfrak{a}$ un idéal fractionnaire propre d'un ordre $\mathcal{O}$ dans un corps quadratique $K$, le but de cette section est d'expliciter la connexion entre $j(\mathfrak{a})$ et l'anneau du corps de classe de $\mathcal{O}$.

## 7.2 La fonction $j$

Soit $\Lambda$ un réseau de $\mathbb{C}$ et $\mathbb{H} = \{z \in \mathbb{C}, z = x + iy/y > 0\}$. Pour $\tau \in \mathbb{H}$, on s'intéresse au réseau $[1, \tau]$. On a donc $j(\tau) = j([1, \tau])$ et

$$g_2(\tau) = g_2([1,\tau]) = 60 \sum_{(m,n)\neq(0,0),m,n\in\mathbb{Z}} \frac{1}{(m+n\tau)^4}$$

$$g_3(\tau) = g_3([1,\tau]) = 140 \sum_{(m,n)\neq(0,0),m,n\in\mathbb{Z}} \frac{1}{(m+n\tau)^6}$$

Ainsi, on a $j(\tau) = 1728\frac{g_2(\tau)^3}{\Delta(\tau)}$. On décrit maintenant l'action de $SL_2(\mathbb{Z})$ sur le demi-plan supérieur $\mathbb{H}$ :
Si $z \in \mathbb{H}, \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ alors $\gamma z = \dfrac{az+b}{cz+d} \in \mathbb{H}$.

**Remarque 7.12.** *On dira que $\gamma z$ et $z$ sont $\mathrm{SL}_2(\mathbb{Z})$-équivalents.*

Explicitons les principales propriétés de la fonction $j$ :

**Théorème 7.13.** *Pour $\tau \in \mathbb{H}$, on a :*

- *i) La fonction $j$ est holomorphe sur $\mathbb{H}$.*
- *ii) Si $\tau, \tau' \in \mathbb{H}$ alors $j(\tau) = j(\tau')$ si et seulement si $\tau$ et $\tau'$ sont $\mathrm{SL}_2(\mathbb{Z})$-équivalents. En particulier, $j(\tau)$ est invariant sous $\mathrm{SL}_2(\mathbb{Z})$.*
- *iii) La fonction $j : \mathbb{H} \to \mathbb{C}$ est surjective.*
- *iv) On a pour tout $\tau \in \mathbb{H}$, $j(\tau) \neq 0$ sauf si :*
  - *Si $\tau = \gamma i$, $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ alors la dérivée première est nulle en $\tau$ mais la dérivée seconde est non nulle est $\tau$.*
  - *Si $\tau = \gamma\zeta_3$, $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ alors la dérivée première et seconde sont nulles en $\tau$ mais la dérivée troisième est non nulle est $\tau$.*

*Démonstration.* Premier item
On rappelle que pour $\tau \in \mathbb{H}, \Delta(\tau) \neq 0$. Il nous suffit donc de montrer que $g_2$ et $g_3$ sont holomorphes en $\tau \in \mathbb{H}$. Pour $g_2(\tau)$ comme $\sum_{\omega\in\Lambda,\omega\neq 0}$ converge absolument pour $r > 2$, on peut affirmer que la somme définissant $g_2(\tau)$ converge absolument. Remarquons que $g_2(\tau + 1) = g_2(\tau)$.
Montrons que la converge est uniforme quand $|\Re(\tau)| \leq \dfrac{1}{2}$ et $|\Im(\tau)| \geq \varepsilon$ avec $\varepsilon \in ]0, 1[$.
Dans ce cas, il est facile de montrer que $|m + n\tau| \geq \dfrac{\varepsilon}{2}\sqrt{m^2+n^2}$ et la convergence uniforme est immédiate. La preuve pour $g_3(\tau)$ est similaire donc

$g_2, g_3, \Delta$ et $j$ sont holomorphe sur $\mathbb{H}$.

Deuxième item
On rappelle que pour $\alpha, \beta \in \mathbb{H}$, $[1, \alpha]$ et $[1, \beta]$ sont homothétique si et seulement si pour $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ $\beta = \gamma\alpha$ si et seulement si $j(\alpha) = j(\beta)$.
En combinant les deux dernières équivalences, on obtient le deuxième item.

Troisième item
Commençons par calculer les limites de $g_2(\tau)$ et $g_3(\tau)$ quand $\Im(\tau) \to +\infty$.
En écrivant :

$$\begin{aligned} g_2(\tau) &= 60 \sum_{(m,n)\neq(0,0), m,n\in\mathbb{Z}} \frac{1}{(m+n\tau)^4} \\ &= 60(2\sum_{m\geq 1} \frac{1}{m^4} + \sum_{(m,n)\in\mathbb{Z}, n\neq 0} \frac{1}{(m+n\tau)^4}) \end{aligned}$$

Grâce à la convergence uniforme du i), on obtient :

$$\lim_{\Im(\tau)\to+\infty} g_2(\tau) = 120 \sum_{m\geq 1} \frac{1}{m^4}.$$

Or $\dfrac{\pi^4}{90} = \sum_{m\geq 1} \dfrac{1}{m^4}$. Ainsi, on a $\lim\limits_{\Im(\tau)\to+\infty} g_2(\tau) = \frac{4}{3}\pi^4$.

De même pour $g_3(\tau)$ sauf qu'on utilise le fait que $\dfrac{\pi^6}{945} = \sum_{m\geq 1} \dfrac{1}{m^6}$ donc on a $\lim\limits_{\Im(\tau)\to+\infty} g_3(\tau) = \frac{8}{27}\pi^6$.
Ainsi, on a on a $\lim\limits_{\Im(\tau)\to+\infty} \Delta(\tau) = (\frac{4}{3}\pi^4)^3 - 27(\frac{8}{27}\pi^6)^2 = 0$.
Donc $\lim\limits_{\Im(\tau)\to+\infty} j(\tau) = \infty$.
On aura besoin du lemme :

**Lemme 7.14.** *Pour tout $\tau \in \mathbb{H}$, il existe $\tau' \in \mathbb{H}$ tel que $\tau$ et $\tau'$ soient $\mathrm{SL}_2(\mathbb{Z})$-équivalents vérifiant $\Re(\tau') \leq \dfrac{1}{2}$ et $\Im(\tau') \geq \dfrac{1}{2}$.*

*Démonstration du lemme.* Si $|\Im(\tau)| \geq \dfrac{1}{2}$ alors il existe $m \in \mathbb{Z}$ tel que $\tau' = \tau + m$ et satisfait les inégalités désirées alors $\tau + m = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau$ et on a fini ce cas.
Si $|\Im(\tau)| < \dfrac{1}{2}$, alors l'argument du paragraphe précédent, on peut supposer $|\Re(\tau)| \leq \dfrac{1}{2}$.

Il suit que $|\tau| < \frac{1}{2}$ donc

$$\Im(\frac{-1}{\tau}) = \frac{\Im(\tau)}{|\tau|^2} > 2\Im(\tau).$$

Comme $\frac{-1}{\tau} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \tau$, on peut prendre plus du double de la partie imaginaire de $\tau$ en utilisant un élément de $\mathrm{SL}_2(\mathbb{Z})$. En répétant ce procédé autant de fois que nécessaire, on obtient $\tau'$ un point $\mathrm{SL}_2(\mathbb{Z})$-équivalent vérifiant $|\Im(\tau')| < \frac{1}{2}$. □

Montrons maintenant que la fonction $j$ est surjective.
Grâce au caractère holomorphe de la fonction $j$ et non constante, son image est un ouvert de $\mathbb{C}$ en vertu du théorème de l'image ouverte.
Si on montre que son image est un fermé alors on pourra en déduire la surjectivité.
Prenons $(j(\tau_k))$ une suite de point convergeant vers $\omega$. Notre but sera de montrer qu'il existe $\tau \in \mathbb{H}$, tel que $\omega = j(\tau)$.
Avec le dernier lemme, on peut se limiter à la région :

$$R = \{\tau \in \mathbb{H}, \Re(\tau') \leq \frac{1}{2} \text{ et } \Im(\tau') \geq \frac{1}{2}\}$$

Si $\Im(\tau_k)$ est non bornée, alors $j(\tau) \to \infty$ quand $\Im(\tau) \to \infty$ alors $(\tau_k)$ admet une sous-suite convergente vers $\infty$ ce qui est impossible.
Du fait que $\Im(\tau_k)$ soit bornée, ils appartiennent tous à un compact de $\mathbb{H}$ donc il existe une sous-suite convergente vers $\tau \in \mathbb{H}$ et on a par unicité de la limite $\omega = j(\tau)$.

Quatrième item

**Lemme 7.15.** *Si $\tau, \tau' \in \mathbb{H}$ alors il existe $U$ un voisinage de $\tau$ et $V$ un voisinage de $\tau'$ tel que l'ensemble $\{\gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma(U) \cap V \neq \emptyset\}$ est fini.*

*Démonstration du lemme.* Voir Exo 11.5 de [2]. □

**Remarque 7.16.** *Ce lemme dit explicitement que $\mathrm{SL}_2(\mathbb{Z})$ agit proprement discontinuement sur $\mathbb{H}$.*

Une reformulation du dernier lemme permet d'obtenir :

**Corollaire 7.17.** *Si $\tau \in \mathbb{H}$, alors $\tau$ a un voisinage $U$ tel que pour tout $\gamma \in \mathrm{SL}_2(\mathbb{Z}), \gamma(U) \cap U \neq \emptyset$ si et seulement $\gamma\tau = \tau$.*

Supposons $j'(\tau) = 0$ alors $\tau$ possède un voisinage $U$ tel que pour tout $\omega$ suffisament proche de $j(\tau)$ on ait $\tau', \tau'' \in U$ et $j(\tau') = j(\tau'') = \omega$.
Grâce au ii), pour $\gamma \neq \pm Id, \tau'' = \gamma\tau'$ donc $\gamma(U) \cap U \neq \emptyset$. En vertu du corollaire 7.17, il suit que $\gamma\tau = \tau$ pour $\gamma \neq \pm Id$.
En effet, soit $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Si $\gamma\tau = \tau$ alors $[1, \tau] = (c\tau + d)[1, \tau]$ et comme $\gamma \neq \pm Id$ on peut affirmer $c \neq 0$.
Donc $\alpha = c\tau + d \notin \mathbb{Z}$ donc $c \in \mathbb{C}\backslash\mathbb{Z}$. Ainsi, le réseau $[1, \tau]$ a une multiplication complexe dans un corps quadratique imaginaire par un ordre $\mathcal{O}$. De plus, $\alpha[1, \tau] = [1, \tau]$ impliquant $\alpha \in \mathcal{O}^*$.
Toutefois, on sait que $\mathcal{O}^* = \{\pm 1\}$ sauf si $\mathcal{O} = \mathcal{O}_K$ pour $K = \mathbb{Q}(i)$ ou $\mathbb{Q}(\zeta_3), \zeta_3 = e^{\frac{2i\pi}{3}}$. Ces deux ordres ayant un nombre de classes égal à un, $[1, \tau]$ est homothétique à $[1, \zeta_3]$ ou $[1, i]$ donc $j'(\tau) = 0$ donc $\tau$ est $\mathrm{SL}_2(\mathbb{Z})$-équivalent à $i$ ou $\zeta_3$.

- Si $\tau = i$, on doit montrer que $j'(i) = 0$ et $j'' \neq 0$.
  Comme $j(\tau) - 1728 = 1728\dfrac{27g_3(\tau)^2}{\Delta(\tau)}$. On a déjà montrer que $g_3(i) = 0$ donc $j(i) = 0$ suit.
  Supposons $j'' \neq 0$ alors $i$ est un zéro d'ordre trois pour $j(\tau) - 1728$. Donc pour $z$ suffisament proche de 1728, il existe $\tau, \tau', \tau''$ distincts et proche de $i$ tel que $j(\tau) = j(\tau') = j(\tau'') = z$.
  Alors il existe $\gamma_1$ et $\gamma_2$ tel que dans $\mathrm{SL}_2(\mathbb{Z})$ on ait $\pm Id \neq \pm\gamma_1 \neq \pm\gamma_2$ vérifie $\tau' = \gamma_1\tau$ et $\tau'' = \gamma_2\tau$.
  Grâce au corollaire 7.17, on obtient $\gamma_1 i = \gamma_2 i = i$. Donc au plus six élements fixe $i$ dans $\mathrm{SL}_2(\mathbb{Z})$.
  Au final (exo 11.6), seulement quatres éléments de $\mathrm{SL}_2(\mathbb{Z})$ fixe $i$, on peut affirmer que $j''(i) \neq 0$.

- Voir l'exercice 11.6 dans [2] pour le cas $\tau = \zeta_3$.

□

**Corollaire 7.18.** *Soient $g_2, g_3 \in \mathbb{C}$ tel que $g_2^3 - 27g_3^2 \neq 0$.*
*Alors il existe un réseau $\Lambda$ tel que $g_2(\Lambda) = g_2$ et $g_3(\Lambda) = g_3$*

*Démonstration.* Comme la $j$-fonction est surjective et $g_2^3 - 27g_3^2 \neq 0$, il existe $\tau \in \mathbb{H}$ tel que $j(\tau) = 1728\dfrac{g_2^3}{g_2^3 - 27g_3^2}$.
Ainsi, il existe $\lambda \in \mathbb{C}$ tel que $\begin{cases} g_2 = \lambda^{-4} g_2(\tau) \\ g_3 = \lambda^{-6} g_3(\tau) \end{cases}$ mais $\begin{cases} g_2(\lambda\Lambda) = \lambda^{-4} g_2(\Lambda) \\ g_3(\lambda\Lambda) = \lambda^{-6} g_3(\Lambda) \end{cases}$
Donc $\Lambda = [1, \tau]$ est le réseau désiré. □

Comme $j(\tau)$ est invariant sous $\mathrm{SL}_2(\mathbb{Z})$ et $j(\tau + 1) = j(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\tau) = j(\tau)$.
Ainsi, $j$ est holomorphe en $q = q(\tau) = e^{2i\pi\tau}$ avec $|q| \in ]0, 1[$.

**Définition 7.19.** *La série de Laurent de* $j(\tau) = \sum_{n\in\mathbb{Z}} c_n q^n$ *est appelée la* $q$*-extension de* $j$ *en* $\tau$ *dans la région* $0 < |q| < 1$.

**Remarque 7.20.** *C'est l'extension de Fourier.*

**Théorème 7.21.** *La* $q$*-extension de* $j$ *en* $\tau$ *est :*

$$\begin{aligned} j(\tau) &= \frac{1}{q} + 744 + 196884q + \dots \\ &= \frac{1}{q} + \sum_{n\geq 1} c_n q^n \ \text{ où } (c_n) \subset \mathbb{Z} \end{aligned}$$

*Démonstration.* Voir le chapitre XII de [2] pour une preuve. □

# 8 Le $j$-invariant est un entier algébrique

On établit maintenant que le $j$-invariant d'un réseau est un entier algébrique. Pour cela, on étudiera les fonctions et l'équation modulaire $\Phi_m(X, Y)$. Pour établir notre résultat, nous réaliserons une première approche de la multiplication complexe. Cela nous permettra d'atteindre notre objectif qui est la généralisation de Kronecker-Weber dans le cas des corps quadratiques. La référence pour cette section est [2].

## 8.1 Fonction modulaires pour $\Gamma_0(m)$

**Définition 8.1.** *On a un sous-groupe $\Gamma_0(m)$ de $\mathrm{SL}_2(\mathbb{Z})$ en posant :*
*Pour $m \in \mathbb{N}^*$, $\Gamma_0(m) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}), c \equiv 0 \mod m \right\}$*

**Remarque 8.2.** *On a $\Gamma_0(1) = \mathrm{SL}_2(\mathbb{Z})$.*

**Définition 8.3.** *Pour $m \in \mathbb{N}^*$, on dira qu'une fonction $f : \mathbb{H} \to \mathbb{C}$, excepté aux singularités isolés, est modulaire pour $\Gamma_0(m)$ si elle vérifie :*

- *$f$ est méromorphe sur $\mathbb{H}$.*
- *$f$ est invariant sous $\Gamma_0(m)$.*
- *Pour $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ et $\tau \in \mathbb{H}$, $f(\gamma\tau)$ possède une $q$-extension ayant un nombre fini de coefficients non nul.*

**Remarque 8.4.** *Si $f$ une fonction à valeurs complexes vérifie le troisième item, on dira qu'elle est méromorphe aux pointes.*

Explicitons ce troisième item.
Supposons que $f$ satisfait les deux premiers items de la définition pour $\tau \in \mathbb{H}$ et $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.
On affirme que $f(\gamma\tau)$ est de période $m$.
Remarquons que si on pose $U = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}$, on a $\tau + m = U\tau$, on a :
$\gamma U \gamma^{-1} \in \Gamma_0(m)$. De plus, comme $f$ est $\Gamma_0(m)$-invarivant, on a :

$$\begin{aligned} f(\gamma(\tau + m)) &= f(\gamma U \tau) \\ &= f(\gamma U \gamma^{-1} \gamma\tau) \\ &= f(\gamma\tau). \end{aligned}$$

Si $q = q(\tau) = e^{2i\pi\tau}$ alors $f$ est holomorphe en $q^{\frac{1}{m}}$ définie dans la région $0 < |q^{\frac{1}{m}}| < 1$. Donc, on dira par abus, que la $q-$extension de ${}^f(\gamma\tau)$ est $\sum_{n\in\mathbb{Z}} a_n q^{\frac{n}{m}}$.

**Remarque 8.5.** *La fonction $j$ est un exemple basique de fonction modulaire. Elle est modulaire pour $\Gamma_0(1) = \mathrm{SL}_2(\mathbb{Z})$.*

**Théorème 8.6.** *Soit $m \in \mathbb{N}^*$, on a :*

- *La fonction $j$ est modulaire pour $\mathrm{SL}_2(\mathbb{Z})$ et toute fonction modulaire sur $\mathrm{SL}_2(\mathbb{Z})$ est une fonction rationnelle en $j$.*
- *En posant $j(m.)$ la fonction $\tau \in \mathbb{H} \mapsto j(m\tau)$, on a que $j$ et $j(m.)$ sont des fonctions modulaires pour $\Gamma_0(m)$ et toute fonction modulaire pour $\Gamma_0(m)$ est une fonction rationnelle en $j$ et $j(m.)$.*

**Remarque 8.7.** *Le deuxième item est un cas particulier du premier.*

*Démonstration.* Nous allons devoir vérifier les $q$-extensions de $f(\gamma\tau)$, quand $\tau \in \mathrm{SL}_2(\mathbb{Z})$. Or $f(\tau)$ est $\Gamma_0(m)$-invariant, on doit seulement considérer les $q$-extensions de $f(\gamma_i\tau)$ où les $\gamma_i$ sont les représentants des classes d'équivalences à droite de $\Gamma_0(m) \subset \mathrm{SL}_2(\mathbb{Z})$. Il n'y a qu'un nombre fini de $q$-extension à considérer.

D'après la remarque 8.5, on sait que $j$ est une fonction modulaire pour $\mathrm{SL}_2(\mathbb{Z})$. On est donc amener à prouver que toute fonction modulaire $f$ pour $\mathrm{SL}_2(\mathbb{Z})$ est rationnelle en $j$. Rappelons une définition :

**Définition 8.8.** *Une fonction $f$ est holomorphe en $\infty$ si sa $q$-extension fait intervenir seulement des puissances non négatives de $q$.*

Avant d'attaquer la démonstration, on établit un lemme qui nous sera utile :

**Lemme 8.9.**

- *i) Une fonction $f$ modulaire holomorphe sur $\mathrm{SL}_2(\mathbb{Z})$ et holomorphe en $\infty$ alors $f$ est constante.*
- *ii) Une fonction $f$ modulaire holomorphe sur $\mathrm{SL}_2(\mathbb{Z})$ est polynomiale en $j$.*

*Démonstration du lemme.* Premier item
Soit $f$ une fonction modulaire que l'on supposera holomorphe en $\infty$.
On sait que $f(\infty) = \lim_{\Im(\tau)\to\infty} f(\tau)$ existe et que c'est un nombre complexe.
On va montrer que $f(\mathbb{H} \cup \{\infty\})$ est compact. Par le principe du maximum, on aura que $f(\tau)$ est constante.

Soit $f(\tau_k)$ une suite de points dans l'image. On devons trouver une sous-suite convergente vers un point de la forme $f(\tau)$ pour $\tau \in \mathbb{H}$. Comme $f(\tau)$ est $\mathrm{SL}_2(\mathbb{Z})$-invariant, on peut supposer, grâce au lemme 7.14, que les $(\tau_k)$ appartiennent tous à la région $R = \{\tau \in \mathbb{H} \text{ tel que } |\Re(\tau)| \leq \frac{1}{2}, |\Im(\tau)| \geq \frac{1}{2}\}$.
Si la partie imaginaire des $(\tau_k)$ est non bornée, grâce à la limite ci-dessus,

une sous-suite converge vers $f(\infty)$.
Sinon, les $(\tau_k)$ appartiennent à un compact de $\mathbb{H}$ et on peut conclure.

Deuxième item
Soit $f(\tau)$ est une fonction modulaire holomorphe pour $\mathrm{SL}_2(\mathbb{Z})$. Sa $q$-extension a un nombre de termes finis pour une puissance négative de $q$. Comme la $q$-extension de $j(\tau)$ débute par $\frac{1}{q}$, on peut trouver un polynôme $A(x)$ tel que $f(\tau) - A(j(\tau))$ est holomorphe en $\infty$. Comme elle est holomorphe sur $\mathbb{H}$, grâce au premier item on peut affirmer elle est constante. Donc $f(\tau)$ est polynomiale en $j(\tau)$ et le lemme est établit. □

Premier item
Pour $f$ une fonction modulaire arbitraire de $\mathrm{SL}_2(\mathbb{Z})$ avec des pôles possibles sur $\mathbb{H}$ : si on peut trouver un polynôme $B(x)$ tel que $B(j(\tau))f(\tau)$ soit holomorphe sur $\mathbb{H}$, alors le lemme précédent implique que $j(\tau)$ est une fonction rationnelle en $j(\tau)$.
Du fait que $j(\tau)$ a une $q$-extension méromorphe, il en découle que $f(\tau)$ a un nombre fini de pôle dans $R = \{\tau \in \mathbb{H} \text{ tel que } |\Re(\tau)| \leq \frac{1}{2}, |\Im(\tau)| \geq \frac{1}{2}\}$.
Comme $f(\tau)$ est $\mathrm{SL}_2(\mathbb{Z})$-invariante, alors le lemme 7.14 implique que tout pôle de $f$ est $\mathrm{SL}_2(\mathbb{Z})$-équivalent à 1 dans $R$. Donc si $B(j(\tau))f(\tau)$ n'a pas de pôle dans $R$, alors elle est holomorphe sur $\mathbb{H}$.

Supposons que $f$ est un pôle d'ordre $m$ en $\tau_0 \in R$.
Si $j'(\tau_0) \neq 0$ alors $(j(\tau) - j(\tau_0))^m f(\tau)$ est holomorphe en $\tau_0$. Dans ce cas, on peut trouver un polynôme $B(x)$ tel que $B(j(\tau))f(\tau)$ n'a pas de pôle dans $R$, excepté possiblement si $j'(\tau_0) = 0$.
Dans ce cas, avec le quatrième item du théorème 7.13, on est ramené à supposer que $\tau_0 \in \{i, \zeta_3\}$.
Si $\tau_0 = i$, remarquons que dans un voisinage de $i$, on a $f(\tau) = \frac{g(\tau)}{(\tau - i)^m}$ avec $g$ holomorphe en $\tau$ et $g(i) \neq 0$. Maintenant, comme $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ fixe $i$ on a :

$$f(\tau) = f(-\frac{1}{\tau}) = \frac{g(-\frac{1}{\tau}}{(-\frac{1}{\tau} - i)^m}.$$
$$\text{Donc } g(-\frac{1}{\tau}) = \frac{1}{(i\tau)^m} g(\tau).$$

En évaluant en $i$, on obtient $g(i) = (-1)^m g(i)$ or $g(i) \neq 0$ donc $m$ est paire.
Toujours avec le théorème 7.13, $j(\tau) - 1728$ a un zéro d'ordre 2 en i donc $(j(\tau) - 1728)^{\frac{m}{2}} f(\tau)$ est holomorphe en $i$.
De même quand $\tau = \zeta_3$.

Deuxième item

Commençons par le fait, que $j(\tau)$ est une fonction modulaire pour $\Gamma_0(m)$. Comme $j(m.)$ est holomorphe, il suffit de vérifier les propriétés d'invariance.
Soit $\gamma \in \Gamma_0(m)$ alors $\gamma' = \begin{pmatrix} a & bm \\ \frac{c}{m} & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ donc $j(m\gamma\tau) = j(\gamma' m\tau) j(m\tau)$ montrant que $j(m.)$ est $\Gamma_0$-invariant.

Pour montrer l'holomorphie aux pointes, on pose :
$C(m) = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : ad = m, a > 0, 0 \leq b < d, \mathrm{pgcd}(a,b,d) = 1 \right\}$ et $\sigma_0 = \begin{pmatrix} m & 0 \\ 0 & 1 \end{pmatrix} \in C(m)$ vérifiant $\begin{cases} \sigma_0 \tau & = m\tau \\ \Gamma_0(m) & = (\sigma_0^{-1} \mathrm{SL}_2(\mathbb{Z}) \sigma_0) \cap \mathrm{SL}_2(\mathbb{Z}) \end{cases}$

**Lemme 8.10.** *Pour $\sigma \in C(m)$, l'ensemble $(\sigma_0^{-1}\mathrm{SL}_2(\mathbb{Z})\sigma_0) \cap \mathrm{SL}_2(\mathbb{Z})$ est l'ensemble des classes d'équivalence à droite de $\Gamma(m)$ dans $\mathrm{SL}_2(\mathbb{Z})$.*
*Cela induit une bijection entre l'ensemble des éléments de $C(m)$ et les classes d'équivalences à droite dans $\Gamma_0(m)$.*

*Démonstration.* Voir exercice 11.8 de [**?**]. □

**Remarque 8.11.** *Avec le lemme on obtient :*

$$\begin{aligned} |C(m)| &= [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(m)] \\ &= m \prod_{p|m} (1 + \frac{1}{p} \end{aligned}$$

*Ainsi, l'indice de $\Gamma_0(m)$ dans $\mathrm{SL}_2(\mathbb{Z})$ est $m \prod_{p|m}(1 + \frac{1}{p})$.*

On peut maintenant calculer les $q$-extensions. Fixons $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ et prenons $\gamma \in C(m)$ donc $\gamma$ appartient à la classe à droite correspondant à $\sigma$ dans le lemme 8.10. Cela signifie que $\sigma_0 \gamma = \overline{\gamma}\sigma$ pour un certains $\overline{\sigma} \in \mathrm{SL}_2(\mathbb{Z})$.

$$\begin{aligned} j(m\gamma\tau) &= j(\sigma_0 \gamma \tau) \\ &= j(\overline{\gamma}\sigma\tau) \\ &= j(\sigma\tau) \end{aligned}$$

car $j(\tau)$ est $\mathrm{SL}_2(\mathbb{Z})$-invariant. On obtient donc :

$$j(m\gamma\tau) = j(\sigma\tau). \tag{11}$$

Supposons $\sigma = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$. En vertu du théorème 7.21, on peut affirmer que la $q$-extension de $j(\tau)$ est :

$$j(\tau) = \frac{1}{q} + \sum_{n \geq 0} c_n q^n, c_n \in \mathbb{Z}$$

et comme $\sigma\tau = \frac{a\tau+b}{d}$, il suit que $q(\sigma\tau) = e^{2i\pi\frac{a\tau+b}{d}} =$, grâce au fait que $ad = m$, on peut écrire $q(\sigma\tau) = \zeta_m^{ab}(q)^{a^2}$. Donc la $q$-extension de $j(m\gamma\tau) = j(\sigma\tau)$ est :

$$\frac{\zeta_m^{-ab}}{(q^{\frac{1}{m}})^{a^2}} + \sum_{n\geq 0} c_n \zeta_m^{abn}, c_n \in \mathbb{Z} \tag{12}$$

Il n'existe qu'un nombre fini d'exposants négatifs montrant que $j(m\tau)$ est méromorphe aux pointes donc $j(m\tau)$ est une fonction modulaire pour $\Gamma_0(m)$.

L'étape suivante consiste à introduire l'équation modulaire pour $\Phi_m(X, Y)$, notion que nous étudierons plus en profondeur lors de la section suivante.
Considérons le polynôme en $X$, $\Phi_m(X, \tau)) = \sum_{1\leq i\leq|C(m)|}(X - j(m\gamma_i\tau))$.
Notre objectif est de montrer que cette expression est polynomiale en $X$ et $j(\tau)$.
Pour cela, considérons les coefficients de $\Phi_m(X, \tau)$. Ce sont des polynômes symétriques pour les $j(m\gamma_i\tau)$ et ils sont holomorphes.
Maintenant, soit $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, les classes d'équivalences $\Gamma_0(m)\gamma_i\gamma$ sont une permutation des $(\sigma_0(m)\gamma_i)$. Comme $j(m\tau)$ est invariant sous $\Gamma_0(m)$, les $j(m\gamma_i\gamma\tau)$ sont une permutation des $j(m\gamma_i\tau)$. Ceci est une preuve que les coefficients de $\Phi_m(X, \tau)$ sont $\mathrm{SL}_2(\mathbb{Z})$-invariants.

Maintenant, on doit montrer que les coefficients sont méromorphes en $\infty$.
En regardant, les puissances de $q$ pour $q^{\frac{1}{m}} = e^{\frac{2i\pi\tau}{m}}$, il faut montrer que des exposants négatifs apparaissent.
Par l'égalité (11), on sait que pour un certain $\sigma \in C(m), j(\sigma\tau) = j(m\gamma_i\tau)$.
L'égalité (12), cela montre que la $q$-extension pour $j(m\gamma_i\tau)$ a un nombre fini d'exposants négatifs. Comme les coefficients sont polynomiaux en $j(m\gamma_i\tau)$, ils sont méromorphes aux pointes. Ceci montre que les coefficients de $\Phi_m(X, \tau)$ sont modulaires et holomorphes. Grâce au lemme 8.9, ce sont des polynômes en $j(\tau)$. Ainsi, $\Phi_m(X, Y) \in \mathbb{C}[X, Y]$ tel que :

$$\Phi_m(X, j(\tau)) = \prod_{1\leq i\leq|C(m)|}(X - j(m\gamma_i\tau)). \tag{13}$$

Montrant ainsi que c'est un polynôme irréductible en $X$.
Par l'égalité (11), chaque $j(m\gamma_i\tau)$ peut s'écrire $j(\sigma\tau)$ pour un unique $\sigma \in C(m)$. De ce fait, on a :

$$\Phi_m(X, j(\tau)) = \prod_{\sigma\in C(m)}(X - j(\sigma\tau)). \tag{14}$$

Donc $j(m\tau)$ est toujours un des $j(\sigma\tau)$ car $\begin{pmatrix} m & 0 \\ 0 & 1 \end{pmatrix} \in C(m)$.
Ainsi, $\Phi_m(j(m\tau), j(\tau)) = 0$.

**Remarque 8.12.** *C'est une des propriétés importantes de l'équation modulaires.*

Notons que le degré des $\Phi_m(X,Y)$ vu comme un polynôme $X$ est $|C(m)| = m\prod_{p|m}(1+\frac{1}{p})$.

Maintenant, soit $f$ une fonction arbitraire modulaire pour $\Gamma_0(m)$. Pour montrer que $f(\tau)$ est rationnelle en $j(\tau)$ et $j(m\tau)$, considérons la fonction :

$$G(X,\tau) = \Phi_m(X, j(\tau)) \sum_{i=1}^{|C(m)|} \frac{f(\gamma_i\tau)}{X - j(m\gamma_i\tau)} \tag{15}$$

$$= \sum_{i=1}^{|C(m)|} f(\gamma_i\tau) \prod_{j\neq i}(X - j(m\gamma_i\tau)) \tag{16}$$

Ainsi, $G(X,\tau)$ est un polynôme en $X$ et on affirme que les coefficients sont des fonctions modulaires pour $\mathrm{SL}_2(\mathbb{Z})$.
Comme certains des coefficients sont des fonctions modulaires pour $\mathrm{SL}_2(\mathbb{Z})$, ce sont des fonctions rationnelles en $j(\tau)$. Donc $G(X, j(\tau)) \in \mathbb{C}(j(\tau))[X]$.

Maintenant, supposons que $\gamma_1$ est la matrice identité. Par la règle du produit, on obtient :

$$\frac{\partial\Phi_m}{\partial X}(j(m\tau), j(\tau)) = \prod_{j\neq 1}(j(m\tau) - j(m\gamma_j\tau)).$$

Alors, en substituant $X = j(m\tau)$ dans (16) on a :

$$G(j(m\tau), j(\tau)) = f(\tau)\frac{\partial\Phi_m}{\partial X}(j(m\tau), j(\tau)).$$

Comme $\Phi_m(X, j(\tau))$ est irréductible, il est séparable. On a donc :

$$\frac{\partial\Phi_m}{\partial X}(j(m\tau), j(\tau)) \neq 0.$$

Donc on peut écrire :

$$f(\tau) = \frac{G(j(m\tau), j(\tau))}{\frac{\partial\Phi_m}{\partial X}(j(m\tau), j(\tau))}. \tag{17}$$

Cela montre que $f(\tau)$ est une fonction rationnelle en $j(\tau)$ et $j(m\tau)$. □

## 8.2 Equation modulaire pour $\Phi_m(X,Y)$

**Définition 8.13.** *Soit $\Phi_m(X,Y) \in \mathbb{C}[X,Y]$ vérifiant :*
*Pour $\tau \in \mathbb{H}$, $\Phi_m(X, j(\tau)) = \prod_{\sigma\in C(m)}(X - j(\sigma\tau))$.*
*On dit que $\Phi_m(X,Y) = 0$ est l'équation modulaire.*

**Théorème 8.14.** *Soit $m$ un entier non nul. On a :*

- *i) Le polynôme $\Phi_m(X,Y)$ est à coefficients entiers.*
- *ii) $\Phi_m(X,Y)$ est irréductible en tant que polynôme en $X$.*
- *iii) $\Phi_m(X,Y) = \Phi_m(Y,X) = 0$.*
- *iv) Si $m$ n'est pas un carré parfait alors $\Phi_m(X,Y)$ alors :* $\deg(\Phi_m(X,Y) > 1$ *de coefficient* $\pm 1$.
- *v)Si $m$ est un premier $p$ alors :* $\Phi_p(X,Y) \equiv (X^p - Y)(X - Y^p) \mod p\mathbb{Z}[X,Y]$.

*Démonstration.* Premier item
Il suffit de montrer qu'une fonction symétrique élémentaire $f(\tau)$ dans $j(\sigma\tau)$ où $\sigma \in C(m)$ est un polynôme en $j(\tau)$ à coefficient entiers.

Commençons par étudier la $q$-extension de $f(\tau)$ plus en détails.
Grâce à (12), chaque $j(\sigma\tau)$ appartient au corps des séries formelles de Laurent méromorphes $\mathbb{Q}(\zeta_m)((q^{\frac{1}{m}}))$.
Montrons que $f(\tau)$ appartient au corps minimal $\mathbb{Q}((q^{\frac{1}{m}})$.
En effet, si $\varepsilon \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ un automorphsime, il détermine un automorphisme de $\mathbb{Q}(\zeta_m)((q^{\frac{1}{m}}))$ en agissant sur les coefficients.
Prenons $\sigma = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in C(m)$, regardons comment $\varepsilon$ affecte $j(\sigma\tau)$.
On sait que pour $k$ entier tel que $\mathrm{pgcd}(k,n) = 1$, on a $\varepsilon(\zeta_m) = \zeta_m^k$.
On a grâce à (12) que :

$$\varepsilon(j(\sigma\tau)) = \frac{\zeta_m^{-abk}}{(q^{\frac{1}{m}})^{a^2 n}} + \sum_{n\geq 0} c_n \zeta_m^{abkn} (q^{\frac{1}{m}})^{a^2}, \text{ où } (c_n) \subset \mathbb{Z}.$$

Soit $b'$ l'unique entier tel que $0 \leq b' < d$ tel que $b' \equiv bk \mod d$.
Comme $ad = m$, on a $\zeta_{abk}^m = \zeta_{ab'}^m$ et par conséquent on peut réécrire l'égalité ci dessus :

$$\varepsilon(j(\sigma\tau)) = \frac{\zeta_m^{-ab'}}{(q^{\frac{1}{m}})^{a^2}} + \sum_{n\geq 0} c_n \zeta_m^{ab'n} (q^{\frac{1}{m}})^{a^2 n}.$$

En posant $\sigma' = \begin{pmatrix} a & b' \\ 0 & d \end{pmatrix}$ alors $\sigma' \in C(m)$. De plus, avec l'égalité (12) implique que $\varepsilon(j(\sigma\tau)) = j(\sigma'\tau)$.
Alors les éléments de $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ permutent les $j(\sigma\tau)$. Or $f(\tau)$ est symétrique pour les $j(\sigma\tau)$ donc on en déduit que $f(\tau) \in \mathbb{Q}((q^{\frac{1}{m}})$. On conclut que $f(\tau) \in \mathbb{Z}((q))$ car la $q$-extension de $f(\tau)$ ne fait intervenir que des puissances

entières de $q$ et les coefficients sont des entiers algébriques. Cela revient à montrer que $f(\tau)$ est un polynôme à coefficients entiers pour $j(\tau)$. Grâce au lemme 8.9, on peut trouver $A(x) \in \mathbb{C}[X]$ tel que $f(\tau) = A(j(\tau))$. On rappelle que $A$ est choisi pour que la $q$-extension de $f(\tau) - A(j(\tau)$ n'ait que des termes de degré strictement positifs.
Du fait que les $q$-extensions de $f(\tau)$ et $j(\tau)$ ont des coefficients entiers et que $j(\tau) = \frac{1}{q} + \ldots$, on a $A(x) \in \mathbb{Z}[X]$. Donc $f(\tau) = A(j(\tau))$.

Deuxième item
Voir l'exercice 11.10 dans [2].

Troisième item
Voir [5].

Quatrième item
Supposons que $m$ n'est pas un carré. On veut étudier le terme dominant du polynôme entier $\Phi_m(X, Y)$. En remplaçant $X$ par $j(\tau)$, il suffit d'étudier le coefficient de la plus grande puissance négative de $q$ dans la $q$-extension de $\Phi_m(j(\tau), j(\tau))$.
Prenons $\sigma = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in C(m)$, l'égalité (12) nous dit que :

$$j(\tau) - j(\sigma\tau) = \frac{1}{q} - \frac{\zeta_m^{ab}}{q^{\frac{a}{d}}} + \sum_{n \geq 0} d_n (q^{\frac{1}{m}})^n \text{ pour des coefficients } d_n. \tag{18}$$

On sait que $a \neq d$ i.e $\frac{a}{d} \neq 1$ car $m$ n'est pas un carré parfait. Alors le coefficient du plus grand terme négatif dans (18) est une racine de l'unité.
Grâce à l'égalité (14), $\Phi_m(j(\tau), j(\tau))$ est le produit des facteurs de (13) donc le coefficient de la plus grande puissance négative de $q$ dans $\Phi_m(j(\tau), j(\tau))$ est aussi une racine de l'unité. Mais comme il est aussi entier on sait que c'est $\pm 1$.

Cinquième item
On suppose que $m = p$ est premier.
Prenons $f(\tau), g(\tau) \in \mathbb{Z}[\zeta_p]((q^{\frac{1}{p}}))$ et $\alpha \in \mathbb{Z}[\zeta_p]$.
On écrira $f(\tau) \equiv g(\tau) \mod \alpha$ pour signifier $f(\tau) - g(\tau) \in \alpha\mathbb{Z}[\zeta_p]((q^{\frac{1}{p}}))$.
Du fait, que $p$ est premier, les éléments de $C(p)$ sont les $\sigma_p = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$ et pour $0 \leq i \leq p-1, \sigma_i = \begin{pmatrix} 1 & i \\ p & 0 \end{pmatrix}$. Si $0 \leq i \leq p-1$, alors (12) nous dit que :

$$j(\sigma_p \tau) = \frac{1}{q^p} + \sum_{n=0}^{\infty} c_n q^{p^n}. \tag{19}$$

Mais $c_n^p \equiv c_n \mod p$ donc $j(\sigma_p\tau) \equiv j(\tau)^p \mod p$.
Comme $1-\zeta_p$ divise $p$ dans $\mathbb{Z}[\zeta_p]$ grâce au lemme 1.5, on peut donc réécrire la congruence ci-dessus :

$$j(\sigma_p\tau) \equiv j(\tau)^p \mod 1-\zeta_p \tag{20}$$

En combinant les égalités (19) et (20) on obtient :

$$\begin{aligned}\Phi_p(X, j(\tau)) &= \prod_{i=0}^{p}(X - j(\sigma_i\tau)) \\ &= (X - j(\sigma_0\tau))^p(X - j(\tau)^p) \mod 1-\zeta_p \\ &= (X^p - j(\sigma_0\tau)^p)(X - j(\tau)^p) \mod 1-\zeta_p\end{aligned}$$

On se place dans l'anneau $\mathbb{Z}[\zeta_p]((q^{\frac{1}{p}}))[X]$. Comme pour l'égalité (19), on a $j(\tau) \equiv j(\sigma_0\tau)^p \mod 1-\zeta_p$ et on obtient :

$$\Phi_p(X, j(\tau)) \equiv (X^p - j(\tau))(X - j(\tau)^p) \mod 1-\zeta_p$$

Les deux membres de la congruence appartenant à $\mathbb{Z}((q))[X]$, les coefficients de la différence sont des entiers divisibles par $1-\zeta_p$ dans l'anneau $\mathbb{Z}[\zeta_p]$ donc tous divisible par $p$ grâce au lemme 1.5.
Ainsi, $\Phi_p(X, j(\tau)) \equiv (X^p - j(\tau))(X - j(\tau)^p) \mod p\mathbb{Z}((q))[X]$.
On obtient comme voulu, $\Phi_p(X, y) \equiv (X^p - Y)(X - Y^p) \mod \mathbb{Z}[X, Y]$. □

Idée : Si $\Lambda$ est un réseau alors les racines de $\Phi_m(X, Y) = 0$ sont données par les $j$-invariants des sous-réseaux $\Lambda' \subset \Lambda$ vérifiant :
$\begin{cases} [\Lambda : \Lambda'] = m \\ \Lambda/\Lambda' \text{ est un groupe cyclique.} \end{cases}$

**Définition 8.15.** *Un tel réseau $\Lambda'$ est un sous-réseau cyclique de $\Lambda$ d'indice $m$.*

**Théorème 8.16.** *Soit $m$ un entier non nul.*
*On a $u, v \in \mathbb{C}, \Phi_m(u, v) = 0$ si et seulement si $\Lambda$ est un réseau et $\Lambda'$ un sous-réseau cyclique de $\Lambda$ d'indice $m$ tel que :* $\begin{cases} u = j(\Lambda') \\ v = j(\Lambda) \end{cases}$

*Démonstration.* On commence par étudier pour $\tau \in \mathbb{H}$, les sous-réseaux cycliques de $[1, \tau]$ :

**Lemme 8.17.** *Soit $\tau \in \mathbb{H}$ et considérons le réseau $[1, \tau]$.*

- *Prenons $\Lambda'$ un sous-réseau cyclique de $[1, \tau]$ d'indice $m$ alors il existe un unique $\sigma = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in C(m)$ tel que $\Lambda' = d[1, \sigma\tau]$.*
- *Réciproquement, si $\sigma = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in C(m)$ alors $d[1, \sigma\tau]$ est un sous-réseau cyclique de $[1, \tau]$ d'indice $m$.*

*Démonstration du lemme.* Premier item
Un sous réseau $\Lambda' \subset \Lambda = [1, \tau]$ peut s'écrire $\Lambda' = [a\tau + b, c\tau + d]$ et on sait (voir l'exercice 7.15 dans le [2]) que $[\Lambda : \Lambda'] = |ad - bc| = m$. Par dimension, on obtient que :

$$\Lambda/\Lambda' \text{ est cyclique si et seulement si } \operatorname{pgcd}(a, b, c, d) = 1. \tag{21}$$

Maintenant, supposons que $\Lambda' \subset [1, \tau]$ est cyclique d'indice $m$. Si $d$ est l'entier minimal positif contenu dans $\Lambda'$ alors on peut affirmer que $\Lambda' = [d, a\tau + b]$.

On peut supposer que $a > 0$ et $ad = m$.
Si $k$ est un entier alors $\Lambda' = [d, (a\tau + d) + kd] = [d, a\tau + (b + kd)]$ donc un $k$ approprié, on peut supposer $0 \leq b < d$ donc avec l'égalité (21) on a $\operatorname{pgcd}(a, b, d) = 1$.
Donc la matrice $\sigma \in \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in C(m)$. Alors, on a :

$$\begin{aligned} \Lambda' = [d, a\tau + b] &= d[1, \frac{a\tau + b}{d}] \\ &= d[1, \sigma\tau] \end{aligned}$$

montrant que $\Lambda'$ est de la forme désirée.
Deuxième item
Provient essentiellement de l'égalité (21). □

Grâce à ce lemme, on sait que les $j$-invariants des sous-réseaux cycliques $\Lambda'$ d'indice $m$ de $[1, \tau]$ sont donnés par :

$$\begin{aligned} j'(\Lambda') &= j(d[1, \sigma\tau]) \\ &= j([1, \sigma\tau]) \\ &= j(\sigma\tau). \end{aligned}$$

Grâce à l'égalité (14), il suit que les racines de $\Phi_m(X, j(\tau)) = 0$ sont exactement les $j$-invariants d'un sous-réseau cyclique d'indice $m$ de $[1, \tau]$. □

## 8.3 Multiplication complexe et anneau du corps de classes

On commence par définir la notion d'idéal (propre) primitif :

**Définition 8.18.** *Soit $\mathcal{O}$ un ordre dans un corps quadratique imaginaire. Un idéal propre $\mathfrak{a}$ de $\mathcal{O}$ est primitif s'il n'est pas de la forme $d\mathfrak{a}$ où $d > 1$ est un entier et $\mathfrak{a}$ un idéal propre de $\mathcal{O}$.*

On caractérise le lien entre les idéaux primitifs et les sous-réseaux cycliques :

**Proposition 8.19.** *Soit $\mathcal{O}$ un ordre dans un corps quadratique imaginaire et soit $\mathfrak{b}$ un idéal fractionnaire propre de $\mathcal{O}$.*
*Alors, en prenant $\mathfrak{a}$ un idéal propre de $\mathcal{O}$, on a que $\mathfrak{ab}$ est un sous réseau de $\mathfrak{b}$ d'indice $N(\mathfrak{a})$. De plus, $\mathfrak{ab}$ est un sous-réseau cyclique si et seulement si $\mathfrak{a}$ est primitif.*

*Démonstration.* En remplaçant $\mathfrak{b}$ par un multiple, on peut supposer que $\mathfrak{b} \subset \mathcal{O}$. Ainsi, on a la suite exacte :

$$0 \to \mathfrak{b}/\mathfrak{ab} \to \mathcal{O}/\mathfrak{ab} \to \mathcal{O}/\mathfrak{b} \to 0$$

Cela implique que $[\mathfrak{b} : \mathfrak{ab}]N(\mathfrak{b}) = N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$ donc $N(\mathfrak{a}) = [\mathfrak{b} : \mathfrak{ab}]$.

Maintenant, supposons que $\mathfrak{b}/\mathfrak{ab}$ soit non cyclique.
Comme $\mathfrak{b}/\mathfrak{ab}$ contient un sous-groupe isomorphe à $(\mathbb{Z}/d\mathbb{Z})^2$ pour un certain $d > 1$. Donc il existe un sous-réseau $\mathfrak{ab} \subset \mathfrak{b}' \subset \mathfrak{b}$ tel que $\mathfrak{b}'/\mathfrak{ab} \simeq (\mathbb{Z}/d\mathbb{Z})^2$. Or $\mathfrak{b}'$ est de rang 2 cela implique que $\mathfrak{ab} = d\mathfrak{b}'$ donc $\mathfrak{a} = d\mathfrak{b}'\mathfrak{b}^{-1}$. Mais $\mathfrak{b}'\mathfrak{b}^{-1} \subset \mathcal{O}$ car $\mathfrak{b}' \subset \mathfrak{b}$. Ainsi, $\mathfrak{a}$ n'est pas primitif.

Réciproquement, si $\mathfrak{a}$ n'est pas primitif alors $\frac{\mathfrak{b}}{\mathfrak{ab}}$ n'est pas cyclique. □

En appliquant cette proposition à $\mathfrak{a}$, il devient un idéal principal $\mathfrak{a} = \alpha\mathcal{O}, \alpha \in \mathcal{O}$. Dans ce cas, $\alpha\mathcal{O}$ est un idéal primitif si et seulement si $\alpha$ est un élment primitif de $\mathcal{O}$ i.e $\alpha$ n'est pas de la forme $d\beta$ avec $d > 1$ et $\beta \in \mathcal{O}$. Et comme $N(\alpha) = N(\alpha\mathcal{O})$, on obtient le corollaire :

**Corollaire 8.20.** *Soient $\mathcal{O}$ et $\mathfrak{b}$ comme précédemment et $\alpha \in \mathcal{O}$. Alors, $\alpha\mathfrak{b}$ est un sous-réseau cyclique de $\mathfrak{b}$ d'indice $N(\alpha)$ si et seulement si $\alpha$ est primitif.*

Il est temps d'établir un des résultats principaux de cette deuxième partie :

**Théorème 8.21.** *Soit $\mathcal{O}$ un ordre dans un corps quadratique imaginaire $K$ et soit $\mathfrak{a}$ un idéal fractionnaire propre de $\mathcal{O}$.*
*Alors, le $j$-invariant $j(\mathfrak{a})$ est un entier algébrique et $K(j(\mathfrak{a}))$ est l'anneau du corps de classe de l'ordre $\mathcal{O}$.*

*Démonstration.* Soit $\mathfrak{a}$ un idéal fractionnaire propre de $\mathcal{O}$ qui est un ordre dans un corps quadratique imaginaire $K$. Notre but est de montrer que $j(\mathfrak{a})$ est un entier algébrique et $K(j(\mathfrak{a}))$ est l'anneau du corps de classe de $\mathcal{O}$.

Tout d'abord, utilisons l'équation modulaire pour prouver que $j(\mathfrak{a})$ est un entier algébrique. Par le dernier corollaire, on sait que $\alpha\mathfrak{a}$ est un sous-réseau cyclique de $\mathfrak{a}$ d'indice $m = N(\alpha)$. En vertu du théorème 8.16 et du fait que $j(\alpha\mathfrak{a}) = j(\mathfrak{a})$, on a :

$$0 = \Phi_m(j(\alpha\mathfrak{a}), j(\mathfrak{a})) = \Phi_m(j(\mathfrak{a}), j(\mathfrak{a}) = 0.$$

Alors $j(\mathfrak{a})$ est une racine de $\Phi_m(X,X)$. Grâce au premier item du théorème 8.14, on sait que $\Phi_m(X,Y)$ est à coefficient entiers. Cela montre que $j(\mathfrak{a})$ est un nombre algébrique. De plus, si on prend $\alpha$ tel que $m = N(\alpha)$ ne soit pas un carré parfait alors le coefficient dominant de $\Phi_m(X,X)$ est $\pm 1$ grâce au quatrième item du théoèreme 8.14 donc $j(\mathfrak{a})$ est un entier algébrique.

Maintenant, soit $f$ le conducteur de $\mathcal{O}$. On a grâce au lemme 4.17, $\mathcal{O} = [1, f\omega_K]$ où $\omega_K = \frac{d_k+\sqrt{d_k}}{2}$. Alors, $\alpha = f\omega_k$ est primitif dans $\mathcal{O}$ donc on sait que $N(\alpha)$ n'est pas un carré parfait.

Soit $L$ l'anneau du corps de classe de $\mathcal{O}$. On va montrer que $L = K(j(\mathfrak{a}))$. Etudions comment les premiers se ramifient dans $L$ et $K(j(\mathfrak{a}))$. Comme d'habitude, $f$ et $D$ désignent le conducteur et le discriminant de $\mathcal{O}$.
On s'intéresse à l'anneau du corps de classe $L$. Soit $\mathcal{S}_{L/\mathbb{Q}}$ l'ensemble des premiers totalement décomposé dans $L$.

**Lemme 8.22.** *$\mathcal{S}_{L/\mathbb{Q}} = \{p$ premier : $p = N(\alpha)$ pour un certain $\alpha \in \mathcal{O}\}$.*

*Démonstration.* Quand $D$ est congru à 0 modulo 4 alors $\mathcal{O} = \mathbb{Z}[\sqrt{-n}]$ pour un entier positif $n$. Alors, on a $N(\alpha) = N(x+y\sqrt{-n}) = x^2+ny^2$ donc grâce au théorème 5.7, on sait que les premiers se décomposant toalement dans $L$ sont représentés par $x^2+ny^2$ à un nombre fini d'exceptions près.

□

Soit $M = K(j(\mathfrak{a}))$. Grâce à la proposition 5.4 on sait que $L/\mathbb{Q}$ est une extension galoisienne et on sait que $M \subset L$ équivaut à $\mathcal{S}_{L/\mathbb{Q}} \subset \mathcal{S}_{M/\mathbb{Q}}$.
Prenons $p \in \mathcal{S}_{L/\mathbb{Q}}$ et supposons que $p$ est non ramifié dans $M$. Grâce au lemme 8.22, on a $p = N(\alpha)$ pour un certain $\alpha \in \mathcal{O}$. Donc $\alpha\mathfrak{a} \subset \mathfrak{a}$ est un sous-réseau d'indice $p$. Comme $p$ est premier donc $\alpha\mathfrak{a}$ est cyclique. Ainsi, on obtient :

$$0 = \Phi_p(j(\alpha\mathfrak{a}), j(\mathfrak{a})) = \Phi_p(j(\mathfrak{a}), j(\mathfrak{a})).$$

Grâce au cinquième item du théorème 8.14, on a :

$$\begin{aligned} 0 &= \Phi_p(j(\mathfrak{a}), j(\mathfrak{a})) \\ &= -(j(\mathfrak{a})^p - j(\mathfrak{a}))^2 + p\beta, \text{ pour } \beta \in \mathcal{O}_M. \end{aligned}$$

Maintenant, soit $\beta$ un premier de $M$ contenant $p$. On a donc :

$$j(\mathfrak{a})^p \equiv j(\mathfrak{a}) \mod \beta. \tag{22}$$

**Lemme 8.23.** *On a :*

- $\mathcal{O}_K[j(\mathfrak{a})] \subset \mathcal{O}_M$ *est d'indice fini.*
- *Si* $p$ *ne divise pas* $[\mathcal{O}_M : \mathcal{O}_K(j(\mathfrak{a}))]$ *alors l'égalité* (22) *implique* $\alpha^p \equiv \alpha \mod \beta$, *pour tout* $\alpha \in \mathcal{O}_M$.

*Démonstration du lemme.* Le premier item découle directement de l'égalité $M = K(j(\mathfrak{a}))$.
Pour le deuxième item, notons que $p$ se décompose totalement dans $L$ donc dans $K$. Ainsi, il existe un idéal $\mathfrak{p} \subset K$ de norme $p$ tel que $p \in \mathfrak{p} \subset \beta$.
Donc $\alpha^p \equiv \alpha \mod \beta$, pour tout $\alpha \in \mathcal{O}_K$ donc cela est vrai pour tout $\alpha \in \mathcal{O}_K[j(\mathfrak{a})]$ grâce à l'égalité (22).

□

Le deuxième item du lemme 8.23 permet d'affirmer que l'indice d'inertie $f_{\beta|p} = 1$. Cela étant vrai pour tout idéal $\beta$ contenant $p$, ainsi $p$ se décompose totalement dans $M$. Donc l'inclusion $M \subset L$ suit. Cette inclusion montre que l'anneau du corps de classe $L$ contient les $j$-invariants de tous les idéaux fractionnaires propre de $\mathcal{O}$.
Posons $h = h(\mathcal{O})$ le nombre de classes de $C(\mathcal{O})$ et soit $(\mathfrak{a}_i)_{1\leq i\leq h}$ un ensemble de représentants pour $C(\mathcal{O})$.
Ainsi, $j(\mathfrak{a})$ est égal à l'un des $j(\mathfrak{a}_i)$ pour $1 \leq i \leq n$. De plus, comme les $(\mathfrak{a}_i)_{1\leq i\leq h}$ sont tous distincts, on a :

$$\Delta = \prod_{i<j}(j(\mathfrak{a}_i) - j(\mathfrak{a}_j)) \text{ est non nul dans } \mathcal{O}_L. \tag{23}$$

Pour prouver l'inclusion inverse $L \subset M$, on utilise le fait que $\tilde{\mathcal{S}}_{M/\mathbb{Q}} \subset \mathcal{S}_{M/\mathbb{Q}}$, en ayant posé au préalabre :
$\tilde{\mathcal{S}}_{M/\mathbb{Q}} = \{\mathfrak{p} \in \mathcal{P}_\mathbb{Q} : \mathfrak{p}$ non ramifié dans $M$ et $f_{\beta|\mathfrak{p}} = 1$ pour un idéal premier $\beta$ de $M\}$. Soit $(p) \in \tilde{\mathcal{S}}_{M/\mathbb{Q}}$, on a que $(p)$ se décompose totalement dans $K$ et $p = N(\mathfrak{p})$ pour un idéal de $\mathcal{O}$. Comme $p = N(\mathfrak{p} \cap \mathcal{O})$. Si on montre que $\mathfrak{p} \cap \mathcal{O}$ est un idéal principal $\alpha\mathcal{O}$ alors $p = N(\alpha)$ implique grâce à l'égalité (8.22) que $p \in \mathcal{S}_{L/\mathbb{Q}}$.

Supposons que $p$ est premier avec chaque terme de $\Delta$. Soit $\mathfrak{a}' = (\mathfrak{p} \cap \mathcal{O})\mathfrak{a}$. Comme $\mathfrak{p} \cap \mathcal{O}$ est de norme $p$ alors $\mathfrak{a}' \subset \mathfrak{a}$ est un sous-réseau d'indice $p$ grâce à la proposition 8.19 et il est cyclique car $p$ est premier. Alors, $\Phi_m(j(\mathfrak{a}'), j(\mathfrak{a})) = 0$. Grâce au cinquième item du théorème 8.14, on a pour un polynôme $Q(X, Y) \in \mathbb{Z}[X, Y]$ :

$$0 = \Phi_p(j(\mathfrak{a}'), j(\mathfrak{a})) = (j(\mathfrak{a}')^p - j(\mathfrak{a})) + pQ(j(\mathfrak{a}'), j(\mathfrak{a})) \in \beta \tag{24}$$

Soit $\tilde{\beta}$ un premier de $L$ contenant $\beta$. Comme $j(\mathfrak{a}')$ et $j(\mathfrak{a})$ sont des entiers algébriques dans $L$, l'équation (24) implique que $pQ(j(\mathfrak{a}'), j(\mathfrak{a})) \in \beta$. Donc

$$j(\mathfrak{a}')^p \equiv j(\mathfrak{a}) \mod \tilde{\beta} \text{ ou } j(\mathfrak{a}') \equiv j(\mathfrak{a})^p \mod \tilde{\beta}. \tag{25}$$

On sait aussi que $f_{\tilde{\beta}|\mathfrak{p}} = 1$ donc $j(\mathfrak{a})^p \equiv j(\mathfrak{a}) \mod \beta$. Comme $\beta \subset \tilde{\beta}$ on a :

$$j(\mathfrak{a})^p \equiv j(\mathfrak{a}) \mod \tilde{\beta}. \tag{26}$$

En combinant les égalités (25) et (26) on a $j(\mathfrak{a}) \equiv j(\mathfrak{a}') \mod \tilde{\beta}$.

Si $\mathfrak{a}$ et $\mathfrak{a}'$ appartiennent à des classes disctinctes dans $C(\mathcal{O})$ alors $j(\mathfrak{a}) - j(\mathfrak{a}')$ est donc un des facteurs de $\Delta$. Ainsi, $\text{pgcd}(\mathfrak{p}, \Delta) \neq 1$ on aboutit à une contradiction donc $\mathfrak{a}$ et $\mathfrak{a}' = (\mathfrak{p} \cap \mathcal{O})\mathfrak{a}$ appartiennent à la même classe dans $C(\mathcal{O})$. Cela oblige que $\mathfrak{p} \cap \mathcal{O}$ est un idéal principal impliquant que $p \in \mathcal{S}_{L/\mathbb{Q}}$ donc $\tilde{\mathcal{S}}_{M/\mathbb{Q}} \subset \mathcal{S}_{L/\mathbb{Q}}$ montrant que $L = M$. □

Comme on sait que le corps de classe de Hilbert de $K$ est son anneau du corps de classe de l'ordre maxiaml $\mathcal{O}_K$, on obtient :

**Corollaire 8.24.** *Si $K$ est un corps quadratique imaginaire alors $K(j(\mathcal{O}_K))$ est le corps de classe d'Hilbert de $K$.*

En combinant le dernier théorème avec le théorème 5.6 on a :

**Corollaire 8.25.** *Soient $K$ est un corps quadratique imaginaire et $L/K$ une extension finie.*
*Alors, $L/K$ est une extension abélienne diédrale généralisée sur $\mathbb{Q}$ si et seulement s'il existe un ordre $\mathcal{O}$ de $K$ tel que $L \subset K(j(\mathcal{O}))$.*

**Théorème 8.26.** *Soient $\mathcal{O}$ un ordre dans un corps quadratique imaginaire de $K$ et $L$ l'anneau du corps de classe de $\mathcal{O}$.*
*Si $\mathfrak{a}$ est un idéal propre de $\mathcal{O}$ et $\mathfrak{p}$ un premier de $\mathcal{O}_K$ alors :*

$$\left(\frac{L/K}{\mathfrak{p}}\right)(j(\mathfrak{a})) = j(\overline{\mathfrak{p} \cap \mathcal{O}\mathfrak{a}})$$

*Démonstration.* Admis voir [5] pour une preuve. □

**Corollaire 8.27.** *Soient $\mathcal{O}$ un ordre dans un corps quadratique imaginaire de $K$ et $L$ l'anneau du corps de classe de $\mathcal{O}$.*
*Si on se donne deux idéaux fractionnaires propres $\mathfrak{a}, \mathfrak{b}$ de $\mathcal{O}$, on peut définir $\sigma_{\mathfrak{a}}(j(\mathfrak{b}))$ par $\sigma_{\mathfrak{a}}(j(\mathfrak{b})) = j(\overline{\mathfrak{a}}\mathfrak{b})$.*
*Alors $\sigma_{\mathfrak{a}}$ est une application bien définie, appartenant à $\text{Gal}(L/K)$ et $\mathfrak{a} \mapsto \sigma_{\mathfrak{a}}$ induit un isomorphisme entre $C(\mathcal{O})$ et $\text{Gal}(L/K)$.*

*Démonstration.* Avec le théorème précédent et en utilisant les isomorphismes $C(\mathcal{O}) \simeq I(\mathcal{O}, f)/P(\mathcal{O}, f) \simeq I_K(f)/P_{K,\mathbb{Z}}(f)$ où $f$ est le conducteur de $\mathcal{O}$ □

Par la théorie du corps de classe, toute extension abélienne appartient à un corps de classe de rayon pour un certain module $\mathfrak{m}$ de $K$. On doit trouver les générateurs pour ce corps de de rayon de $K$. On va travailler avec un

module de la forme $N\mathcal{O}_K$ où $N$ est un entier positif non nul.

On obtient le corps de classe de rayon de $K$ pour le module $N\mathcal{O}_K$ en adjoignant le $j$-invariant $j(\Lambda)$ d'un réseau $\Lambda$ d'un côté et certaines valeurs de la $\wp$-fonction de Weierstrass évalué aux $N$ points de torsion d'un réseau $\Lambda$ i.e si $L = [\alpha, \beta]$, on utilise $\wp_\Lambda\left(\frac{m\alpha + n\beta}{N}\right)$ pour $m$ et $n$ qui conviennent pour engendrer les extensions abéliennes de $K$. Le soucis étant que ces valeurs ne sont pas invariantes.

**Définition 8.28.** *Pour tout réseau $\Lambda$, on appellera fonction de Weber la fonction $\tau_\Lambda : \mathbb{C} \to \mathbb{C}$ définie par :*

$$\tau_\Lambda(z) = \begin{cases} \frac{g_2(\Lambda)^2}{\Delta(\Lambda)}\wp_\Lambda(z)^2 & \text{si } g_3(\Lambda) = 0 \\ \frac{g_3(\Lambda)}{\Delta(\Lambda)}\wp_\Lambda(z)^3 & \text{si } g_2(\Lambda) = 0 \quad \text{où } \Delta(\Lambda) = g_2(\Lambda)^3 - 27g_3(\Lambda)^2. \\ \frac{g_2(\Lambda)g_3(\Lambda)}{\Delta(\Lambda)}\wp_\Lambda(z)^3 & \text{sinon.} \end{cases}$$

**Remarque 8.29.** *On a pour tout $\lambda \in \mathbb{C}, \lambda \neq 0$, $\tau_{\lambda\Lambda}(\lambda z) = \tau_\Lambda(z)$.*

On peut maintenant classifier les extensions abéliennes d'un corps $K$ qui est quadratique imaginaire. L'objectif initial est donc atteint :

**Théorème 8.30.** *Soient $K$ un corps quadratique imaginaire de discriminant $d_K$ et $N$ un entier non nul.*

- *$K(j(\mathcal{O}_K), \tau_{\mathcal{O}_K}(\frac{1}{N}))$ est le corps de classe de rayon de $K$ pour le module $N\mathcal{O}_K$.*
- *Soit $\mathcal{O}$ un ordre de conducteur $N$ dans $K$.*
  *Alors, en posant $\omega_K = \frac{d_K + \sqrt{d_K}}{2}$, $K(j(\mathcal{O}), \tau_{\mathcal{O}}(\omega_K))$ est le corps de classe de rayon pour le module $N\mathcal{O}_K$.*

*Démonstration.* Lire [5]. □

Troisième partie

# Courbes elliptiques et corps de fonctions

Après avoir utilisé l'analyse complexe pour parvenir à notre objectif lors du chapitre précédent, nous utilisons la connexion naturelle qui existe entre la description analytique et géométrique d'un objet pour généraliser notre cadre de travail et faciliter à l'avenir la construction explicite des extensions abéliennes d'un corps quadratique imaginaire.
La première section définit les courbes elliptiques. Nous introduisons uniquement les notions qui nous seront utiles pour « remplacer $j(\Lambda)$ par $j(E)$ » où $\Lambda$ et $E$ sont respectivement un réseau et une courbe elliptique bien choisies. La seconde est une ouverture pour continuer le travail au delà du cadre du stage. Elle évoque les corps de fonctions, objets indispensable pour pouvoir faire de la géométrie algébrique.

## 9 Introduction aux courbes elliptiques

La principale source cette troisième partie fut encore une fois l'ouvrage de Cox [2]. Nous avons ensuite utilisé ceux de Lang [5] et Silvermann [11] pour compléter les preuves et approfondir les intuitions donné par le livre de Cox.

Soit $K$ un corps de caractéristique différente de 2 ou 3.

### 9.1 Equation de Weierstrass

Commençons par évoquer les équations de Weierstrass :

**Définition 9.1.** *On appelle équation de Weierstrass, les équations de la forme :*

$$y^2 = 4x^3 - g_2x - g_3 \text{ où } g_2, g_3 \in K \tag{27}$$
$$\text{avec } \Delta = g_2^3 - 27g_3^2 \neq 0 \tag{28}$$

**Définition 9.2.** *On dit que $E$ est une courbe elliptique $E$ sur $K$ si $E$ est une équation de Weierstrass.*

**Remarque 9.3.** *L'équation (27) définit une courbe dans l'espace affine $K^2$.*

**Définition 9.4.** *Pour une courbe elliptique $E$ dans $K$, on note $E(K) = \{(x, y) \in K^2 : y^2 = 4x^3 - g_2x - g_3\} \cup \{\infty\}$ l'ensemble des solutions de $E$.*

**Remarque 9.5.** *Pour une extension $L \subset K$, on aura $E(K) \subset E(L)$.*

Dans $\mathbb{C}$, les $\wp$-fonction de Weierstrass fournissent des courbes elliptiques.
En effet, soit $\Lambda$ un réseau de $\mathbb{C}$ et soit $\wp = \wp_\Lambda$ la $\wp$-fonction de Weierstrass correspondante.
On a l'équation différentielle $\wp'(z)^2 = 4\wp(z) - g_2(L)\wp(z) - g_3(\Lambda)$ nous fournissant ainsi une courbe elliptique $y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$.
Si $z \notin \Lambda$ alors $\wp$ et $\wp'$ sont des fonctions bien définies et l'équation différentielle montre que $\wp(z)$ et $\wp'(z)$ appartiennent à $E(\mathbb{C})$. Du fait, qu'ils sont doublement périodiques, l'application $(\mathbb{C} \setminus \Lambda)/\Lambda \to \mathbb{E} \setminus \infty$ est bien définie et induit un biholomorphisme $\mathbb{C}/\Lambda \simeq \mathbb{E}(\mathbb{C})$ où $0 \mapsto \infty$.

**Remarque 9.6.** *$C/\Lambda \simeq \mathbb{E}(\mathbb{C})$ est une surface de Riemmann.*

**Proposition 9.7.** *Soit $E$ une courbe elliptique sur $\mathbb{C}$ donné par l'équation :*

$$y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda) \text{ où } g_2, g_3 \in \mathbb{C} \text{ avec } \Delta = g_2^3 - 27g_3^2 \neq 0.$$

*Alors, il existe un unique réseau $\Lambda$ de $\mathbb{C}$ tel que $g_2 = g_2(\Lambda)$ et $g_3 = g_3(\Lambda)$.*

*Démonstration.* L'existence provient du corollaire 7.18 tandis que l'unicité provient de la preuve du théorème 6.15. □

**Définition 9.8.** *On définit le $j$-invariant d'une courbe elliptique $E$ sur $K$ comme le nombre :*

$$j(E) = 1728\frac{g_2^3}{g_2^3 - 27g_3^2} = 1728\frac{g_2^3}{\Delta} \in K.$$

**Remarque 9.9.** *Sur $\mathbb{C}$, grâce à la proposition 9.7, on a $j(L) = j(E)$.*

**Définition 9.10.** *On prend deux courbes elliptiques $E$ et $E'$ sur $K$ :*

$$E : y^2 = 4x^3 - g_2x - g_3$$
$$E' : y^2 = 4x^3 - g_2'x - g_3'$$

*On dit que $E$ et $E'$ sont isomorphes sur $K$ s'il existe $c \in K, c \neq 0$ tel que $g_2' = c^4 g_2$ et $g_3' = c^6 g_3$.*

**Remarque 9.11.** *Dans le cas de la définition, $(x, y) \mapsto (c^2x, c^3y)$ induit une bijection $E(K) \simeq E'(K)$.*

**Proposition 9.12.** *Soient $E$ et $E'$ deux courbes elliptiques sur $\mathbb{C}$ correspondant à $\Lambda$ et $\Lambda'$.*

- *i) $E$ et $E'$ sont isomorphes sur $\mathbb{C}$.*
- *si et seulement si ii) les réseaux $\Lambda$ et $\Lambda'$ sont homothétiques.*
- *si et seulement si iii) les $j$-invariants sont égaux i.e $j(E) = j(E')$.*

*Démonstration.* Découle du théorème 6.15.
Voir l'exercice 14.4 dans [2] pour les détails. □

**Corollaire 9.13.** *Soient $E$ et $E'$ deux courbes elliptiques sur $K$.*

- *Les courbes elliptiques $E$ et $E'$ ont le même $j$-invariant si et seulement si $E$ et $E'$ sont isomorphes sur une extension finie de $K$.*
- *Si $K$ est algébriquement clos alors $E$ et $E'$ ont le même $j$-invariant si et seulement si $E$ et $E'$ sont isomorphes sur $K$.*

**Remarque 9.14.** *C'est la version algébrique théorème 6.15.*

*Démonstration.* Voir l'exercice 14.4 dans dans [2] □

## 9.2 Addition sur une courbe elliptique

Soit $E$ une courbe elliptique sur $K$. Soient $P_1$ et $P_2$ deux points de $E(K)$. Notre but est de définir $P_1 + P_2 \in E(K)$.

Si $P_1 = \infty$, on définit $P_1 + P_2 = \infty + P_2 = P_2$.
Si $P_2 = \infty$, on définit $P_1 + P_2 = P_1 + \infty = P_1$.
De ce fait, $\infty$ est l'élément identité de $E(K)$.

Pour $P_1 = (x_1, y_1)$ et $P_2 = (x_2, y_2)$.
Si $x_1 \neq x_2$, on a $P_1 + P_2 = (x_3, y_3)$ avec :

$$x_3 = -x_1 - x_2 - \frac{1}{4}\left(\frac{y_1 - y_2}{x_1 - x_2}\right)^2$$
$$y_3 = -y_1 - y_2 - (x_3 - x_1)\left(\frac{y_1 - y_2}{x_1 - x_2}\right)$$

Si $x_1 = x_2$ alors $y_1 = \pm y_2$.
Si $y_1 = -y_2$, on a $P_1 + P_2 = \infty$. De cela, on en déduit que l'inverse de $(x, y)$ est $(x, -y)$.
Si $P_1 = P_2$ avec $y_1 = y_2 \neq 0$ alors $P_1 + P_2 = 2P_1 = (x_3, y_3)$ avec :

$$x_3 = -x_1 - x_2 - \frac{1}{16}\left(\frac{12x_1^2 - g_2}{y_1}\right)^2$$
$$y_3 = -y_1 - (x_3 - x_1)\left(\frac{12x_1 - g_2}{2y_1}\right)$$

**Théorème 9.15.** *Si $E$ est une courbe elliptique sur $K$ alors $E(K)$ est un groupe où $\infty$ est l'identité sous l'opération binaire définie ci-dessus.*

*Démonstration.* Voir [11]. □

## 9.3 Multiplication complexe

### 9.3.1 Sur $\mathbb{C}$

Soit $E$ une courbe elliptique sur $\mathbb{C}$. Elle correspond à un réseau $\Lambda$. On a un sous-anneau $\mathrm{End}_{\mathbb{C}}(E) = \{\alpha \in \mathbb{C} : \alpha\Lambda \subset \Lambda\}$ de $\mathbb{C}$ où $\mathbb{Z} \subset \mathrm{End}_{\mathbb{C}}(E)$.

**Définition 9.16.** *On dit qu'une courbe elliptique $E$ a une multiplication complexe si $\mathbb{Z} \neq \mathrm{End}_{\mathbb{C}}(E)$.*

**Remarque 9.17.** *Avec la partie précédente, on a qu'une courbe elliptique $E$ a une multiplication complexe si et seulement si $\Lambda$ possède une multiplication complexe.*
*Dans ce cas, $\mathrm{End}_{\mathbb{C}}(E)$ est un ordre $\mathcal{O}$ dans un corps quadratique imaginaire.*

On conserve les notations de la remarque, prenons $\alpha \in \mathcal{O}$, l'inclusion $\alpha\Lambda \subset \Lambda$ nous fournit un homomorphisme de groupe $\alpha : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda$.
Comme $E(\mathbb{C}) \simeq \mathbb{C}/\Lambda$, on voit $\alpha \in \mathrm{End}_{\mathbb{C}}(E)$ induit un morphisme de groupe $\alpha : E(\mathbb{C}) \to E(\mathbb{C})$.
Reformulons ce constat en termes de coordonnées :

**Proposition 9.18.** *Soit $0 \neq \alpha \in \mathrm{End}_{\mathbb{C}}(E)$ alors il existe une fonction rationnelle $R(x) \in \mathbb{C}(x)$ tel que pour $(x, y) \in E(\mathbb{C})$, on a :*

$$\alpha(x, y) = \left(R(x), \frac{1}{\alpha}R'(x)y\right) \text{ avec } R'(x) = \left(\frac{d}{dx}\right)R(x).$$

*Démonstration.* Pour $\alpha\Lambda \subset \Lambda$, le théorème 7.5 nous assure l'existence d'une fonction rationnelle $R$ tel que $\wp(\alpha z) = R(\wp(z))$. En dérivant par rapport à $z$, on obtient $\wp'(\alpha z) = \frac{1}{\alpha}\wp'(z)R'(\wp(z))$.

Or $\alpha : E(\mathbb{C}) \to E(\mathbb{C})$ provient de $\alpha : z \in \mathbb{C}/\Lambda \longmapsto (\wp(z), \wp'(z))$. Et la proposition suit immédiatement. □

A cause de la nature algébrique de $\alpha \in \mathrm{End}_{\mathbb{C}}(E)$, on écrira $\alpha : E \to E$ à la place de $\alpha : E(\mathbb{C}) \to E(\mathbb{C})$.
On commence par rappeler une définition de géométrie algébrique :

**Définition 9.19.** *Une isogénie est un morphisme de groupes algébriques qui est surjectif avec un noyau fini.*

**Remarque 9.20.** *Si $\alpha \neq 0$, on dira que $\alpha$ est une isogénie de $E$ sur lui même.*

On évoque maitnenant un invariant important des courbes elliptiques :

**Définition 9.21.** *Pour $\alpha \neq 0$, $\alpha \in E$. On pose* $\deg(\alpha) = |\mathrm{Ker}(\alpha)|$.

Si une courbe elliptique $E$ correspond au réseau $L$, on voit que le noyau de $\alpha : E \to E$ est isomorphe à $L/\alpha L$.
Grâce au théorème 7.5, on peut affirmer pour $\alpha \in \mathcal{O} = \mathrm{End}_{\mathbb{C}}(E)$ que $\deg(\alpha) = |L/\alpha L| = N(\alpha)$.

### 9.3.2 Cas général

Dans le cas où $E$ est un courbe elliptique sur un corps $K$ (qui est de caractéristique différente de 2 ou 3), on a une définition purement algébrique de l'anneau des endomorphismes $\mathrm{End}_K(E)$ qui est seulement dépendant de l'équation de Weierstrass correspondant à $E$.

**Définition 9.22.** *On dit qu'une courbe elliptique $E$ est munie d'une multiplication complexe si $\mathbb{Z} \neq \mathrm{End}_{\overline{K}}(E)$*

**Remarque 9.23.** *Dans le cas où $K$ est un corps de nombres, on a :*
$\mathbb{Z} \subset \mathrm{End}_K(E)$.
*Dans le cas où $K$ est de caractéristique positique, on a toujours :*
$\mathbb{Z} \subset \mathrm{End}_K(E) \neq \mathbb{Z}$.

Quand $K \subset \mathbb{C}$, on a pour $\alpha \in \mathrm{End}_{\mathbb{C}}(E)$ et $(x, y) \in E(\mathbb{C})$ :

$$\alpha(x, y) = \left( R(x), \frac{1}{\alpha} R'(x) y \right).$$

De ce fait, on a $\alpha \in \mathrm{End}_K(E)$ si et seulement si $R(x), \frac{1}{\alpha} R'(x) \in K(x)$.
Pour $K = \mathbb{C}$, si deux courbes elliptiques $E$ et $E'$ correspondent aux réseaux $L$ et $L'$ alors pour un complexe $\alpha \neq 0$ tel que $\alpha L \subset L'$, la multiplication par $\alpha$ induit une application $\alpha : E(\mathbb{C}) \to E'(\mathbb{C})$ de noyau $L'/\alpha L$ et $\alpha$ est une isogénie de $E$ vers $E'$.
De plus, $\alpha$ est de nature essentiellement algébrique.
Comme précédemment on écrira $\alpha : E \to E'$.

**Définition 9.24.** *On dit qu'un élement $\alpha$ est cyclique si son noyau est cyclique.*

**Proposition 9.25.** *Soient deux courbes elliptiques $E$ et $E'$ sur $\mathbb{C}$.*
*Alors, une isogénie cyclique $\alpha : E \to E'$ est de degré $m$ si et seulement si $\Phi_m(j(E), j(E')) = 0$.*

*Démonstration.* Cela provient de l'analyse de l'équation modulaire $\Phi_m(u, v) = 0$ réalisé dans la démonstration du théorème 8.16.
Voir l'exercice 14.10 dans le [2] pour les détails. □

# 10 Corps de fonctions

Nous découvrons ici les corps de fonctions. Après une brève introduction, nous construirons explicitement un corps de fonction puis nous dégagerons quelques propriétés générales de tels objets.
La principale référence ici est le [7] malgré tout [8] et [1] permettent de réaliser beaucoup d'analogies (parfois trompeuses) avec le cas des corps de nombres.

## 10.1 Introduction

Commençons par rappeler des définitions d'objets déjà rencontrés en théorie algébrique des nombres :

**Définition 10.1.** *Un anneau de valuation discrète $\mathcal{O}$ est un anneau principal ayant un unique idéal premier $\mathfrak{p}$.*

Caractérisons les générateurs de tels idéaux :

**Définition 10.2.** *Si $t$ engendre l'unique idéal premier $\mathfrak{p}$ de $\mathcal{O}$ alors $t$ sera un paramètre local.*

**Remarque 10.3.** *Pour tout $x \in \mathcal{O}$, on a $x = t^r y$ avec $r \in \mathbb{N}$ et $y$ une unité.*

Maintenant avec cette remarque on peut définir la valuation d'un élément :

**Définition 10.4.** *Si $K$ est le corps de fraction de $\mathcal{O}$ alors pour $x \in K$, on a $x = t^r y$ où $r \in \mathbb{Z}$. Le nombre $r$ est la valuation (ou l'ordre) d'un élément.*
*Si $r > 0$, on dit que $x$ est un zéro de la valuation.*
*Si $r < 0$, on dit que $x$ est un pôle de la valuation.*

**Remarque 10.5.** *On rappelle qu'avec la projection canonique $\mathcal{O} \to \mathcal{O}/\mathfrak{p}$, si $x \notin \mathcal{O} \mapsto \infty$ est la place de la valuation.*

Maintenant prenons $E$ une extension finie de $K$ qui est le corps de fraction de l'anneau de valuation discrète $\mathcal{O}$ d'idéal maximal $\mathfrak{p}$ (engendré par un élément $t$) alors il existe $\mathcal{O}_E$ un anneau de valuation discrète dans $E$ d'idéal premier $\mathfrak{P}$.
On a $\mathcal{O} = \mathcal{O}_E \cap K$ et $\mathfrak{p} = \mathfrak{P} \cap K$.

**Définition 10.6.** *Si $u \in \mathcal{O}_E$ alors $t\mathcal{O}_E = u^e \mathcal{O}_E$, le nombre $e$ est l'indice de ramification de $\mathcal{O}_E$ sur $\mathcal{O}$.*

**Remarque 10.7.** *Si $\Gamma_{\mathcal{O}_E}$ et $\Gamma_{\mathcal{O}}$ sont les groupes de valuations associés aux anneaux $\mathcal{O}_E$ et $\mathcal{O}$ alors $[\Gamma_{\mathcal{O}_E} : \Gamma_{\mathcal{O}}] = e$.*

## 10.2 Construction d'un corps de fonction

En théorie algébrique des nombres, on s'intéresse particulièrement à la notion d'élément algébrique. Ici, à contrario, nous allons nous intéresser aux éléments transcendants. Prenons $k$ un corps et $K/k$ une extension. On rappelle que :

**Définition 10.8.** *L'élément $x \in K$ est transcendant sur $k$ s'il n'est pas algébrique.*

Pour $x \in k$ on définit la fonction $\varphi_x$ par :

$$\begin{aligned} \varphi_x : k[x] &\longrightarrow K \\ P &\longmapsto P(x). \end{aligned}$$

Cette fonction est injective et c'est à la fois un homomorphisme d'anneaux et un homomorphisme de $k$-espace vectoriel. De plus, l'image de $\varphi_x$ est $k[x]$.

**Proposition 10.9.** *Si $x \in K$ est transcendant sur $k$ alors $\varphi_x$ est un isomorphisme et $k[x]$ est un $k$-espace vectoriel de dimension infinie.*

*Démonstration.* Si $x$ est transcendant alors $\varphi_x$ est surjective donc c'est un isomorphisme. Ainsi, en tant que $k$-espace vectoriel on a $\dim_k k[x] = +\infty$. □

Par simplicité, on supposera que $k$ est un corps algébriquement clos. On choisit un élément $x$ transcendant sur $k$, on considère l'extension $k(x)/k$. On rappelle que $k(x)$ est le corps de fractions rationnelles en $x$ sur $k$. On a toujours $k[X] \subset k(X)$ et on en profite pour rappeler un lemme basique de théorie des corps :

**Proposition 10.10.** *Soit $k$ un corps quelconque. On a que $x$ est algébrique sur $k$ si et seulement si $k[X] = k(X)$.*

*Démonstration.* Voir [1] pour un preuve. □

Soit $\mathcal{O}$ un anneau de valuation discrète dans $k(x)$ contenant $k$. Quitte en échangeant $x$ par $\frac{1}{x}$ si nécessaire, on peut supposer $x \in \mathcal{O}$.
Alors, $\mathfrak{p} \cup k[x]$ est engendré par un polynôme irréductible $P(x)$ qui est de degré 1 car $k$ est algébriquement clos. Donc $P(x) = x - a$ pour $a \in k$ donc la projection canonique $\mathcal{O} \to \mathcal{O}/\mathfrak{p}$ induit l'application $f(x) \mapsto f(a)$.
Ainsi, $\mathcal{O}$ est l'ensemble des fonctions rationnelles $\frac{f(x)}{g(x)}$ avec $f(x), g(x) \in k[x]$ et $g(a) \neq 0$. En outre, $\mathfrak{p}$ est constitué des quotients tel que $f(x) = 0$.

**Définition 10.11.** *Un corps de fonction $K$ est une extension finie de $k(x)$ et $x$ transcendant sur $k$. Parfois, les éléments de $K$ sont dénommés fonctions.*

**Remarque 10.12.** *Quand $k$ est algébriquement clos, le corps résiduel de tout anneau de valuation discrète contenant $k$ est égal à $k$. Cet ensemble est un corps.*

**Définition 10.13.** *On appelle corps des constantes de $K/k$ l'ensemble des éléments algébriques de $K$ sur $k$.*

**Remarque 10.14.** *Dans notre cas, $k$ est le corps des constantes.*

## 10.3 Propriétés générales

On suppose par simplicité $k$ algébriquement clos. Soit $K$ un corps de fonction. On commence par appréhender quelques propriétés liées à ce nouvel objet :

**Proposition 10.15.** *Soient $\mathcal{O}_1$ et $\mathcal{O}_2$ sont deux anneaux de valuations discrètes avec $K$ comme corps de fractions. Si $\mathcal{O}_1 \subset \mathcal{O}_2$ alors $\mathcal{O}_1 = \mathcal{O}_2$.*

*Démonstration.* Tout d'abord, si $\mathfrak{p}_1$ et $\mathfrak{p}_2$ désigent les idéaux maximaux, montrons que $\mathfrak{p}_2 \subset \mathfrak{p}_1$.
Soit $y \in \mathfrak{p}_2$, si $y \notin \mathfrak{p}_1$ alors $\frac{1}{y} \in \mathcal{O}_1$ donc $\frac{1}{y} \in \mathfrak{p}_2$ aboutissant à une contradiction. Donc $\mathfrak{p}_2 \subset \mathfrak{p}_1$. Toute unité de $\mathcal{O}_1$ est a fortiori une unité de $\mathcal{O}_2$.

Un élément $y$ de $\mathfrak{p}_2$ peut s'écrire $y = \pi_1^{r_1} u$ où $u$ est unité de $\mathcal{O}_1$ et $\pi_1$ est un élément d'ordre 1 dans $\mathfrak{p}_1$.
Si $\pi_1 \notin \mathfrak{p}_2$ alors c'est une unité de $\mathcal{O}_2$ nous fournissant ainsi une contradiction. Donc $\pi_1 \in \mathfrak{p}_2$ donc si $\mathfrak{p}_1 = \mathcal{O}_1\pi_1$ alors on a $\mathfrak{p}_2 = \mathfrak{p}_1$.
Finalement, si $u$ est une unité de $\mathcal{O}_2$ et $u \notin \mathcal{O}_1$ alors $\frac{1}{u} \in \mathfrak{p}_1$. Et $u$ ne peut être une unité dans $\mathcal{O}_2$. □

**Proposition 10.16.** *Supposons que l'on ait une famille $(\mathcal{O}_i)_{1\leq i\leq n}$ d'anneaux de valuations (discrètes) distincts et qu'il n'existe aucune relation d'inclusion. Alors, il existe $y \in K$ ayant un zéro en $\mathcal{O}_1$ et un pôle en $\mathcal{O}_j$ pour $2 \leq j \leq n$.*

*Démonstration.* On montre la proposition par récurrence.
Pour le cas $n = 2$, comme il n'existe pas de relation d'inclusion entre $\mathcal{O}_1$ et $\mathcal{O}_2$, on peut trouver $y \in \mathcal{O}_2$ et $y \notin \mathcal{O}_1$. De même, on peut trouver $z$ tel que $z \in \mathcal{O}_1$ et $z \notin \mathcal{O}_2$. Alors $\frac{z}{y}$ a un zéro en $\mathcal{O}_1$ et un pôle en $\mathcal{O}_2$.

Maintenant, supposons que nous pouvons trouver un élément $y \in K$ tel que $y$ ait un zéro en $\mathcal{O}_1$ et un pôle en $(\mathcal{O}_j)_{2\leq j\leq n-1}$. Soit $z$ ayant un zéro en $\mathcal{O}_1$ et un pôle en $\mathcal{O}_n$. Alors pour $r$ suffisament grand, $y + z^r$ satisfait la propriété voulue car schématiquement « 0+0=0, 0+pôle=pôle ». De plus, la somme de deux éléments de $K$ ayant des pôles d'ordre différent possède encore un pôle. □

On continue avec un certain nombre de définitions pour terminer notre première approche des corps de fonctions.

**Définition 10.17.** *Par point (ou premier), de $K$ sur $k$, on désigne un anneau de valuation discrète de $K$ contenant $k$ (sur $k$).*

**Définition 10.18.** *L'ensemble des points de $K$ est une courbe dont le corps de fonction est $K$. Pour renforcer l'analogie géométrie on utilise $P$ et $Q$ pour désigner les points de la courbe.*

**Définition 10.19.** *On appelle diviseur sur une courbe (ou de $K$ sur $k$) un élément d'un groupe abélien libre engendré par les points.*

Un diviseur $\mathfrak{a}$ est une somme formelle :

$$\mathfrak{a} = \sum n_i P_i = \sum n_P P,\ n_i \in \mathbb{N},\ P_i \text{ des points}$$

**Définition 10.20.** *Le degré d'un diviseur $\mathfrak{a}$ est $\sum n_i = \sum_P n_p$ et $n_i$ est l'ordre de $\mathfrak{a}$ en $P_i$.*

**Remarque 10.21.** *Si $x \in K$, $x \neq 0$ alors il existe un nombre fini de point $P$ tel que $n_P \neq 0$.*
*Si $x$ est constant alors pour tout point $P$, on a $n_P = 0$*

Dans le cas où $x$ n'est pas constant, il existe un point de $k(x)$ qui possède $x$ pour 0 et pour lequel $x$ n'est pas un pôle. Chacun de ses points s'étend à un nombre fini de points de $K$.
Ainsi, on peut associer un diviseur avec $x$ $(x) = \sum n_P P$ où $n_P$ est l'ordre de $x$ en $P$.

**Définition 10.22.** *Des diviseurs $\mathfrak{a}$ et $\mathfrak{b}$ sont linéairements équivalents si $\mathfrak{a} - \mathfrak{b}$ est un diviseur d'une fonction.*

On peut définir maintenant un ordre partiel parmi les diviseurs. Pour deux diviseurs $\mathfrak{a} = \sum n_P P$ et $\mathfrak{b} = \sum m_P P$, on écrira :

$$\mathfrak{a} \geq \mathfrak{b} \text{ si et seulment si } n_P \geq m_P \text{ pour tout } P$$

**Définition 10.23.** *Un diviseur $\mathfrak{a}$ est positif si $\mathfrak{a} \geq 0$.*

Pour conclure cette partie, si $\mathfrak{a}$ est un diviseur, on notera $L(\mathfrak{a})$ l'ensemble des $x \in K$ tel que $(x) \geq -\mathfrak{a}$.

**Proposition 10.24.** *Si $\mathfrak{a}$ est positif alors $L(\mathfrak{a})$ consiste en l'ensemble des fonctions dans $K$ qui ont des pôles seulement en $\mathfrak{a}$ de multiplicité au plus celle de $\mathfrak{a}$. De plus, $L(\mathfrak{a})$ est un espace vectoriel sur le corps des constantes $k$ et $\mathfrak{l}(\mathfrak{a})$ désignera sa dimension.*

## Quatrième partie

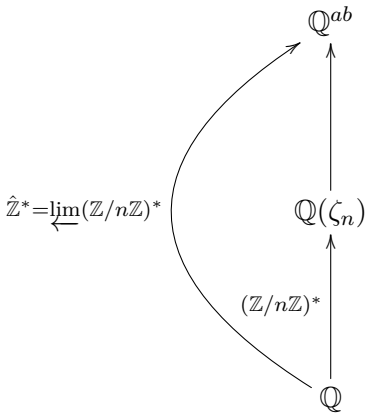
# Analogie et conclusion

Nous allons maintenant essayer de mettre en lumière les différents liens que nous avons réalisé. Rappelons notre point de départ, le corps de base fut celui des rationnels $\mathbb{Q}$, on a posé $\mathbb{Q}^{ab}$ l'extension abélienne maximale de $\mathbb{Q}$. Lors du chapitre I, la théorie de Galois et celle du corps du corps combiné avec nos connaissances topologiques étudiées lors de l'annexe 11 nous ont permis d'établir le théorème 3.2 (de Kronecker-Weber) :

$$\mathbb{Q}^{ab} = \bigcup_{n\in\mathbb{N}^*} \mathbb{Q}(\zeta_n) \text{ avec } \zeta_n \text{ une racine de } n\text{-ième l'unité et } \mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q}) \simeq \hat{\mathbb{Z}}^*$$

où $\hat{\mathbb{Z}}^* = \varprojlim(\mathbb{Z}/n\mathbb{Z})^*$

Tout cela permet d'obtenir le diagramme ci-dessous (les groupes au dessus des flèches étant les groupes de Galois associés) :




Notre principal but pour le chapitre II fut donc de généraliser cette situation au cas des corps $K$ quadratiques imaginaires. Notre réel but étant d'établir le corps de classe de rayon $\mathfrak{n}O_K$ du corps $K$ qui jouera un rôle analogue à $\mathbb{Q}^{ab}$.
Pour y parvenir, nous avons du combiner des outils provenant de trois domaines des mathématiques (théorie du corps de classe, analyse complexe et géométrie algébrique).
Pour débuter, nous avons introduit à la section 4 la notion d'ordre et l'avons relié à la théorie du corps de classe au travers des propositions 4.36 et 5.2 en montrant les isomorphismes $C(\mathcal{O}) \simeq I(\mathcal{O}, f)/P(\mathcal{O}, f) \simeq I_K(f)/P_{K,\mathbb{Z}}(f) \simeq \mathrm{Gal}(L/K)$ où $L$ l'anneau du corps de classe de l'ordre $\mathcal{O}$.
Ensuite, l'introduction et l'étude d'objets de nature analytique comme la notion de réseaux et de fonctions elliptiques sur le plan complexe $\mathbb{C}$ (et plus particulièrement le demi-plan supérieur de Poincarré $\mathbb{H}$) lors de la section

5 nous permit d'introduire lors de la section 6 la fonction $j$, fonction qui permet de caractériser les classes d'homothéthie des réseaux $\Lambda$ de $\mathbb{C}$ lors du théorème 6.15.

Nous faisions tout cela pour établir que le nombre $j(\Lambda)$ est un entier algébrique. L'introduction de la multiplication complexe avec le théorème 7.5 permet de relier la notion de réseau à celle d'ordre avec le corollaire 7.10. Enfin, en établissant que le $j$-invariant est un entier algébrique en le liant à l'anneau du corps de classe d'un ordre lors du théorème 8.21, on établit que l'extension $\mathbb{K}(j(\mathcal{O}_K))$ est l'extension abélienne non ramifiée maximale grâce au corollaire 8.24. On obtient donc le diagramme commutatif suivant :

$$\begin{array}{c} H = K(j(\mathcal{O}_K)) \\ \Big\uparrow {\scriptstyle C(\mathcal{O}_K)} \\ K \\ \Big\uparrow {\scriptstyle \mathrm{Gal}(L/K)} \\ \mathbb{Q} \end{array}$$

Grâce au théorème 5.6, on peut affirmer que l'extension $H/K$ est une extension diédrale où la conjugaison complexe agit sur $C(\mathcal{O}_K)$ par l'application $(g \mapsto g^{-1})$.

Pour conclure notre étude algbérique, nous introduisions lors de la section 8 la fonction de Weber, pour établir le théorème 8.30 qui expose le corps de classe de rayon de $K$ pour le module $n\mathcal{O}_K$. Ainsi, on a le diagramme :

$$\begin{array}{c} K^{ab} = \bigcup_n H(\tau_{\mathcal{O}_K}(\frac{1}{n})) \\ \Big\uparrow \\ H = K(j(\mathcal{O}_K)) \\ \Big\uparrow {\scriptstyle C(\mathcal{O}_K)} \\ K \\ \Big\uparrow {\scriptstyle \mathrm{Gal}(L/K)} \\ \mathbb{Q} \end{array}$$

Enfin, les fonction elliptiques définissant naturellement des courbes elliptiques, la section 9 introduit l'équation de Weierstrass. La proposition 9.12 permet de créer le lien entre courbe elliptiques, la notion de réseaux et celles d'ordre (et donc d'anneau du corps de classe) au travers des classes d'homothétie des courbes elliptiques.
Puis, on montre que l'ensemble des solutions de l'équation de Weierstrass

$E$ est un groupe additif et on redéfinit la multiplication complexe pour une courbe elliptique permettant d'utiliser le théorème 8.30 dans un cadre un peu plus large (on peut aussi se référer au chapitre 11 de [11]). Soit $E$ une courbe elliptique sur $H = K(j(E))$ ayant $\mathcal{O}_K$ comme anneau de multiplication complexe. Soit $n \in \mathbb{N}^*$, on pose $E[n]$ les points de $n$-torsion de $E$. Ainsi, on peut donc modifier le dernier diagramme :

$$\begin{array}{c} K^{ab} = \bigcup_n H(E[n]) \\ \uparrow \\ H = K(j(E)) \\ {\scriptstyle C(\mathcal{O}_K)} \uparrow \\ K \\ {\scriptstyle \mathrm{Gal}(L/K)} \uparrow \\ \mathbb{Q} \end{array}$$

Malgré notre but initial atteint, ces résultats ouvrent de nouveaux questionnements qui mériteraient et pourraient nous occuper pendant encore de nombreuses années. Le temps du stage étant court, nous ne pourrons que donner quelques pistes dans ce mémoire.

Tout d'abord, l'introduction des courbes elliptiques nous incite fortement à vouloir généraliser nos résultats à des espaces plus généraux que le plan complexe. La seconde annexe, qui établit le théorème de Riemmann-Roch, est un début de travail en direction de la géométrie algébrique.
Aussi, nous avons établit l'existence d'un corps de classe particulier, sa construction explicite est donc un problème naturel. Vouloir résoudre d'office le cas global semble contre-productif et se restreindre au cas local parait plus fructueux malgré une certaine difficulté apparente. Les travaux de Lubin-Tate vont en ce sens et mérite grandement d'être étudiés en profondeur. Le principe local-global et les constructions adéliques permettent de nourrir l'espoir de comprendre le cas global par les constructions locales.
L'implantation informatique de ces constructions, une fois établies, est aussi une question riche.

## Cinquième partie

# Annexes

La première annexe relie la topologie et la théorie de Galois. On en profite pour introduire la notion de limite projective, la topologie de Krull et établir le fait que tout groupe de Galois est profini et que tout groupe profini est un groupe de Galois.
La seconde est la continuité directe de la section 10, on y établit le théorème de Riemann-Roch qui est indispensable pour espérer prolonger nos résultats dans le cadre de variété algébrique.

## 11 Groupe de Galois et topologie de Krull

Le but de cette annexe est de montrer le lien entre le groupe de Galois et la notion de groupe profini.

### 11.1 Les groupes de Galois sont des groupes profinis

Introduisons la notion de limite projective. On a besoin de plusieurs notions avant cela. Commençons par une première définition :

**Définition 11.1.** *Un ensemble dirigé est un ensemble ordonné $I$ vérifiant pour tout $i, j \in I$, il existe $k \in I$ tel que $i, j \leq k$.*

On peut maintenant définir la notion de système projectif :

**Définition 11.2.** *Un système projectif d'ensemble ordonné sur $I$ est une famille $\{G_i,\ f_{ij}$ tel que $i, j \in I,\ i \leq j\}$ d'ensemble $G_i$ et d'homomorphismes $f_{ij} : G_j \to G_i$ tel que pour tout $i \leq j \leq k$, $f_{ik} = f_{ij} \circ f_{jk}$.*

Maintenant, celle de limite projective :

**Définition 11.3.** *On appelle limite projective $G = \varprojlim G_i$ système projectif défini comme l'ensemble :*

$$G = \{\prod_{i \in I} \sigma_i \in \prod_{i \in I} G_i \text{ tel que } f_{ij}(\sigma_j) = \sigma_i \text{ si } i \leq j\}.$$

**Remarque 11.4.** *On a choisit d'être le plus général possible dans notre présentation mais toutes ces notions se généralisent à toute structure algébrique (groupes, anneaux, corps....).*

Avec cette remarque, si les $(G_i)$ sont des groupes topologiques et que les $f_{ij}$ sont des applications continues alors $G$ est un sous-espace fermé de l'espace topologique $\prod_{i \in I} G_i$.
Ensuite, rappelons les notions que nous connaissons au sujet des groupes profinis :

**Définition 11.5.** *Un groupe $G$ est topologique profini s'il est la limite projective d'un système projectif de groupes finis.*

**Proposition 11.6.** *Soit $G$ un groupe topologique.*
*Un groupe $G$ est profini si et seulement s'il est séparé, compact et totalement discontinu.*

*Démonstration.* Voir [3] ou [12]. □

On en profite pour rappeler un fait de la théorie de Galois :

**Lemme 11.7.** *Soient $K, L, M$ trois corps tel que $K \subset L$ et $K \subset M$.*

1. *Si $L/K$ est une extension finie et $M/K$ une extension galoisienne alors $LM/K$ est une extension galoisienne où le corps $LM$ est appelé le compositum de $M$ et $L$.*
2. *Si $K \subset L \subset M$ avec $L/K$ et $M/K$ des extensions galoisiennes alors $M/L$ est une extension galoisienne.*

Cette partie sera l'occasion d'évoquer la topologie de Krull, topologie compatible avec la topologie profinie.

Soit $L/K$ une extension galoisienne de corps de nombres et soit $\Delta$ un ensemble d'extensions galoisiennes finies $L_i/K$ tel que $L = \bigcup_i L_i$.
De tels ensembles existent en prenant par exemple celui de toutes les extensions finies de $K$. Introduisons maintenant la notion de filtre :

**Définition 11.8** (Filtre)**.**
*Soit $E$ un ensemble. On appelera filtre sur $E$, toute partie $\mathcal{F} \in \mathcal{P}(E)$ telle que :*

1. *Si $A \in \mathcal{P}(E)$ et qu'il existe $B \in \mathcal{F}$ tel que $B \subset A \subset E$ alors $A \in \mathcal{F}$.*
2. *Toute union finie d'éléments de $\mathcal{F}$ appartient à $\mathcal{F}$.*
3. *$\varnothing \notin \mathcal{F}$.*

En ordonnant $\Delta$, on obtient un ordre filtrant à droite.
En effet, si $L_i, L_j \in \Delta$ alors, grâce au lemme 11.7, $L_iL_j/K$ est une extension galoisienne. De ce fait, il existe $\alpha \in L$ tel que $L_iL_j = K(\alpha)$. Par hypothèse, il existe $L_k \in \Delta$ tel que $\alpha \in L_k$ donc on a $L_i \subset L_k$ et $L_j \subset L_k$.

Pour tout $L_i \subset L_j$, si $\Delta_{ij} : L_i \to L_j$ est l'injection canonique alors on a $L = \varprojlim L_i$. Comme $L_i/K$ est une extension galoisienne, on sait grâce au lemme 11.7 et à la proposition 11.18 que le groupe $G^i = Gal(L/L_i)$ est un sous-groupe distingué de $Gal(L/K)$.

Considérons $\mathcal{V} = \{G^i\}$, nous allons utiliser les bases de filtre :

**Définition 11.9** (Base de filtre)**.**
*Soient $E$ un ensemble et $\mathcal{F}$ un filtre de $E$. On dira que $\mathcal{B} \in \mathcal{P}(E)$ est une base de filtre de $\mathcal{F}$ si $\mathcal{F} = \{A \in \mathcal{P}(E) / \exists F \in \mathcal{B}, F \subset A\}$.*

On peut maintenant s'intéresser au lemme suivant qui relie les bases de filtre et les groupes profinis :

**Lemme 11.10.** *Soit $G$ un groupe topologique profini. L'ensemble des sous-groupes distingués et ouverts de $G$ constituent une base de filtre des voisinages de l'élément neutre.*

*Démonstration.* Soient $\pi_i : G \to G_i$ les différentes projections et $U$ un voisinage de 1 dans $G$. Il existe donc des indices $(i_j)_{1 \leq j \leq n}$ et des parties $A_{i_j} \subset G_{i_j}$ tels que

$$\bigcap_{1 \leq j \leq n} \pi_{i_j}^{-1}(A_{i_j}) \subset U.$$

Or $U$ contient 1 donc pour tout $j$, on a $1 \in A_{i_j}$. Ainsi, on a :

$$V = \bigcap_{1 \leq j \leq n} \pi_{i_j}^{-1}(1) \subset U$$

et $V$ est un sous-groupe distingué de $G$. □

**Lemme 11.11.** *$\mathcal{V}$ est une base de filtre pour $\Delta$.*

*Démonstration.*
Soient $G^i, G^j \in \mathcal{V}$ alors $G^i \cap G^j$ est un sous-groupe distingué de $\mathrm{Gal}(L/K)$. Considérons le compositum $L_iL_j$, on a que $L_iL_j/K$ est une extension galoisienne de degré fini et $G^i \cap G^j = \mathrm{Gal}(L/L_iL_j)$.

Soit $\alpha \in L$ un élément primitif de $L_iL_j/K$. Par hypothèse, il existe $k$ tel que $\alpha \in L_k$. On a alors $G^k \subset \mathrm{Gal}(L/L_iL_j) = G^i \cap G^j$. □

Ainsi, on a :

1. Pour tout $U \in \mathcal{V}$, il existe $V \in \mathcal{V}$ tel que $V.V \subset U$.
2. Pour tout $U \in \mathcal{V}$, il existe $V \in \mathcal{V}$ tel que $V^{-1} \subset U$.
3. Pour tout $U \in \mathcal{V}$, pour tout $a \in \mathrm{Gal}(L/K), \exists V \in \mathcal{V}, V \subset aUa^{-1}$.

Il existe donc une unique topologie sur $\mathrm{Gal}(L/K)$ compatible avec la structure de groupe topologique pour laquelle $\mathcal{V}$ est une base de filtre des voisinages pour l'élément neutre. Montrons le :

**Lemme 11.12** (**ou définition**)**.**
*La topologie que l'on vient de décrire est indépendante du choix de $\Delta$. On l'appelle la topologie de Krull.*

*Démonstration.* Soient $\mathcal{V}$ et $\mathcal{W}$ deux bases de voisinages de l'élément neutre dans $\mathrm{Gal}(L/K)$ associées à $\Delta$ et $\Delta'$ d'extensions galoisiennes finies engendrant $L$.

Soit $G = \mathrm{Gal}(L/L_i) \in \mathcal{V}, \alpha \in L$ primitif. Il existe $L_i' \in \Delta$ tel que $\alpha \in L_i'$ on a alors $G' \subset G$ si $G' = \mathrm{Gal}(L/L_i) \in \mathcal{W}$ donc les topologies ainsi définies sont les mêmes. □

Considérons $\Delta$ un ensemble d'extensions galoisiennes finies $L_i/K$ tel que $L = \bigcup_i L_i$.
Pour tout $i$, on a les surjections canoniques $\pi_i : \mathrm{Gal}(L/K) \to \mathrm{Gal}(L_i/K)$.
Ce sont des homomorphismes de groupes. De plus, si on munit $\mathrm{Gal}(L/K)$ de la topologie de Krull et chaque $\mathrm{Gal}(L_i/K)$ de la topologie discrète alors les $(\pi_i)$ sont continues car :
$\pi_i^{-1}(\{1\})$ est ouvert puisque $\Psi_\sigma : \mu \mapsto \sigma\mu$ est un homémomorphisme de $\mathrm{Gal}(L_i/K)$. De ce fait, $\pi_i^{-1}(\{1\}) = \mathrm{Gal}(L/L_i) = G^i$ est ouvert par définition.

Pour tout $i$, si $G_i = \mathrm{Gal}(L_i/K)$ et $L_i \subset L_j$, en notant $\varphi_{ij} : G_i \to G_j$, les surjections canoniques, on obtient un système projectif $(G_i, \varphi_{ij})$.
On est donc amené à considérer le groupe profini $\varprojlim G_i$ muni de sa structure de groupe topologique. On peut donc énoncer le résultat central de cette partie :

**Proposition 11.13.** *On a* $\mathrm{Gal}(L/K) \cong \varprojlim G_i$ *en tant que groupe topologique en munissant* $\mathrm{Gal}(L/K)$ *de la topologie de Krull.*

*Démonstration.* Soit $G$ un groupe topologique, pour tout $i$, $\varphi_i : G \to G_i$ désignera un morphisme de groupe continu tel que pour tout $i \leq j$,
$\varphi_i = \varphi_{ji} \circ \varphi_j$.

Pour tout $\sigma \in G$, on définit $\theta(\sigma) : L \to L, x \mapsto \varphi_i(\sigma)x$, si $x \in L_i$.
L'application $\theta(\sigma)$ est bien définie car si $x \in L_j$ et si $L_iL_j \subset L_k$ alors :

$$\begin{aligned}\varphi_i(\sigma)(x) &= \varphi_{ki} \circ \varphi_k(\sigma)(x) \\ &= \varphi_k(\sigma)(x) \\ &= \varphi_{kj} \circ \varphi_k(\sigma)(x) \\ &= \varphi_j(\sigma)(x)\end{aligned}$$

C'est donc un $K$-automorphisme de $L$ et $\theta : G \to \mathrm{Gal}(L/K)$ est l'unique application vérifiant $\varphi_i = \pi_i \circ \theta$.
Donc $\theta$ est un morphisme de groupes, continu car $\theta^{-1}(G) = \varphi_i^{-1}(\{Id\})$ d'où l'isomorphisme de groupes topologiques. □

Ainsi, le groupe de Galois d'une extension galoisienne est un groupe profini. S'il est muni de la topologie de Krull il est bien compact, séparé, totalement discontinu et l'ensemble des sous-groupes distingués (et ouverts) constitue une base de filtre des voisinages de l'élément neutre.

## 11.2 Le théorème de Waterhouse

On commence par rappeler le lemme d'Artin qui sera central dans les démonstrations de cette partie :

**Lemme 11.14** (d'Artin)**.**
*Soient $L$ un corps, $G$ un groupe d'automorphisme de $L$ de cardinal $n$. Posons $K = L^G$ le sous-corps de $L$ fixé par $G$. Alors, l'extension $L/K$ est galoisienne de degré $n$.*

*Démonstration.* Voir [1]. □

On commence par résoudre le cas où $G$ est un groupe fini (un groupe fini étant profini).

**Lemme 11.15** (de Noether)**.**
*Soit $G$ un groupe fini. Alors il existe une extension galoisienne $L/K$ telle que $G = \mathrm{Gal}(L/K)$.*

*Démonstration.* Soit $n$ le cardinal de $G$. On plonge $G$ dans $S_n$. On sait que $S_n$ agit en permutant les variables sur $F(X_1, \ldots, X_n)$ avec $F$ un corps commutatif quelconque.
Ainsi, si $R \in F(X_1, \ldots, X_n)$ et $\sigma \in S_n$ alors :

$$\sigma(R(X_1, \ldots, X_n)) = R(X_{\sigma(1)}, \ldots, X_{\sigma(n)}).$$

Ainsi, $G$ agit comme groupe de permutations sur $F(X_1, \ldots, X_n)$.
Si on pose $K = F(X_1, \ldots, X_n)^G$ et $L = F(X_1, \ldots, X_n)$, le lemme 11.14 permet d'affirmer que l'extension $L/K$ est galoisienne de groupe de Galois $G$ et de degré $n$. □

Avant de prouver le théorème de Waterhouse, on propose une généralisation du lemme 11.14 au cas des extensions infinies :

**Lemme 11.16** (Généralisation du théorème d'Artin)**.**
*Si $G$ est un groupe profini d'automorphisme d'un corps $L$ tel que $\forall x \in L, S(x) = \{\sigma \in G / \sigma(x) = x\}$ soit un sous-groupe ouvert de $G$.*
*Alors $L/K$ est une extension galoisienne et $G = \mathrm{Gal}(L/K)$ avec $K = L^G$.*

*Démonstration.* Soit $K = L^G$ et $(x_i)_{1 \leq i \leq n} \subset L$. Le groupe

$$H = \bigcap_{1 \leq i \leq n} S(x_i)$$

est un sous-groupe ouvert de $G$. Posons $N$ l'intersection de tout les conjugués de $H$. C'est un sous-groupe fermé de $G$. Soit $n$ l'indice de $H$ dans $G$. $G$ agit sur $G/H$ par multiplication. Cette action induit un morphisme de $G$ vers $S_n$ dont le noyau est $N$.

De ce fait, $G/N$ est isomorphe à un sous-groupe de $S_n$ donc l'indice de $N$ dans G est inférieur à $n!$. Ainsi, $N$ est un sous-groupe ouvert de $G$.
Comme $G/N$ est fini et agit comme groupe d'automorphisme sur le corps $F = K(Gx_1, \dots, Gx_n)$.
Le corps des invariants est alors égal à $L$ donc d'après le lemme 11.14, $F/K$ est galoisienne de groupe de Galois $G/N$.

Le corps $L$ est la réunion des extensions $F/K$ donc c'est une extension galoisienne. L'intersection des $N$ est réduite à l'élément neutre, on a donc :

$$\begin{aligned} \mathrm{Gal}(L/K) &= \varprojlim \mathrm{Gal}(F/K) \\ &= \varprojlim G/N \\ &= G. \end{aligned}$$

□

Montrons maintenant la réciproque de la proposition 11.13 qui est un résultat récent datant des années 70 qui généralise la méthode du lemme 11.15 :

**Proposition 11.17** (Théorème de Waterhouse)**.**
*Soit $G$ un groupe profini alors il existe une extension galoisienne $L/K$ telle que $G = \mathrm{Gal}(L/K)$.*

*Démonstration.* Considérons un groupe profini $G$ et $\mathcal{N}$ l'ensemble des sous-groupes ouverts et distingués de $G$. Soit $K$ un corps de nombres.
Posons $\Omega = \bigsqcup_{N \in \mathcal{N}} G/N$ (union disjointe) et $F = K(X_\omega)_{\omega \in \Omega}$ le corps des fractions rationnelles en $(X_\omega)$.

Soit $\omega \in \Omega, \sigma \in G$, il existe $N \in \mathcal{N}, \tau \in G$ tel que $\omega$ soit la classe de $\tau N$ dans $G/N$. Posons $\sigma(x_\omega) = X_{\sigma(\omega)}$ où $\sigma(\omega)$ est la classe de $\sigma\tau N$ dans $G/N$. On voit que $G$ permute les fractions rationnelles c'est donc un groupe d'automorphismes de $F$.
Ainsi, le stabilisateur $S(X_\omega)$ de $X_\omega$ pour chaque $\omega$ représentant de la classe de $\tau N$ est $N$ donc c'est un sous-groupe ouvert de $G$. Si $R(X_{\omega_1}, \dots, X_{\omega_n}) \in F$. Alors, l'intersection

$$\bigcap_{1 \leq i \leq n} S(X_{\omega_i})$$

est incluse dans $S(R)$ qui est ouvert donc l'intersection est ouverte.
En posant $L$ la réunion des extensions $F/K$, on en déduit le théorème de Waterhouse grâce au lemme 11.16. □

## 11.3 Une généralisation de la correspondance de Galois

Cette caractérisation topologique des groupes de Galois nous permet de généraliser le théorème de correspondance de Galois dans le cas des extensions infinies. Tout d'abord, rappelons le théorème de correspondance de Galois dans le cas des extensions finies.

**Proposition 11.18** (Correspondance de Galois)**.**
*Soit $L/K$ une extension galoisienne finie, on pose $G = \mathrm{Gal}(L/K)$.*
*Les applications $M \longmapsto H = \mathrm{Gal}(L/M)$ et $H \longmapsto M = L^H$ établissent une bijection décroissante entre les extensions intermédiaires $K \subset M \subset L$ et les sous-groupes ouverts et distingués $H$ de $G$.*

*Démonstration.* Voir [1]. □

**Théorème 11.19** (Généralisation de la correspondance de Galois)**.**
*Soit $\Omega/K$ une extension galoisienne. L'application $L \longmapsto Gal(\Omega/L)$ met en bijection les sous-extensions $L/K$ de $\Omega/K$ et les sous-groupes fermés de $\mathrm{Gal}(\Omega/K)$. Les sous-groupes ouverts d'indices finis correspondent quant à eux aux extensions finies de $\Omega/K$.*

*Démonstration.* Chaque sous-groupe ouvert de $\mathrm{Gal}(\Omega/K)$ est aussi fermé car il est le complémentaire de l'union des classes d'équivalences ouvertes dans $\mathrm{Gal}(\Omega/L)$.

Si $L/K$ est une sous-extension finie de $\Omega/K$ alors $\mathrm{Gal}(\Omega/L)$ est ouvert car si $\sigma \in \mathrm{Gal}(\Omega/L)$ alors $\sigma$ possède une voisinage ouvert $\sigma Gal(\Omega/N) \subset \mathrm{Gal}(\Omega/L)$ où $N/K$ est la clôture normale de $L/K$. Si L/K est une sous-extension de $\Omega/K$ alors

$$\mathrm{Gal}(\Omega/L) = \bigcap_i \mathrm{Gal}(\Omega/L_i)$$

où $L_i/L$ varie parmi les sous-extensions finies de $\Omega/L$. De plus $\mathrm{Gal}(\Omega/L)$ est fermé.

Maintenant, regardons l'application $L \longmapsto Gal(\Omega/L)$ qui est injective avec $L$ le corps fixé par $\mathrm{Gal}(\Omega/K)$.

Pour la surjectivité, montrons que si $H$ est un sous-groupe fermé de $\mathrm{Gal}(\Omega/K)$ alors $H = \mathrm{Gal}(\Omega/L)$ et $L$ le corps fixé par $H$.
On a clairement, $H \subset \mathrm{Gal}(\Omega/K)$. Soit $\sigma \in \mathrm{Gal}(\Omega/L)$. Si $M/L$ est une sous-extension galoisienne finie de $\Omega/L$ alors $\sigma\mathrm{Gal}(\Omega/M)$ est un voisinage ouvert de $\sigma$ dans $\mathrm{Gal}(\Omega/L)$.
L'application $H \longmapsto \mathrm{Gal}(M/L)$ est surjective car son image $\overline{H}$ fixe le corps $L$ et $\overline{H} = \mathrm{Gal}(M/L)$ grâce à la correspondance de Galois dans le cas fini.

Ensuite, prenons $\tau \in H$ tel que $\tau_{|M} = \sigma_{|M}$ on a $\tau \in H \cap \sigma\mathrm{Gal}(\Omega/M)$ montrant ainsi que $\sigma$ appartient à la clôture de $H$.
i.e $\sigma \in \overline{H}$ donc comme $H$ est fermé on a $H = \mathrm{Gal}(\Omega/L)$.

Enfin, si $H$ est un sous-groupe ouvert de $\mathrm{Gal}(\Omega/K)$, $H$ est aussi fermé et de la forme $\mathrm{Gal}(\Omega/L)$. Cela implique que $\mathrm{Gal}(\Omega/K)$ est l'union disjointe des classes d'équivalences de $H$. Comme $\mathrm{Gal}(\Omega/K)$ est compact, un nombre fini de classes d'équivalences recouvre $\mathrm{Gal}(\Omega/K)$).

On a donc $H = \mathrm{Gal}(\Omega/L)$ qui est d'indice fini dans $\mathrm{Gal}(\Omega/K)$ impliquant que $L/K$ est de degré fini. □

## 11.4 Conclusion

Tout d'abord, grâce aux proposition 11.13 et 11.17, on a obtenu le théorème suivant :

**Théorème 11.20.**
*$K$ et $L$ désigneront des corps de nombres.*

1. *Soit $G$ un groupe topologique profini alors $G$ est le groupe de Galois d'une extension $L/K$ galoisienne.*
2. *Soit $G$ le groupe de Galois d'une extension galoisienne $L/K$ alors $G$ est un groupe topologique profini.*

Maintenant, soit $\overline{\mathbb{Q}}$ une clôture algébrique de $\mathbb{Q}$. L'extension $\overline{\mathbb{Q}}/\mathbb{Q}$ est une extension normale et comme nous sommes en caractéristique 0, c'est une extension galoisienne de degré infini. On peut donc définir :

**Définition 11.21** (Groupe de Galois absolu)**.**
*Si on note $\overline{\mathbb{Q}}$ la clôture algébrique de $\mathbb{Q}$. Le groupe $\mathcal{G}_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ sera appelé le groupe de Galois absolu.*

En vertu du théorème 11.19 et 11.20, on obient le résultat final de ce devoir :

**Théorème 11.22.**
*En notant $\overline{\mathbb{Q}}$ la clôture algébrique de $\mathbb{Q}$, on a :*

1. *$\mathcal{G}_{\mathbb{Q}}$ est un groupe profini et $\mathcal{G}_{\mathbb{Q}} \cong \varprojlim \mathrm{Gal}(K/\mathbb{Q})$ où $K$ parcourt les extensions galoisiennes finies de $\mathbb{Q}$.*
2. *Les sous-groupes fermés de $\mathcal{G}_{\mathbb{Q}}$ correspondent aux extensions intermédiaires galoisiennes de $\mathbb{Q}$.*
3. *Les sous-groupes ouverts d'indices finis de $\mathcal{G}_{\mathbb{Q}}$ correspondent aux extensions galoisiennes intermédiaires finies de $\mathbb{Q}$.*

# 12 Théorème de Riemann-Roch

Originellement, ce théorème répond au problème portant sur l'existence de fonctions méromorphes sur une surface de Riemann $S$ donnée, sous la contrainte de pôles de multiplicité imposée en certains points. Nous avons étudié ce théorème dans la continuité du travail entamé par la section 10. Nous proposons une preuve analytique du théorème de Riemann-Roch. Ce résultat de géométrie algébrique permet de généraliser notre raisonnement sur le plan complexe avec les courbes elliptiques. La référence pour cette partie est [7].

**Théorème 12.1** (de Riemann-Roch)**.** *Soit $\mathfrak{a}$ un diviseur d'un corps de fonction $K$ (sur $k$ algébriquement clos). Alors, si $\mathfrak{c}$ est un diviseur de la classe canonique, on a :*

$$ł(\mathfrak{a}) = \deg(\mathfrak{a}) + 1 - g + l(\mathfrak{c} - \mathfrak{a}).$$

*En d'autres termes, $\delta(\mathfrak{a}) = ł(\mathfrak{c} - \mathfrak{a})$.*

Avant de pouvoir s'ateler à la démonstration, il nous reste quelques objets à définir.

## 12.1 Préliminaires

Soit $P$ un point d'une courbe $V$, $\mathcal{O}$ désignera son anneau local dans un corps de fonction $K$. Notons $\mathfrak{p}$ son idéal maximal et on rappelle que comme $k$ est algébriquement clos, $\mathcal{O}/\mathfrak{p} \simeq k$. On sait que $\mathcal{O}$ est un anneau de valuation muni d'une valuation discrète. Prenons $t$ un générateur de $\mathfrak{p}$. Soit $x \in \mathcal{O}$, pour une certaine constante $a_0 \in k$, on a $x \equiv a_0 \mod \mathfrak{p}$ donc la fonction $x - a_0 \in \mathfrak{p}$ et elle possède un zéro dans $\mathcal{O}$.
Ainsi, pour un certain $y_0 \in \mathcal{O}$, $x - a_0 = ty_0$.
Par un procédé similaire, on obtient $y_0 = a_1 + ty_1$, $y_1 \in \mathcal{O}$ et $x = a_0 + a_1 t + y_1 t^2$. En itérant ce processus, on obtient $x = a_0 + a_1 t + a_2 t^2 + \dots$.

**Remarque 12.2.** *Trivialement, pour chaque $a_i = 0$ on a $x = 0$.*

Ainsi, le corps de fraction $K$ de $\mathcal{O}$ peut s'injecter dans le corps des séries formelles $k((t))$. On suit un procédé similaire à la section 10.2, en prenant $\mathcal{O} = k[[t]]$ l'anneau des séries formelles en une variable. C'est un anneau de valuation discrète et son idéal maximal est engendré par $t$. Chaque élément $x$ de $K$ le corps de fraction s'écrit comme une série formelle :
$x = a_m t^{-m} + \dots + a_{-1} t^{-1} + a_0 + a_1 t + a_2 t^2 + \dots$, où chaque coefficient $a_i \in k$.

**Remarque 12.3.** *Si $x$ n'a pas de pôle alors la projection canonique $\mathcal{O} \to \mathcal{O}/\mathfrak{p}$ envoie $x$ sur $a_0$.*

Le corps $K$ dépend seulement de l'idéal maximal $\mathfrak{p}$. En effet, si $u$ est un autre générateur de $\mathfrak{p}$, on a $k((t)) = k((u))$, on note ce corps $K_\mathfrak{p}$.
Ainsi, si $x \in K_\mathfrak{p}$, on a $x = \sum_{m \leq k \leq \infty} a_k t^k$ avec $a_m \neq 0$.

**Définition 12.4.** *Si $m > 0$ (resp. $m < 0$) alors $x$ est un zéro (resp. un pôle) d'ordre $m$. Dans les deux cas, on dit que $m$ est l'ordre de $x$.*

**Lemme 12.5.** *Pour un diviseur $\mathfrak{a}$ et un point $P$, on a :*

- $l(\mathfrak{a} + P) \leq l(\mathfrak{a}) + 1$.
- *La dimension de $L(\mathfrak{a})$ est fini i.e $l(\mathfrak{a})$ est fini.*

*Démonstration.* Si $\mathfrak{a} = 0$ alors $l(\mathfrak{a}) = 1$ et $L(\mathfrak{a})$ est un corps de constante car une fonction sans pôle est constante.
si on établit l'inégalité désirée, pour tout diviseur $\mathfrak{a}$, $l(\mathfrak{a})$ est fini .

Soit $m$ la multiplicité de $P$ dans $\mathfrak{a}$. Supposons qu'il existe une fonction telle que $z \in L(\mathfrak{a} + P)$ et $z \notin L(\mathfrak{a})$. Alors, l'ordre $x$ en $P$ est $-(m+1)$.

Soit $w \in L(\mathfrak{a} + P)$, en regardant le coefficient dominant dans la série formellle de $P$ en $w$, on remarque qu'il existe une constante $c$ tel que $w - cz$ soit d'ordre au moins $-m$ en $P$. Donc $w \in L(\mathfrak{a})$ établit l'inégalité du lemme. □

## 12.2 Construction adéliques et diviseurs

L'introduction des adèles va nous permettre une certaine souplesse technique, ce qui va faciliter le cheminement vers le théorème de Riemann-Roch.

Si on prend l'ensemble des points $P$, soit $\mathbb{A}^*$ le produit carthésien de l'ensemble des $K_P$. Un élément de $\mathbb{A}^*$ peut être vu comme un vecteur infini $\xi = (\dots, \xi_P, \dots)$ où $\xi_P \in K_P$. L'ensemble $\mathbb{A}^*$ muni de l'addition et de la multiplication est un anneau.
Nous considérerons le sous-anneau $\mathbb{A} \subset \mathbb{A}^*$ constitué de l'ensemble des vecteurs tel que $\xi_P$ n'ai pas de pôle en $P$ pour un nombre fini de point $P$.

**Définition 12.6.** *L'anneau $\mathbb{A}$ s'appelle l'anneau des adèles.*

**Remarque 12.7.** *Comme dans le cas des corps nombres, notre corps de fonction $K$ s'injecte dans $\mathbb{A}$ grâce à l'application $x \mapsto (\dots, x, x, x, \dots)$ où la $P$-ième composante prise en $x$ est vu comme une série formelle de $K_P$.*
*En outre, le corps des constantes $k$ s'injecte dans $\mathbb{A}$ qui peut être vu comme un algèbre sur $k$ de dimension infinie.*

**Définition 12.8.** *Soit $\mathfrak{a}$ un diviseur de notre courbe. On désigne par parralélotopes qu'on désigne par $\Lambda(\mathfrak{a})$ le $k$-sous-espace vectoriel de $\mathbb{A}$ consistant en l'ensemble des adèles $\xi$ tel que l'ordre de $\xi_P$ soit supérieur ou égal à l'opposée de $\mathfrak{a}$ en $P$.*

**Remarque 12.9.** *L'ensemble des $\Lambda(\mathfrak{a})$ est un système fondamental de voisinage de 0 dans $\mathbb{A}$ permettant à $\mathfrak{A}$ un anneau topologique.*

L'ensemble des fonction $x$ tel que $(x) \leq -\mathfrak{a}$ est l'espace vectoriel $L(\mathfrak{a})$ donc $L(\mathfrak{a}) = \Lambda(\mathfrak{a}) \cap K$.

On prend $\mathfrak{a}$ un diviseur, $\mathfrak{a} = \sum n_i P_i$ et $\sum n_i$ est son degré.
Notre but est de montrer que $\deg(\mathfrak{a})$ et $l(\mathfrak{a})$ ont le même ordre de grandeur et on désire obtenir des informations précises sur $l(\mathfrak{a}) - \deg(\mathfrak{a})$. Eventuellement, on veut aussi prouver qu'il existe une constrante $g$ ne dépendant que du corps $K$ tel que :

$$l(\mathfrak{a}) = \deg(\mathfrak{a}) + 1 - g - \delta(\mathfrak{a}), \delta(a) \in \mathbb{N}.$$

De plus, $l(\mathfrak{a})$ est nul si $\deg(\mathfrak{a}) > 2g - 2$.

On établit maintenant quelques formules pour les calculs futurs. Si $B$ et $C$ sont deux $k$-sous-espace de $\mathbb{A}$ et $C \subset B$ alors on notera $(B : C)$ la dimension de l'espace $B \mod C$ sur $k$.

**Proposition 12.10.** *Soient $\mathfrak{a}$ et $\mathfrak{b}$ deux diviseurs. Alors $\Lambda(\mathfrak{b}) \subset \Lambda(\mathfrak{a})$ si et seulement si $\mathfrak{a} \leq \mathfrak{b}$. Dans ce cas, on a :*

- *1)* $(\Lambda(\mathfrak{a}) : \Lambda(\mathfrak{b})) = \deg(\mathfrak{a}) - \deg(\mathfrak{b})$.
- *2)* $(\Lambda(\mathfrak{a}) : \Lambda(\mathfrak{b})) = (\Lambda(\mathfrak{a}) + K : \Lambda(\mathfrak{b}) + K) + ((\Lambda(\mathfrak{a}) \cap K) : (\Lambda(\mathfrak{b}) \cap K))$.

*Démonstration.* La première assertion est directe. Pour les deux items :

- 1) Si $P \in \mathfrak{a}$ est un point de multiplicité $d$ et $P \in \mathfrak{b}$ avec une multiplicité $e$ alors $d \geq e$. Si $t$ est un élément d'ordre 1 en $P$ dans $K_P$ alors l'indice $(t^{-d}K_P : t^{-e}K_P)$ est égal à $d - e$. L'indice de 1) est la somme des indices locaux d'un nombre fini de point de ce type. Cela donc s'étend à tous les points de $\mathfrak{a}$ et $\mathfrak{b}$.
- 2) Cela découle directement des théorèmes d'homomorphisme dans le cas des espaces vectoriels.

□

Prenons deux diviseurs $\mathfrak{a}$ et $\mathfrak{b}$ tel que $\mathfrak{a} \geq \mathfrak{b}$, grâce à la proposition 12.10, on obtient :

$$\deg(\mathfrak{a}) - \deg(\mathfrak{b}) = (\Lambda(\mathfrak{a}) + K : \Lambda(\mathfrak{b}) + K) + l(\mathfrak{a}) - l(\mathfrak{b}). \tag{29}$$

Soit $y$ une fonction non constante de $K$. Soit $\mathfrak{c}$ le diviseur de ses pôles, on écrit $\mathfrak{c} = \sum e_i P_i$. Les points $P_i \in \mathfrak{c}$ induisent tous le même point $Q$ de la

courbe elliptique rationnelle ayant pour corps de fonction $k(y)$ et $e_i$ est l'indice de ramification par définition du groupe de valuation discrète dans $k(y)$ associé au point $Q$ et aux extensions du groupe de valuations de $K$. Ces extensions correspondent aux points $P_i$.
On va montrer que le degré $\sum e_i$ de $\mathfrak{c}$ est égal à $[K : k(y)] = n$.

Soit $z_1, \ldots, z_n$ une base linéaire de $K$ sur $k(y)$. Après avoir multiplié chaque $z_j$ avec un polynôme approprié dans $k[y]$ que l'on peut supposer entier sur $k[y]$. Ainsi, aucune place finie de $K$ sur $k[y]$ n'est un pôle de $z_j$.

Tous les pôles de $z_j$ étant parmi les $P_i$ qui apparaissent dans $\mathfrak{c}$, il existe un entier $\mu_0$ tel que $z_j \in L(\mu_0\mathfrak{c})$. Soit $\mu$ un entier positif suffisamment grand, pour tout entier $0 \leq s \leq \mu - \mu_0$, on a $y^s z_j \in L(\mu\mathfrak{c})$ donc $l(\mu\mathfrak{c}) \geq (\mu - \mu_0 + 1)n$. Soit $N_\mu$ l'entier $(\Lambda(\mu\mathfrak{c}) + K : \Lambda(0) + K)$ donc $N_\mu \geq 0$. Posons $\mathfrak{b} = 0$ et $\mathfrak{a} = \mu\mathfrak{c}$ dans (29), on a :

$$\mu(\sum e_i) = N_\mu + l(\mu\mathfrak{c}) - 1 \geq N_\mu + (\mu - \mu_0 + 1)n - 1 \tag{30}$$

En divisant (30) par $\mu$ et en faisant tendre $\mu \to +\infty$, on a $\sum e_i \geq n$. On admet le théorème d'approximation suivant :

**Théorème 12.11.** *Soit $E$ une extension algébrique finie de $K$. Soit $\Gamma$ le groupe de valuation (discrète) de $K$ et $\Gamma_i$ le groupe de valuation d'un nombre fini de valuation discrète qui se pas équivalentes celle de $E$ qui étend celle de $K$. Soit $[\Gamma_i : \Gamma]$ alors $\sum e_i \leq [E : K]$*

*Démonstration.* Voir [7]. □

Grâce a ce résultat, on peut établir :

**Théorème 12.12.** *Soit $y \in K$ une fonction non constante. Si $\mathfrak{c}$ est le diviseur des pôles de $y$ alors $\deg(\mathfrak{c}) = [K : k(y)]$ donc le degré d'un diviseur d'une fonction est égal à 0 (une fonction a autant de zéros que de pôles).*

*Démonstration.* Si on prend $\mathfrak{c}'$ est le diviseur des zéros de $y$ alors $\mathfrak{c}'$ est le diviseur des pôles de $\frac{1}{y}$ et $[K : k(\frac{1}{y})] = n$. □

**Corollaire 12.13.** *La fonction $\deg(\mathfrak{a})$ est une fonction de la classe d'équivalence linéaire de $\mathfrak{a}$.*

**Définition 12.14.** *On appelle fonction classe une fonction qui ne dépend que la classe d'équivalence linéaire d'un diviseur.*

Revenons à (30), on peut écrire $\mu n \geq N_\mu + \mu n - \mu_0 n + n - 1$ d'où
$N_\mu \leq \mu_0 n - n + 1$ montrant que $N_\mu$ est uniformément bornée. Donc pour un $\mu$ assez grand on a $N_\mu = (\Lambda(\mu\mathfrak{c} + K : \Lambda(0) + K)$ est constant car c'est

toujours un entier positif.

Définissons une nouvelle fonction de divisieurs $r(\mathfrak{a}) = \deg(\mathfrak{a}) - l(\mathfrak{a})$. Les deux fonctions deg et $l$ sont des fonctions classes, la première grâce au théorème 12.12 et l'autre car l'application $z \mapsto yz$, pour $z \in L(\mathfrak{a})$ est un $k$-isomorphisme entre $L(\mathfrak{a})$ et $L(\mathfrak{a} - (y))$. Pour deux diviseurs $\mathfrak{a}$ et $\mathfrak{b}$ tels que $\mathfrak{a} \geq \mathfrak{b}$, on peut réécrire (29) :

$$0 \leq (\Lambda(\mathfrak{a}) + K : \Lambda(\mathfrak{b}) + K) = r(\mathfrak{a}) - r(\mathfrak{b}). \tag{31}$$

Posons $\mathfrak{b} = 0$ et $\mathfrak{a} = \mu\mathfrak{c}$ donc $(\Lambda(\mu\mathfrak{c}) + K : \Lambda(0) + K) = r(\mu\mathfrak{c}) - r(0)$ et ce qui précède permet d'affirmer que $r(\mu\mathfrak{c})$ est uniformément borné pour un $\mu$ assez grand.

Soit $\mathfrak{b}$ un diviseur quelconque, prenons une fonction $z \in k[y]$ ayant des zéros en tous les points de $\mathfrak{b}$ excepté ceux en commun avec $\mathfrak{c}$ (ce sont les pôles de $y$). Alors pour un certain $\mu$, $(z) + \mu\mathfrak{c} \geq \mathfrak{b}$. Posons $\mathfrak{a} = \mu\mathfrak{c}$ dans (31) et en utilisant le fait que $r(\mathfrak{a})$ est une fonction classe on a alors $r(\mathfrak{b}) \leq r(\mu\mathfrak{c})$. Cela montre que $r(\mathfrak{b})$ est borné pour tout diviseur $\mathfrak{b}$. Ceci montre aussi que $l(\mathfrak{b})$ et $\deg(\mathfrak{b})$ ont le même ordre de grandeur. De plus, remarquons que si $\mathfrak{b}$ est fixé et que $\mathfrak{a}$ varie dans (31) alors $\Lambda(\mathfrak{a})$ peut être agrandi de manière à inclure tout élément de $A$.

D'un autre côté, l'indice dans cette formule est bornée car on a juste à voir que $r(\mathfrak{a})$ est bornée. Donc pour un diviseur $\mathfrak{a}$ ayant atteint son maximum et pour ce diviseur on doit avoir $A = \Lambda(\mathfrak{a}) + K$. On a donc obtenu :

**Théorème 12.15.** *Il existe un diviseur $\mathfrak{a}$ tel que $A = \Lambda(\mathfrak{a}) + K$ i.e Les éléments de $K$ peuvent être vu comme des réseaux de $A$. De ce fait, un voisinage $\Lambda(\mathfrak{a})$ peut se traduire comme tous les points du réseau recouvrant $A$.*

Ce résultat permet de séparer l'indice dans (29). Notons par $\delta(\mathfrak{a})$ la dimension de $(A : \Lambda(\mathfrak{a}) + K)$. Du fait que l'on a établit que la dimension était finie, l'égalité (29) devient :

$$\deg(\mathfrak{a}) - \deg(\mathfrak{b}) = \delta(\mathfrak{b}) - \delta(\mathfrak{a}) + l(\mathfrak{a}) - l(\mathfrak{b}). \tag{32}$$

Ce qui équivaut à :

$$l(\mathfrak{a}) - \deg(\mathfrak{a}) - \delta(\mathfrak{a}) = l(\mathfrak{b}) - \deg(\mathfrak{b}) - \delta(\mathfrak{b}).$$

Et cela se vérifie pour $\mathfrak{a} \geq \mathfrak{b}$.

**Définition 12.16.** *Le genre de $K$ est définie pour être l'entier $g$ tel que $l(\mathfrak{a}) - \deg(\mathfrak{a}) - \delta(\mathfrak{a}) = 1 - g$.*

**Remarque 12.17.** *C'est un invariant de $K$.*

Posons $\mathfrak{a} = 0$ dans cette définition, on voit que $\delta(0) = g$ donc $g \in \mathbb{N}$ donc $g = (A : \Gamma(0) : K)$. En résumant, on a :

**Théorème 12.18.** *Il existe un entier $g \in \mathbb{N}$ dépendant seulement de $K$ tel que pour tout diviseur $\mathfrak{a}$, on a $\delta(\mathfrak{a}) \geq 0$ et $l(\mathfrak{a}) = \deg(\mathfrak{a}) + 1 - g + \delta(\mathfrak{a})$.*

**Définition 12.19.** *Une fonctionnelle $\lambda$ qui est $k$-linéaire de $A$ et s'annule sur un certain $\Lambda(\mathfrak{a})$ et sur $K$ est appelé différentielle de $K$.*

**Remarque 12.20.** *La première condition impose la continuité de $\lambda$ quand on prend la topologie discrète sur $k$.*
*Pour la deuxième condition, comme $(A : \Lambda(\mathfrak{a}) + K)$ est fini, en prenant $\lambda$ une différentielle s'annulant sur $\Lambda(\mathfrak{a})$, on peut peut considérer $\lambda$ comme une fonctionnelle s'annulant sur l'espace quotient $A \mod \Lambda(\mathfrak{a}) + K$*

On peut donc énoncer le théorème :

**Théorème 12.21.** *Si $\lambda$ est différentiable alors il existe un parallélotope $\Lambda(\mathfrak{a})$ sur lequel $\lambda$ s'annule.*

*Démonstration.* Si une différentielle $\lambda$ s'annule sur $\Lambda(\mathfrak{a}_1)$ et $\Lambda(\mathfrak{a}_2)$ et que l'on pose $\mathfrak{a} = \sup(\mathfrak{a}_1, \mathfrak{a}_2)$ alors $\lambda$ s'annule sur $\Lambda(\mathfrak{a})$. Alors, pour prouver le théorème, il suffit de prouver que le degré de $\mathfrak{a}$ est borné.

Si $y \in L(\mathfrak{a})$ alors $(y) \geq -\mathfrak{a}$ alors $y\lambda$ s'annule sur $\Lambda(\mathfrak{a} + (y))$ et comme $\mathfrak{a} + (y) \geq 0$, on a $\Lambda(0) \in \Lambda(\mathfrak{a} + (y))$.
Si $(y_1, \ldots, y_n)$ sont linéairements indépendants sur $k$, alors $(\lambda y_1, \ldots, \lambda y_n)$ le sont aussi donc $\delta(0) \geq l(a) = \deg(\mathfrak{a}) + 1 - g - \delta(\mathfrak{a})$ mais $\delta(\mathfrak{a}) \geq 0$ donc on a $\deg(\mathfrak{a} \leq \delta(0) + g - 1$ montrant la borne désirée. □

**Théorème 12.22.** *Les formes différentiables muni de l'addition forment un $K$-espace vectoriel de dimension 1.*

*Démonstration.* Soient $\lambda$ est une forme différentielle s'annulant sur $\Lambda(\mathfrak{a})$, $\xi \in A$ et $y \in K$, on peut définir $y\lambda$ par $(y\lambda)(\xi) = \lambda(y\xi)$.
Cette fonctionnelle est encore différentiable car elle s'annule sur $K$ et par addition elle s'annule sur $\Lambda(\mathfrak{a} + (y))$.
Maintenant, prenons deux formes différentielles $\lambda$ et $\mu$ linéairement indépendantes sur $K$. Supposons $(x_i)_{1 \leq i \leq n}$ et $(y_i)_{1 \leq i \leq n}$ deux ensembles d'éléments de $K$ linéairement indépendants sur $k$. Alors $(x_i\lambda)_{1 \leq i \leq n}$ et $(y_i\mu)_{1 \leq i \leq n}$ sont linéairement indépendant sur $k$ donc on a une relation :

$$\sum a_i x_i \lambda + \sum b_i y_i \mu = 0.$$

Posons $x = \sum a_i x_i$ et $y = \sum b_i y_i$, on a donc $\sum x\lambda + \sum y\mu = 0$. On a une contradiction de l'indépendance linéaire de $\lambda, \mu$ sur $K$.

Ainsi, $\lambda, \mu$ s'annule sur un parallélotope $\Lambda(\mathfrak{a})$. En effet, si $\lambda$ s'annule sur $\Lambda(\mathfrak{a}_1)$ et sur $\Lambda(\mathfrak{a}_2)$ alors en posant $\mathfrak{a} = \inf(\mathfrak{a}_1, \mathfrak{a}_2)$ on a $\Lambda(\mathfrak{a}) = \Lambda(\mathfrak{a}_1) \bigcup \Lambda(\mathfrak{a}_2)$.

Maintenant, soit $\mathfrak{b}$ un diviseur arbitraire. Si $y \in L(\mathfrak{b})$ alors $(y) \geq -b$ alors $y\lambda$ s'annule sur $\Lambda(\mathfrak{a} + (y))$ qui contient $\Lambda(\mathfrak{a} - \mathfrak{b})$ car $\mathfrak{a} + (y) \geq \mathfrak{a} - \mathfrak{b}$.
De même, $y\mu$ s'annule sur $\Lambda(\mathfrak{a} - \mathfrak{b})$ et par définition de $\Lambda(.)$ et la remarque au début de la preuve, on peut conclure $\delta(\mathfrak{a} - \mathfrak{b}) \geq 2l(\mathfrak{b})$.
Grâce au théorème 12.18, on a :

$$\begin{aligned} l(\mathfrak{a} - \mathfrak{b}) - \deg(\mathfrak{a}) + \deg(\mathfrak{b}) - 1 + g &\geq 2l(\mathfrak{b}) \\ &\geq 2(\deg(\mathfrak{b}) + 1 - g - \delta(b) \\ &\geq 2\deg(\mathfrak{b}) + 2 - 2g. \end{aligned}$$

Si $b \geq 0$ est assez grand, alors $L(\mathfrak{a} - \mathfrak{b}) = \{0\}$ car une fonction ne peut avoir plus de zéros que de pôles. Or $\deg(\mathfrak{a})$ est constante dans l'inégalité dessus aboutissant sur une contradiction qui permet de conclure. □

Si $\lambda$ est une forme différentielle non nulle alors toutes les différentielles sont de la forme $y\lambda$. Si $\Lambda(\mathfrak{a})$ est le parallélotope maximal sur lequel $\lambda$ s'annule alors $\Lambda(\mathfrak{a} + (y))$ est le le parallélotope maximal sur lequel $y\lambda$. On a donc obtenu une équivalence de diviseur :
Si on définit le diviseur $(\lambda)$ associé à $\lambda$ comme étant $\mathfrak{a}$ alors le diviseur associé à $y\lambda$ est $\mathfrak{a} + (y)$.

**Définition 12.23.** *Cette classe est la classe canonique de $K$ et le diviseur associé est le diviseur canonique.*

Nous avons tous les outils pour établir notre résultat final :

**Théorème 12.24** (Théorème de Riemann-Roch)**.** *Soit $\mathfrak{a}$ un diviseur arbitraire de $K$. Si $\mathfrak{c}$ est un diviseur canonique alors $l(\mathfrak{a}) = \deg(\mathfrak{a}) + 1 - g + l(\mathfrak{c} - \mathfrak{a})$. En d'autre termes, $\delta(\mathfrak{a}) = l(\mathfrak{c} - \mathfrak{a})$.*

*Démonstration.* Soit $\mathfrak{c}$ un diviseur tel que $\Lambda(\mathfrak{c})$ soit le parallélotope maximal sur lequel une forme différentielle $\lambda$ non nulle s'annule. Si $\mathfrak{b}$ est un diviseur arbitraire et $y \in L(\mathfrak{b})$ alors on sait que $y\lambda$ s'annule sur $\Lambda(\mathfrak{c} - \mathfrak{b})$.

Réciproquement, grâce au théorème 12.22, toute forme différentielle s'annule sur $\Lambda(\mathfrak{c} - \mathfrak{b})$ est de la forme $z\lambda$ pour $z \in K$. De plus, le parallélotope sur lequel $z\lambda$ est défini est $(z) + \mathfrak{c}$ qui doit contenir $\Lambda(\mathfrak{c} - \mathfrak{b})$. Donc $(z) \geq -\mathfrak{b}$ i.e $z \in L(\mathfrak{b})$. Ainsi, on a montré que $\delta(\mathfrak{c} - \mathfrak{b}) = l(\mathfrak{b})$. Comme $\mathfrak{b}$ est arbitraire, on peut le remplacer par $\mathfrak{c} - \mathfrak{a}$ prouvant le théorème. □

On a aussi quelques corollaires directs :

**Corollaire 12.25.** *Si $\mathfrak{c}$ est un diviseur canonique alors $l(\mathfrak{c}) = g$.*

*Démonstration.* Pour $\mathfrak{a} = 0$, en appliquant le théorème 12.24 alors $L(\mathfrak{a})$ est constitué seulement des constantes donc $l(\mathfrak{a}) = 1$ or $\deg(0) = 0$. CQFD. □

**Corollaire 12.26.** *Le degré de la classe canonique est le $2g - 2$.*

*Démonstration.* Pour $\mathfrak{a} = \mathfrak{c}$, en appliquant le théorème 12.24 puis le corollaire précédent, on a le résultat voulu. □

**Corollaire 12.27.** *Si $\deg(\mathfrak{a}) > 2g - 2$ alors $\delta(\mathfrak{a}) = 0$.*

*Démonstration.* On a $\delta(\mathfrak{a})$ qui est égal à $l(\mathfrak{c} - \mathfrak{a})$ mais une fonction ne peut avoir plus de zéros que de pôle et $L(\mathfrak{c} - \mathfrak{a}) = 0$ si $\deg(\mathfrak{a}) > 2g - 2$. □

# Table des matières

## Sixième partie

# Bibliographie

## Références


[1] Algèbre Corporelle, Antoine Chambert-Loir, Editions Polytechniques, 2005

[2] Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication, Wiley, 1989

[3] Class Field Theory, J. Neukirch, Springer, 1986

[4] Algebraic Number Theory, J. Neukirch Springer, Springer, 1994

[5] Elliptic Curves, Diophantine Analysis, Serge Lang, Springer, 1978

[6] Elliptic Fonction, Graduate Texts in Mathematics, Serge Lang, Springer, 1987

[7] Introduction to Algebraic and Abelian Functions, Serge Lang, Springer, 1982

[8] Théorie Algébrique des nombres, P.Samuel, Hermann, 1997

[9] On the History of Hilbert's Twelfth Problem, N.Schappacher, SMF, 1999

[10] Cohomologie Galoisienne, J.P Serre, Springer, 1994

[11] The Arithmetic of Elliptic Curves, Joseph H.Silvermann, Springer, 2009

[12] Fourier Analysis on Number Fields, D.Ramakrishnan, R.Valenza, Springer, 1999

[13] Introduction to Cyclotomic Fields, Part of the Graduate Texts in Mathematics book series (GTM, volume 83), Lawrence C. Washington, Springer, 1950-2021

[14] Profinite groups are galois groups, W.C Waterhouse, AMS, 1974