Multiplication Complexe

C. Berenfeld, L. Lerer, M. Tamiozzo

16 juin 2015

Sous la direction de Jan Nekovář

Table des matières

Introduction

"The theory of complex multiplication is not only the most beautiful part of mathematics but also of all science."

David Hilbert (1862-1943)

Étant donné un corps de nombres K (c'est à dire, une extension finie de $\mathbb{Q}$), l'un des problèmes fondamentaux en théorie algébrique des nombres consiste à étudier ses extensions galoisiennes finies. La théorie des corps de classe, développée entre la fin du 19ème et le début du 20ème siècle, donne une classification *abstraite* des extensions galoisiennes L/K lorsque $Gal(L/K)$ est *abélien* : le groupe de Galois d'une telle extension est décrit à l'aide de certains "groupes des classes d'idéaux généralisés" associés au corps de base K.

Si $K = \mathbb{Q}$, on montre aisément que les corps $\mathbb{Q}(\zeta_n)$, où $\zeta_n = e^{2i\pi/n}$, sont des extensions abéliennes de $\mathbb{Q}$, appelées *corps cyclotomiques*. Le célèbre théorème de Kronecker-Weber stipule qu'en fait toute extension abélienne de $\mathbb{Q}$ est contenue dans un tel corps. Cela donne une description *concrète* des extensions abéliennes de $\mathbb{Q}$, obtenues en y ajoutant les valeurs de la fonction exponentielle évaluée en les points de torsion du groupe $\mathbb{R}/2i\pi\mathbb{Z}$.

Plus généralment, le problème se pose de décrire explicitement les extensions abéliennes d'un corps de nombres K quelconque. A l'aide des fonctions elliptiques et des fonctions modulaires, Kronecker réussit à construire certaines extensions abéliennes des corps quadratiques imaginaires, c'est à dire, les corps de la forme $K = \mathbb{Q}(\sqrt{-n})$. Son rêve de jeunesse (*Kronecker Jugendtraum*) était de montrer que toute extension abélienne d'un corps quadratique imaginaire s'obtient en ajoutant les valeurs de certaines fonctions elliptiques et modulaires. L'un des objectifs de cet exposé sera de réaliser ce rêve de jeunesse.

Nous traiterons tout d'abord le cas classique des extensions abéliennes de $\mathbb{Q}$, et nous montrerons comment déduire des énoncés de la théorie des corps de classe le théorème de Kronecker-Weber.

Nous étudierons ensuite les fonctions elliptiques et modulaires, ainsi que les objets arithmético-géométriques naturellement liés à ces fonctions : les courbes elliptiques, définies sur $\mathbb{C}$, obtenues comme quotient de $\mathbb{C}$ par un réseau, et munies d'une structure de groupe compatible avec leur structure naturelle de variété analytique. Nous verrons que l'ensemble des classes d'isomorphisme des courbes elliptiques sur $\mathbb{C}$ a lui-même une structure de variété analytique, et que les fonctions modulaires les plus simples s'interprètent naturellement comme des fonctions méromorphes sur cette variété. On peut ainsi obtenir énormément d'informations sur les fonctions modulaires grâce à l'étude géométrique et arithmétique des courbes elliptiques.

Grâce à ce principe, nous démontrerons enfin que le $j-$invariant d'une courbe elliptique *à multiplication complexe* par l'anneau des entiers $\mathcal{O}_K$ d'un corps quadratique imaginaire K engendre le corps de classe de Hilbert $\mathcal{H}_K$ de K. Une étude plus détaillée des propriétés des courbes elliptiques à multiplication complexe nous permettra d'aboutir à un résultat analogue au théorème de Kronecker-Weber. Nous montrerons en effet que toute extension abélienne d'un corps quadratique imaginaire K est contenue dans un corps obtenu en ajoutant à $\mathcal{H}_K$ les abscisses des points de torsion d'une courbe elliptique à multiplication complexe par $\mathcal{O}_K$, ce qui réalisera le *Jugendtraum* de Kronecker.

1 Quelques préliminaires de théorie algébrique des nombres

1.1 Anneaux des entiers algébriques

Les résultats de cette sous-section ne seront pas démontrés. Le lecteur intéressé par les preuves manquantes pourra se référer à tout bon cours d'algèbre commutative (par exemple [8]).

Définition 1.1.1. *Soit $A \subset B$ une extension d'anneaux. On dit qu'un élément $x \in B$ est* entier sur A *s'il est racine d'un polynôme unitaire à coefficients dans A.*
On appelle normalisation de A dans B *l'ensemble des éléments de B entiers sur A. C'est un sous-anneau de B.*

Si $L/\mathbb{Q}$ est une extension de corps, on définit l'anneau des entiers algébriques $\mathcal{O}_L$ comme la normalisation de $\mathbb{Z}$ dans L.

Proposition 1.1.2. *Soit A un anneau intègre, K son corps des fractions, L une extension algébrique de K et B la normalisation de A dans L. Alors L est le corps des fractions de B.*

Définition 1.1.3. *Un anneau intègre A est* intégralement clos *s'il coïncide avec sa normalisation dans $Frac(A)$.*

Remarque 1.1.4. L'anneau des entiers d'un corps de nombres K est intégralement clos.

Soit A un anneau intègre, K son corps des fractions, L une extension finie de K. Si le polynôme caractéristique (où minimal) d'un élément $x \in L$ sur K à ses coefficients dans A, alors x est clairement entier sur A. La réciproque est également vraie si A est intégralement clos, et fournit un critère pratique pour déterminer l'anneau des entiers de certains corps :

Proposition 1.1.5. *Soit A un anneau intégralement clos et L une extension finie de $Frac(A)$. Alors un élément $x \in L$ est entier sur A si et seulement si son polynôme caractéristique sur K est dans $A[X]$, si et seulement si son polynôme minimal sur K est dans $A[X]$.*

Exemple 1.1.6. Donnons nous un entier relatif n non nul, sans facteurs carrés. Posons $K = \mathbb{Q}(\sqrt{n})$, et essayons de determiner $\mathcal{O}_K$. Un élément $x = a + \sqrt{n}b \in K$ est dans $\mathcal{O}_K$ si et seulement si son polynôme caractéristique sur $\mathbb{Q}$ est à coefficients entiers, c'est à dire si et seulement si $Tr_{K/\mathbb{Q}}(x) = 2a \in \mathbb{Z}$ et $N_{K/\mathbb{Q}}(x) = a^2 - nb^2 \in \mathbb{Z}$ (voir la section (1.2)). Après quelques considérations arithmétiques élémentaires, on aboutit à :

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

C'est un résultat qu'il sera bon de retenir.

La normalisation d'un anneau A dans un anneau B est munie d'une structure naturelle de A-module. En restreignant un peu les hypothèses faîtes sur A et B, on peut décrire cette structure de manière précise :

Proposition 1.1.7. *Soit A un anneau intégralement clos et principal, K son corps des fractions, L une extension séparable de K de degré fini n. Soit B la normalisation de A dans L. Alors B est un A-module libre de rang n.*

Ainsi, si K est un corps de nombres, $\mathcal{O}_K$ est un $\mathbb{Z}$-module libre de rang $[K : \mathbb{Q}]$.

1.2 Trace, norme et discriminant

On définit dans ce paragraphe quelques notions incontournables pour l'étude des entiers algébriques. On se donne pour cela une extension d'anneaux $A \subset B$ et on suppose que B est un A-module libre de rang $n \in \mathbb{N}$.

Soit $x \in B$. L'application $m_x : y \in B \mapsto xy \in B$ définit un endomorphisme de A-modules. On appelle alors *trace de* x, et on la note $Tr_{B/A}(x)$, la trace de la matrice de l'application m_x dans n'importe quelle base de B. Cette quantité ne dépend bien sur pas du choix de la base. De même, on définit la norme de x par $N_{B/A}(x) = det(m_x)$ où le déterminant est encore une fois calculé dans n'importe quelle base de B.

Définissons maintenant le discriminant de l'extension B/A. La trace telle que définie ci dessus définit une forme bilinéaire sur B via $(x, y) \mapsto Tr(xy)$. Si $(e_1, \dots, e_n) \in B^n$ est une base de B, on définit $D(e_1, \dots, e_n) = det\{Tr(e_i e_j)\}_{i,j}$. En choisissant maintenant une autre base $(f_1, \dots, f_n)$ de B et en notant P la matrice de passage entre ces deux bases, on aboutit à la formule :

$$D(e_1, \dots e_n) = (det\, P)^2 D(f_1, \dots, f_n)$$

Or il est bien connu que $\mathbb{GL}_n(A) = \{M \in \mathcal{M}_n(A) : \ det(M) \in A^\times\}$. On peut donc définir le discriminant de B/A, unique à un facteur de $A^{\times 2}$ près, par

$$disc(B/A) = D(e_1, \dots, e_n) \in A/A^{\times 2}$$

Exemple 1.2.1.

1. Si $K = \mathbb{Q}(\sqrt{n})$, où n est un entier relatif sans facteurs carrés, la matrice de la forme trace dans la base entière $(1, \sqrt{n})$ s'écrit $\begin{pmatrix} 2 & 0 \\ 0 & 2n \end{pmatrix}$, et ainsi $D(1, \sqrt{n}) = 4n$.
2. On regarde maintenant l'anneau des entiers $\mathcal{O}_K$ d'un corps de nombres K. Comme $\mathbb{Z}^{\times 2} = \{1\}$, le discriminant de l'extension $\mathcal{O}_K/\mathbb{Z}$ est un unique entier relatif. D'après l'exemple 1.1.6, si $n \equiv 2, 3 \pmod 4$, on a $\mathcal{O}_K = \mathbb{Z}[\sqrt{n}]$, et on a donc $disc(\mathcal{O}_K/\mathbb{Z}) = 4n$. Mais, si $n \equiv 1 \pmod 4$, la matrice de multiplication par un entier $a + b\frac{1+\sqrt{n}}{2} \in \mathcal{O}_K$ dans la base $(1, \frac{1+\sqrt{n}}{2})$ s'écrit $\begin{pmatrix} a & b + (n-1)/4 \\ b & a + b \end{pmatrix}$, de sorte que la matrice de la forme trace dans cette même base devient $\begin{pmatrix} 2 & 1 \\ 1 & (n-1)/2 + 1 \end{pmatrix}$. On trouve ainsi $disc(\mathcal{O}_K/\mathbb{Z}) = n$.

Définition 1.2.2. *Soit L/K une extension de corps de nombres. On définit $\Delta_{L/K}$ comme étant l'idéal de $\mathcal{O}_K$ engendré par tous les $D(a_1, \cdots, a_n)$ où les $a_1, \cdots, a_n$ forment une base entière de L/K.*

Remarque 1.2.3. Lorsque L/K est une extension de corps de nombres on appelle $\Delta_{L/K}$ le *discriminant* de L sur K. Mais attention : $disc(L/K)$ et $\Delta_{L/K}$ ont le même nom mais sont des objets tout à fait différents.

1.3 Anneaux de Dedekind

Nous aurons tout d'abord besoin de quelques propriétés des anneaux locaux. Un anneau A non nul est dit *local* s'il possède un unique idéal maximal. Si tel est le cas, et si $\mathfrak{m}$ est l'unique idéal maximal de A, alors $A^\times = A \setminus \mathfrak{m}$. En effet, $\mathfrak{m}$ est un idéal propre de A donc $\mathfrak{m} \subset A \setminus A^\times$. Réciproquement, si $x \in A \setminus A^\times$ alors (x) est un idéal propre de A, contenu dans un idéal maximal de A, donc dans $\mathfrak{m}$.

Définition 1.3.1. *Soit A un anneau intègre et S une partie multiplicative de A (i.e contenant 1 et stable par multiplication). On appelle* localisation de l'anneau A selon S *l'anneau*

$$S^{-1}A = \left\{ \frac{a}{s} : a \in A, s \in S \right\} \subset Frac(A)$$

C'est un sous-anneau de $Frac(A)$.

Soit A un anneau intègre, $\mathfrak{p} \subset A$ un idéal premier. On définit

$$A_{\mathfrak{p}} = S_{\mathfrak{p}}^{-1}A \quad \text{où} \quad S_{\mathfrak{p}} = A \setminus \mathfrak{p}$$

C'est un anneau local, d'idéal maximal $\mathfrak{p}A_{\mathfrak{p}}$. Pour montrer ce résultat, choisissons $\mathfrak{B}$ un idéal propre de $A_{\mathfrak{p}}$. Alors $\mathfrak{B} \cap A$ est un idéal de A disjoint de S (en effet, sinon $\mathfrak{B}$ contiendrait 1), c'est-à-dire inclus dans $\mathfrak{p}$. Si donc $b = a/s$ est un élément de $\mathfrak{B}$, on a $sb \in \mathfrak{B} \cap A \subset \mathfrak{p}$ et ainsi $b = (bs)/s \in \mathfrak{p}A_{\mathfrak{p}}$. On en déduit que $\mathfrak{B} \subset \mathfrak{p}A_{\mathfrak{p}}$, et qu'ainsi $\mathfrak{p}A_{\mathfrak{p}}$ est l'unique idéal maximal de $A_{\mathfrak{p}}$.

Lorsqu'un anneau A est local et principal, et que son unique idéal maximal $\mathfrak{m}$ est non nul, on dit que A est un *anneau de valuation discrète*. Si A est un tel anneau, tout idéal de A est de la forme $\mathfrak{m}^n = (x^n)$ avec n un entier naturel et x un générateur de $\mathfrak{m}$.
On peut montrer qu'un anneau intègre est de valuation discrète si et seulement si il est intégralement clos, noethérien et possède un unique idéal premier non nul. Cette caractérisation nous sera utile par la suite.

On introduit enfin la notion phare de cette section :

Définition 1.3.2. *Un anneau intègre A est un* anneau de Dedekind *s'il est intégralement clos, noethérien, et si tout idéal premier non nul de A est maximal.*

On montre facilement que les propriétés d'être intégralement clos et noethérien passent à la localisation. On en déduit alors que, si $\mathfrak{p}$ est un idéal premier non nul d'un anneau de Dedekind A, le localisé $A_{\mathfrak{p}}$ est un anneau de valuation discrète. La réciproque est également vraie :

Proposition 1.3.3. *Soit A un anneau intègre noethérien. Alors A est un anneau de Dedekind si et seulement si, pour tout idéal premier non nul $\mathfrak{p} \subset A$, le localisé $A_{\mathfrak{p}}$ est un anneau de valuation discrète.*

L'une des propriétés les plus fondamentales des anneaux de Dedekind est la suivante :

Théorème 1.3.4. *Soit A un anneau de Dedekind et $\mathfrak{a}$ un idéal non nul de A. Alors $\mathfrak{a}$ se factorise de la manière suivante :*

$$\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_n^{r_n}$$

où les $\mathfrak{p}_i$ sont des idéaux premiers de A distincts et chaque r_i est un entier > 0. De plus, cette factorisation est unique à l'ordre des termes près.

Démonstration. Soit $\mathfrak{a}$ un idéal non nul de A. Si $\mathfrak{a}$ est premier, c'est terminé. Sinon montrons que $\mathfrak{a}$ contient un produit d'idéaux premiers. Supposons en effet que $\mathfrak{a}$ n'en contienne pas et fixons $\mathfrak{B}$ un idéal maximal parmi les idéaux ne contenant pas de produit d'idéaux premiers. Comme $\mathfrak{B}$ n'est pas premier, il existent x et y dans $A \setminus \mathfrak{B}$ tels que $xy \in \mathfrak{B}$. Alors $\mathfrak{B} + (x)$ et $\mathfrak{B} + (y)$ contiennent un produit d'idéaux premiers (par maximalité de

$\mathfrak{B}$), et il en est donc de même pour $(\mathfrak{B}+(x))(\mathfrak{B}+(y))=\mathfrak{B}$, ce qui est une contradiction. Il existent donc des idéaux premiers distincts $\mathfrak{p}_1,\dots,\mathfrak{p}_n$ et des entiers $r_1,\dots,r_n$ tels que

$$\mathfrak{q}=\mathfrak{p}_1^{r_1}\cdots\mathfrak{p}_n^{r_n}\subset\mathfrak{a}$$

Comme les $\mathfrak{p}_i^{r_i}$ sont premiers entre eux on a, d'après le théorème chinois :

$$A/\mathfrak{q}\cong A/\mathfrak{p}_1^{r_1}\oplus\cdots\oplus A/\mathfrak{p}_n^{r_n} \tag{1.3.1}$$

Montrons maintenant le résultat suivant : si $\mathfrak{p}$ est un idéal maximal de A et r un entier, alors $A/\mathfrak{p}^r\cong A_\mathfrak{p}/(\mathfrak{p}A_\mathfrak{p})^r$. Pour cela, établissons l'égalité suivante :

$$(\mathfrak{p}A_\mathfrak{p})^r\cap A=\mathfrak{p}^r \tag{1.3.2}$$

On a $(\mathfrak{p}A_\mathfrak{p})^r=(A\smallsetminus\mathfrak{p})^{-1}\mathfrak{p}^r$ donc si $a\in(\mathfrak{p}A_\mathfrak{p})^r\cap A$, on peu écrire a sous la forme p/s où $p\in\mathfrak{p}^r$ et $s\in A\smallsetminus\mathfrak{p}$. Donc la projection $\overline{sa}$ de sa dans $A/\mathfrak{p}^r$ est nulle. Or $A/\mathfrak{p}^r$ est un anneau local d'unique idéal maximal $\mathfrak{p}/\mathfrak{p}^r$, et comme $\bar{s}\notin\mathfrak{p}/\mathfrak{p}^r$, on en déduit que $\bar{s}$ est inversible, est qu'ainsi $a\in\mathfrak{p}^r$, ce qui achève la preuve de l'égalité (1.3.2). On en déduit que le morphisme suivant

$$\phi:\bar{x}\in A/\mathfrak{p}^r\mapsto\widetilde{x}\in A_\mathfrak{p}/(\mathfrak{p}A_\mathfrak{p})^r$$

est bien défini, et est injectif ! Montrons enfin la surjectivité de ϕ : soit $a/s\in A_\mathfrak{p}$. On a, par maximalité de $\mathfrak{p}$, $(s)+\mathfrak{p}=A$: ainsi (s) et $\mathfrak{p}$ sont premiers entre eux, et donc $\mathfrak{p}^r$ et (s) également et il existe donc $b\in A$ tel que $\bar{b}=\bar{s}^{-1}$. On a donc $\phi(\overline{ab})=\widetilde{(a/s)}$ et ϕ et bien surjective.
Revenons maintenant à l'égalité (1.3.1). Elle se réécrit :

$$A/\mathfrak{q}\cong A_{\mathfrak{p}_1}/\mathfrak{B}_1^{r_1}\oplus\cdots\oplus A_{\mathfrak{p}_n}/\mathfrak{B}_n^{r_n}$$

où $\mathfrak{B}_i=p_iA_{\mathfrak{p}_i}$. Comme les anneaux $A_{\mathfrak{p}_i}$ sont de valuation discrète, on en déduit que l'idéal $\mathfrak{a}/\mathfrak{q}$ correspond via l'isomorphisme à un idéal de la forme

$$\mathfrak{a}/\mathfrak{q}\cong\mathfrak{B}_1^{s_1}/\mathfrak{B}_1^{r_1}\oplus\cdots\oplus\mathfrak{B}_n^{s_n}/\mathfrak{B}_n^{r_n}$$

pour certains entiers $s_i\leq r_i$. Comme cet idéal correspond à l'idéal $\mathfrak{p}_1^{s_1}\cdots\mathfrak{p}_n^{s_n}$ via les isomorphismes ϕ, on en déduit que $\mathfrak{a}/\mathfrak{q}=\mathfrak{p}_1^{s_1}\cdots\mathfrak{p}_n^{s_n}/\mathfrak{q}$. Puis, comme $\mathfrak{q}$ est inclus dans chacun de ces idéaux, on a enfin

$$\mathfrak{a}=\mathfrak{p}_1^{s_1}\cdots\mathfrak{p}_n^{s_n}$$

Il reste enfin à montrer l'unicité : supposons que l'on ait

$$\mathfrak{a}=\mathfrak{p}_1^{s_1}\cdots\mathfrak{p}_n^{s_n}=\mathfrak{p}_1^{t_1}\cdots\mathfrak{p}_n^{t_n}$$

avec $t_i,s_i\geq 0$. On vu qu'alors $\mathfrak{a}A_{\mathfrak{p}_i}=\mathfrak{B}_i^{s_i}=\mathfrak{B}_i^{t_i}$ où $\mathfrak{B}_i=\mathfrak{p}_iA_{\mathfrak{p}_i}$. D'où $s_i=t_i$. □

Notons alors un corollaire immédiat de la démonstration de l'unicité :

Corollaire 1.3.5. *Un idéal premier non nul $\mathfrak{p}$ divise $\mathfrak{a}$ (c'est-à-dire qu'il existe un idéal $\mathfrak{b}$ tel que $\mathfrak{a}=\mathfrak{b}\mathfrak{p}$) si, et seulement si $\mathfrak{a}\subset\mathfrak{p}$.*

Démonstration. On écrit $\mathfrak{a}=\mathfrak{p}_1^{r_1}\cdots\mathfrak{p}_n^{r_n}$ avec $r_i\geq 0$. On a alors $r_i>0$ si, et seulement si $(\mathfrak{p}_iA_{\mathfrak{p}_i})^{r_i}\neq A_{\mathfrak{p}_i}$. Or $(\mathfrak{p}_iA_{\mathfrak{p}_i})^{r_i}=\mathfrak{a}A_{\mathfrak{p}_i}$, donc $r_i>0$ si et seulement si $\mathfrak{a}A_{\mathfrak{p}_i}\neq A_{\mathfrak{p}_i}$, c'est-à-dire si et seulement si $\mathfrak{a}\subset\mathfrak{p}_i$. □

Comme nous aurions envie que l'anneau des entiers d'un corps de nombres soit un anneau de Dedekind, regardons si cette propriété passe à la normalisation.

Soit donc A un anneau de Dedekind, K son corps des fractions, L une extension finie et séparable de K et B la normalisation de A dans L. On sait que l'anneau B est intégralement clos, et qu'il est noethérien : en effet, c'est un A module de type fini et A est noethérien.

Montrons enfin que tout idéal premier non nul de B est maximal. Soit $\mathfrak{q}$ un tel idéal, et soit $b \in \mathfrak{q}$ non nul. Soit $P \in A[X]$ le polynôme minimal de b. On a alors $0 \neq P(0) \in bB \cap A \subset \mathfrak{q} \cap A$. Ainsi, $\mathfrak{p} := \mathfrak{q} \cap A$ est un idéal non nul de A. Comme il est premier, il est maximal ! Ainsi l'anneau $B/\mathfrak{q}$ contient le corps $A/\mathfrak{p}$.

Soit donc $c \in B$ tel que sa projection $\bar{c}$ dans $B/\mathfrak{q}$ soit non nulle. Soit $Q \in A[X]$ son polynôme minimal. Alors $\bar{Q}$ est un polynôme non nul (car unitaire) de $A/\mathfrak{p}[X]$ qui annule $\bar{c}$; $\bar{c}$ est donc algébrique sur $A/\mathfrak{p}$. Ainsi le morphisme d'espaces vectoriels de dimension finie

$$x \in A/\mathfrak{p}[\bar{c}] \mapsto \bar{c}x \in A/\mathfrak{p}[\bar{c}]$$

qui est injectif (par le fait que $B/\mathfrak{q}$ soit intègre) est finalement bijectif. On peut donc conclure que $\bar{c}$ est inversible dans $B/\mathfrak{q}$. Ainsi, $\mathfrak{q}$ est maximal. Donc B est un anneau de Dedekind.

Remarque 1.3.6. En particulier, si K est un corps de nombres, alors $\mathcal{O}_K$ est un anneau de Dedekind.

1.4 Groupe des classes d'idéaux

On fixe dans cette section un anneau de Dedekind A, et on note K son corps des fractions.

Définition 1.4.1. *Un* idéal fractionnaire $\mathfrak{a}$ *de A est un sous-A-module non nul de K tel qu'il existe $q \in A$ tel que $q\mathfrak{a} \subset A$. On note $I(A)$ l'ensemble des idéaux fractionnaires de A. Un idéal fractionnaire est dit* principal *s'il est de la forme $(r) = rA$ pour un certain $r \in K^*$. On note $P(A)$ l'ensemble des idéaux fractionnaires principaux de A.*

On montre aisément que $I(A)$ est stable par multiplication. De plus si $\mathfrak{a} \in I(A)$, et $q \in A$ est tel que $q\mathfrak{a} \subset A$, on peut écrire

$$q\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_n^{r_n} \quad \text{et} \quad (q) = \mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_n^{s_n}$$

où les r_i, s_i sont des entiers (éventuellement nuls) et les $\mathfrak{p}_i$ sont des idéaux premiers de A. En notant $t_i = r_i - s_i \in \mathbb{Z}$, on a finalement

$$\mathfrak{a} = \mathfrak{p}_1^{t_1} \cdots \mathfrak{p}_n^{t_n}$$

De plus, si $a \in q\mathfrak{a}$ est non nul, on peut de même écrire

$$(a) = \mathfrak{p}_1^{u_1} \cdots \mathfrak{p}_n^{u_n}$$

avec $r_i \leq u_i$ pour tout i. En posant donc

$$\mathfrak{B} = \mathfrak{p}_1^{u_1 - r_1} \cdots \mathfrak{p}_n^{u_n - r_n}$$

on obtient l'égalité $\mathfrak{a}((aq)^{-1}\mathfrak{B}) = A$, avec $(aq)^{-1}\mathfrak{B} \in I(A)$. Ces remarques nous permettent d'aboutir au théorème suivant :

Théorème 1.4.2. *L'ensemble $I(A)$ muni de la multiplication d'idéaux fractionnaires forme un groupe abélien libre, d'élément neutre A, engendré par les idéaux premiers de A. De plus, $P(A)$ est un sous-groupe de $I(A)$.*

On peut donc définir le quotient de $I(A)$ par $P(A)$:

Définition 1.4.3. *On appelle* groupe des classes d'idéaux *de A le quotient $Cl(A) := I(A)/P(A)$. Lorsque celui-ci est fini, on note $h(A)$ son ordre et on l'appelle* nombre des classes *de A.*

Remarque 1.4.4. On montre que si K est un corps des nombres alors $Cl(\mathcal{O}_K)$ est fini. Voir [9].

1.5 Idéaux premiers et ramification

On se donne deux corps de nombres $K \subset L$. Soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$. Alors $\mathfrak{p}\mathcal{O}_L$ est un idéal de $\mathcal{O}_L$, et comme ce dernier anneau est de Dedekind, on a la factorisation suivante :

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{B}_1^{e_1} \cdots \mathfrak{B}_g^{e_g}$$

où les $\mathfrak{B}_i$ sont des idéaux premiers de $\mathcal{O}_L$ distincts, appelés les idéaux premiers *au dessus* de $\mathfrak{p}$, et les e_i sont des entiers non nuls. L'entier e_i est appelé *indice de ramification* de $\mathfrak{B}_i$.

Remarquons de plus qu'un idéal premier non nul $\mathfrak{B} \subset \mathcal{O}_L$ apparaît dans la décomposition de $\mathfrak{p}$ si et seulement si $\mathfrak{p} = \mathfrak{B} \cap \mathcal{O}_K$. En effet si $\mathfrak{B}$ apparaît dans la factorisation de $\mathfrak{p}$ alors $\mathfrak{p} \subset \mathfrak{B} \cap \mathcal{O}_K$ et par maximalité de $\mathfrak{p}$, on a bien $\mathfrak{p} = \mathfrak{B} \cap \mathcal{O}_K$. La réciproque est une conséquence du corollaire (1.3.5).

On a donc, pour tout $\mathfrak{p}$, $\mathfrak{p} = \mathfrak{B}_i \cap \mathcal{O}_K$, ainsi qu'une extension de corps $\mathcal{O}_K/\mathfrak{p} \hookrightarrow \mathcal{O}_L/\mathfrak{B}_i$. Montrons maintenant que ces deux corps sont finis :

Proposition 1.5.1. *Soit $\mathfrak{a}$ un idéal non nul de $\mathcal{O}_K$. Alors le quotient $\mathcal{O}_K/\mathfrak{a}$ est fini.*

Démonstration. On se donne un élément $a \in \mathfrak{a}$. Il existent des entiers $b_0, \ldots, b_{r-1}$ tels que $b_0 + \cdots + b_{r-1}a^{r-1} + a^r = 0$. En posant $m = b_0$, on a $m \in a\mathcal{O}_K \subset \mathfrak{a}$. Ainsi, on a une surjection

$$\mathcal{O}_K/m\mathcal{O}_K \to \mathcal{O}_K/\mathfrak{a}$$

Finalement, on sait que $\mathcal{O}_K$ est un $\mathbb{Z}$-module libre de rang $n = [K : \mathbb{Q}]$, donc

$$\mathcal{O}_K/m\mathcal{O}_K \cong \mathbb{Z}^n/(m\mathbb{Z})^n \cong (\mathbb{Z}/m\mathbb{Z})^n$$

est fini d'ordre mn. On en conclut que $\mathcal{O}_K/\mathfrak{a}$ est fini. □

Si $\mathfrak{a}$ est un idéal de $\mathcal{O}_K$, on appelle *norme* de $\mathfrak{a}$, notée $N(\mathfrak{a})$, son indice dans $\mathcal{O}_K$.

Revenons à nos considérations premières. Le théorème précédant montre en particulier que l'extension $\mathcal{O}_K/\mathfrak{p} \hookrightarrow \mathcal{O}_L/\mathfrak{B}_i$ est finie. L'entier $f_i = [\mathcal{O}_L/\mathfrak{B}_i : \mathcal{O}_K/\mathfrak{p}]$ est appelé le *degré d'inertie* de $\mathfrak{B}_i$. On dispose alors de l'important résultat suivant :

Théorème 1.5.2. *Avec les notations précédentes, on a*

$$[L : K] = \sum_{k=1}^{g} e_i f_i$$

Démonstration. Par le théorème chinois, on a

$$\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \cong \mathcal{O}_L/\mathfrak{B}_1^{e_1} \oplus \cdots \oplus \mathcal{O}_L/\mathfrak{B}_g^{e_g}$$

Montrons maintenant que

$$Card(\mathcal{O}_L/\mathfrak{B}_i^{e_i}) = N(\mathfrak{p})^{e_i f_i} \tag{1.5.1}$$

Par définition $[\mathcal{O}_L/\mathfrak{B}_i : \mathcal{O}_K/\mathfrak{p}] = f_i$, et pour tout j, on a que $\mathfrak{B}_i^j/\mathfrak{B}_i^{j+1}$ est un $B/\mathfrak{B}_i$-espace vectoriel de dimension 1 (car il n'existe pas d'idéal strictement compris entre $\mathfrak{B}_i^{j+1}$ et $\mathfrak{B}_i^j$). En conséquence, les e_i quotients $\mathcal{O}_L/\mathfrak{B}_i, \ldots, \mathfrak{B}_i^{e_i-1}/\mathfrak{B}_i^{e_i}$ sont tous des $\mathcal{O}_K/\mathfrak{p}$-espaces vectoriels de dimension f_i, ce qui permet d'obtenir (1.5.1). Ainsi on a

$$Card(\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L) = N(\mathfrak{p})^{\sum_{k=1}^{g} e_i f_i}$$

Montrons que si $\mathcal{O}_K$ est principal on a l'égalité $Card(\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L) = N(\mathfrak{p})^{[L:K]}$. En effet, d'après la proposition (1.1.7), $\mathcal{O}_L$ est un $\mathcal{O}_K$-module libre de rang $[L : K]$, et la réduction modulo $\mathfrak{p}$ donne alors un isomorphisme $(\mathcal{O}_K/\mathfrak{p})^{[L:K]} \to \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$. Cela montre le théorème dans le cas où $\mathcal{O}_K$ est principal.

Dans le cas où $\mathcal{O}_K$ n'est pas principal, on pose $A = S^{-1}\mathcal{O}_K$ et $B = S^{-1}\mathcal{O}_L$ où $S = \mathcal{O}_K \setminus \mathfrak{p}$. Nous avons vu que A est principal (c'est un anneau de valuation discrète). De plus, il est facile de voir que B est la normalisation de A dans L. On a donc $[L : K] = [B : A]$, et par réduction modulo $\mathfrak{p}$, $[L : K] = [B/\mathfrak{p}B : A/\mathfrak{p}A]$. Enfin, de la décomposition $\mathfrak{p}\mathcal{O}_L = \mathfrak{B}_1^{e_1} \cdots \mathfrak{B}_g^{e_g}$, on déduit que $\mathfrak{p}B = (B\mathfrak{B}_1)^{e_1} \cdots (B\mathfrak{B}_g)^{e_g}$. Comme de plus $\mathfrak{B}_i \cap S = \varnothing$, $B\mathfrak{B}_i$ est un idéal premier non nul de B, et finalement

$$B/\mathfrak{p}B \cong B/(B\mathfrak{B}_1)^{e_1} \oplus \cdots \oplus B/(B\mathfrak{B}_g)^{e_g}$$

Comme $A/\mathfrak{p}A \cong \mathcal{O}_K/\mathfrak{p}$ et $B/B\mathfrak{B}_i \cong \mathcal{O}_L/\mathfrak{B}_i$, on en déduit, de la même manière que dans la première partie de la preuve, que

$$Card(B/\mathfrak{p}B) = N(\mathfrak{p})^{\sum_{k=1}^{g} e_i f_i}$$

Or $Card(B/\mathfrak{p}B) = Card(A/\mathfrak{p}A)^{[L:K]} = N(\mathfrak{p})^{[L:K]}$, ce qui achève la démonstration. □

Soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$ et on note $\mathfrak{p}\mathcal{O}_L = \mathfrak{B}_1^{e_1} \cdots \mathfrak{B}_g^{e_g}$ sa factorisation. On dit que $\mathfrak{p}$ est *ramifié* dans L s'il existe i tel que $e_i \geq 2$. On dira que $\mathfrak{p}$ est *totalement décomposé* si $e_i = f_i = 1$ pour tout i, $1 \leq i \leq g$. On note $Spl(L/K)$ l'ensemble des idéaux premiers de $\mathcal{O}_K$ totalement décomposes dans L.

Remarque 1.5.3. L'anneau des entiers algébriques $\mathcal{O}_K$ d'un corps de nombres K est une "*courbe reguliere arithmétique*", dont les points sont les idéaux premiers de $\mathcal{O}_K$. Si $i : K \hookrightarrow L$ est une extension de corps de nombres, alors on a un "revêtement"

$$\begin{aligned} i^* : Spec(\mathcal{O}_L) &\longrightarrow Spec(\mathcal{O}_K) \\ \mathfrak{B} &\mapsto i^{-1}(\mathfrak{B}) \end{aligned}$$

Si $\mathfrak{p}$ est un point de $\mathcal{O}_K$, les premiers $\mathfrak{B}_i$ de $\mathcal{O}_L$ au dessus de $\mathfrak{p}$ sont les points dans la fibre du point $\mathfrak{p}$. Les premiers de $\mathcal{O}_K$ ramifiés dans L correspondent aux "points de ramification" du revêtement $i^* : Spec(\mathcal{O}_L) \longrightarrow Spec(\mathcal{O}_K)$.
Il est très utile de retenir cette interprétation géométrique des anneaux des entiers algébriques (qu'on pourrait formuler de façon précise à l'aide du langage des schémas), qui permet de mieux comprendre beaucoup de phénomènes en théorie algébrique des nombres.

Regardons maintenant ce qu'il se passe du côté des automorphismes de l'extension L/K. Donnons nous $\sigma \in Aut(L/K)$. Soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$ et $\mathfrak{B}$ un idéal premier de $\mathcal{O}_L$ apparaissant dans la factorisation de $\mathfrak{p}\mathcal{O}_L$. Alors $\sigma(\mathfrak{B})$ est encore un idéal premier de $\mathcal{O}_L$ et $\sigma(\mathfrak{B}) \cap \mathcal{O}_K = \mathfrak{B} \cap \mathcal{O}_K = \mathfrak{p}$. Ainsi $\sigma(\mathfrak{B})$ apparaît dans la factorisation de $\mathfrak{p}\mathcal{O}_L$. L'ensemble $Aut(L/K)$ agît donc sur l'ensemble $\{\mathfrak{B}_i, 1 \leq i \leq g\}$ des idéaux premiers de $\mathcal{O}_L$ divisant $\mathfrak{p}\mathcal{O}_L$.

Il est alors intéressant de regarder ce qu'il se passe dans le cas d'une extension galoisienne :

Proposition 1.5.4. *Soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$ et $\{\mathfrak{B}_i, 1 \leq i \leq g\}$ l'ensemble des diviseurs premiers de $\mathfrak{p}\mathcal{O}_L$. Si l'extension L/K est galoisienne, alors*

1. *$Gal(L/K)$ agît transitivement sur $\{\mathfrak{B}_i, 1 \leq i \leq g\}$*
2. *Les indices de ramification e_i (resp. les degrés d'inertie f_i) sont tous égaux entre eux. Si l'on note $e = e_i$ (resp. $f = f_i$) on a ainsi $[L : K] = efg$.*

Démonstration. Supposons qu'il existe $\mathfrak{B}_i$ et $\mathfrak{B}_j$ qui ne soient pas conjugués. On choisit un élément $\beta \in \mathfrak{B}_j$ qui ne soit dans aucun des $\sigma(\mathfrak{B}_i), \sigma \in Gal(L/K)$ (on le peut grâce au théorème chinois). On pose alors

$$b = N_{L/K}(\beta) = \prod_{\sigma \in Gal(L/K)} \sigma(\beta)$$

On a $b \in \mathfrak{B}_j \cap \mathcal{O}_K = \mathfrak{p}$ et ainsi $b \in \mathfrak{B}_i$. Or $\sigma(\beta) \notin \mathfrak{B}_i$ pour tout $\sigma \in Gal(L/K)$, ce qui contredit la primalité de $\mathfrak{B}_i$. Enfin, il est clair que si $\sigma(\mathfrak{B}_i) = \mathfrak{B}_j$, alors, par unicité de la factorisation, $e_i = e_j$. De plus,

$$f_i = [\mathcal{O}_L/\mathfrak{B}_i : \mathcal{O}_K/\mathfrak{p}] = [\sigma(\mathcal{O}_L/\mathfrak{B}_i) : \sigma(\mathcal{O}_K/\mathfrak{p})] = [\mathcal{O}_L/\sigma(\mathfrak{B}_i) : \mathcal{O}_K/\mathfrak{p}] = f_j.$$

□

On fixe maintenant un idéal maximal $\mathfrak{B}$ de $\mathcal{O}_L$ divisant $\mathfrak{p}$. On définit le *groupe de décomposition de* $\mathfrak{B}$ comme le stabilisateur de $\mathfrak{B}$ pour l'action de $Gal(L/K)$:

$$D_{\mathfrak{B}} = \{\sigma \in Gal(L/K) : \sigma(\mathfrak{B}) = \mathfrak{B}\}$$

Il est clair que c'est un sous-groupe de $Gal(L/K)$. De plus, on a :

$$|Gal(L/K)| = |\Omega_{\mathfrak{B}}||D_{\mathfrak{B}}|$$

où $\Omega_{\mathfrak{B}}$ désigne l'orbite de $\mathfrak{B}$. Or, $|Gal(L/K)| = efg$, et comme l'action est transitive, on a $|\Omega_{\mathfrak{B}}| = g$. On en déduit que $|D_{\mathfrak{B}}| = ef$.

En notant G le groupe de Galois de $\mathcal{O}_K/\mathfrak{p} \hookrightarrow \mathcal{O}_L/\mathfrak{B}$, on obtient un morphisme

$$\psi : \sigma \in D_{\mathfrak{B}} \mapsto \bar{\sigma} \in G$$

où $\bar{\sigma}$ désigne l'automorphisme induit par σ sur $\mathcal{O}_L/\mathfrak{B}$. De plus, on montre que :

Proposition 1.5.5. *ψ est surjective.*

Démonstration. Notons $M = L^{D_{\mathfrak{B}}}$ le corps fixé par $D_{\mathfrak{B}}$, et $\mathcal{O}_M = \mathcal{O}_L \cap M$ sa normalisation sur $\mathcal{O}_K$. On pose $\mathfrak{q} = \mathfrak{B} \cap \mathcal{O}_M$; c'est un idéal premier de $\mathcal{O}_M$. On sait que $D_{\mathfrak{B}} = Gal(L/M)$ agit transitivement sur les diviseurs premiers de $\mathfrak{q}\mathcal{O}_L$. Comme $\mathfrak{B}$ divise $\mathfrak{q}\mathcal{O}_L$ et que l'orbite de $\mathfrak{B}$ pour l'action de $D_{\mathfrak{B}}$ est triviale, on en déduit que $\mathfrak{q}\mathcal{O}_L = \mathfrak{B}^{e'}$ pour un certain entier e'. Notons f' le degré d'inertie de $\mathfrak{B}$ sur M. On a

$$e'f' = [L : M] = |D_{\mathfrak{B}}| = ef$$

Or $\mathfrak{q}$ divise $\mathfrak{p}\mathcal{O}_M$ donc $e' \leq e$ et $\mathcal{O}_K/\mathfrak{p} \subset \mathcal{O}_M/\mathfrak{q} \subset \mathcal{O}_L/\mathfrak{B}$, donc $f' \leq f$. Finalement, $e = e'$, $f = f'$, et on en déduit que $\mathcal{O}_M/\mathfrak{q} = \mathcal{O}_K/\mathfrak{p}$.

Donnons nous $x \in \mathcal{O}_L$ tel que sa projection sur $\mathcal{O}_L/\mathfrak{B}$, $\bar{x}$, soit un élément primitif de l'extension $(\mathcal{O}_L/\mathfrak{B})/(\mathcal{O}_K/\mathfrak{p})$. On note $P \in \mathcal{O}_M[X]$ son polynôme minimal sur M. Sa projection $\overline{P}$ est à coefficient dans $\mathcal{O}_M/\mathfrak{q} = \mathcal{O}_K/\mathfrak{p}$. Ses racines sont donc les éléments $\psi(\sigma)(\bar{x})$, où σ parcourt $D_{\mathfrak{B}}$. Comme un élément de $g \in G$ envoie $\bar{x}$ sur un de ses conjugués $\psi(\sigma)(\bar{x})$, pour un certain $\sigma \in D_{\mathfrak{B}}$, on en déduit que $g = \psi(\sigma)$. Ainsi ψ est bien surjective. □

On définit alors le *groupe d'inertie de* $\mathfrak{B}$ comme étant le noyau de l'application ψ :

$$I_{\mathfrak{B}} = \{\sigma \in Gal(L/K) : \ \forall a \in \mathcal{O}_L, \ \sigma(a) \equiv a \ (\text{mod } \mathfrak{B})\}$$

Par surjectivité de ψ, on obtient finalement un isomorphisme $D_{\mathfrak{B}}/I_{\mathfrak{B}} \cong G$ ainsi que l'égalité $|I_{\mathfrak{B}}||G| = |D_{\mathfrak{B}}| = ef$, soit enfin $|I_{\mathfrak{B}}| = e$.

La dernière question que nous nous poserons dans cette section est la suivante : si $\mathfrak{p}$ est un idéal premier de $\mathcal{O}_K$, peut-on calculer les diviseurs de $\mathfrak{p}$? La réponse est oui, sous certaines conditions :

Proposition 1.5.6. *Supposons L/K galoisienne, et soit $h \in \mathcal{O}_K[X]$ son polynôme minimal. Soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$. On suppose que h est séparable modulo $\mathfrak{p}$ et on décompose h en produit de facteurs irréductibles distincts : $h = h_1 \cdots h_n$ (mod $\mathfrak{p}$). Alors :*

1. *pour tout i, l'idéal $\mathfrak{B}_i = \mathfrak{p}\mathcal{O}_L + h_i(\alpha)\mathcal{O}_L$ est premier dans $\mathcal{O}_L$*
2. *pour i, j distincts, $\mathfrak{B}_i$ et $\mathfrak{B}_j$ sont distincts, et $\mathfrak{p}\mathcal{O}_L = \mathfrak{B}_1 \cdots \mathfrak{B}_n$*
3. *$\mathfrak{p}$ est totalement décomposé si et seulement si h admet un racine modulo $\mathfrak{p}$ dans $\mathcal{O}_K$*

Démonstration. On se référera à l'ouvrage de D. A. Cox [3], p.91, proposition 5.11. □

1.6 Application d'Artin

On a vu dans la partie précédente que si un idéal premier $\mathfrak{p} \subset \mathcal{O}_K$ se décompose sous la forme

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{B}_1^{e_1} \cdots \mathfrak{B}_g^{e_g}$$

alors on a un morphisme surjectif $\psi_i : \sigma \in D_{\mathfrak{B}_i} \mapsto \bar{\sigma} \in G_i$. Pour que ce morphisme soit toujours un isomorphisme, il faut et il suffit que $I_{\mathfrak{B}_i}$ soit réduit au groupe trivial pour tout i, i.e. que $\mathfrak{p}$ soit non ramifié dans $\mathcal{O}_L$. Nous aurions donc envie de savoir quels sont les idéaux premiers de $\mathcal{O}_K$ non ramifiés dans $\mathcal{O}_L$.

Proposition 1.6.1. *Un idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ est ramifié dans $\mathcal{O}_L$ si et seulement si il divise l'idéal $\Delta_{L/K}$ (voir définition 1.2.2). En particulier, seul un nombre fini d'idéaux premiers de $\mathcal{O}_K$ sont ramifiés.*

Démonstration. Soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$. L'anneau $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ est un $\mathcal{O}_K/\mathfrak{p}$-espace vectoriel de dimension finie (car fini). Comme $Card(\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L) = N(p)^{[L:K]}$ (voir la démonstration du théorème 1.5.2), on en déduit que sa dimension est $[L : K]$. Finalement, on a un isomorphisme $(\mathcal{O}_K/\mathfrak{p})^{[L:K]} \to \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$, et une base de $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ se relève en une base de L/K. Ainsi, si $(\overline{a_1}, \cdots, \overline{a_n})$ est une base de $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$, alors :

$$D(a_1, \cdots, a_n) \equiv disc((\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L)/(\mathcal{O}_K/\mathfrak{p})) \pmod{\mathfrak{p}} \tag{1.6.1}$$

On sait en outre que $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \cong \mathcal{O}_L/\mathfrak{B}_1^{e_1} \oplus \cdots \oplus \mathcal{O}_L/\mathfrak{B}_g^{e_g}$ où $\mathfrak{p}\mathcal{O}_L = \mathfrak{B}_1^{e_1} \dots \mathfrak{B}_g^{e_g}$. En regardant une base de ce produit en tant que $\mathcal{O}_K/\mathfrak{p}$-algèbre, on montre que

$$disc((\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L)/(\mathcal{O}_K/\mathfrak{p})) = \prod disc((\mathcal{O}_L/\mathfrak{B}_i^{e_i})/(\mathcal{O}_K/\mathfrak{p}))$$

Notons $k = \mathcal{O}_K/\mathfrak{p}$,et montrons maintenant l'équivalence suivante : *une k-algèbre finie B est réduite si et seulement si $disc(B/k) \neq 0$.*

Supposons en effet que B soit non réduite. On choisit e_1 un élément non nul nilpotent de B et on le complète en une base $(e_1, \dots, e_n)$ de B. Pour tout i l'application $x \in B \mapsto e_1 e_i x$ est nilpotente et ainsi $Tr(e_1 e_i) = 0$, ce qui montre que $disc(B/k) = 0$.

Réciproquement, supposons B réduite. Alors l'intersection de tout les idéaux premiers de B est réduite à 0. D'autre part, si $\mathfrak{a}$ est un idéal premier de B, le quotient $B/\mathfrak{a}$ est intègre et de dimension finie sur k, c'est donc un corps et $\mathfrak{a}$ est maximal. Si maintenant $\mathfrak{a}_1, \dots, \mathfrak{a}_r$ sont des idéaux premiers distincts de B, on a d'après le théorème chinois :

$$B/\left(\cap \mathfrak{a}_i\right) \cong \mathfrak{B}/\mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{B}/\mathfrak{a}_r$$

Ainsi en notant n le degré B, on a $n \geq \sum [\mathfrak{B}/\mathfrak{a}_i : k] \geq r$. B a donc un nombre fini d'idéaux premiers. On en déduit l'isomorphisme :

$$B \cong \prod_{\mathfrak{a} \in Spec(B)} B/\mathfrak{a}$$

Chaque $B/\mathfrak{a}$ est une extension finie de k. Comme k est parfait (car fini), on en déduit que $B/\mathfrak{a}$ est une extension séparable, et ainsi $disc(B/\mathfrak{a}) \neq 0$ pour tout $\mathfrak{a}$, et donc $disc(B/k) \neq 0$.

Revenons au problème initial. On sait que

$$\mathfrak{p} \mid \Delta_{L/K} \Longleftrightarrow D(a_1, \cdots, a_n) \in \mathfrak{p} \text{ pour toute base entière de } a_1, \cdots, a_n \text{ de } L/K$$

D'après la congruence (1.6.1), cela est équivalent à $disc((\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L)/(\mathcal{O}_K/\mathfrak{p})) = 0$, c'est-à-dire à l'existence d'un entier i tel que $disc((\mathcal{O}_L/\mathfrak{B}_i^{e_i})/(\mathcal{O}_K/\mathfrak{p})) = 0$. Or la $\mathcal{O}_K/\mathfrak{p}-$algèbre $\mathcal{O}_L/\mathfrak{B}_i^{e_i}$ est réduite si, et seulement si $e_i > 1$, ce qui termine la démonstration. □

On fixe maintenant un corps de nombres K et une extension finie galoisienne L/K. On se donne $\mathfrak{B}$ un idéal premier de $\mathcal{O}_L$. Alors $\mathfrak{B}$ divise l'idéal premier $\mathfrak{p} = \mathfrak{B} \cap \mathcal{O}_K$. Si $\mathfrak{p}$ est non ramifié, on a un isomorphisme $\psi : D_{\mathfrak{B}} \to G$ où G est le groupe de Galois de $\mathcal{O}_K/\mathfrak{p} \hookrightarrow \mathcal{O}_L/\mathfrak{B}$. En particulier, il existe un unique antécédent $\sigma \in D_{\mathfrak{B}}$ au morphisme de Frobenius : $x \mapsto x^{N(\mathfrak{p})}$. On note cet élément $\sigma := ((L/K)/\mathfrak{B})$ (*symbole d'Artin*). C'est l'unique élément de $Gal(L/K)$ tel que

$$\left(\frac{L/K}{\mathfrak{B}}\right)(x) \equiv x^{N(\mathfrak{p})} \pmod{\mathfrak{B}}$$

pour tout $x \in \mathcal{O}_L$. En notant f le degré d'inertie de $\mathfrak{B}$, on constate que

$$\psi\left(\left(\frac{L/K}{\mathfrak{B}}\right)^f\right) = (x \mapsto x^{N(\mathfrak{p})})^f = Id_{\mathcal{O}_L/\mathfrak{B}}$$

et comme ψ est bijective, on en déduit que l'ordre de $((L/K)/\mathfrak{B})$ est f. Ainsi $\mathfrak{p}$ est totalement décomposé si et seulement si $((L/K)/\mathfrak{B}) = Id$.

Choisissons maintenant un autre idéal premier $\mathfrak{B}'$ divisant $\mathfrak{p}$. Il existe un automorphisme $\sigma \in Gal(L/K)$ tel que $\mathfrak{B}' = \sigma(\mathfrak{B})$. Si $x \in \mathcal{O}_L$ on a alors

$$\sigma\left(\frac{L/K}{\mathfrak{B}}\right)\sigma^{-1}(x) \equiv \sigma(\sigma^{-1}(x)^{N(\mathfrak{p})}) \equiv x^{N(\mathfrak{p})} \pmod{\mathfrak{B}'}$$

par unicité, on en déduit que :

$$\left(\frac{L/K}{\mathfrak{B}'}\right) = \sigma\left(\frac{L/K}{\mathfrak{B}}\right)\sigma^{-1}$$

Donc, si $\mathfrak{p}$ est un idéal premier de $\mathcal{O}_K$ non ramifié dans L, les $((L/K)/\mathfrak{B})$, pour $\mathfrak{B}$ idéal premier de $\mathcal{O}_L$ au dessus de $\mathfrak{p}$, forment une classe de conjugaison dans $Gal(L/K)$. Si G est *abélien* ses classes de conjugaisons sont des singletons, et ainsi la valeur de $((L/K)/\mathfrak{B})$ dépend uniquement de l'idéal premier sous-jacent $\mathfrak{p}$. On peut donc noter cet automorphisme $((L/K)/\mathfrak{p})$.

Si enfin on note $I_{\Delta_{L/K}}$ le sous groupe de $I(\mathcal{O}_K)$ engendré par les idéaux premiers ne divisant pas $\Delta_{L/K}$ (voir la proposition 1.6.1), on peut étendre la définition du symbole d'Artin au groupe $I_{\Delta_{L/K}}$ tout entier par la relation suivante : si $\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_n^{r_n}$, on pose :

$$\left(\frac{L/K}{\mathfrak{a}}\right) := \left(\frac{L/K}{\mathfrak{p}_1}\right)^{r_1} \cdots \left(\frac{L/K}{\mathfrak{p}_n}\right)^{r_n}$$

Le morphisme ainsi défini :

$$\left(\frac{L/K}{\cdot}\right) : I_{\Delta_{L/K}} \to Gal(L/K)$$

est appelé *application d'Artin*. Elle est définie pour toute extension *abélienne* finie L de K, et joue un rôle absolument crucial dans l'étude de ces extensions.

Exemple 1.6.2. (Extensions quadratiques imaginaires de $\mathbb{Q}$)
Une extension quadratique imaginaire de $\mathbb{Q}$ est un corps de la forme $\mathbb{Q}(\sqrt{N})$ avec $N \in \mathbb{Z}$, $N < 0$ (dorénavant on supposera que N n'a pas de diviseur carré). L'extension $\mathbb{Q}(\sqrt{N})/\mathbb{Q}$ est galoisienne, son groupe de Galois contient un seul automorphisme non trivial, à savoir, le morphisme qui envoit $\sqrt{N}$ sur $-\sqrt{N}$: c'est la restriction à $\mathbb{Q}(\sqrt{N})$ de la conjugaison complexe. On note d le discriminant de l'extension $\mathbb{Q}(\sqrt{N})/\mathbb{Q}$: on a $d = N$ si $N \equiv 1 \pmod 4$ et $d = 4N$ dans les autres cas. La proposition (1.5.6) nous permet de décrire le comportement des nombres premiers dans cette extension. Si $p \nmid d$, on a deux cas : si $(d/p) = 1$ alors p est totalement decomposé dans $\mathcal{O}_{\mathbb{Q}(\sqrt{N})}$, si $(d/p) = -1$ alors p reste premier dans $\mathcal{O}_{\mathbb{Q}(\sqrt{N})}$ (où (d/p) est le symbole de Legendre). Ce calcul donne une description de l'application d'Artin. On a

$$\left(\frac{\mathbb{Q}(\sqrt{N})/\mathbb{Q}}{\cdot}\right) : I_\Delta \longrightarrow \{\pm 1\} \cong Gal(\mathbb{Q}(\sqrt{N})/\mathbb{Q})$$

$$\left(\frac{a}{b}\right) \mapsto \left[\frac{d}{a}\right]\left[\frac{d}{b}\right]^{-1}$$

avec $a, b \in \mathbb{Z}$, $(a, d) = (b, d) = 1$ et $[\cdot/\cdot]$ est le symbole de Jacobi.

Exemple 1.6.3. (Extensions cyclotomiques de $\mathbb{Q}$)
Soit $\zeta_N = exp(2i\pi/N)$. On sait le polynôme minimal de ζ_N, appelé le N-ieme polynôme cyclotomique, est irréductible de degré $\phi(N) = |(\mathbb{Z}/N\mathbb{Z})^*|$. On en déduit que ζ_N est un entier algébrique. En plus, l'extension $\mathbb{Q}(\zeta_N)/\mathbb{Q}$ est galoisienne, et on a un isomorphisme de groupes :

$$\begin{aligned} Gal(\mathbb{Q}(\zeta_N)/\mathbb{Q}) &\longrightarrow (\mathbb{Z}/N\mathbb{Z})^* \\ \sigma &\mapsto a_\sigma \end{aligned}$$

où a_σ est caractérise par l'égalité $\sigma(\zeta_N) = \zeta_N^{a_\sigma}$. Donc $\mathbb{Q}(\zeta_N)$ est une extension abélienne de $\mathbb{Q}$. Si $N \not\equiv 2 \pmod 4$, on peut montrer que les premiers $p \in \mathbb{Z}$ qui se ramifient dans $\mathbb{Q}(\zeta_N)$ sont ceux qui divisent N. Par conséquence, l'application d'Artin est définie sur $I_N = \{(\frac{a}{b}) : r, s \in \mathbb{Z}, (r, N) = (s, N) = 1\}$. En identifiant $Gal(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ avec $(\mathbb{Z}/N\mathbb{Z})^*$ elle est donnée explicitement par :

$$\begin{aligned} \left(\frac{\mathbb{Q}(\zeta_N)/\mathbb{Q}}{\cdot}\right) : I_N &\longrightarrow \mathbb{Z}/N\mathbb{Z}^* \\ \left(\frac{r}{s}\right) &\mapsto \bar{r}\bar{s}^{-1} \pmod N \end{aligned}$$

Pour p premier qui ne divise pas N, l'action de $\left(\frac{\mathbb{Q}(\zeta_N)/\mathbb{Q}}{p}\right)$ sur $\mathbb{Q}(\zeta_N)$ est donnée par la formule :

$$\left(\frac{\mathbb{Q}(\zeta_N)/\mathbb{Q}}{p}\right)(\zeta_N^a) = \zeta_N^{ap} \tag{1.6.2}$$

En particulier, on a les équivalences :

$$p \text{ totalement décomposé } \iff \left(\frac{\mathbb{Q}(\zeta_N)/\mathbb{Q}}{p}\right) = Id \iff p \equiv 1 \pmod N$$

2 Théorie des corps de classe

2.1 Les énoncés de la théorie des corps de classe

La théorie des corps de classe classifie les extensions *abéliennes* finies d'un corps de nombres K quelconque. En utilisant l'application d'Artin, on identifie le groupe de Galois d'une extension abélienne L de K avec un certain "groupe des classes d'idéaux généralisé" de K, ce qui donne une description *abstraite* des extensions abéliennes de K en termes du corps K lui-même.

On va énoncer les résultats fondamentaux de la théorie dont on se servira dans la suite, en utilisant le langage classique des cycles arithmétiques. Voir [9] pour une description détaillée de la théorie.

On introduit d'abord la notion de *place* d'un corps de nombres K. C'est une généralisation de la notion d'idéal premier de $\mathcal{O}_K$, qui inclut aussi les "premiers à l'infini" de K. Géométriquement, cela correspond à ajouter les points à l'infini à la courbe affine $\mathcal{O}_K$ (voir la remarque 1.5.3).

Définition 2.1.1. *Une* valuation *sur un corps K est une fonction*

$$|\cdot| : K \to \mathbb{R}$$

telle que, pour tout $x, y \in K$:

1. $|x| \geq 0$ *et* $|x| = 0 \iff x = 0$,
2. $|xy| = |x||y|$,
3. $|x + y| \leq |x| + |y|$.

On donne ici deux exemples de valuation.

Exemple 2.1.2.
1. On appelle *valuation triviale* la valuation $|\cdot|$ telle que $|x| = 1$ pour tout $x \neq 0$.
2. Soit K un corps de nombres et $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$. Pour tout $x \in K$ l'idéal fractionnaire $x\mathcal{O}_K$ se factorise en un produit

$$x\mathcal{O}_K = \prod_{\mathfrak{q} \in Spec(\mathcal{O}_K)} \mathfrak{q}^{e(\mathfrak{q})}$$

avec les $e(\mathfrak{q}) \in \mathbb{Z}$ et égaux à zéro sauf un nombre fini. On définit $|x|_\mathfrak{p} = \frac{1}{N(\mathfrak{p})^{e(\mathfrak{p})}}$, où $N(\mathfrak{p})$ indique la norme de $\mathfrak{p}$. Cette formule définit bien une valuation sur K, appelée *valuation* $\mathfrak{p}$*-adique.*

Si $|\cdot|$ est une valuation sur K, on peut munir K d'une structure d'espace métrique avec la distance définie par $d(x, y) = |x - y|$. Si deux valuations induisent la même topologie sur K en tant qu'espace métrique, on dira qu'elles sont *équivalentes.*

Définition 2.1.3. *Une* place *d'un corps de nombres K est une classe d'équivalence de valuations non triviales sur K. Explicitement :*

1. *Une* place finie *(ou* non archimedièn*ne) est la classe d'équivalence de la valuation* $\mathfrak{p}$*-adique associée a un idéal premier* $\mathfrak{p}$ *de* $\mathcal{O}_K$*. On la note toujours* $\mathfrak{p}$*.*
2. *Une* place à l'infini *(ou* place archimedièn*ne) est la classe d'équivalence de la valuation associée a un plongement $i : K \longrightarrow \mathbb{C}$. Plus précisément, si $i : K \longrightarrow \mathbb{R}$ est un plongement réel on parle de* place réelle*. Si $i : K \longrightarrow \mathbb{C}$ est un plongement tel que $i(K) \not\subseteq \mathbb{R}$ on dit que c'est une* place complexe*.*

Les valuations considérées dans la définition précendante sont, à équivalence près, toutes les valuations possibles sur un corps de nombres. En fait, on a le théorème suivant du a Ostrowski :

Théorème 2.1.4 (Ostrowski)**.** *Soit K un corps de nombres. Une valuation non-triviale sur K est equivalente soit à une valuation* $\mathfrak{p}$*-adique pour un certain ideal premier* $\mathfrak{p}$ *de* $\mathcal{O}_K$*, soit à une valuation induite par un plongement réel ou complèxe.*

Démonstration. Voir [1]. □

Dans la suite, on utilisera la notation $\mathfrak{p}$ par indiquer à la fois les place finies et infinies.

Définition 2.1.5. *Soit L/K une extension de corps de nombres.*

1. *Soit* $\mathfrak{p}$ *une place finie de K. On dit que* $\mathfrak{p}$ *est* ramifiée *dans L si l'idéal premier* $\mathfrak{p}$ *est ramifié dans L.*
2. *Soit* $\mathfrak{p}$ *une place infinie de K. On dit que* $\mathfrak{p}$ *est* ramifiée *dans L si* $\mathfrak{p}$ *est une place réelle de K qui se prolonge en une place complexe de L.*
3. *L'extension L/K est dite* non ramifiée *si toute place (finie ou infinie) de K est non ramifiée dans L.*

Définition 2.1.6. *Un* cycle arithmétique *dans un corps de nombres K est un produit formel :*

$$\mathfrak{m} = \prod_{\mathfrak{p} \text{ place de } K} \mathfrak{p}^{n_\mathfrak{p}}$$

avec :

1. *$n_p \geq 0$, et $n_\mathfrak{p} = 0$ pour tout $\mathfrak{p}$ sauf un nombre fini.*
2. *$n_\mathfrak{p} = 0$ si $\mathfrak{p}$ est une place complexe, et $n_p \leq 1$ si $\mathfrak{p}$ est une place réelle,*

Si $\mathfrak{m} = \prod_{\mathfrak{p} \text{ place de } K} \mathfrak{p}^{n_\mathfrak{p}}$ est un cycle arithmétique, on note $\mathfrak{m}_0 = \prod_{\mathfrak{p} \text{ place finie de } K} \mathfrak{p}^{n_\mathfrak{p}}$. On peut identifier $\mathfrak{m}_0$ avec un idéal de $\mathcal{O}_K$.
On dit que une place $\mathfrak{p}$ de K divise *le cycle arithmétique $\mathfrak{m} = \prod_\mathfrak{p} \mathfrak{p}^{n_\mathfrak{p}}$ si $n_p > 0$.*
Si $\mathfrak{m} = \prod_\mathfrak{p} \mathfrak{p}^{n_\mathfrak{p}}$ et $\mathfrak{n} = \prod_\mathfrak{p} \mathfrak{p}^{n'_\mathfrak{p}}$ sont deux cycles, on dit que $\mathfrak{m}$ divise *$\mathfrak{n}$, et on écrit $\mathfrak{m}|\mathfrak{n}$, si $n_\mathfrak{p} \leq n'_\mathfrak{p}$ pour chaque place $\mathfrak{p}$.*

Définition 2.1.7. *Si $\mathfrak{m}$ est un cycle arithmétique de K, on pose :*

$$\mathcal{I}_K(\mathfrak{m}) = \{\mathfrak{a} \text{ idéal fractionnaire de } K \ : \ (\mathfrak{a}, \mathfrak{m}_0) = 1\}$$

$$\mathcal{P}_K(\mathfrak{m}) = \{\mathfrak{a} = (\alpha) : \ \alpha \equiv 1 \pmod{\mathfrak{m}_0},\ \mathfrak{p}(\alpha) > 0 \ \forall \ \mathfrak{p} \text{ place réelle telle que } n_\mathfrak{p} = 1\}$$

On vérifie sans difficulté que $\mathcal{I}_K(\mathfrak{m})$ est un groupe, et que $\mathcal{P}_K(\mathfrak{m})$ est un sous groupe de $\mathcal{I}_K(\mathfrak{m})$. On peut aussi montrer que le quotient $\mathcal{I}_K(\mathfrak{m})/\mathcal{P}_K(\mathfrak{m})$ est un groupe fini.
Un sous groupe H de $\mathcal{I}_K(\mathfrak{m})$ est appelé *sous groupe de congruence* pour $\mathfrak{m}$ si $\mathcal{P}_K(\mathfrak{m}) \subseteq H \subseteq \mathcal{I}_K(\mathfrak{m})$.

Exemple 2.1.8. Si $\mathfrak{m} = 1 = \prod_\mathfrak{p} \mathfrak{p}^0$ alors $\mathcal{I}_K := \mathcal{I}_K(1) = \{$idéaux fractionnaires de K$\}$ et $\mathcal{P}_K := \mathcal{P}_K(1) = \{$idéaux fractionnaires principaux de K$\}$, donc $\mathcal{I}_K/\mathcal{P}_K = Cl(\mathcal{O}_K)$, le groupe des classes d'idéaux de $\mathcal{O}_K$.

Exemple 2.1.9. Notons ∞ l'unique place archimedienne de $\mathbb{Q}$. Chaque cycle arithmétique de $\mathbb{Q}$ est alors de la forme $\mathfrak{m} = a$ ou $\mathfrak{m} = a\infty$, avec $a \in \mathbb{Z}$. En particulier, tout cycle de $\mathbb{Q}$ divise un cycle de la forme $N\infty$, avec $N \in \mathbb{Z}$.

Exemple 2.1.10. Soit $K = \mathbb{Q}(\tau)$ une extension *quadratique imaginaire* de $\mathbb{Q}$. Alors K n'a pas de place réelle, donc on peut toujours identifier un cycle arithmétique $\mathfrak{m}$ avec un idéal de $\mathcal{O}_K$, qu'on note toujours $\mathfrak{m}$. On a alors $\mathcal{I}_K(\mathfrak{m}) = \{\mathfrak{a}$ idéal fractionnaire de K $: (\mathfrak{a}, \mathfrak{m}) = 1\}$ et $\mathcal{P}_K(\mathfrak{m}) = \{\mathfrak{a} = (\alpha),\ \alpha \in K, \alpha \equiv 1 \pmod{\mathfrak{m}}\}$.
On remarque que, si $\mathfrak{p}$ est un idéal premier non nul de $\mathcal{O}_K$, alors $\mathfrak{p}\overline{\mathfrak{p}} = N(\mathfrak{p}) \in \mathbb{Z}$. On en déduit que chaque cycle de K divise un cycle de la forme $\mathfrak{m} = N$, avec $N \in \mathbb{Z}$.

Remarque 2.1.11. Soit L/K une extension abélienne de corps de nombres, et soit $\mathfrak{m}$ un cycle arithmétique divisible par chaque place de K ramifiée dans L. Alors l'application d'Artin est bien définie sur $\mathcal{I}_K(\mathfrak{m})$.

Avec ce vocabulaire, on peut énoncer les résultats fondamentaux de la théorie des corps de classe.

Théorème 2.1.12. *(Loi de réciprocité d'Artin) Soit L/K une extension abélienne de corps de nombres. Soit $\mathfrak{m}$ un cycle arithmétique de K divisible par toute place de $\mathcal{O}_K$ ramifiée dans L. Soit*

$$\Phi_\mathfrak{m} : \mathcal{I}_K(\mathfrak{m}) \longrightarrow Gal(L/K)$$

l'application d'Artin. On a :

1. *$\Phi_\mathfrak{m}$ est surjective.*

2. *Si les exposants $n_\mathfrak{p}$ des places finies $\mathfrak{p}$ dans $\mathfrak{m}_0$ sont assez grands, alors $ker(\Phi_\mathfrak{m})$ est un sous groupe de congruence pour $\mathfrak{m}$.*

Démonstration. Voir [4]. □

Remarque 2.1.13. Le point 2. dans le théorème implique que le noyau de l'application d'Artin est décrit par des congruences modulo un certain cycle arithmétique de K. En particulier, on peut caractériser l'ensemble $Spl(L/K)$ à l'aide d'un nombre fini de conditions de congruence dans K. Cette loi est donc une généralisation de la loi de réciprocité quadratique, ainsi que des autres lois de réciprocité classiques.

Remarque 2.1.14. Etant donnée une extension abélienne L/K et un cycle arithmétique $\mathfrak{m}$ tel que $\Phi_\mathfrak{m}$ soit définie et $ker(\Phi_m)$ soit un sous groupe de congruence pour $\mathfrak{m}$, on vérifie que, si $\mathfrak{n}$ est un cycle arithmétique tel que $\mathfrak{m}|\mathfrak{n}$, alors $ker(\Phi_\mathfrak{n})$ est aussi un sous groupe de congruence pour $\mathfrak{n}$.

La remarque 2.1.14 implique qu'il existe une infinité de cycles qui vérifient les conclusions du théorème 2.1.12. On peut quand-même choisir un unique cycle "minimal" :

Théorème 2.1.15. *Soit L/K une extension abélienne de corps de nombres. Il existe un unique cycle arithmétique $\mathfrak{f}(L/K)$, appelé le* conducteur *de l'extension L/K, tel que :*

1. *Une place de K est ramifiée dans L si et seulement si elle divise $\mathfrak{f}(L/K)$.*
2. *Si $\mathfrak{m}$ est un cycle arithmétique de K divisible par toute place de K ramifiée dans L, alors $ker(\Phi_\mathfrak{m})$ est un sous groupe de congruence pour $\mathfrak{m}$ si et seulement si $\mathfrak{f}(L/K)|\,\mathfrak{m}$.*

Démonstration. Voir [4]. □

Enfin, il y a une sorte de réciproque du théorème 2.1.12 :

Théorème 2.1.16. *(Théorème d'existence) Soit $\mathfrak{m}$ un cycle arithmétique de K, H un sous groupe de congruence pour $\mathfrak{m}$. Alors il existe une unique extension abélienne L de K telle que :*

1. *Les places de K ramifiées dans L divisent $\mathfrak{m}$.*
2. *le noyau de l'application d'Artin $\Phi_\mathfrak{m} : \mathcal{I}_\mathfrak{m} \longrightarrow Gal(L/K)$ est H.*

Démonstration. Voir [4]. □

Ce théorème nous permet de donner la définition suivante :

Définition 2.1.17. *Soit $\mathfrak{m}$ un cycle arithmétique de K. Le* corps de classe de rayon $\mathfrak{m}$ *est l'unique extension abélienne $K_\mathfrak{m}$ de K telle que les premiers de K ramifiés dans $K_\mathfrak{m}$ divisent $\mathfrak{m}$, et $ker(\Phi_\mathfrak{m}^{K_m/K}) = \mathcal{P}_K(\mathfrak{m})$.*
En particulier, le corps de classe de rayon $\mathfrak{m} = 1$ est appelé le corps de classe de Hilbert *de K, noté $\mathcal{H}_K$. L'application d'Artin donne un isomorphisme entre $Gal(\mathcal{H}_K)$ et $Cl(\mathcal{O}_K)$.*

Par définition, un idéal premier $\mathfrak{p}$ de K est totalement décompose dans $K_\mathfrak{m}$ si et seulement si $\mathfrak{p} = (\alpha)$ et $\alpha \equiv 1 \pmod{\mathfrak{m}}$. En particulier, on a :

$$Spl(\mathcal{H}_K) = \{\text{Idéaux premiers principaux de } \mathcal{O}_K\}$$

Exemple 2.1.18. Soit $K = \mathbb{Q}$ et $\mathfrak{m} = N\infty$. Alors $\mathcal{I}_\mathbb{Q}(\mathfrak{m}) = \{(\frac{r}{s}) : (r, N) = (s, N) = 1\}$ et $\mathcal{P}_\mathbb{Q}(\mathfrak{m}) = \{\left(\frac{r}{s}\right) : \frac{r}{s} > 0, (r, N) = 1, r \equiv s \pmod{N}\}$. Soit $L = \mathbb{Q}(\zeta_N)$. On a vu dans

l'exemple 1.6.3 que L/K est abélienne de groupe de Galois isomorphe à $(\mathbb{Z}/N\mathbb{Z})^*$, et on a explicité l'application d'Artin :

$$\begin{aligned}\Phi_{\mathfrak{m}}^{\mathbb{Q}(\zeta(N))/\mathbb{Q}} : \mathcal{I}_{\mathbb{Q}}(\mathfrak{m}) &\longrightarrow (\mathbb{Z}/N\mathbb{Z})^* \\ \left(\frac{r}{s}\right) &\mapsto \bar{r}\bar{s}^{-1} \pmod N\end{aligned}$$

Il est alors clair que $ker(\Phi_{\mathfrak{m}}^{\mathbb{Q}(\zeta(N))/\mathbb{Q}}) = \mathcal{P}_{\mathbb{Q}}(\mathfrak{m})$. Donc le corps de classe de rayon $\mathfrak{m} = N\infty$ de $\mathbb{Q}$ est $\mathbb{Q}(\zeta_N)$.

Les théorèmes 2.1.12, 2.1.15 et 2.1.16 sont les résultats fondamentaux de la théorie des corps de classe ; ils sont les outils abstraits essentiels pour étudier les extension abéliennes des corps de nombres. On verra tout de suite certaines conséquences étonnantes de ces résultats.

2.2 Conséquences de la théorie des corps de classe

On commence par un lemme technique assez simple mais très utile.

Lemme 2.2.1. *Soient $L, M \subset \mathbb{C}$ deux extensions abéliennes finies d'un corps de nombres K. Les assertions suivantes sont équivalentes :*

1. *$L \subseteq M$*
2. *Il existe un cycle $\mathfrak{m}$ de K, divisible par toutes les places de K ramifiées dans L ou M, tel que*
$$\mathcal{P}_K(\mathfrak{m}) \subseteq ker(\Phi_{\mathfrak{m}}^{M/K}) \subseteq ker(\Phi_{\mathfrak{m}}^{L/K})$$

Démonstration. 1. $\Rightarrow$ 2.
Supposons $L \subseteq M$. La remarque 2.1.14 implique que il existe un cycle arithmétique $\mathfrak{m}$ de K tel que $ker(\Phi_{\mathfrak{m}}^{M/K})$ et $ker(\Phi_{\mathfrak{m}}^{L/K})$ sont des sous groupes de congruence pour $\mathfrak{m}$. Notons $r : Gal(M/K) \longrightarrow Gal(L/K)$ l'application de restriction. Alors on vérifie que $\Phi_{\mathfrak{m}}^{L/K} = r \circ (\Phi_{\mathfrak{m}}^{M/K})$, ce qui implique $ker(\Phi_{\mathfrak{m}}^{M/K}) \subseteq ker(\Phi_{\mathfrak{m}}^{L/K})$.
2. $\Rightarrow$ 1.
Soit $\mathfrak{m}$ cycle qui vérifie 2. Soit $H = \Phi_{\mathfrak{m}}^{M/K}(ker(\Phi_{\mathfrak{m}}^{L/K}))$. Soit $K \subseteq \tilde{L} \subseteq M$ le corps fixé par H. Alors on a $ker(\Phi_{\mathfrak{m}}^{L/K}) = ker(\Phi_{\mathfrak{m}}^{\tilde{L}/K})$, donc, par l'unicité dans le théorème 2.1.16, on a $L = \tilde{L} \subseteq M$. □

Une première conséquence du lemme 2.2.1 est la caractérisation suivante du corps de classe de Hilbert d'un corps de nombres K.

Proposition 2.2.2. *Le corps de classe de Hilbert $\mathcal{H}_K$ d'un corps de nombres K est l'extension abélienne non ramifiée maximale de K. Autrement dit, toute extension L de K abélienne non ramifiée est contenue dans $\mathcal{H}_K$.*

Démonstration. Par définition, $\mathcal{H}_K$ est une extension abélienne de K. En plus, le conducteur de $\mathcal{H}_K/K$ est forcement le cycle 1, donc le théorème 2.1.15 nous dit que cette extension est non ramifiée.

Soit maintenant L/K une extension abélienne non ramifiée. Par le théorème 2.1.15 on a $\mathfrak{f}(L/K) = 1$, donc par le même théorème on a $\mathcal{P}_{\mathbb{Q}}(1) = ker(\Phi_1^{\mathcal{H}_K/K}) \subseteq ker(\Phi_1^{L/K})$. Le lemme 2.2.1 implique alors que $L \subseteq \mathcal{H}_K$. □

Plus généralement, le lemme 2.2.1 nous permet de décrire, au moins de façon abstraite, l'extension abélienne maximale d'un corps de nombres K quelconque.

Proposition 2.2.3. *Soit K un corps de nombres, et $(\mathfrak{m}_i)_{i\in I}$ une famille de cycles de K telle que pour tout cycle $\mathfrak{n}$ de K il existe $i_\mathfrak{n} \in I$ tel que $\mathfrak{n}|\mathfrak{m}_{i_\mathfrak{n}}$. Alors le compositum des corps de classe de rayon $K_{\mathfrak{m}_i}$ est l'extension abélienne maximale de K. Autrement dit, toute extension abélienne de K est contenue dans $K_{\mathfrak{m}_i}$ pour un certain $i \in I$.*

Démonstration. Soit L/K une extension abélienne, $\mathfrak{n}$ un cycle arithmétique qui vérifie les hypothèses du théorème 2.1.12, $i_\mathfrak{n} \in I$ tel que $\mathfrak{n}|\mathfrak{m}_{i_\mathfrak{n}}$. La remarque 2.1.14 implique que on a l'inclusion :

$$\mathcal{P}_K(\mathfrak{m}_{i_\mathfrak{n}}) \subseteq ker(\Phi^{L/K}_{\mathfrak{m}_{i_\mathfrak{n}}})$$

Comme par définition on a $\mathcal{P}_K(\mathfrak{m}_{i_\mathfrak{n}}) = ker(\Phi^{K_{i_\mathfrak{n}}/K}_{\mathfrak{m}_{i_\mathfrak{n}}})$, le lemme 2.2.1 implique que $L \subseteq K_{i_\mathfrak{n}}$. □

2.3 Le Théorème de Chebotarev et ses conséquences

Définition 2.3.1. *Soit K un corps de nombres, et $\mathbf{P}$ un ensemble d'idéaux premiers non nuls de $\mathcal{O}_K$. Si la limite*

$$\delta(\mathbf{P}) = \lim_{s\to 1^+} \frac{\sum_{\mathfrak{p}\in\mathbf{P}} \frac{1}{N(\mathfrak{p})^s}}{log\frac{1}{s-1}}$$

existe, on l'appelle densité de Dirichlet *de l'ensemble $\mathbf{P}$.*

Notation 2.3.2. Si $\mathbf{P}$ est un ensemble d'idéaux premiers non nuls de $\mathcal{O}_K$ on note $\mathbf{P}^* = \{\mathfrak{p} \in \mathbf{P} : \mathfrak{p}$ a degré d'inertie 1 dans $K/\mathbb{Q}\}$.

Proposition 2.3.3.
1. *$\delta(\mathbf{P}) \leq 1$ pour tout $\mathbf{P}$. Si $\mathbf{P}$ est un ensemble fini, alors $\delta(\mathbf{P})$=0.*
2. *$\delta(\mathbf{P}) = \delta(\mathbf{P}^*)$.*
3. *$\delta(\mathbf{P} \sqcup \mathbf{Q}) = \delta(\mathbf{P}) + \delta(\mathbf{Q})$.*
4. *$\delta(\mathbf{P}) = \delta(\mathbf{Q})$ si $\mathbf{P}^*$ et $\mathbf{Q}^*$ différent pour un nombre fini d'idéaux.*

Démonstration. Voir [3], pp.153-154. □

Notation 2.3.4. Soit L/K une extension galoisienne de corps de nombres. Soit $\mathfrak{p}$ idéal premier de $\mathcal{O}_K$. On note $\sigma_\mathfrak{p}$ la classe de conjugaison formée des $((L/K)/\mathfrak{B}_i)$ avec $\mathfrak{B}_i$ idéal premier de $\mathcal{O}_L$ au dessus de $\mathfrak{p}$.
Si C est une classe de conjugaison dans $Gal(L/K)$, on note $\mathbf{P}_C$ l'ensemble des $\mathfrak{p}$ tels que $\sigma_\mathfrak{p} = C$.

Théorème 2.3.5. *(Théorème de densité de Chebotarev) Soit L/K une extension galoisienne de corps de nombres, C une classe de conjugaison de $Gal(L/K)$. Alors on a :*

$$\delta(\mathbf{P}_C) = \frac{|C|}{|Gal(L/K)|}$$

Démonstration. Voir [9]. □

Corollaire 2.3.6. *Soit L/K une extension galoisienne de corps de nombres. Alors*

$$\delta(Spl(L/K)) = \frac{1}{|Gal(L/K)|} = \frac{1}{[L:K]}$$

Ce corollaire entraine le fait remarquable, et très important, que une extension galoisienne de corps de nombres L/K est *caractérisée* par l'ensemble $Spl(L/K)$.

Proposition 2.3.7. *Soient $L, M \subseteq \mathbb{C}$ deux extensions galoisiennes d'un corps de nombres K.*

1. *$M \subseteq L$ si et seulement si $Spl(L/K)^* \subseteq Spl(M/K)^*$ à un nombre fini d'idéaux premiers prés.*
2. *$L = M \iff Spl(L/K)^* = Spl(M/K)^*$ à un nombre fini d'idéaux premiers prés.*

Démonstration. Supposons que $Spl(L/K)^* \subseteq Spl(M/K)^*$, sauf peut être pour un nombre fini d'idéaux. Comme un idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ est totalement décomposé dans LM si et seulement si il est totalement décomposé dans L et M, on a :

$$Spl(LM/K) = Spl(L/K) \cap Spl(M/K)$$

En utilisant le corollaire du théorème de Chebotarev on a alors les égalités :

$$\begin{aligned}\frac{1}{[LM:K]} &= \delta(Spl(LM/K)) = \delta(Spl(LM/K)^*) \\ &= \delta(Spl(L/K)^*) \cap Spl((M/K)^*) = \delta(Spl(L/K)^*) \\ &= \delta(Spl(L/K)) = \frac{1}{[L:K]}\end{aligned}$$

donc

$$\frac{1}{[LM:K]} = \frac{1}{[L:K]}$$

ce qui implique $M \subseteq L$. L'implication réciproque est immédiate, et 2. découle de 1. □

Remarque 2.3.8. On a vu que $\mathfrak{p} \in Spl(\mathcal{H}_K/K)$ si et seulement si $\mathfrak{p}$ est principal. D'après la proposition 2.3.7, cette propriété caractérise le corps de classe de Hilbert de K parmi toutes les extensions galoisiennes finies de K. Si L est une extension galoisienne finie de K telle que, pour tout idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ de degré d'inertie 1 sauf au plus un nombre fini on a équivalence :

$$\mathfrak{p} \text{ totalement décomposé dans } L \iff \mathfrak{p} \text{ est principal}$$

alors $L = \mathcal{H}_K$.

Plus généralement, soit $\mathfrak{m}$ un cycle arithmétique de K. Si L une extension galoisienne finie de K telle que $Spl(L/K)^* = \{\mathfrak{p} \in \mathcal{P}_k(\mathfrak{m})\}^*$ sauf au plus pour un nombre fini d'idéaux premiers alors $L = K_{\mathfrak{m}}$.

2.4 Extensions abéliennes de $\mathbb{Q}$

Les résultats de la section précédente nous permettent de déterminer l'extension abélienne maximale de $\mathbb{Q}$, notée $\mathbb{Q}^{ab}$. En dépit de son nom, le résultat classique suivant a été démontré pour la première fois par Hilbert.

Théorème 2.4.1. *(Kronecker-Weber) Toute extension abélienne de $\mathbb{Q}$ est contenue dans une extension cyclotomique $\mathbb{Q}(\zeta_N)$ pour un certain N.*

Soit $\mu(\mathbb{C}^*)$ l'ensemble des racines de l'unité dans $\mathbb{C}^*$. On a alors :

$$\mathbb{Q}^{ab} = \mathbb{Q}(\mu(\mathbb{C}^*))$$

et

$$Gal(\mathbb{Q}^{ab}/\mathbb{Q}) \cong \varprojlim_N (\mathbb{Z}/N\mathbb{Z})^* = \hat{\mathbb{Z}}^*$$

Démonstration. On a vu dans l'exemple 2.1.9 que tout cycle $\mathfrak{m}$ de $\mathbb{Q}$ divise un cycle de la forme $N\infty$, et on a montré dans l'exemple 1.6.3 que le corps de classe de rayon $N\infty$ pour $\mathbb{Q}$ est $\mathbb{Q}(\zeta_N)$. Le théorème découle alors de la proposition 2.2.3. □

Notation 2.4.2. Soit G un groupe abélien, et $N \in \mathbb{N}$. On note $G[N]$ le sous groupe de $N-$torsion de G, c'est à dire :

$$G[N] = \{g \in G \ : Ng = 1\}$$

et on note $G_{tors} = \cup_{N\in\mathbb{N}} G[N]$ la partie de torsion de G. Par exemple, si $G = \mathbb{C}^* \cong \mathbb{GL}_1(\mathbb{C})$, alors $G[N] = \{e^{2i\pi a/N},\ a \in \mathbb{Z}\}$ et $G_{tors} = \mu(\mathbb{C})$.

On peut résumer ce qu'on a vu sur les extensions abéliennes de $\mathbb{Q}$ de la façon suivante :

Théorème 2.4.3. *1. Soit $N \in \mathbb{N}$. Alors $\zeta_N = e^{2i\pi/N}$ est un entier algébrique.*

2. L'extension $\mathbb{Q}(\zeta_N)/\mathbb{Q} = \mathbb{Q}(\mathbb{GL}_1(\mathbb{C})[N]/\mathbb{Q})$ est abélienne.

3. Toute extension abélienne de $\mathbb{Q}$ est contenue dans $\mathbb{Q}(\mathbb{GL}_1(\mathbb{C})[N])$ pour un certain $N \in \mathbb{N}$.

Les trois points du théorème 2.4.3 correspondent à trois miracles :

1. La fonction exponentielle, qui est une fonction transcendante, prend des valeurs algébriques si elle est évaluée sur les points $2i\pi k/N$, avec $k, N \in \mathbb{N}$. Mieux, ces valeurs sont des entiers algébriques.
2. Les coordonnées des points de $N-$torsion du groupe $\mathbb{GL}_1(\mathbb{C})$ engendrent des extensions abéliennes de $\mathbb{Q}$.
3. Toute extension abélienne de $\mathbb{Q}$ est contenue dans une extension obtenue comme dans 2.

Dans la suite, on va essayer d'obtenir un résultat analogue au théorème 2.4.3, mais sur un corps de base $K = \mathbb{Q}(\tau)$ quadratique imaginaire.

3 Courbes elliptiques et fonctions modulaires

3.1 Courbes elliptiques sur $\mathbb{C}$

Définition 3.1.1. *Un* réseau Λ *de $\mathbb{C}$ est un sous groupe discret de rang 2 de $\mathbb{C}$. Si $\{\omega_1, \omega_2\}$ est une base de Λ, on écrit $\Lambda = [\omega_1, \omega_2]$.*

Définition 3.1.2. *Une* courbe elliptique E_Λ *est le quotient de $\mathbb{C}$ par l'action d'un réseau Λ.*

Remarque 3.1.3. Comme l'action de Λ sur $\mathbb{C}$ est libre et proprement discontinue, E_Λ admet une structure naturelle de variété analytique quotiente, qui fait de la projection $\pi : \mathbb{C} \to E_\Lambda$ une application holomorphe et aussi un revêtement. De plus, E_Λ est munie d'une structure de groupe naturelle compatible avec sa structure de variété complexe.

Définition 3.1.4. *Soient E_Λ et $E_{\Lambda'}$ deux courbes elliptiques. On appelle* isogénie *une application non constante $\phi : E_\Lambda \longrightarrow E_{\Lambda'}$ qui est à la fois une application holomorphe et un morphisme de groupes. Si ϕ est bijective, elle est appelée un* isomorphisme *entre E_Λ et $E_{\Lambda'}$.*
Le noyau *d'une isogénie est son noyau en tant que morphisme de groupes. Son cardinal est appelée le* degré *de l'isogénie.*
Un endomorphisme *de E_Λ est une isogénie de E dans elle-même. Un endomorphisme bijectif est un* automorphisme.

Notation 3.1.5. Si $\alpha \in \mathbb{C}$, on note $m_\alpha : \mathbb{C} \longrightarrow \mathbb{C}$ la multiplication par α, $z \mapsto \alpha z$.

Lemme 3.1.6. *Soit $\phi : E_\Lambda \longrightarrow E_{\Lambda'}$ une isogénie entre deux courbes elliptiques. Alors il existe $\alpha_\phi \in \mathbb{C}$ tel que $\alpha_\phi \Lambda \subseteq \Lambda'$ et que le diagramme suivant commute :*

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{m_{\alpha_\phi}} & \mathbb{C} \\ \pi_\Lambda \downarrow & & \downarrow \pi_{\Lambda'} \\ E_\Lambda & \xrightarrow[\phi]{} & E_{\Lambda'} \end{array}$$

où les fléchés verticales sont les projections canoniques.
Réciproquement, si $\alpha \in \mathbb{C}$ est tel que $\alpha\Lambda \subseteq \Lambda'$, alors m_α induit une isogénie $\phi : E_\Lambda \longrightarrow E_{\Lambda'}$ qui fait commuter le diagramme.
En plus, ϕ est un isomorphisme si et seulement si $\alpha\Lambda = \Lambda'$.

Démonstration. Soit $\phi : E_\Lambda \longrightarrow E_{\Lambda'}$ une isogénie. Comme la projection $\pi_{\Lambda'}$ est un revêtement et $\mathbb{C}$ est simplement connexe, il existe un (unique) relèvement holomorphe $\tilde{\phi} : \mathbb{C} \longrightarrow \mathbb{C}$ de l'application $\phi \circ \pi_\Lambda$ qui envoie 0 en 0.

Soit $\lambda \in \Lambda$. Alors l'application $z \mapsto \tilde{\phi}(z+\lambda) - \tilde{\phi}(z)$ prend ses valeurs dans Λ', donc, comme elle est continue, on a $\tilde{\phi}(z+\lambda) - \tilde{\phi}(z) = const$, ce qui donne $\tilde{\phi}'(z+\lambda) - \tilde{\phi}'(z) = 0$. Donc $\tilde{\phi}'$ est Λ-périodique et holomorphe, donc constante. On en déduit que $\tilde{\phi}(z)$ est de la forme $z \mapsto \alpha z + \beta$, et $\beta = 0$ comme $\tilde{\phi}(0) = 0$, donc $\tilde{\phi} = m_\alpha$. Enfin, $\alpha\Lambda \subseteq \Lambda'$ par commutativité du diagramme.

Le reste du lemme est facile. □

Remarque 3.1.7. La preuve montre que toute application holomorphe $\phi : E \to E'$ qui envoi 0_E sur $0_{E'}$ est automatiquement une isogénie.

Le lemme 3.1.6 donne des bijections :

$$\begin{array}{ccc} \{\text{isogénies } \phi : E_\Lambda \longrightarrow E_{\Lambda'}\} & \longleftrightarrow & \{\alpha \in \mathbb{C} : \ \alpha\Lambda \subseteq \Lambda'\} \\ \phi & \longmapsto & \alpha_\phi \end{array}$$

$$\begin{array}{ccc} \{\text{isomorphismes } \phi : E_\Lambda \longrightarrow E_{\Lambda'}\} & \longleftrightarrow & \{\alpha \in \mathbb{C} : \ \alpha\Lambda = \Lambda'\} \\ \phi & \longmapsto & \alpha_\phi \end{array}$$

$$\begin{array}{ccc} \{\text{endomorphismes } \phi : E_\Lambda \longrightarrow E_\Lambda\} & \longleftrightarrow & \{\alpha \in \mathbb{C} : \ \alpha\Lambda \subseteq \Lambda\} \\ \phi & \longmapsto & \alpha_\phi \end{array}$$

En particulier, on obtient :

Proposition 3.1.8. *Soient Λ et Λ' deux réseaux de $\mathbb{C}$. Alors les courbes elliptiques E_Λ et $E_{\Lambda'}$ sont isomorphes si et seulement si il existe $\alpha \in \mathbb{C}$ tel que $\alpha\Lambda = \Lambda'$. Les classes d'isomorphisme des courbes elliptiques correspondent donc aux classes d'homothétie des réseaux de $\mathbb{C}$.*

L'étude des classes d'isomorphisme des courbes elliptiques est donc équivalente à l'étude des réseaux complexes à homothétie prés. Soit $\Lambda = [\omega_1, \omega_2]$ un tel réseau. L'homothétie

de rapport $1/\omega_1$ l'envoi sur le réseau $[1, \omega_2/\omega_1]$. Quitte à effectuer une réflexion, on peut supposer $\tau = \omega_2/\omega_1 \in \mathbb{H}$, où $\mathbb{H}$ est le *demi-plan de Poincaré* :

$$\mathbb{H} = \{z \in \mathbb{C} : Im(z) > 0\}$$

Enfin, on a le résultat suivant :

Proposition 3.1.9. *1. La formule* $\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, z\right) \mapsto \frac{az+b}{cz+d}$ *définit une action de* $\mathbb{SL}_2(\mathbb{Z})$ *sur* $\mathbb{H}$.

2. Les réseaux $\Lambda = [1, \tau]$ *et* $\Lambda' = [1, \tau']$ *sont homothétiques si et seulement si* τ *et* τ' *sont dans la même orbite sous cette action.*

Démonstration. 1. Simple calcul, en utilisant la formule : $Im\left(\frac{az+b}{cz+d}\right) = \frac{Im(z)}{|cz+d|^2}$ pour $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{SL}_2(\mathbb{Z})$.

2. On a $\alpha[1, \tau] = [1, \tau']$ si et seulement si :

$$\alpha \cdot 1 = c\tau' + d$$
$$\alpha \cdot \tau = a\tau' + b$$

avec $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{SL}_2(\mathbb{Z})$ (comme $Im(\tau') > 0,\ Im(\tau) > 0$).

□

Cette proposition nous dit que l'ensemble des orbites $Y(1) = \mathbb{SL}_2(\mathbb{Z}) \setminus \mathbb{H}$ s'identifie naturellement à l'ensemble des classes d'isomorphisme des courbes elliptiques. On dit que $Y(1)$ est l'*espace de modules* des courbes elliptiques.

3.2 Fonctions modulaires

L'ensemble $Y(1)$, qui paramétrise les courbes elliptiques à isomorphisme prés, possède lui-même une riche structure géométrique, que l'on va étudier maintenant. Son étude permet d'obtenir une grande quantité d'informations sur les courbes elliptiques.

Définition 3.2.1. *Soit* $k \in \mathbb{N}$, $\mathcal{M}(\mathbb{H})$ *le corps des fonctions méromorphes sur* $\mathbb{H}$. *La formule suivante définit une action a droite de* $\mathbb{SL}_2(\mathbb{Z})$ *sur* $\mathcal{M}(\mathbb{H})$, *appelée l'*action modulaire de poids k *:*

$$\begin{aligned} \mathcal{M}(\mathbb{H}) \times \mathbb{SL}_2(\mathbb{Z}) &\longrightarrow \mathcal{M}(\mathbb{H}) \\ f(z), \begin{pmatrix} a & b \\ c & d \end{pmatrix} &\longmapsto \frac{1}{(cz+d)^k} f\left(\frac{az+b}{cz+d}\right) \end{aligned}$$

Si $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, *on note* $f[\gamma]_k = \frac{1}{(cz+d)^k} f\left(\frac{az+b}{cz+d}\right)$.

Notation 3.2.2. On va utiliser dans la suite la notation plus pratique $f \circ \gamma(z)$ pour $f[\gamma]_0(z)$.

On peut munir $Y(1)$ d'une structure de variété analytique complexe de façon que la projection $\pi : \mathbb{H} \longrightarrow Y(1) = \mathbb{SL}_2(\mathbb{Z}) \backslash \mathbb{H}$ soit holomorphe. Avec cette structure, une fonction $f : Y(1) \longrightarrow \mathbb{C}$ est méromorphe si et seulement si $f \circ \pi$ l'est. Les fonctions méromorphes

sur $Y(1)$ correspondent donc aux fonctions méromorphes sur $\mathbb{H}$ qui sont invariantes par l'action de poids 0 de $\mathbb{SL}_2(\mathbb{Z})$.

On rajoute un point à l'infini, noté ∞, à $Y(1)$ pour en faire une surface de Riemann compacte, qu'on note $X(1)$. Pour donner des cartes autour du point à l'infini, on remarque que l'application $z \mapsto q(z) := exp(2i\pi z)$ envoi un demi plan $\{Im(z) > c\}$ sur un disque privé du centre : $\{|z| < r, z \neq 0\}$. On prolonge cette application en envoyant ∞ sur 0.

Maintenant, soit $f \in \mathcal{M}(\mathbb{H})$ invariante par l'action de poids 0 de $\mathbb{SL}_2(\mathbb{Z})$. Notons $\tilde{f}$ la fonction méromorphe correspondante sur $Y(1)$. En prenant $\gamma = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ on trouve que $f(z+1) = f(z)$, donc f s'écrit sous la forme $f(z) = \sum_{n\in\mathbb{Z}} a_n q(z)^n$, avec $a_n \in \mathbb{C}$. On a alors que $\tilde{f}$ est méromorphe sur $X(1)$ si et seulement si $f(z) = \sum_{n\geq -m} a_n q(z)^n$ pour un certain m. On dit alors que f est *méromorphe à l'infini*.

Si $k \in \mathbb{N}$ est *pair* et f est invariante par l'action de poids k de $\mathbb{SL}_2(\mathbb{Z})$, alors on a toujours $f(z+1) = f(z)$; comme on a fait pour les fonctions de poids 0, on dit que f est *méromorphe à l'infini* si elle s'écrit sous la forme $f = \sum_{n\geq -m} a_n q^n$. On dit que f est *holomorphe à l'infini* si elle s'écrit sous la forme $f = \sum_{n\geq 0} a_n q^n$.

Définition 3.2.3. *Soit $k \in \mathbb{N}$ pair. Une fonction $f : \mathbb{H} \longrightarrow \mathbb{C}$ est appelée* fonction modulaire *de poids k si :*

1. *f est méromorphe sur $\mathbb{H}$.*
2. *f est invariante par l'action de poids k de $\mathbb{SL}_2(\mathbb{Z})$.*
3. *f est méromorphe à l'infini.*

On dit que f est une forme modulaire *de poids k si elle est holomorphe sur $\mathbb{H}$ et à l'infini. Enfin, on dit que f est une* forme parabolique *si f est une forme modulaire nulle à l'infini, c'est à dire, si elle s'écrit sous la forme $f = \sum_{n\geq 1} a_n q^n$. On note $\mathcal{M}_k(\mathbb{SL}_2(\mathbb{Z}))$ l'espace vectoriel des formes modulaires de poids k, et $\mathcal{S}_k(\mathbb{SL}_2(\mathbb{Z}))$ le sous espace des formes paraboliques de poids k.*

D'après la discussion qu'on a mené, les fonctions modulaires de poids 0 correspondent aux fonctions méromorphes sur $X(1)$. On peut aussi donner une interprétation géométrique aux fonctions modulaires de poids k quelconque (pair) à l'aide des $k-$formes différentielles sur $X(1)$ (voir [7]).

Exemple 3.2.4.

- Comme $X(1)$ est compacte, les seules formes modulaires de poids 0 sont les constantes.
- Soit $k \geq 4$ pair. La série

$$G_k(\tau) = {\sum_{m,n\in\mathbb{Z}}}' \frac{1}{(m+n\tau)^k}$$

où $\sum'$ dénote la somme sur $(m,n) \neq (0,0)$, converge uniformément sur les compacts de $\mathbb{C}$ et définit une forme modulaire de poids k, qui vaut $2\zeta(k)$ à l'infini. Elle est appelée la *série d'Eisenstein de poids k.*
En général, si Λ est un réseau de $\mathbb{C}$, on définit $G_k(\Lambda) = \sum'_{\omega\in\Lambda} \frac{1}{\omega^k}$.

- Soit $g_2 = 60G_4$, $g_3 = 140G_6$. La fonction $\Delta = g_2^3 - 27g_3^2$ est une forme parabolique de poids 12. On peut montrer que $\Delta(\tau) \neq 0$ pour tout $\tau \in \mathbb{H}$.
- La fonction

$$j = 1728\,\frac{g_2^3}{\Delta}$$

est une fonction modulaire de poids 0. Elle a un pôle simple à l'infini, et son $q-$développement est de la forme $j(\tau) = \frac{1}{q(\tau)} + \sum_{n=0}^{\infty} c_n q(\tau)^n$ avec $c_n \in \mathbb{Z}$ pour

tout $n \in \mathbb{N}$. En effet, les coefficients du $q-$développement de $g_2/4\pi^4$ et de $\Delta/(2\pi)^{12}$ sont entiers, et le premier coefficient du $q-$développement de $\Delta/(2\pi)^{12}$ est 1, ce qui entraine que les coefficients du $q-$développement de $j = 1728\frac{g_2^3}{\Delta}$ sont entiers.
Si $\Lambda = [\omega_1, \omega_2]$ est un réseau quelconque, on sait que il est homothétique à un réseau de la forme $[1, \tau]$ avec $\tau \in \mathbb{H}$. On définit alors $j(\Lambda) = j(\tau)$ (c'est une bonne définition, comme j est modulaire de poids 0). On appelle $j(\Lambda)$ le *j-invariant* de la courbe E_Λ.

Proposition 3.2.5. *1. La fonction j induit un biholomorphisme de surfaces de Riemann $\tilde{j} : X(1) \longrightarrow \mathbb{P}^1(\mathbb{C})$.*

2. Le corps des fonctions méromorphes sur $X(1)$ est :

$$\mathcal{M}(X(1)) = \mathbb{C}(\tilde{j})$$

3. (Principe du $q-$développement) Si f est une fonction modulaire de poids 0 holomorphe sur $\mathbb{H}$, avec $q-$développement $f(z) = \sum_{n \geq -m} a_n q(z)^n$, alors $f \in \mathbb{C}[j]$. De plus, si $f = P(j)$, avec $P = \sum_n b_n x^n$, alors le $\mathbb{Z}-$module engendré par les b_n est inclus dans $\mathbb{Z}-$module engendré par les a_n.

Démonstration. 1. On a que $\tilde{j}$ est une fonction holomorphe non constante entre surfaces de Riemann compactes, donc elle est surjective. Soient maintenant τ et τ' dans $\mathbb{H}$ tels que $j(\tau) = j(\tau')$. On a alors $\frac{g_3(\tau)^2}{g_2(\tau)^3} = \frac{g_3(\tau')^2}{g_2(\tau')^3}$. En posant μ une racine carré du rapport $g_2(\tau)/g_2(\tau')$, on obtient $\mu^6 = g_3(\tau)^2/g_3(\tau')^2$ et donc $g_3(\tau)/g_3(\tau') = \pm\mu^3$. Quitte à changer μ en son opposé, on peut supposer que $\mu^3 = g_3(\tau)/g_3(\tau')$. En considérant λ un racine carré de μ, on a alors

$$g_2(\tau') = \lambda^{-4} g_2(\tau) = g_2(\lambda[1, \tau])$$

$$g_3(\tau') = \lambda^{-6} g_3(\tau) = g_3(\lambda[1, \tau])$$

Ceci implique que les fonctions de Weierstrass (voir exemple 3.3.3) associées aux réseaux $[1, \tau']$ et $\lambda[1, \tau]$ sont égales, et qu'ainsi $[1, \tau'] = \lambda[1, \tau]$. Finalement, la proposition 3.1.9 permet d'affirmer que τ et τ' sont dans la même orbite pour l'action de $\mathbb{SL}_2(\mathbb{Z})$ sur $\mathbb{H}$, ce qui démontre l'injectivité de $\tilde{j}$.

2. L'assertion découle de 1. et du fait que $\mathcal{M}(\mathbb{P}^1(\mathbb{C})) \cong \mathbb{C}(x)$.

3. D'après 2., on a $f \in \mathbb{C}(j)$. Comme f est holomorphe sur $\mathbb{H}$ on a $f \in \mathbb{C}[j]$. Pour montrer la dernière assertion, on procède par récurrence sur m. Pour $m = 0$, c'est triviale. Puis supposons $m > 0$. Considerons $g = f - a_{-m} j^m$. Cette fonction est modulaire, holomorphe sur $\mathbb{H}$ et on a

$$g(z) = \sum_{n \geq -m+1} d_n q(z)^n$$

où les d_n appartiennent au $\mathbb{Z}-$module engendré par les a_n, car le $q-$développement de j a coefficients entiers. Par récurrence, on conclut.

□

Le point 1. de la proposition précédente, et l'interprétation de $Y(1)$ comme espace de modules des courbes elliptiques, impliquent le résultat suivant :

Corollaire 3.2.6. *Soient $\Lambda = [1, \tau]$ et $\Lambda' = [1, \tau']$ deux réseaux. Alors les courbes elliptiques E_Λ et $E_{\Lambda'}$ sont isomorphes si et seulement si $j(\tau) = j(\tau')$.*

3.3 Algébrisation des courbes elliptiques

Dans cette section, on va montrer qu'une courbe elliptique E_Λ quelconque (qui à été définie comme étant un objet *analytique*) est isomorphe, en tant que surface de Riemann, à une courbe *algébrique* projective lisse de degré 3 définie sur $\mathbb{Q}(j(\Lambda))$, dont on va donner une equation explicite.

Définition 3.3.1. *Soit Λ un réseau de $\mathbb{C}$. Une* fonction elliptique *pour Λ est une fonction méromorphe sur $\mathbb{C}$ qui est $\Lambda-$périodique.*

Remarque 3.3.2. Chaque fonction elliptique pour un réseau Λ définit naturellement une fonction méromorphe sur le quotient $E_\Lambda = \mathbb{C}/\Lambda$, et toute fonction méromorphe sur E_Λ s'obtient de cette façon.

Exemple 3.3.3.

- Comme toute fonction holomorphe sur $\mathbb{C}$ bornée est constante, les seules fonctions elliptiques holomorphes sont constantes.
- La série de fonctions $\frac{1}{z^2}+\sum'_{\omega\in\Lambda}\frac{1}{(z-\omega)^2}-\frac{1}{\omega^2}$ converge uniformément sur les compacts de $\mathbb{C}$ qui ne rencontrent pas Λ, et définit une fonction elliptique pour Λ :

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{\omega\in\Lambda}{}' \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}$$

appelée *fonction $\wp$ de Weierstrass*. Elle a un pôle double en 0, et son développement en série de Laurent en 0 est :

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

Théorème 3.3.4. *Soit Λ un réseau de $\mathbb{C}$, $E_\Lambda = \mathbb{C}/\Lambda$ la courbe elliptique correspondante.*

1. *La fonction $\wp'_\Lambda$ vérifie l'équation différentielle suivante :*

$$\wp'_\Lambda(z)^2 = 4\wp_\Lambda(z)^3 - g_2(\Lambda)\wp_\Lambda(z) - g_3(\Lambda)$$

pour tout $z \in \mathbb{C} \setminus \Lambda$.

2. *Toute fonction $\Lambda-$elliptique est une fonction rationnelle en $\wp_\Lambda, \wp'_\Lambda$. Donc le corps des fonctions méromorphes sur E_Λ est isomorphe à $\mathbb{C}(x)[y]/(y^2 - 4x^3 + g_2(\Lambda)x + g_3(\Lambda))$.*
3. *L'application*

$$\begin{aligned}\phi_\Lambda : \mathbb{C} &\longrightarrow \mathbb{P}^2(\mathbb{C}) \\ z &\longmapsto \begin{cases}[\wp_\Lambda(z), \wp'_\Lambda(z), 1] & si\ z \notin \Lambda \\ [0,1,0] & si\ z \in \Lambda\end{cases}\end{aligned}$$

passe au quotient et définit un biholomorphisme, noté toujours ϕ_Λ, entre E_Λ et la courbe projective lisse d'équation $zy^2 = 4x^3 - g_2(\Lambda)xz^2 - g_3(\Lambda)z^3$.

4. *Toute courbe projective lisse avec équation de la forme $zy^2 = 4x^3 - axz^2 - bz^3$ s'obtient comme l'image $\phi(E_\Lambda)$ d'une courbe elliptique E_Λ.*

Démonstration. 1. La fonction $\wp'^2_\Lambda(z) - 4\wp^3_\Lambda(z) + g_2(\Lambda)\wp_\Lambda(z) + g_3(\Lambda)$ est holomorphe (regarder son développement en 0) et elliptique, donc constante, donc nulle, comme elle vaut 0 en 0.

2. On montre d'abord que toute fonction elliptique paire est une fonction rationnelle en $\wp$; pour une fonction elliptique f quelconque, on écrit $f(z) = \frac{f(z)+f(-z)}{2} + \wp'_\Lambda(z)\frac{f(z)-f(-z)}{2\wp'_\Lambda(z)}$.
3. D'après 1. ϕ est bien définie et holomorphe. On vérifie que l'application induite sur le quotient E_Λ est bijective.
4. C'est une conséquence de la surjectivité de la fonction j.

□

Lemme 3.3.5. *Soit $E = \mathbb{C}/\Lambda$ une courbe elliptique,*

1. *E est isomorphe à une courbe définie sur $\mathbb{Q}(j(E))$.*
2. *L'application ϕ_Λ définie dans le théorème 3.3.4 transforme la loi de groupe sur E en une loi de groupe* algébrique *sur $\phi(E)$.*
3. *Soient $\mathbb{C}/\Lambda$, $\mathbb{C}/\Lambda'$ deux courbes elliptiques, ϕ_Λ, $\phi_{\Lambda'}$ les applications décrites dans le théorème 3.3.4. Soit $\psi : \mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\Lambda'$ une isogénie. Il existe un unique morphisme* algébrique *$[\psi] : \phi_\Lambda(\mathbb{C}/\Lambda) \longrightarrow \phi_{\Lambda'}(\mathbb{C}/\Lambda')$ tel que le diagramme suivant commute :*

$$\begin{array}{ccc} \mathbb{C}/\Lambda & \xrightarrow{\psi} & \mathbb{C}/\Lambda' \\ \Big\downarrow{\scriptstyle \phi_\Lambda} & & \Big\downarrow{\scriptstyle \phi_{\Lambda'}} \\ \phi_\Lambda(\mathbb{C}/\Lambda) & \xrightarrow[[\psi]]{} & \phi_{\Lambda'}(\mathbb{C}/\Lambda') \end{array}$$

En plus, $[\psi]$ est un morphisme de groupes.

Démonstration. 1. Soit $j := j(E)$. Si $j \neq 0, 1728$, la courbe elliptique E' d'équation $y^2 + xy = x^3 - 36x/(j-1728) - 1/(j-1728)$ vérifie $j(E') = j(E)$, et est définie sur $\mathbb{Q}(j(E))$. Si $j = 0$ (resp. 1728) on considère $E' : y^2 + y = x^3$ (resp. $y^2 = x^3 + x$).

2. On vérifie que la somme de trois points est 0 si et seulement si ils sont alignés, ce qui permet d'écrire des formules explicites pour la loi de groupe, et donc de constater que c'est bien une loi algébrique.
3. On sait que toute isogénie est induite par passage au quotient d'une application $z \mapsto \alpha z$, avec $\alpha\Lambda \subseteq \Lambda'$. L'existence de $[\psi]$ découle donc du fait que $\wp_{\Lambda'}(\alpha(z))$ est une fonction Λ-périodique, donc une fonction rationnelle en $\wp_\Lambda, \wp'_\Lambda$ (théorème 3.3.4). L'unicité et le fait que $[\psi]$ soit un morphisme de groupes sont des conséquences immédiates de la commutativité du diagramme.

□

Le théorème 3.3.4 entraine, après un changement de variable linéaire, que tout tore complexe $E = \mathbb{C}/\Lambda$ est en fait isomorphe, en tant que variété complexe, à une courbe algébrique projective lisse dont l'équation affine est de la forme $y^2 = x^3 + ax + b$. Réciproquement, toute courbe projective lisse sur $\mathbb{C}$ d'équation $y^2 = x^3 + ax + b$ est isomorphe à un tore $\mathbb{C}/\Lambda$ pour un certain réseau Λ. On peut donc donner la définition algébrique suivante de courbe elliptique, qui est valable sur n'importe quel corps de caractéristique différente de 2, 3.

Définition 3.3.6. *Soit K un corps de caractéristique différente de 2, 3. Une* courbe elliptique *sur K est une courbe projective d'équation affine*

$$y^2 = x^3 + ax + b$$

avec $a, b \in K$, et $\Delta = -4a^3 - 27b^2 \neq 0$.

Remarque 3.3.7. On vérifie par un calcul explicit que la condition $\Delta \neq 0$ équivaut au fait que la courbe soit lisse sur $\bar{K}$.

Le lemme 3.3.5 nous dit que toute courbe elliptique E est isomorphe à un courbe définie sur le corps $K = \mathbb{Q}(j(E))$. Lorsque $j(E)$ est un nombre algébrique, on peut donc identifier E à une courbe définie sur le corps des nombres K, ce qui permet en particulier de considérer, pour chaque idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$, la *réduction modulo* $\mathfrak{p}$ de la courbe. C'est une courbe définie sur le corps fini $\mathcal{O}_K/\mathfrak{p}$ dont l'équation s'obtient en réduisant modulo $\mathfrak{p}$ les coefficients de l'équation de E. On va maintenant étudier quelques propriétés des courbes elliptiques définies sur les corps finis.

Notation 3.3.8. Si E est une courbe elliptique définie sur un corps $K \subseteq L$, $\sigma : L \longrightarrow M$ un morphisme de corps, on note $\sigma(E)$ la courbe dont l'équation s'obtient en appliquant σ à chaque coefficient de l'équation de E.

3.4 Courbes elliptiques sur les corps finis

On va énoncer les propriétés de base des courbes elliptiques définies sur les corps finis, qui seront utilisées dans la suite. Voir [13] pour une exposition plus détaillée, comprenant les preuves des résultats énoncés. Pour simplifier la tractation, dans cette section tous les corps seront supposés parfaits et de caractéristique différente de 2, 3.

3.4.1 Propriétés générales

Soit E une courbe elliptique définie sur un corps K, d'équation affine :

$$y^2 = x^3 + ax + b$$

avec $\Delta = -4a^3 - 27b^2 \neq 0$. Le corps $K(E) = K(x, y)/(y^2 - x^3 - ax - b)$ est appelé le *corps des fonctions rationnelles* sur E.

Soient E, E' deux courbes elliptiques définies sur K. Un morphisme algébrique non constant $\phi : E \longrightarrow E'$ qui envoi 0_E sur $0_{E'}$ est appelé *isogénie*. Il induit un morphisme de corps :

$$\begin{aligned} \phi^* : K(E') &\longrightarrow K(E) \\ f &\mapsto f \circ \phi \end{aligned}$$

L'extension de corps $K(E)/\phi^*(K(E'))$ est finie. Son degré est appelé le *degré* de l'isogénie ϕ. Si $\psi : E' \longrightarrow E''$ est une isogénie, on a $deg(\psi \circ \phi) = deg(\psi)deg(\phi)$. On a que ϕ est un isomorphisme si et seulement si $deg(\phi) = 1$. On dit que ϕ est *séparable* (resp. *inséparable*, *purement inséparable*) si l'extension $K(E)/\phi^*(K(E'))$ l'est.

Remarque 3.4.1. On peut vérifier que, dans le cas $K = \mathbb{C}$, les définitions d'isogénie et degré d'une isogénie coïncident avec celles qu'on a donné dans la section 3.1.

Exemple 3.4.2 (Le morphisme de Frobenius)**.** Soit K un corps de caractéristique p, $F : K \longrightarrow K$ le morphisme de Frobenius $x \mapsto x^p$. Soit E une courbe elliptique définie sur K :

$$E : y^2 = x^3 + ax + b$$

Notons $E^{(p)}$ la courbe elliptique d'équation $y^2 = x^3 + F(a)x + F(b)$. On a une isogénie, notée toujours F :

$$\begin{aligned} F : \quad E &\longrightarrow E^{(p)} \\ (x, y) &\longmapsto (x^p, y^p) \\ 0 &\longmapsto 0 \end{aligned}$$

appelée le *morphisme de Frobenius*. C'est une isogénie purement inséparable de degré p.

On note $\Omega(E)$ le $\bar{K}$-espace vectoriel des formes différentielles méromorphes sur E, et $\Omega^{hol}(E)$ le sous espace des formes différentielles *holomorphes* (c'est à dire, sans zéros ni pôles). On peut montrer que $\Omega^{hol}(E)$ est un $\bar{K}-$espace vectoriel de dimension 1, engendré par la forme différentielle :

$$\omega = \frac{\mathrm{d}x}{y}$$

appelée la différentielle invariante de E (parce que elle est invariante par translation).

Remarque 3.4.3. Soit Λ un réseau de $\mathbb{C}$, $E = \mathbb{C}/\Lambda$,

$$\begin{aligned} \phi_\Lambda : \mathbb{C}/\Lambda &\longrightarrow \mathbb{P}^2(\mathbb{C}) \\ z &\longmapsto [\wp_\Lambda(z), \wp'_\Lambda(z), 1] \quad \text{si } z \neq 0 \\ 0 &\longmapsto [0, 1, 0] \end{aligned}$$

On a alors :

$$\phi_\Lambda^*(\omega) = \phi_\Lambda^* \left(\frac{\mathrm{d}x}{y} \right) = \frac{\mathrm{d}\wp(z)}{\wp'(z)} = dz$$

Le lemme suivant donne deux conditions différentes pour la séparabilité d'une isogénie.

Lemme 3.4.4. *Soient E, E' deux courbes elliptiques définies sur un corps K de caractéristique p. Soit $\phi : E \longrightarrow E'$ une isogénie. Les propriétés suivantes sont équivalentes :*

1. *ϕ est inséparable.*
2. *$\phi^*(\omega') = 0$, où ω' est la différentielle invariante de E'.*
3. *ϕ se factorise par le Frobenius, c'est à dire, il existe une isogénie $\tau : E^{(p)} \longrightarrow E'$ telle que le diagramme suivant commute :*

$$\begin{array}{ccc} E & \xrightarrow{\phi} & E' \\ \downarrow{\scriptstyle F} & \nearrow{\scriptstyle \tau} & \\ E^{(p)} & & \end{array}$$

Démonstration. Voir [13]. □

3.4.2 Réduction modulo $\mathfrak{p}$

Soit K un corps de nombres, et soit E une courbe elliptique définie sur K, d'équation affine :

$$y^2 = x^3 + ax + b$$

Quitte à changer coordonnées, on peut se ramener au cas où $a, b \in \mathcal{O}_K$. Choisissons donc un *modèle de E défini sur* $\mathcal{O}_K$. Soit $\mathfrak{p}$ un idéal premier non nul de $\mathcal{O}_K$. La *reduction modulo* $\mathfrak{p}$ de E est la courbe $\overline{E}$ définie sur le corps fini $\mathcal{O}_K/\mathfrak{p}$ d'équation :

$$y^2 = x^3 + \bar{a}x + \bar{b}$$

Si $P = [x, y, z]$ est un point de E défini sur K, la réduction modulo $\mathfrak{p}$ de P, $\bar{P} = [\bar{x}, \bar{y}, \bar{z}]$, est un point de $\overline{E}$. De la même façon, on peut réduire modulo $\mathfrak{p}$ toute isogénie $\phi : E \longrightarrow E'$ lorsque E, E' et ϕ sont définies sur K, ainsi que les formes différentielles définies sur K. On dit que le premier $\mathfrak{p}$ de $\mathcal{O}_K$ est un premier de *bonne réduction* pour E si la courbe réduite $\overline{E}$ est une courbe elliptique. C'est équivalent au fait que $\mathfrak{p}$ ne divise pas le discriminant $\Delta = -4a^3 - 27b^2$. Un premier qui n'est pas de bonne réduction pour E est dit de *mauvaise réduction* pour E.

Remarque 3.4.5. Les notions qu'on vient d'introduire, notamment la notion de bonne et mauvaise réduction, *dépendent du modèle choisi pour la courbe E*. On pourrait donner des définitions plus intrinsèques à l'aide du langage des schémas, mais on ne va pas le faire ici. Le point de vue naïf qu'on a adopté sera suffisant pour nos applications.

Le lemme suivant résume les propriétés fondamentales de la réduction modulo $\mathfrak{p}$ dont on va se servir. On remarquera que l'énoncé 1., très important, est vrai pour *n'importe quel modèle* de la courbe E.

Lemme 3.4.6. *Soient E, E' deux courbes elliptiques définies sur un corps de nombres K.*

1. *Il n'y a qu'un nombre* fini *de premiers de mauvaise réduction pour E.*
2. *Soit $\phi : E \longrightarrow E'$ une isogénie définie sur K, et $\overline{\phi}$ sa réduction modulo un premier $\mathfrak{p}$ de bonne réduction pour E et E'. Alors $deg(\phi) = deg(\overline{\phi})$.*
3. *Soit $\mathfrak{p}$ un premier de bonne réduction pour E, et N un entier premier avec $p = \mathfrak{p} \cap \mathbb{Z}$. Alors la restriction de la réduction modulo $\mathfrak{p}$ aux points de N-torsion :*

$$\begin{aligned} E[N] &\longrightarrow \bar{E}[N] \\ [x, y, z] &\mapsto [\bar{x}, \bar{y}, \bar{z}] \end{aligned}$$

est injective.

Démonstration. Voir [13]. □

3.5 La fonction de Weber

Notation 3.5.1. On note $Aut(E)$ le groupe des automorphismes de la courbe elliptique E.

Proposition 3.5.2. *Soit E une courbe elliptique, $E = \mathbb{C}/\Lambda$.*

1. *Si E est isomorphe à $E_i = \mathbb{C}/[1, i]$ alors $Aut(E) \cong \mathbb{Z}/4\mathbb{Z}$*
2. *Si E est isomorphe à $E_\rho = \mathbb{C}/[1, \rho]$, où $\rho = exp(2i\pi/3)$, alors $Aut(E) \cong \mathbb{Z}/6\mathbb{Z}$*
3. *Dans les autres cas, on a $Aut(E) \cong \mathbb{Z}/2\mathbb{Z}$*

Démonstration. Calcul direct, en utilisant l'identification

$$\begin{aligned} \{\text{automorphismes } \phi : E_\Lambda \longrightarrow E_\Lambda\} &\longleftrightarrow \{\alpha \in \mathbb{C},\ \alpha\Lambda = \Lambda\} \\ \phi &\longmapsto \alpha_\phi \end{aligned}$$

□

Définition 3.5.3. *Soit $E = E_\Lambda$ une courbe elliptique. La* fonction de Weber *de E est la fonction :*

$$f_E(z) = \begin{cases} \frac{g_2(\Lambda)g_3(\Lambda)}{\Delta(\Lambda)}\wp_\Lambda(z) & si\ g_2(\Lambda)g_3(\Lambda) \neq 0 \\ \frac{g_3(\Lambda)}{\Delta(\Lambda)}\wp_\Lambda^3(z) & si\ g_2(\Lambda) = 0 \\ \frac{g_2(\Lambda)^2}{\Delta(\Lambda)}\wp_\Lambda^2(z) & si\ g_3(\Lambda) = 0 \end{cases}$$

Remarque 3.5.4. On vérifie la relation $f_{E_\Lambda}(z) = f_{E_{\alpha\Lambda}}(\alpha z)$, donc la fonction de Weber est invariante par isomorphisme. Dans le cas $g_2(\Lambda)g_3(\Lambda) \neq 0$, si l'on voit E comme une courbe projective comme dans le théorème 3.3.4, alors $f_E(z)$ est la première coordonnée du point $\phi_\Lambda(z)$, renormalisée de façon que cela soit invariante par isomorphisme.

Lemme 3.5.5. *Soit f_E la fonction de Weber d'une courbe elliptique E, et soient $P, Q \in E$. Alors on a $f_E(P) = f_E(Q)$ si et seulement s'il existe un automorphisme de E qui envoi P sur Q.*

Démonstration. C'est une vérification directe en utilisant la Proposition 3.5.2 et l'invariance de f_E par isomorphisme (qui permet de se ramener à l'étude de E_i, E_ρ). □

3.6 Le polynôme modulaire

Notation 3.6.1. On dit que $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z})$ est *primitive* si $(a, b, c, d) = 1$. On note Δ_n l'ensemble des matrices de déterminant $n \in \mathbb{N}$ dans $M_2(\mathbb{Z})$, et Δ_n^* le sous ensemble de Δ_n formé des matrices primitives.

Lemme 3.6.2. *$\mathbb{SL}_2(\mathbb{Z})$ agit à gauche par multiplication sur Δ_n^*. L'ensemble*

$$C(n) = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \Delta_n^* : ad = n, 0 < a, 0 \leq b < d \right\}$$

est un système complet de représentants des orbites de cette action.

Démonstration. On prouve d'abord que pour tout $\sigma \in \Delta_n^*$ il existe $\gamma \in C(n)$ dans l'orbite de σ. Soit $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Si on note $h = \text{pgcd}(a, c)$, on a $a = ha'$ e $c = hc'$ avec $\text{pgcd}(a', c') = 1$. Par le lemme de Bezout, il existent $x, y \in \mathbb{Z}$ avec $xa' + yc' = 1$. On déduit que la matrice

$$\delta = \begin{pmatrix} x & y \\ -c' & a' \end{pmatrix}$$

appartient à $\mathbb{SL}_2(\mathbb{Z})$ et que le produit $\delta\sigma$ est de la forme $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$. Il suffit de démontrer le résultat pour les matrices de cette forme. Soit donc σ comme avant et on suppose de plus que $c = 0$. Quitte à multiplier par $-\text{Id}$, on peut supposer que $a, d > 0$. Soit b' l'unique entier congru à $b \pmod d$ et appartenant à $\{0, \ldots, d-1\}$ et soit r tel que $rd = b' - b$. On à alors :

$$\begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} a & b' \\ 0 & d \end{pmatrix}$$

On voit que cette dernière matrice appartient bien à $C(n)$.

Maintenant on prouve que si $\sigma, \sigma' \in C(n)$ et $\sigma' = \gamma\sigma$ pour un certain $\gamma \in \mathbb{SL}_2(\mathbb{Z})$, alors $\gamma = \text{Id}$. Soient donc :

$$\sigma = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}, \sigma' = \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix}, \gamma = \begin{pmatrix} x & y \\ z & w \end{pmatrix}$$

En regardant le produit $\gamma\sigma$, on déduit que $z = 0$ et donc $x = w = \pm 1$. Comme $d, d' > 0$ on trouve que $x = w = 1$ et ainsi $d = d'$. On a $b' = b + yd$, mais comme $b, b' \in \{0, \dots, d-1\}$ la seule possibilité pour y est $y = 0$. □

Définition 3.6.3. *Soit $n \in \mathbb{N}$. Le* n-ieme polynôme modulaire *est le polynôme*

$$\Phi_n(X) = \prod_{\gamma \in \mathcal{L}} (X - j \circ \gamma)$$

où $\mathcal{L}$ est un ensemble quelconque de représentants des orbites de $\mathbb{SL}_2(\mathbb{Z}) \setminus \Delta_n^*$.

Remarque 3.6.4. Comme j est $\mathbb{SL}_2(\mathbb{Z})$-invariante, la définition ne dépend pas du choix de $\mathcal{L}$.

Soit $\sigma = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \Delta_n^*$. On explicite le q-développement de $j \circ \sigma$. On rappelle que :

$$j(\tau) = \frac{1}{q} + \sum_{k=0}^{\infty} c_k q^k$$

On a aussi $q(\sigma\tau) = e^{\frac{2i\pi(a\tau+b)}{d}} = e^{\frac{2i\pi b}{d}} q(\tau)^{a/d}$; en posant $\zeta_n = e^{\frac{2i\pi}{n}}$ on obtient $q(\sigma\tau) = \zeta_n^{ab}(q^{1/n})^{a^2}$. Ainsi on en déduit le développement suivant :

$$j \circ \sigma(\tau) = j(\sigma\tau) = \frac{\zeta_n^{-ab}}{(q^{1/n})^{a^2}} + \sum_{k=0}^{\infty} c_k \zeta_n^{abk} (q^{1/n})^{a^2 k} \tag{3.6.1}$$

Lemme 3.6.5. *Les coefficients de $\Phi_n(X)$ sont des polynômes en j à coefficients dans $\mathbb{Z}$.*

Démonstration. Les coefficients de $\Phi_n(X)$ sont des fonctions symétriques des $j \circ \gamma$, $\gamma \in \mathcal{L}$, donc ils sont holomorphes et $\mathbb{SL}_2(\mathbb{Z})$-invariantes, donc sont des polynômes en j à coefficients dans $\mathbb{Z}[\zeta_n]$ (regarder le $q-$développement de $j \circ \gamma$ et utiliser la Proposition 3.2.5). Enfin, ils sont $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})-$invariantes. □

On peut donc voir $\Phi_n(X)$ comme un polynôme en les deux variables X et j, qu'on note $\Phi_n(X, j)$. La proposition suivante, très importante, décrit les propriétés fondamentales du polynôme $\Phi_n(X, j)$.

Proposition 3.6.6.

1. *$\Phi_n(X, j)$ est irréductible dans $\mathbb{C}(j)$.*
2. *$\Phi_n(X, j) = \Phi_n(j, X)$*
3. *Si n n'est pas un carré, alors $\Phi_n(j, j) \in \mathbb{Z}[j]$ est un polynôme de degré > 1 dont le coefficient dominant est ± 1.*
4. *Si p est un nombre premier, on a la congruence dite "de Kronecker" :*

$$\Phi_p(X, j) \equiv (X^p - j)(X - j^p) \pmod{p\mathbb{Z}[X, j]}$$

Démonstration. 1) On note $\mathcal{M}$ l'ensemble de fonctions méromorphes sur $\mathbb{H}$. On rappelle l'action de $\mathbb{SL}_2(\mathbb{Z})$ sur $\mathcal{M}$ de poids 0, définie pour tout $\gamma \in \mathbb{SL}_2(\mathbb{Z})$ par $f[\gamma]_0(\tau) = f(\gamma\tau)$. Soit $\sigma \in \Delta_n^*$ et soit $\gamma \in \mathbb{SL}_2(\mathbb{Z})$. On a en particulier

$$(j \circ \sigma)[\gamma]_0 = j \circ \sigma\gamma \tag{3.6.2}$$

Soit $\mathcal{L} = \{\sigma_1, \dots, \sigma_N\}$ un ensemble quelconque de représentants des orbites de $\mathbb{SL}_2(\mathbb{Z}) \setminus \Delta_n^*$. On démontre que l'action de $\mathbb{SL}_2(\mathbb{Z})$ par automorphismes sur $\mathbb{C}(j, j \circ \sigma_1, \dots, j \circ \sigma_N)/\mathbb{C}(j)$

permute transitivement les $j\circ\sigma_i$ et fixe $\mathbb{C}(j)$. Cette dernière assertion est triviale. Pour voir que l'action permute transitivement les $j\circ\sigma_i$, vue la relation (3.6.2), il suffit de démontrer que $\Gamma\sigma_1\Gamma = \Delta_n^*$, où $\Gamma = \mathbb{SL}_2(\mathbb{Z})$. Soit G un $\mathbb{Z}$-module libre de rang 2, et $\{w_1, w_2\}$ une base. Soit $\sigma_1 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ et $H \subset G$ le sous-module de base $\{aw_1 + bw_2, cw_1 + dw_2\}$. Par le théorème de diviseurs élémentaires, il existe une base $\{v_1, v_2\}$ de G telle que $\{e_1v_1, e_2v_2\}$ soit une base de H avec $e_1, e_2 \in \mathbb{Z}$ et $e_1|e_2$. Donc il existent deux matrices $\gamma, \gamma' \in \mathbb{GL}_2(\mathbb{Z})$ telles que

$$\gamma\sigma_1\gamma' = \begin{pmatrix} e_1 & 0 \\ 0 & e_2 \end{pmatrix}$$

Quitte à remplacer v_1 par $-v_1$ on peut supposer que $\gamma, \gamma' \in \mathbb{SL}_2(\mathbb{Z})$. Comme σ_1 est primitive, il en est de même du produit (a gauche ou à droit) par un élément de $\mathbb{SL}_2(\mathbb{Z})$. On en déduit que $e_1 = 1$ et donc $e_2 = n$. Comme σ_1 était arbitraire, on trouve que

$$\Gamma \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix} \Gamma = \Delta_n^*$$

et de cela on conclut que $\Gamma\sigma_1\Gamma = \Delta_n^*$. Ainsi l'action de Γ permute transitivement les racines de $\Phi_n(X)$ sur $\mathbb{C}(j)$. Le résultat découle.

2) On a par définition

$$\Phi_n(X, j) = \prod_{\sigma\in C(n)} (X - j\circ\sigma)$$

Soit $\sigma = \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix}$ et $\sigma' = \begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix}$. On a $\Phi_n(j(\sigma\tau), j(\tau)) = 0$ pour tout $\tau \in \mathbb{H}$, i.e. $\Phi_n(j\left(\frac{\tau}{n}\right), j(\tau))$ pour tout $\tau \in \mathbb{H}$, ce qui entraine que $\Phi_n(j(\tau), j(n\tau)) = 0$ pour tout $\tau \in \mathbb{H}$. On trouve ainsi que $j \circ \sigma'$ est une racine du polynôme $\Phi_n(j, X)$ et aussi, par définition, du polynôme $\Phi_n(X, j)$. Comme celui-ci est le polynôme minimale de $j \circ \sigma'$ sur $\mathbb{Q}(j)$ on déduit que $\Phi_n(X, j)$ divise $\Phi_n(j, X)$ dans $\mathbb{Q}(j)[X]$. Par le lemme de Gauss, $\Phi_n(X, j)$ divise $\Phi_n(j, X)$ dans $\mathbb{Z}[j][X]$, c'est-à-dire qu'il existe un polynôme $g(X, j) \in \mathbb{Z}[X, j]$ tel que

$$\Phi_n(j, X) = g(X, j)\Phi_n(X, j)$$

En échangeant les variables, on obtient

$$\Phi_n(j, X) = g(X, j)g(j, X)\Phi_n(j, X)$$

Par conséquence, $g(X, j)$ est constante et vaut ± 1. Si $g(X, j) = -1$ on aurait $\Phi_n(j, j) = -\Phi_n(j, j)$, et donc $\Phi(j, j) = 0$. On aurait que j est une racine de $\Phi_n(X, j)$, en contradiction avec l'irreductibilité de $\Phi_n(X, j)$ sur $\mathbb{C}(j)$.

3) Supposons que n n'est pas un carré. Le fait que le degré de $\Phi_n(j, j)$ soit supérieur à 1 est évident. Pour voir qu'est-ce que c'est le coefficient dominant, il suffit d'étudier le coefficient de la plus grande puissance négative dans le q-développement de $\Phi_n(j, j)$. Soit $\sigma = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \Delta_n^*$. On a le q-développement suivante :

$$j(\tau) - j(\sigma\tau) = \frac{1}{q} - \frac{\zeta_n^{-ab}}{q^{a/d}} + \sum_{k=0}^{\infty} d_k(q^{1/m})^k$$

pour certains coefficients d_k. Comme n n'est pas un carré, on a $a \neq d$. Par conséquence, le coefficient de la plus grande puissance négative de q est soit 1 soit $-\zeta_n^{-ab}$, selon le cas : en tout cas, il s'agit d'une racine de l'unité. Comme $\Phi_n(j,j)$ est un produit de termes de la forme $j(\tau) - j(\sigma\tau)$, le coefficient de la plus grande puissance négative de q dans le q-développement est une racine de l'unité. Puisque le polynôme $\Phi_n(j,j)$ a coefficients entiers, on conclut que le terme dominant est 1 ou -1.

4) Fixons d'abord comme ensemble de representants de $\mathbb{SL}_2(\mathbb{Z})\backslash\Delta_p^*$ le suivant :

$$\sigma_i = \begin{pmatrix} 1 & i-1 \\ 0 & p \end{pmatrix} \qquad \text{pour } i = 1, \ldots, p$$

$$\sigma_{p+1} = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$$

Soit $A(q)$ une série a coefficients entiers qui définit une fonction méromorphe sur $\mathbb{H}$. On note $\zeta_p = e^{\frac{2i\pi}{p}}$. On a les congruences suivantes :

$$\begin{aligned} A(\sigma_i\tau) = A(q^{1/p}\zeta_p^i) \equiv A(q^{1/p}) \pmod{1-\zeta_p} \qquad i = 1, \ldots, p \\ A(\sigma_{p+1}\tau) = A(q^p) \end{aligned} \tag{3.6.3}$$

En travaillant dans l'anneau $\mathbb{Z}[\zeta_p, X][[q^{1/p}]]$, on a

$$\begin{aligned} \prod_{i=1}^{p+1}(X - j(\sigma_i q)) &= \left(\prod_{i=1}^{p}(X - j(\sigma_i q))\right)(X - j(\sigma_{p+1}q)) \\ &\equiv (X - j(q^{1/p}))^p (X - j(q^p)) \pmod{1-\zeta_p} \\ &\equiv (X^p - j(q))(X - j(q)^p) \pmod{1-\zeta_p} \\ &\equiv (X^p - j(q))(X - j(q)^p) \pmod{p} \end{aligned}$$

où la dernière égalité découle du fait que $j(q)$ a coefficients entiers et $(p) = (1-\zeta_p) \cap \mathbb{Z}$. Ainsi on a que les coefficients du polynôme

$$\left(\prod_{i=1}^{p+1}(X - j(\sigma_i q))\right) - (X^p - j(q))(X - j(q)^p)$$

sont des fonctions modulaires dont le $q-$développement a ses coefficients dans $p\mathbb{Z}$. Par le principe de $q-$développement, en écrivant les coefficients de ce polynôme comme polynômes en j, on voit que ces coefficients sont divisibles par p, ce qui donne la congruence. □

Etant donné $\tau \in \mathbb{C}$, on peut considérer la spécialisation $\Phi_n(X, j(\tau)) \in \mathbb{Z}[j(\tau)][X]$ du polynôme $\Phi_n(X,j) \in \mathbb{Z}[j,X]$. Les racines de $\Phi_n(X, j(\tau))$ dans $\mathbb{C}$ s'interprètent de la façon suivante, dans le langage des courbes elliptiques :

Proposition 3.6.7. *$j(\tau')$ est une racine de $\Phi_n(X, j(\tau))$ si et seulement s'il existe une isogénie $\phi : E_{[1,\tau']} \longrightarrow E_{[1,\tau]}$ de degré n dont le noyau est cyclique.*

Démonstration. $\Phi_n(X, j(\tau)) = \prod_{\gamma\in\mathcal{L}}(X - j\circ\gamma(\tau))$, donc les racines de $\Phi_n(X, j(\tau))$ sont les nombres complexes $j\circ\gamma(\tau)$, avec $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Delta_n^*$. Maintenant, il existe une isogénie

$\phi : E_{[1,\tau']} \longrightarrow E_{[1,\tau]}$ dont le noyau est cyclique de cardinal n si et seulement si $E_{[1,\tau']}$ est isomorphe à E_Λ avec $\Lambda \subseteq [1,\tau]$ sous-réseau tel que $[1,\tau]/\Lambda$ soit cyclique de cardinal n. Pour conclure, il suffit de remarquer que $\Lambda = [a+b\tau, c+d\tau]$ est un sous-réseau de $[1,\tau]$ tel que $[1,\tau]/\Lambda$ est cyclique de degré n si et seulement si $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Delta_n^*$ (conséquence immédiate du théorème des diviseurs élémentaires). □

4 Multiplication complexe

4.1 Définition et propriétés fondamentales

Soit $\Lambda = [1,\tau]$ un réseau dans $\mathbb{C}$. On étudie plus en détaille l'ensemble des endomorphismes de E_Λ, qu'on note $End(E_\Lambda)$ ou aussi $End(\Lambda)$. C'est un anneau avec les opérations de somme ponctuelle des endomorphismes et de composition d'endomorphismes. On rappelle que, en conséquence du lemme 3.1.6, on a une bijection :

$$\begin{aligned} \{\text{endomorphismes } \phi : E_\Lambda \longrightarrow E_\Lambda\} &\longleftrightarrow \{\alpha \in \mathbb{C},\ \alpha\Lambda \subseteq \Lambda\} \\ \phi &\longmapsto \alpha_\phi \end{aligned}$$

on peut donc identifier $End(\Lambda)$ à un sous anneau de $\mathbb{C}$. Avec cette identification, on a manifestement $\mathbb{Z} \subseteq End(\Lambda)$.

Proposition 4.1.1. *Soit $\Lambda = [1,\tau]$ un réseau dans $\mathbb{C}$.*

1. *Si $\mathbb{Q}(\tau)/\mathbb{Q}$ est une extension quadratique imaginaire, alors $End(\Lambda)$ est un ordre dans l'anneau des entiers algébriques de $K = \mathbb{Q}(\tau)$, c'est à dire, il est un sous anneau de $\mathcal{O}_K$ de rang 2 sur $\mathbb{Z}$.*
2. *Dans tous les autres cas, $End(\Lambda) \cong \mathbb{Z}$.*

Démonstration. On utilise l'identification $End(\Lambda) = \{\alpha \in \mathbb{C} : \alpha\Lambda \subseteq \Lambda\}$ La condition $\alpha[1,\tau] \subseteq [1,\tau]$ s'écrit :

$$\begin{aligned} \alpha \cdot 1 &= a\tau + b \\ \alpha \cdot \tau &= c\tau + d \end{aligned}$$

avec $a,b,c,d \in \mathbb{Z}$. On a donc : $\tau = \frac{c\tau+d}{a\tau+b} \Rightarrow a\tau^2 + (b-c)\tau - d = 0$. Si $\alpha \notin \mathbb{Z}$ on a $a \neq 0$, donc $\mathbb{Q}(\tau)/\mathbb{Q}$ est une extension de degré 2, qui est imaginaire comme $\tau \in \mathbb{C} \setminus \mathbb{R}$. En plus dans ce cas $\alpha - b = a\tau \in End(\Lambda)$ est un entier algébrique, donc α l'est, ce qui donne $End(\Lambda) \subseteq \mathcal{O}_K$. Donc $\mathbb{Z} \subseteq End(\Lambda) \subseteq \mathcal{O}_K$ et la première inclusion est stricte, donc $End(\Lambda)$ a rang 2 sur $\mathbb{Z}$. □

Définition 4.1.2. *On dit que la courbe elliptique E a* multiplication complexe *si $End(E)$ contient strictement $\mathbb{Z}$.*

Pour simplifier, on va étudier dans la suite les courbes elliptiques à multiplication complexe dont l'anneau des endomorphismes est l'anneau des entiers algébriques $\mathcal{O}_K$ d'un corps quadratique imaginaire K. La théorie générale est développée dans [5].

Si on plonge un tel corps K dans $\mathbb{C}$, tout idéal fractionnaire $\mathfrak{a}$ de $\mathcal{O}_K$ devient un réseau dans $\mathbb{C}$. On lui associe la courbe elliptique $\mathbb{C}/\mathfrak{a}$, notée $E_\mathfrak{a}$. Comme $\mathfrak{a}$ est un idéal fractionnaire de $\mathcal{O}_K$ on a $\mathcal{O}_K\mathfrak{a} \subseteq \mathfrak{a}$, donc $\mathcal{O}_K \subseteq End(E_\mathfrak{a})$. Cette dernière inclusion est donc une égalité, comme on a vu que $End(E_\mathfrak{a}) \subseteq \mathcal{O}_K$.

Réciproquement, si $\Lambda = [1,\tau]$ est tel que $End(E_\Lambda) = \mathcal{O}_K$ alors Λ est un $\mathbb{Z}-$module libre de rang 2 inclus dans K tel que $\mathcal{O}_K\Lambda \subseteq \Lambda$, donc Λ est un idéal fractionnaire de K. On a presque montré le théorème fondamental suivant :

Théorème 4.1.3. *Soit K un corps quadratique imaginaire, $Ell(K)$ l'ensemble des classes d'isomorphisme de courbes elliptiques dont l'anneau des endomorphismes est isomorphe à $\mathcal{O}_K$.*

1. *Si $\mathfrak{a}$ est un idéal fractionnaire de K, alors $E_\mathfrak{a}$ est un courbe elliptique telle que $End(E_\mathfrak{a}) \cong \mathcal{O}_K$.*
2. *$E_\mathfrak{a}$ est isomorphe à $E_\mathfrak{b}$ si et seulement si $\mathfrak{a} = \lambda\mathfrak{b}$ avec $\lambda \in K^*$.*
3. *L'application*

$$\begin{aligned} Cl(\mathcal{O}_K) = \mathcal{I}_K/\mathcal{P}_K &\longrightarrow Ell(K) \\ \mathfrak{a} &\longmapsto E_\mathfrak{a} \end{aligned}$$

est une bijection.

Démonstration. On a déjà montré 1. L'assertion 2. découle du fait que deux courbes elliptiques sont isomorphes si et seulement si les réseaux correspondantes sont homothétiques. D'après 2., l'application dans 3. est bien définie et injective ; la surjectivité est conséquence de ce qu'on a dit avant d'énoncer le théorème. □

Ce résultat crucial nous donne une représentation concrète d'une courbe elliptique dont l'anneau des endomorphismes est isomorphe à $\mathcal{O}_K$, comme quotient $\mathbb{C}/\mathfrak{a}$. Il permet d'établir une relation très stricte entre l'ensemble $Ell(K)$ (objet géométrique) et l'anneau $\mathcal{O}_K$ (objet algébrique). On peut donc exploiter les propriétés de $\mathcal{O}_K$ pour étudier $Ell(K)$. Cette idée permet d'obtenir le résultat non trivial suivant :

Proposition 4.1.4. *Soit $E_\mathfrak{a}$ une courbe elliptique avec multiplication complexe par l'anneau des entiers $\mathcal{O}_K$ d'un corps quadratique imaginaire K. Alors $j(\mathfrak{a})$ est algébrique sur $\mathbb{Q}$, de degré inférieur ou égal à $|Cl(\mathcal{O}_K)|$.*

Démonstration. Soit σ un automorphisme de $\mathbb{C}$. En identifiant $E_\mathfrak{a}$ avec une courbe projective comme dans le théorème 3.3.4 on obtient un isomorphisme évident $End(E_\mathfrak{a}) \cong End(\sigma(E_\mathfrak{a}))$, donc $End(\sigma(E_\mathfrak{a})) \cong \mathcal{O}_K$. Le théorème 4.1.3 nous dit que $\sigma(E_\mathfrak{a})$ est isomorphe à $E_\mathfrak{b}$ pour un certain idéal fractionnaire $\mathfrak{b}$ de K, qu'on peut choisir dans un ensemble (fini) de représentants des classes d'idéaux de K. On a donc :

$$\sigma(j(\mathfrak{a})) = \sigma(j(E_\mathfrak{a})) = j(\sigma(E_\mathfrak{a})) = j(\mathfrak{b})$$

$j(\mathfrak{a})$ a alors au plus $|Cl(\mathcal{O}_K)|$ conjugués, ce qui montre le théorème. □

En fait, en utilisant astucieusement les propriétés du polynôme modulaire, on peut faire mieux. Le résultat suivant est l'analogue du point 1. du théorème 2.4.3. Les notations sont le mêmes que dans la proposition 4.1.4.

Théorème 4.1.5. *$j(\mathfrak{a})$ est un entier algébrique.*

Démonstration. Soit $\alpha \in \mathcal{O}_K$ tel que $n = N(\alpha)$ est sans carrés. Alors on vérifie que $\alpha\mathfrak{a}$ est un sous-réseau de $\mathfrak{a}$ cyclique primitif d'indice n. La proposition 3.6.7 implique que :

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

donc

$$\Phi_n(j(\mathfrak{a}), j(\mathfrak{a})) = 0$$

Mais n n'es pas un carré, donc pour la proposition 3.6.6, $\Phi_n(j, j) \in \mathbb{Z}[j]$ est unitaire, donc $j(\mathfrak{a})$ est un entier algébrique. □

Exemple 4.1.6. On considère $K = \mathbb{Q}(\sqrt{-163})$. Son anneau des entiers $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{-163}}{2}\right]$ est principal, c'est à dire $|Cl(\mathcal{O}_K)| = 1$. La proposition 4.1.4 entraine que $j\left(\frac{1+\sqrt{-163}}{2}\right)$ est algébrique de degré 1 sur $\mathbb{Q}$: il est donc dans $\mathbb{Q}$. D'après le théorème 4.1.5, on en déduit finalement que $j\left(\frac{1+\sqrt{-163}}{2}\right) \in \mathbb{Z}$. En considérant le q-développement de j (voir exemple 3.2.4), on trouve que :

$$j\left(\frac{1+\sqrt{-163}}{2}\right) = -e^{\pi\sqrt{163}} + 744 - \sum_{k\geq 1} c_k e^{-k\pi\sqrt{163}}$$

Un calcul approché de la somme restante rend un résultat de l'ordre de 10^{-12} ! Ainsi $e^{\pi\sqrt{163}}$ est un entier à 10^{-12} près. C'est pour ces mêmes raisons que les nombres $e^{\pi\sqrt{67}}$ et $e^{\pi\sqrt{43}}$, entre autres, sont eux aussi très proches de certains entiers.

4.2 Le corps de classe de Hilbert des corps quadratiques imaginaires

On voudrait maintenant obtenir des résultats analogues aux points 2., 3. du théorème 2.4.3. On montre d'abord une congruence similaire à (1.6.2).

Théorème 4.2.1. *Soit K un corps quadratique imaginaire. Soient $\mathfrak{a}_1, \dots \mathfrak{a}_k$ représentants distincts des classes d'idéaux de $Cl(\mathcal{O}_K)$. Notons $L = K(j(\mathfrak{a}_1), \dots, j(\mathfrak{a}_k))$. Pour presque tout idéal premier $\mathfrak{p}$ non ramifié de $\mathcal{O}_K$ tel que $N(\mathfrak{p}) = p$ premier dans $\mathbb{Z}$ on a la congruence :*

$$j(\mathfrak{p}^{-1}\mathfrak{a}) \equiv j(\mathfrak{a})^p \pmod{\mathfrak{B}} \tag{4.2.1}$$

où $\mathfrak{B}$ est un idéal premier de L au dessus de $\mathfrak{p}$ et $\mathfrak{a}$ est un idéal fractionnaire de K.

Avant de démontrer ce théorème, voyons une conséquence étonnante de cette simple congruence. Les notations sont les mêmes que dans le théorème précédent.

Théorème 4.2.2. *1. Le corps $K(j(\mathfrak{a}_1)) = K(j(\mathfrak{a}_1), \dots, j(\mathfrak{a}_k))$ est le corps de classe de Hilbert de K :*

$$K(j(\mathfrak{a}_1)) = \mathcal{H}_K$$

2. Les $j(\mathfrak{a}_i)$, $1 \leq i \leq k$ sont conjugués sur K.

3. L'application d'Artin $\left(\frac{\mathcal{H}_K/K}{\cdot}\right) : \mathcal{I}(K) \longrightarrow Gal(\mathcal{H}_K/K)$ est donnée par :

$$\left(\frac{\mathcal{H}_K/K}{\mathfrak{a}}\right)(j(\mathfrak{a}_1)) = j(\mathfrak{a}^{-1}\mathfrak{a}_1)$$

pour tout idéal fractionnaire $\mathfrak{a}$ de K.

Démonstration. Soient $\mathfrak{a}_1, \dots \mathfrak{a}_k$ des représentants des classes d'idéaux de $Cl(\mathcal{O}_K)$. La preuve de la proposition 4.1.4 montre que $L = K(j(\mathfrak{a}_1), \dots, j(\mathfrak{a}_k))$ est une extension galoisienne de K. Soit

$$B = \prod_{1\leq i<j\leq k} (j(\mathfrak{a}_i) - j(\mathfrak{a}_j))$$

Notons $\mathbf{P}$ l'ensemble des idéaux premiers de $\mathcal{O}_K$ non ramifiés dans L, de degré d'inertie 1 sur $\mathbb{Q}$, qui ne divisent pas B et tels que la congruence dans le théorème 4.2.1 soit vérifiée. On remarque que $\mathbf{P}$ contient tous les idéaux premiers de $\mathcal{O}_K$ de degré d'inertie 1 sur $\mathbb{Q}$ sauf au plus un nombre fini.

Soit $\mathfrak{p} \in \mathbf{P}$, $p = N(\mathfrak{p})$, $\mathfrak{a}$ un idéal fractionnaire de K. Pour tout premier $\mathfrak{B}$ au dessus de $\mathfrak{p}$ on a, d'après le théorème 4.2.1 :

$$j(\mathfrak{p}^{-1}\mathfrak{a}) \equiv j(\mathfrak{a})^p \pmod{\mathfrak{B}}$$

Notons $\sigma_{\mathfrak{B}}$ le Frobenius en $\mathfrak{B}$. Comme $j(\mathfrak{a}) \in \mathcal{O}_L$ (théorème 4.1.5) on a par définition :

$$\sigma_{\mathfrak{B}}(j(\mathfrak{a})) \equiv j(\mathfrak{a})^p \pmod{\mathfrak{B}}$$

On a aussi $\sigma_{\mathfrak{B}}(j(\mathfrak{a})) = j(\mathfrak{b})$ pour un certain idéal fractionnaire $\mathfrak{b}$ de K (voir la preuve de la proposition 4.1.4). Donc :

$$j(\mathfrak{b}) = \sigma_{\mathfrak{B}}(j(\mathfrak{a})) \equiv j(\mathfrak{p}^{-1}\mathfrak{a}) \pmod{\mathfrak{B}}$$

Comme $\mathfrak{p}$ ne divise pas B, $j(\mathfrak{b}) - j(\mathfrak{p}^{-1}\mathfrak{a}) \in \mathfrak{B}$ entraine que $j(\mathfrak{b}) - j(\mathfrak{p}^{-1}\mathfrak{a}) = 0$. Donc :

$$\sigma_{\mathfrak{B}}(j(\mathfrak{a})) = j(\mathfrak{p}^{-1}\mathfrak{a})$$

On en déduit que $\sigma_{\mathfrak{B}} = Id$ si et seulement si $j(\mathfrak{p}^{-1}\mathfrak{a}) = j(\mathfrak{a})$ pour tout idéal fractionnaire $\mathfrak{a}$ de K. Mais la fonction j prend la même valeur sur deux réseaux si et seulement si ils sont homothétiques, donc $\sigma_{\mathfrak{B}} = Id$ si et seulement si $\mathfrak{p}$ est principal.

On a donc montré que, pour tout $\mathfrak{p} \in \mathbf{P}$, $\mathfrak{p}$ est totalement décomposé dans L si et seulement si il est principal. Comme $\mathbf{P}$ contient tous les idéaux premiers de K de degré d'inertie 1, sauf un nombre fini, la remarque 2.3.8 implique que $K(j(\mathfrak{a}_1), \dots j(\mathfrak{a}_k))$ est le corps de classe de Hilbert de K.

Soient $\mathfrak{a}$ et $\mathfrak{b}$ deux idéaux fractionnaires de K. La classe de $\mathfrak{a}\mathfrak{b}^{-1}$ dans $Cl(\mathcal{O}_K)$ contient un idéal premier $\mathfrak{p} \in \mathbf{P}$ (cela découle du fait que les idéaux premiers de K sont equidistribués dans les classes d'idéaux de K par rapport à la densité de Dirichlet). Alors

$$j(\mathfrak{b}) = j(\mathfrak{a}\mathfrak{p}^{-1}) = \sigma_{\mathfrak{B}}(j(\mathfrak{a}))$$

Donc les $\mathfrak{a}_i, 1 \leq i \leq k$ sont conjugués, ce qui montre 2. Donc, comme $K(j(\mathfrak{a}_1), \dots, j(\mathfrak{a}_k))$ est une extension abélienne de K, elle est engendrée par n'importe quel des $j(\mathfrak{a}_i)$, ce qui termine la preuve de 1.

Enfin, montrons 3. Notons que l'égalité

$$\sigma_{\mathfrak{B}}(j(\mathfrak{a})) = j(\mathfrak{p}^{-1}\mathfrak{a})$$

valable pour tout $\mathfrak{p} \in \mathbf{P}$ et tout $\mathfrak{B}$ qui divise $\mathfrak{p}$ s'écrit de façon équivalente :

$$\left(\frac{\mathcal{H}_K/K}{\mathfrak{p}}\right)(j(\mathfrak{a}_1)) = j(\mathfrak{p}^{-1}\mathfrak{a}_1)$$

donc l'égalité dans 3. est vraie pour tout $\mathfrak{p} \in \mathbf{P}$.

Si $\mathfrak{a}$ est un idéal fractionnaire quelconque de K, il existe $\mathfrak{p} \in \mathbf{P}$ qui est dans la même classe que $\mathfrak{a}$. On a alors :

$$\left(\frac{\mathcal{H}_K/K}{\mathfrak{a}}\right)(j(\mathfrak{a}_1)) = \left(\frac{\mathcal{H}_K/K}{\mathfrak{p}}\right)(j(\mathfrak{a}_1)) = j(\mathfrak{p}^{-1}\mathfrak{a}_1) = j(\mathfrak{a}^{-1}\mathfrak{a}_1)$$

ce qui prouve 3. □

Remarque 4.2.3. L'équation

$$\left(\frac{\mathcal{H}_K/K}{\mathfrak{a}}\right)(j(\mathfrak{a}_1)) = j(\mathfrak{a}^{-1}\mathfrak{a}_1)$$

exprime le fait, tout a fait non trivial, que l'action *algébrique* de l'application d'Artin en $\mathfrak{a}$ sur $\mathcal{H}_K = K(j(\mathfrak{a}_1))$ correspond à l'action *géométrique* de multiplication du réseau $\mathfrak{a}_1$ par $\mathfrak{a}^{-1}$.

4.2.1 Preuve analytique de la congruence de Kronecker (Hasse)

La preuve est assez longue et technique.
Il sera plus commode d'utiliser des coordonnées homogènes pour les fonction modulaires : si f est une fonction modulaire de poids k, et $w_1, w_2 \in \mathbb{C}$ avec $\mathrm{Im}(w_1/w_2) > 0$ on pose

$$f(w_1, w_2) := w_2^{-2k} f\left(\frac{w_1}{w_2}\right)$$

Si on fait agir $\mathbb{SL}_2(\mathbb{Z})$ par $(w_1, w_2) \mapsto (aw_1 + bw_2, cw_1 + dw_2)$ on voit bien que $f(w_1, w_2)$ est invariante sous cette action. On rappelle que $\Delta(\tau) = g_2^3(\tau) - 27g_3^2(\tau)$.

Définition 4.2.4. *Soit $\sigma \in \Delta_n^*$. On définit la fonction φ_σ par*

$$\varphi_\sigma(w_1, w_2) = n^{12} \frac{\Delta(\sigma(w_1, w_2))}{\Delta(w_1, w_2)}$$

Manifestement, la définition de φ_σ ne dépend que de la classe de σ sous l'action de $\mathbb{SL}_2(\mathbb{Z})$. On donne ensuite quelques propriétés de cette fonction. Soit $\{\sigma_1, \ldots, \sigma_N\}$ un ensemble de représentants des orbites de Δ_n^* sous $\mathbb{SL}_2(\mathbb{Z})$.

Proposition 4.2.5. *1. Si $n = p$ est un nombre premier, alors*

$$\prod_{k=1}^{N} \varphi_{\sigma_k}(w_1, w_2) = (-1)^{p-1} p^{12}$$

pour tout w_1, w_2.

2. Soit K un corps quadratique imaginaire, $\mathfrak{a}$ un idéal fractionnaire de K et soit $\{\alpha_1, \alpha_2\} \subset \mathbb{C}$ une base de $\mathfrak{a}$ telle que $\mathrm{Im}(\alpha_1/\alpha_2) > 0$. Alors pour tout $\sigma \in \Delta_n^*$, on a que $\varphi_\sigma(\alpha_1, \alpha_2)$ est un entier algébrique.

Démonstration. Dans cette preuve fixons comme ensemble de representants de $\mathbb{SL}_2(\mathbb{Z})\backslash\Delta_p^*$ le suivant :

$$\sigma_i = \begin{pmatrix} 1 & i-1 \\ 0 & p \end{pmatrix} \qquad \text{pour } i = 1, \ldots, p$$

$$\sigma_{p+1} = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$$

1) C'est un calcul explicite en utilisant comme représentants de $\mathbb{SL}_2(\mathbb{Z})\backslash\Delta_p^*$ ceux qu'on a choisi et en regardant les q-développements.
2) On définit le polynôme suivant, de manière analogue à la définition du polynôme modulaire :

$$\Psi_n(X) = \prod_{k=1}^{N} (X - \varphi_{\sigma_i}(w_1, w_2))$$

Comme dans le cas de $\Phi_n(X)$ on montre qu'on peut voir $\Psi_n(X)$ comme un polynôme en X et j. Ainsi, on le note $\Psi_n(X, j)$. On a donc :

$$\Psi_n(X, j(\mathfrak{a})) = \prod_{k=0}^{N} (X - \varphi_{\sigma_i}(\alpha_1, \alpha_2))$$

Comme $j(\mathfrak{a})$ est un entier algébrique, on a un polynôme unitaire en X avec des coefficients qui sont des entiers algébriques. Par conséquence, ses racines sont des entiers algébriques. Cela montre que $\varphi_{\sigma_i}(\alpha_1, \alpha_2)$ est un entier algébrique. Le premier point de la proposition implique que $\varphi_{\sigma_i}(\alpha_1, \alpha_2)$ divise (p^{12}). □

Théorème 4.2.6. *Soit K un corps quadratique imaginaire, $\mathfrak{a}$ un idéal fractionnaire de K et $\{\alpha_1, \alpha_2\} \subset \mathbb{C}$ une base de $\mathfrak{a}$. Soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$ de degré d'inertie égal à 1. Choisissons $P \in \Delta_p^*$ (resp. $\bar{P} \in \Delta_p^*$) une matrice telle que $P(\alpha_1, \alpha_2)$ (resp. $\bar{P}(\alpha_1, \alpha_2)$) soit une base de l'idéal $\mathfrak{p}\mathfrak{a}$ (resp. $\bar{\mathfrak{p}}\mathfrak{a}$). Alors*

$$(\varphi_P(\alpha_1, \alpha_2)) = \bar{\mathfrak{p}}^{12}, \qquad (\varphi_{\bar{P}}(\alpha_1, \alpha_2)) = \mathfrak{p}^{12}$$

De plus, si $\sigma \in \Delta_p^*$ n'est pas dans les orbites de P et $\bar{P}$ alors $\varphi_\sigma(\alpha_1, \alpha_2)$ est une unité.

Démonstration. Comme le nombre des classes de $\mathcal{O}_K$ est fini, il existe $f \in \mathbb{N}$ tel que $\mathfrak{p}^f = (\beta)$. Pour chaque $1 \leq i \leq f$, $\mathfrak{p}^i\mathfrak{a}$ est un sous-module d'indice p dans $\mathfrak{p}^{i-1}\mathfrak{a}$. On peut donc choisir une matrice $P_i \in \Delta_p^*$ telle que, si $\{w_1, w_2\}$ est une base de $\mathfrak{p}^{i-1}\mathfrak{a}$, alors $P_i(w_1, w_2)$ est une base de $\mathfrak{p}^i\mathfrak{a}$. En partant de la base $\{\alpha_1, \alpha_2\}$ de $\mathfrak{a}$, on obtient des matrices $P_1, \ldots, P_f$ telles que, pour chaque $1 \leq i \leq f$, on a que $P_iP_{i-1} \ldots P_1(\alpha_1, \alpha_2)$ est une base de $\mathfrak{p}^i\mathfrak{a}$. En particulier, $[P_fP_{f-1} \ldots P_1(\alpha_1, \alpha_2)] = [\beta\alpha_1, \beta\alpha_2]$. On pose pour chaque $1 \leq i \leq f$:

$$\lambda_i = \varphi_{P_i}(P_{i-1} \ldots P_1(\alpha_1, \alpha_2)) = p^{12}\frac{\Delta(P_i \ldots P_1(\alpha_1, \alpha_2))}{\Delta(P_{i-1} \ldots P_1(\alpha_1, \alpha_2))}$$

Alors,

$$\prod_{i=1}^{f} \lambda_i = p^{12f}\frac{\Delta(P_f \ldots P_1(\alpha_1, \alpha_2))}{\Delta(\alpha_1, \alpha_2)} = p^{12f}\frac{\Delta(\beta\alpha_1, \beta\alpha_2)}{\Delta(\alpha_1, \alpha_2)} = p^{12f}\beta^{-12} = \bar{\mathfrak{p}}^{12f}\mathfrak{p}^{12f}\beta^{-12} = \bar{\beta}^{12}$$

Comme les λ_i sont entiers algébriques on a que, pour chaque i, (λ_i) divise $(\bar{\beta})^{12} = \bar{\mathfrak{p}}^{12f}$. Par le point 1 de la proposition précédente, on a aussi que (λ_i) divise $(p^{12}) = \mathfrak{p}^{12}\bar{\mathfrak{p}}^{12}$. Par conséquence, (λ_i) divise $(\bar{\mathfrak{p}}^{12f}, \mathfrak{p}^{12}\bar{\mathfrak{p}}^{12}) = \bar{\mathfrak{p}}^{12}$. Comme $\prod_{i=1}^{f} \lambda_i = \bar{\mathfrak{p}}^{12f}$, on a forcement que $(\lambda_i) = \bar{\mathfrak{p}}^{12}$, pour chaque i. En particulier, $(\lambda_1) = (\varphi_P(\alpha_1, \alpha_2)) = \bar{\mathfrak{p}}^{12}$. En faisant le même raisonnement avec $\bar{P}$ au lieu de P, on obtient $(\varphi_{\bar{P}}(\alpha_1, \alpha_2)) = \mathfrak{p}^{12}$. Comme $\mathfrak{p} \neq \bar{\mathfrak{p}}$, les classes de P et $\bar{P}$ sous l'action de $\mathbb{SL}_2(\mathbb{Z})$ sont distinctes. Ainsi :

$$\prod_{i=1}^{N}(\varphi_{\sigma_1}(\alpha_1, \alpha_2)) = (p^{12}) = \mathfrak{p}^{12}\bar{\mathfrak{p}}^{12}$$

On conclut que, si σ_i n'est pas dans l'orbite de P ou $\bar{P}$, $\varphi_{\sigma_i}(\alpha_1, \alpha_2)$ est une unité. □

Revenons-nous à la démonstration du théorème principal. On remarque que c'est équivalent de démontrer l'assertion avec la congruence suivante

$$j(\mathfrak{p}^{-1}\mathfrak{a}) \equiv j(\mathfrak{a})^p \pmod{\mathfrak{p}\mathcal{O}_L}$$

En fait, si on a la congruence pour chaque idéal $\mathfrak{B}_j$ au-dessus de $\mathfrak{p}$ alors on aura la congruence modulo leur intersection qui est égale à leur produit $\mathfrak{p}\mathcal{O}_L$, comme ils sont premiers entre eux. Comme $\mathfrak{p}\bar{\mathfrak{p}} = (p)$ on a l'égalité $\bar{\mathfrak{p}} = \mathfrak{p}^{-1}$ dans le groupe des classes. On s'est ramené à démontrer

$$j(\bar{\mathfrak{p}}\mathfrak{a}) \equiv j(\mathfrak{a})^p \pmod{\mathfrak{p}\mathcal{O}_L}$$

Soit $\{\alpha_1, \alpha_2\}$ un base de $\mathfrak{a}$, et $P \in \Delta_p^*$ (resp. $\bar{P} \in \Delta_p^*$) telle que $P(\alpha_1, \alpha_2)$ (resp. $\bar{P}(\alpha_1, \alpha_2)$) soit une base de $\mathfrak{p}\mathfrak{a}$ (resp. de $\bar{\mathfrak{p}}\mathfrak{a}$). Soient r, s tels que σ_r soit dans l'orbite de P et σ_s soit dans l'orbite de $\bar{P}$.

On veut montrer la congruence suivante.

$$(j(\mathfrak{a})^p - j \circ \sigma_s(\mathfrak{a})) \prod_{i \neq s} (\varphi_{\sigma_s}(\alpha_1, \alpha_2) - \varphi_{\sigma_i}(\alpha_1, \alpha_2)) \equiv 0 \pmod{p} \tag{4.2.2}$$

Définissons le polynôme :

$$F(X, Y, \tau) = \sum_{i=1}^{p+1} \left((X - j \circ \sigma_i(\tau)) \prod_{h \neq i} (Y - \varphi_{\sigma_h}(\tau)) \right)$$

où $\varphi_{\sigma_i}(\tau) := \varphi_{\sigma_i}(\tau, 1)$. Comme on a déjà fait pour le polynôme modulaire, on montre que les coefficients de X, Y sont des fonctions modulaires holomorphes et ainsi on peut voir $F(X, Y, \tau)$ comme un polynôme $G(X, Y, j)$ en X, Y et j. De plus les coefficients de G sont entiers.
En appliquant les congruences (3.6.3) aux fonctions j et $(2\pi)^{-12}\Delta$, on voit que les premiers p termes de la somme de F ont $q-$développements congrus entre eux modulo $(1 - \zeta_p)$, où $\zeta_p = e^{\frac{2i\pi}{p}}$. Pour le dernier terme

$$(X - j \circ \sigma_{p+1}(\tau)) \prod_{h \neq p+1} (Y - \varphi_{\sigma_h}(\tau))$$

en posant $X = j^p$ on voit que le $q-$développement de $X - j \circ \sigma_{p+1}(\tau) = j^p - j(q^p)$ a ses coefficients divisibles par p. Donc on trouve que les coefficients du $q-$développement de $F(j^p, Y)$ sont divisibles par p. Pour le principe de $q-$développement on obtient que $G(j^p, Y, j) \in p\mathbb{Z}[Y, j]$. On rappelle que l'indice s est tel que $[\sigma_s(\alpha_1, \alpha_2)] = \bar{\mathfrak{p}}\mathfrak{a}$. Posons $\mu = \alpha_1/\alpha_2$. Comme les coefficients de $G(j^p, Y, j)$ sont divisibles par p et $\mathfrak{p}$ divise p, en spécialisant $Y = \varphi_{\sigma_s}(\mu)$ on trouve :

$$G(j(\mathfrak{a})^p, \varphi_{\sigma_s}(\mu), j(\mathfrak{a})) \equiv 0 \pmod{\mathfrak{p}} \tag{4.2.3}$$

Comme $F(X, \varphi_{\sigma_i}(\mu), \tau) = (X - j \circ \sigma_s(\tau)) \prod_{h \neq s} (\varphi_{\sigma_s}(\mu) - \varphi_{\sigma_h}(\mu))$, on obtient dans la formule (4.2.3)

$$(j(\mathfrak{a})^p - j \circ \sigma_s(\mathfrak{a})) \prod_{h \neq i} (\varphi_{\sigma_s}(\mu) - \varphi_{\sigma_h}(\mu)) \equiv 0 \pmod{p}$$

c'est-à-dire :

$$(j(\mathfrak{a})^p - j \circ \sigma_s(\mathfrak{a})) \prod_{h \neq s} (\varphi_{\sigma_s}(\alpha_1, \alpha_2) - \varphi_{\sigma_h}(\alpha_1, \alpha_2)) \equiv 0 \pmod{\mathfrak{p}}$$

Par le théorème (4.2.6), on a que $\varphi_{\sigma_s}(\alpha_1, \alpha_2) \equiv 0 \pmod{\mathfrak{p}}$. Ainsi on obtient :

$$\prod_{h \neq s} (\varphi_{\sigma_s}(\alpha_1, \alpha_2) - \varphi_{\sigma_h}(\alpha_1, \alpha_2)) \equiv \prod_{h \neq s} (-1)^p \varphi_{\sigma_h}(\alpha_1, \alpha_2) \pmod{\mathfrak{p}}$$

On remarque que, par le théorème (4.2.6)

$$\left(\prod_{h \neq s} (-1)^p \varphi_{\sigma_h}(\alpha_1, \alpha_2) \right) = \bar{\mathfrak{p}}^{12}$$

où le membre à gauche indique l'idéal engendré par $\prod_{h\neq s}(-1)^p\varphi_{\sigma_h}(\alpha_1,\alpha_2)$. En remarquant que $\bar{\mathfrak{p}}^{12}$ est premier avec $\mathfrak{p}$, la congruence (4.2.2) donne :

$$j(\mathfrak{a})^p - j\circ\sigma_s(\mathfrak{a}) \equiv 0 \pmod{\mathfrak{p}}$$

Cela est bien la congruence qu'on voulait.

4.2.2 Preuve géométrique de la congruence de Kronecker (Deuring)

Soit $L = K(j(\mathfrak{a}_1),\ldots,j(\mathfrak{a}_k))$. Pour chaque i, $1\leq i\leq k$, on choisit une courbe elliptique E_i isomorphe à $\mathbb{C}/\mathfrak{a}_i$ définie sur L (ce qui est possible d'après le lemme 3.3.5). Soit $\mathbf{S}$ l'ensemble des idéaux premiers $\mathfrak{p}$ de $\mathcal{O}_K$ qui vérifient les conditions suivantes :

1. $\mathfrak{p}$ est de degré d'inertie 1 sur $\mathbb{Q}$.
2. $\mathfrak{p}$ est non ramifié dans L
3. Chaque courbe elliptique E_i a bonne réduction modulo $\mathfrak{B}$, pour tout $\mathfrak{B}$ idéal premier de L au dessus de $\mathfrak{p}$.

On va montrer que la congruence du théorème 4.2.1 est vérifiée pour tout $\mathfrak{p}\in\mathbf{S}$. Soit donc $\mathfrak{p}\in\mathbf{S}$, $\mathfrak{B}$ idéal premier de L au dessus de $\mathfrak{p}$, $\mathfrak{a}$ un idéal fractionnaire de $\mathcal{O}_K$. Montrons que

$$j(\mathfrak{p}^{-1}\mathfrak{a}) \equiv j(\mathfrak{a})^p \pmod{\mathfrak{B}}$$

Soit $\mathfrak{b}$ un idéal de $\mathcal{O}_K$ premier avec p tel que $\mathfrak{p}\mathfrak{b} = (\alpha)$ est principal. L'inclusion $\mathfrak{a}\subseteq\mathfrak{p}^{-1}\mathfrak{a}$ donne un'isogénie

$$\rho : \mathbb{C}/\mathfrak{a} \longrightarrow \mathbb{C}/\mathfrak{p}^{-1}\mathfrak{a}$$

Comme $\mathfrak{p}^{-1}(\alpha) = \mathfrak{b}$, la multiplication par α induit un isomorphisme

$$m_\alpha : \mathbb{C}/\mathfrak{p}^{-1}\mathfrak{a} \longrightarrow \mathbb{C}/\mathfrak{a}\mathfrak{b}$$

Enfin, l'inclusion $\mathfrak{a}\mathfrak{b}\subseteq\mathfrak{a}$ donne une isogénie :

$$\psi : \mathbb{C}/\mathfrak{a}\mathfrak{b} \longrightarrow \mathbb{C}/\mathfrak{a}$$

Notons $E_\mathfrak{a}$ (resp. $E_{\mathfrak{p}^{-1}\mathfrak{a}}$, $E_{\mathfrak{a}\mathfrak{b}}$) la courbe elliptique parmi les E_i qui est isomorphe à $\mathbb{C}/\mathfrak{a}$ (resp. $\mathbb{C}/\mathfrak{p}^{-1}\mathfrak{a}$, $\mathbb{C}/\mathfrak{a}\mathfrak{b}$). Soit $\phi_\mathfrak{a}$ (resp. $\phi_{\mathfrak{p}^{-1}\mathfrak{a}}$, $\phi_{\mathfrak{a}\mathfrak{b}}$) l'isomorphisme, décrit dans le théorème 3.3.4, entre $\mathbb{C}/\mathfrak{a}$ et $E_\mathfrak{a}$ (resp. $\mathbb{C}/\mathfrak{p}^{-1}\mathfrak{a}$ et $E_{\mathfrak{p}^{-1}\mathfrak{a}}$, $\mathbb{C}/\mathfrak{a}\mathfrak{b}$ et $E_{\mathfrak{a}\mathfrak{b}}$). Le lemme 3.3.5 permet d'associer à chacune des isogénies décrites un morphisme entre les courbes projectives correspondantes, ce qui donne le magnifique diagramme commutatif suivant :

$$\begin{array}{ccccccc}
\mathbb{C} & \xrightarrow{z\mapsto z} & \mathbb{C} & \xrightarrow{z\mapsto \alpha z} & \mathbb{C} & \xrightarrow{z\mapsto z} & \mathbb{C} \\
\downarrow{\scriptstyle\pi} & & \downarrow{\scriptstyle\pi} & & \downarrow{\scriptstyle\pi} & & \downarrow{\scriptstyle\pi} \\
\mathbb{C}/\mathfrak{a} & \xrightarrow{\rho} & \mathbb{C}/\mathfrak{p}^{-1}\mathfrak{a} & \xrightarrow{m_\alpha} & \mathbb{C}/\mathfrak{a}\mathfrak{b} & \xrightarrow{\psi} & \mathbb{C}/\mathfrak{a} \\
\downarrow{\scriptstyle\phi_\mathfrak{a}} & & \downarrow{\scriptstyle\phi_{\mathfrak{p}^{-1}\mathfrak{a}}} & & \downarrow{\scriptstyle\phi_{\mathfrak{a}\mathfrak{b}}} & & \downarrow{\scriptstyle\phi_\mathfrak{a}} \\
E_\mathfrak{a} & \xrightarrow[[\rho]]{} & E_{\mathfrak{p}^{-1}\mathfrak{a}} & \xrightarrow[[m_\alpha]]{} & E_{\mathfrak{a}\mathfrak{b}} & \xrightarrow[[\psi]]{} & E_\mathfrak{a}
\end{array}$$

On a :

$$deg([\rho]) = deg(\rho) = [\mathfrak{p}^{-1}\mathfrak{a} : \mathfrak{a}] = N(\mathfrak{p}) = p$$

$$deg([\psi] \circ [m_\alpha]) = deg(\psi \circ m_\alpha) = deg(\psi) = [\mathfrak{a} : \mathfrak{b}\mathfrak{a}] = N(\mathfrak{b})$$

et $(N(\mathfrak{b}), p) = 1$ comme on a choisi $\mathfrak{b}$ premier avec p.
Soit ω la différentielle invariante sur $E_\mathfrak{a}$. Comme la composée des applications dans la première ligne du diagramme est $z \mapsto \alpha z$, on a :

$$([\psi] \circ [m_\alpha] \circ [\rho])^* \omega = \alpha\omega$$

Maintenant, on "réduit la dernière ligne du diagramme modulo $\mathfrak{B}$". Si on note $\lambda = [\psi] \circ [m_\alpha] \circ [\rho]$ et $\bar{A}$ la réduction modulo $\mathfrak{B}$ d'un objet A, la dernière égalité devient :

$$\bar{\lambda}^* \bar{\omega} = \bar{\alpha}\bar{\omega} \equiv 0 \pmod{\mathfrak{B}}$$

comme $\alpha \in \mathfrak{p}$ et $\mathfrak{B}$ divise $\mathfrak{p}$.

On en déduit grâce au lemme 3.4.4 que $\bar{\lambda}$ est inséparable. Comme le degré d'une isogénie est égal au degré de sa réduction modulo $\mathfrak{B}$ (lemme 3.4.6), et comme $deg([\psi]\circ[m_\alpha]) = N(\mathfrak{b})$ est premier avec p, $\overline{[\psi] \circ [m_\alpha]}$ est séparable, donc $\overline{[\rho]}$ est inséparable.

En conséquence, $\overline{[\rho]}$ se factorise par le Frobenius : si on note $\bar{E}_\mathfrak{a}^{(p)}$ l'image de la courbe $\bar{E}_\mathfrak{a}$ par le morphisme de Frobenius $F : [x, y, z] \mapsto [x^p, y^p, z^p]$, il existe un morphisme $\tau : \bar{E}_\mathfrak{a}^{(p)} \longrightarrow \bar{E}_{\mathfrak{a}\mathfrak{p}^{-1}}$ tel que le diagramme suivant commute :

$$\begin{array}{ccc} \bar{E}_\mathfrak{a} & \xrightarrow{\overline{[\rho]}} & \bar{E}_{\mathfrak{a}\mathfrak{p}^{-1}} \\ \downarrow F & \nearrow \tau & \\ \bar{E}_\mathfrak{a}^{(p)} & & \end{array}$$

Comme

$$deg(\overline{[\rho]}) = deg([\rho]) = p = deg(F)$$

on a $deg(\tau) = 1$, c'est à dire, τ est un isomorphisme. Mais deux courbes elliptiques sont isomorphes si et seulement si elles ont le même invariant j. Donc on obtient :

$$j(\bar{E}_\mathfrak{a})^p = j(\bar{E}_\mathfrak{a}^{(p)}) = j(\bar{E}_{\mathfrak{a}\mathfrak{p}^{-1}})$$

donc

$$j(E_\mathfrak{a})^p \equiv j(E_{\mathfrak{a}\mathfrak{p}^{-1}}) \pmod{\mathfrak{B}}$$

et finalement

$$j(\mathfrak{a})^p \equiv j(\mathfrak{a}\mathfrak{p}^{-1}) \pmod{\mathfrak{B}}$$

4.3 Kronecker Jugendtraum

Soit K un corps quadratique imaginaire. On a vu dans la section précédente que le $j-$invariant d'une courbe elliptique E avec multiplication complexe par l'anneau $\mathcal{O}_K$ engendre l'extension abélienne *non ramifiée* maximale $\mathcal{H}_K$ de K.

Dans cette section, on va montrer comment engendrer l'*extension abélienne maximale* de K en ajoutant à $\mathcal{H}_K$ les valeurs de la fonction de Weber f_E évaluée sur les points de torsion de E. C'est l'analogue pour les corps quadratiques imaginaires de ce qu'on a fait pour $\mathbb{Q}$ dans la section 2.4.

Proposition 4.3.1. *Soit $E = \mathbb{C}/\Lambda$ une courbe elliptique, $N \in \mathbb{N}$, $E[N]$ le groupe des points de $N-$torsion de E.*

1. *$E[N]$ est isomorphe à $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$*
2. *Si E a multiplication complexe par $\mathcal{O}_K$, alors $\mathcal{H}_K(f_E(E[N]))$ est une extension galoisienne finie de $\mathcal{H}_K$.*

Démonstration. 1. Clair, comme $E = \mathbb{C}/\Lambda$.

2. Supposons $Aut(E) = \{\pm 1\}$ (les autres deux cas se traitent de la même façon). Alors $f_E(z) = \frac{g_2(\Lambda)g_3(\Lambda)}{\Delta(\Lambda)}\wp_\Lambda(z)$. On a montré que $\mathcal{H}_K = K(j(E))$, donc E est isomorphe à une courbe définie sur $\mathcal{H}_K$. On peut alors supposer que $g_2(\Lambda), g_3(\Lambda), \Delta(\Lambda) \in \mathcal{H}_K$. Il faut montrer que $\mathcal{H}_K(\wp_\Lambda(E[N]))/\mathcal{H}_K$ est galoisienne finie.
Soit donc $\sigma : \mathcal{H}_K(\wp_\Lambda(E[N])) \longrightarrow \mathbb{C}$ un morphisme de $\mathcal{H}_K$-algèbres. Comme E a un modèle défini sur $\mathcal{H}_K$, et la loi de groupe algébrique sur E est elle même définie sur $\mathcal{H}_K$, σ permute les points de torsion de E (vue comme courbe projective), et permute en particulier leurs premières coordonnées. On a ainsi $\sigma(\wp_\Lambda(E[N])) \subseteq \wp_\Lambda(E[N])$, ce qui montre la proposition.

□

Remarque 4.3.2. 1. L'idée essentielle utilisée dans la preuve de la proposition précédente est le fait que $Gal(\mathcal{H}_K(E[N])/\mathcal{H}_K)$ agit sur $E[N] \cong \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$, ce qui donne une représentation injective

$$\rho : Gal(\mathcal{H}_K(E[N])/\mathcal{H}_K) \longrightarrow \mathbb{GL}_2(\mathbb{Z}/N\mathbb{Z})$$

En utilisant le fait que E a multiplication complexe, on peut montrer que l'image de ρ est un groupe *abélien*. Donc $\mathcal{H}_K(E[N])$ est une extension *abélienne* de $\mathcal{H}_K$. Néanmoins, ce n'est *pas* en général une extension abélienne de K.

2. La proposition précédente entraine que $K(j(\mathfrak{a}), f_E(E[N]))$ est une extension *finie* de K.
3. Attention ! On ne sait pas, à ce stade, si $K(j(\mathfrak{a}), f_E(E[N]))$ est une extension *galoisienne de K* !

On énonce maintenant le résultat fondamental suivant qu'on va montrer en plusieurs étapes.

Théorème 4.3.3. *Soit K un corps quadratique imaginaire, E une courbe elliptique avec multiplication complexe par $\mathcal{O}_K$, j_E son invariant j, f_E la fonction de Weber de E. Alors $K(j_E, f_E(E[N]))$ est le corps de classe de rayon de K pour le cycle arithmétique N.*

4.3.1 Deux résultats préliminaires

Lemme 4.3.4. *Pour presque tout idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ de degré d'inertie 1 sur $\mathbb{Q}$ tel que $\left(\frac{\mathcal{H}_K/K}{\mathfrak{p}}\right) = Id$ il existe $\lambda \in \mathcal{O}_K$ tel que $\mathfrak{p} = (\lambda)$ et que le digramme suivant commute :*

$$\begin{array}{ccc} E & \xrightarrow{[\lambda]} & E \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi} \\ \bar{E} & \xrightarrow[F]{} & \bar{E} \end{array}$$

où $\bar{E}$ dénote la réduction de E (vue comme courbe projective) modulo un idéal $\mathfrak{B}$ de $\mathcal{H}_K$ au dessus de $\mathfrak{p}$, $F : [x, y, z] \mapsto [x^p, y^p, z^p]$ est le Frobenius.

Démonstration. Voir [14] □

Lemme 4.3.5. *Soit $K \subseteq L \subseteq \mathbb{C}$ une extension de corps de nombres, $\overline{L}$ la clôture normale de L. Soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$ non ramifié dans $\overline{L}$.*
Si, pour tout idéal premier $\mathfrak{B}$ dans $\overline{L}$ au dessus de $\mathfrak{p}$, on a :

$$\sigma_{\mathfrak{B}}|_L = Id$$

où $\sigma_{\mathfrak{B}}$ dénote le Frobenius de $\overline{L}/K$ en $\mathfrak{B}$, alors $\mathfrak{p}$ est totalement décomposé dans $\overline{L}$.

Démonstration. Notons $G = Gal(\overline{L}/K)$, $H = Gal(\overline{L}/L)$. Soit $\mathfrak{B}$ un idéal premier dans $\overline{L}$ au dessus de $\mathfrak{p}$. Les autres idéaux premiers qui divisent $\mathfrak{p}$ sont alors de la forme $\phi(\mathfrak{B})$ avec $\phi \in G$.
Par hypothèse, on a $\phi\sigma_{\mathfrak{B}}\phi^{-1} \in H$ pour tout $\phi \in G$, c'est à dire :

$$\sigma_{\mathfrak{B}} \in \bigcap_{\phi \in G} \phi^{-1} H \phi =: J$$

Maintenant, J est un sous groupe de H et distingué dans G, donc $\overline{L}^J$ est une extension galoisienne de K qui contient $L = \overline{L}^H$. Mais $\overline{L}$ est la clôture normale de L, donc $\overline{L}^J = \overline{L}$, ce qui implique $J = \{Id\}$. On obtient ainsi $\sigma_{\mathfrak{B}} = Id$, donc $\mathfrak{p}$ est totalement décomposé dans $\overline{L}$. □

Notation 4.3.6. Soit $E = \mathbb{C}/\Lambda$ une courbe elliptique, et f_E la fonction de Weber associée :

$$f_E(z) = \begin{cases} \frac{g_2(\Lambda)g_3(\Lambda)}{\Delta(\Lambda)}\wp_\Lambda(z) & \text{si } g_2(\Lambda)g_3(\Lambda) \neq 0 \\ \frac{g_3(\Lambda)}{\Delta(\Lambda)}\wp_\Lambda^3(z) & \text{ai } g_2(\Lambda) = 0 \\ \frac{g_2(\Lambda)^2}{\Delta(\Lambda)}\wp_\Lambda^2(z) & \text{si } g_3(\Lambda) = 0 \end{cases}$$

Soit $\phi_\Lambda : z \mapsto [\wp(z), \wp'(z), 1]$ l'application introduite dans le théorème 3.3.4. Si $P = \phi_\Lambda(z)$, on notera dans la preuve du théorème $f_E(P) := f_E(z)$. Les formules qui définissent f_E montrent que $P \mapsto f_E(P)$ est un morphisme algébrique défini sur $\mathcal{H}_K$, si E a multiplication complexe par $\mathcal{O}_K$.

4.3.2 Preuve du théorème 4.3.3

Soit K_N le corps de classe de rayon N pour K. Par définition, on a $\mathfrak{p} \in Spl(K_N/K) \iff \mathfrak{p} = (\alpha)$ avec $\alpha \equiv 1 \pmod N$. Soit $L = K(j_E, f_E(E[N]))$ et $\overline{L}$ la clôture normale de L/K. On veut montrer que $L = K_N$. Montrons d'abord que $\overline{L} \subseteq K_N$.

On va utiliser la proposition 2.3.7. Soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$ de degré 1, tel que $\mathfrak{p} \in Spl(K_N/K)$. On a alors $\mathfrak{p} = (\alpha)$ avec $\alpha \equiv 1 \pmod N$. En particulier $\mathfrak{p}$ est principal, donc $\left(\frac{\mathcal{H}_K/K}{\mathfrak{p}}\right) = Id$.

Quitte à éliminer un nombre fini d'idéaux premiers, on sait donc, grâce au lemme 4.3.4, qu'il existe $\lambda \in \mathcal{O}_K$ tel que $\mathfrak{p} = (\lambda)$ et que le diagramme suivant commute :

$$\begin{array}{ccc} E & \xrightarrow{[\lambda]} & E \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi} \\ \bar{E} & \xrightarrow[F]{} & \bar{E} \end{array}$$

où $\bar{E}$ dénote la réduction de E modulo un idéal premier $\mathfrak{B}$ fixé de $\overline{L}$ au dessus de $\mathfrak{p}$.

Comme $\mathfrak{p} = (\alpha) = (\lambda)$, on a $\lambda = u\alpha$, où u est une unité de $\mathcal{O}_K$. Donc $[\alpha]$ et $[\lambda]$ diffèrent par un automorphisme de E. Soit $\sigma_{\mathfrak{B}} \in Gal(\overline{L}/K)$ le Frobenius de $\overline{L}/K$ en $\mathfrak{B}$. On a, pour tout $P = [\wp(z), \wp'(z), 1]$, $z \in E[N]$:

$$\overline{\sigma_{\mathfrak{B}}(P)} = F(P) = \overline{[\lambda](P)}$$

Si on élimine les premiers $\mathfrak{p}$ qui divisent N (qui sont en nombre fini), on sait que la réduction $E[N] \longrightarrow \bar{E}[N]$ est injective (lemme 3.4.6), donc on a :

$$\sigma_{\mathfrak{B}}(P) = [\lambda](P)$$

Maintenant on calcule :

$$\begin{aligned}
\sigma_{\mathfrak{B}}(f_E(P)) = f_E(\sigma_{\mathfrak{B}}(P)) \qquad & \text{comme } \left(\frac{\mathcal{H}_K/K}{\mathfrak{p}}\right) = Id \text{ et } f_E \text{ est définie sur } \mathcal{H}_K \\
= f_E([\lambda](P)) \qquad & \text{comme } \sigma_{\mathfrak{B}}(P) = [\lambda](P) \\
= f_E([\alpha](P)) \qquad & \text{comme } f_E \text{ est } Aut(E) - \text{invariante (proposition 3.5.5)} \\
= f_E(P) \qquad & \text{comme } P \in E[N] \text{ et } \alpha \equiv 1 \pmod{N}
\end{aligned}$$

On a donc montré que, pour tout idéal premier $\mathfrak{B}$ de $\overline{L}$ au dessus de $\mathfrak{p}$ on a :

$$\sigma_{\mathfrak{B}}(f_E(P)) = f_E(P)$$

pour tout point de $N-$torsion P.

Comme on sait aussi que $\sigma_{\mathfrak{B}}(j_E) = \left(\frac{\mathcal{H}_K/K}{\mathfrak{p}}\right)(j_E) = j_E$, on obtient que

$$\sigma_{\mathfrak{B}}|_L = Id$$

Le lemme 4.3.5 nous dit alors que $\mathfrak{p}$ est totalement décomposé dans $\overline{L}$.

On a donc montré l'implication :

$$\mathfrak{p} \in Spl(K_N/K) \Rightarrow \mathfrak{p} \in Spl(\overline{L}/K)$$

pour presque tout $\mathfrak{p}$ de degré d'inertie 1. La proposition 2.3.7 nous dit alors que

$$\overline{L} \subseteq K_N$$

Donc on a aussi $L \subseteq K_N$, ce qui implique que L/K est une extension galoisienne abélienne.

Pour montrer que $L = K_N$, il suffit maintenant de montrer l'inclusion :

$$Spl(L/K) \subseteq Spl(K_N/K)$$

Soit $\mathfrak{p}$ de degré d'inertie 1 sur $\mathbb{Q}$ tel que $\left(\frac{L/K}{\mathfrak{p}}\right) = Id$. Alors on a aussi

$$\left(\frac{\mathcal{H}_K/K}{\mathfrak{p}}\right) = \left(\frac{L/K}{\mathfrak{p}}\right)\Big|_{\mathcal{H}_K} = Id$$

Quitte à éliminer un nombre fini d'idéaux premiers, on peut appliquer le lemme 4.3.4, qui donne $\lambda \in \mathcal{O}_K$ tel que $\mathfrak{p} = (\lambda)$ et tel que le diagramme

$$\begin{array}{ccc} E & \xrightarrow{[\lambda]} & E \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi} \\ \bar{E} & \xrightarrow[F]{} & \bar{E} \end{array}$$

commute.

Choisissons $\sigma \in Gal(\overline{K}/K)$ tel que $\sigma|_F = \left(\frac{F/K}{\mathfrak{p}}\right)$ pour toute extension abélienne F de K. En particulier, $\sigma|_L = \left(\frac{L/K}{\mathfrak{p}}\right) = Id$. Soit P un point de N-torsion de E. On a :

$$\begin{aligned} \bar{f}_E(\overline{[\lambda]}(\bar{P})) &= \bar{f}_E(F(\bar{P})) && \text{d'après le diagramme} \\ &= \bar{f}_E(\overline{\sigma(P)}) && \text{puisque la reduction de } \sigma \text{ est } F \\ &= \overline{f_E(\sigma(P))} \\ &= \overline{\sigma(f_E(P))} && \text{comme } \sigma|_{\mathcal{H}_K} = Id \text{ et } f_E \text{ est définie sur } \mathcal{H}_K \\ &= \overline{f_E(P)} && \text{comme } f_E(P) \in L \text{ et } \sigma|_L = Id \\ &= \bar{f}_E(\bar{P}) \end{aligned}$$

Donc

$$\bar{f}_E(\overline{[\lambda]}(\bar{P})) = \bar{f}_E(\bar{P})$$

Ceci implique l'existence d'une unité $u \in \mathcal{O}_K^*$ telle que :

$$\overline{[\lambda]}(\bar{P}) = \overline{[u]}(\bar{P})$$

Pour presque tout premier $\mathfrak{p}$ la réduction $E[N] \mapsto \bar{E}[N]$ est injective, donc on obtient

$$[\lambda - u](P) = 0_E$$

On a donc montré que $[\lambda - u](P) = 0_E$ pour un point P de N-torsion *fixé*. Mais $E[N]$ est un $\mathcal{O}_K/N\mathcal{O}_K$ module libre de rang 1, donc cette égalité est vraie pour chaque $Q \in E[N]$. Donc $[\lambda - u]$ tue $E[N]$, ce qui donne

$$\lambda \equiv u \pmod{N} \Longrightarrow \lambda u^{-1} \equiv 1 \pmod{N}$$

Donc $\mathfrak{p} = (\lambda) = (\lambda u^{-1})$ (comme u est une unité) est de la forme $\mathfrak{p} = (\alpha)$, avec $\alpha = \lambda u^{-1} \equiv 1 \pmod{N}$, c'est à dire, $\mathfrak{p} \in Spl(K_N/K)$, ce qui termine la preuve du théorème.

Corollaire 4.3.7. *Toute extension abélienne d'un corps quadratique imaginaire K est contenue dans une extension de la forme $K(j_E, f_E(E[N]))$ pour un certain $N \in \mathbb{N}$.*

Démonstration. On a vu dans l'exemple 2.1.10 que tout cycle $\mathfrak{m}$ de K divise un cycle de la forme $\mathfrak{n} = N$. Le résultat découle alors de la proposition 2.2.3 et du théorème précédent. □

$\mathbb{Q}$	$K = \mathbb{Q}(\tau)$
$exp(z) = e^{2i\pi z}$	$j(z),\ f_E(z)$
$\mathbb{GL}_1(\mathbb{C})$	$E = \mathbb{C}/\mathfrak{a}$
$\mathbb{Q}$	$\mathcal{H}_K = K(j(E))$
$\mathbb{Q}(\mathbb{GL}_1(\mathbb{C})[N])$	$\mathcal{H}_K(f_E(E[N]))$
$exp(k/N)^p = exp(pk/N)$	$j(\mathfrak{p}^{-1}\mathfrak{a}) \equiv j(\mathfrak{a})^p \pmod{\mathfrak{B}}$

5 Applications de la théorie de la multiplication complexe

5.1 Les nombres premiers de la forme $x^2 + ny^2$

Au XVIIe siècle, Fermat démontra le résultat suivant, connu sous le nom de *théorème des deux carrés* : un nombre premier p impair s'écrit sous la forme $x^2 + y^2$, où x et y sont des entiers non nuls, si et seulement si p est congru à 1 modulo 4.

Rapidement, Fermat conjectura deux autres résultats similaires : si p est premier impair, alors

$$\exists x, y \in \mathbb{N},\ p \equiv x^2 + 2y^2 \Longleftrightarrow p = 1, 3 \pmod 8$$
$$\text{si } p \neq 3, \exists x, y \in \mathbb{N},\ p \equiv x^2 + 3y^2 \Longleftrightarrow p = 1 \pmod 3$$

Ces résultats seront démontrés par Lagrange un siècle plus tard. La question suivante se pose alors : peut-on déterminer tout les nombres premiers de la forme $x^2 + ny^2$, où n est un entier naturel sans facteurs carrés fixé à l'avance ?

La réponse est oui, et nous le montrerons dans le cas particulier où $n \in \mathbb{N}$ est sans facteur carré et vérifie $-n \equiv 2, 3 \pmod 4$. Notons $K = \mathbb{Q}(\sqrt{-n})$ (on a alors $\mathcal{O}_K = \mathbb{Z}[\sqrt{-n}]$) et soit p un premier impair tel que $p = x^2 + ny^2$, pour $x, y \in \mathbb{Z}$. Supposons que p divise $4n = disc(K/Q)$. Alors p divise n et, en particulier, $p \leq n$. En conséquence, la seule possibilité c'est que $p = n$. Supposons maintenant que p ne divise pas $4n$. Le polynôme minimal de $\sqrt{-n}$ est $h = X^2 + n$, qui est séparable modulo p. D'après la proposition 1.5.6, $p\mathcal{O}_K$ est alors non ramifié dans K. On a $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$ où $\mathfrak{p} = (x + \sqrt{-n}y)$. De plus $\mathfrak{p} \neq \bar{\mathfrak{p}}$ car p n'est pas ramifié. Donc on a démontre que si p est de la forme $x^2 + ny^2$ et $p \nmid 4n$ alors $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$, avec $\mathfrak{p}$ principal.

Réciproquement, si $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$ où $\mathfrak{p}$ est un idéal principal de $\mathcal{O}_K$, on peut écrire $\mathfrak{p} = (x+\sqrt{-n}y)$ de sorte que $p\mathcal{O}_K = (x^2+ny^2)\mathcal{O}_K$. Ainsi il existe $u \in \mathcal{O}_K^\times$ tel que $up = x^2+ny^2$. En prenant la valeur absolue, on en déduit que $p = x^2 + ny^2$.

Mais un idéal $\mathfrak{p}$ de $\mathcal{O}_K$ est principal si et seulement si $\mathfrak{p}$ se décompose totalement dans $\mathcal{H}_K$, le corps de classe de Hilbert de K. Ainsi, si $p = x^2 + ny^2$, alors p est totalement décomposé dans $\mathcal{H}_K$. Réciproquement, si p est totalement décomposé dans $\mathcal{H}_K$, on écrit

$$p\mathcal{O}_{\mathcal{H}_K} = \mathfrak{q}_1 \cdots \mathfrak{q}_{2n}$$

Comme p est totalement décomposé, le stabilisateur de tout diviseur de p pour l'action de $Gal(\mathcal{H}_K/\mathbb{Q})$ est trivial. En faisant agir la conjugaison complexe, on peut donc regrouper les termes deux par deux, quitte à les renuméroter :

$$p\mathcal{O}_{\mathcal{H}_K} = \mathfrak{q}_1\bar{\mathfrak{q}_1} \cdots \mathfrak{q}_n\bar{\mathfrak{q}_n} = \mathfrak{q}\bar{\mathfrak{q}}$$

où $\mathfrak{q} = \mathfrak{q}_1 \cdots \mathfrak{q}_n$. En notant $\mathfrak{p} = \mathfrak{q} \cap \mathcal{O}_K$, on obtient $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$. De plus, comme $\mathfrak{p}$ est totalement décomposé dans $\mathcal{H}_K$, il est principal, et p est bien de la forme $x^2 + ny^2$. Nous avons donc montré l'équivalence suivante :

$$p = x^2 + ny^2 \Longleftrightarrow p \text{ se décompose totalement dans } \mathcal{H}_K$$

De plus, on sait que $\mathcal{H}_K = K(j(\sqrt{-n}))$, où $j(\sqrt{-n})$ est un entier algébrique réel. On note $f_n \in \mathcal{O}_K[X]$ son polynôme minimal. En effet, on a $f_n \in \mathbb{Z}[X]$: on sait que le polynôme minimal de $j(\sqrt{-n})$ sur $\mathbb{Q}$ est à coefficients dans $\mathbb{Z}$; c'est f_n puisque $[\mathcal{H}_K : K] = [\mathbb{Q}(j(\sqrt{-n})) : \mathbb{Q}]$. On suppose que f_n est séparable modulo $p\mathcal{O}_K$. D'après le théorème 1.5.6, on sait que $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$, avec $\mathfrak{p} \neq \bar{\mathfrak{p}}$ si et seulement si $X^2 + n$ a une solution modulo p, c'est à dire si et seulement si $(-n/p) = 1$. D'après le même théorème, on déduit que $\mathfrak{p}$ est totalement décomposé dans $\mathcal{H}_K$ si et seulement si f_n a une racine dans $\mathcal{O}_K/\mathfrak{p}$. Comme $\mathcal{O}_K/\mathfrak{p} = \mathbb{Z}/p\mathbb{Z}$, la dernière condition est équivalente au fait que f_n ait une racine modulo p.

En résumé, si p est un nombre premier impair ne divisant pas n ni le discriminant de f_n, alors

$$\exists\, x, y \in \mathbb{N},\ p = x^2 + ny^2 \Longleftrightarrow \left\{ \begin{array}{l} \left(\frac{-n}{p}\right) = 1 \\ \\ f_n(x) = 0 \quad \text{a une solution dans } \mathbb{Z}/p\mathbb{Z} \end{array} \right\}$$

5.1.1 Un exemple explicite

On va montrer que, si p est un premier impair différent de 5 :

$$\begin{aligned} & \exists x, y \in \mathbb{Z} :\ p = x^2 + 5y^2 \\ \Longleftrightarrow & \left(\frac{-5}{p}\right) = 1 \text{ et } x^2 - 5 \text{ a un zéro dans } \mathbb{F}_p \\ \Longleftrightarrow & p \equiv 1, 9 \pmod{20} \end{aligned}$$

Montrons d'abord la deuxième équivalence. On a :

$$\left(\frac{-5}{p}\right) = 1 \Leftrightarrow \left\{ \begin{array}{l} p \equiv \pm 1 \pmod 5 \\ \\ p \equiv 1 \pmod 4 \end{array} \right\} \text{ ou } \left\{ \begin{array}{l} p \equiv \pm 2 \pmod 5 \\ \\ p \equiv 3 \pmod 4 \end{array} \right\} \Leftrightarrow p \equiv 1, 9, 7, 3 \pmod{20}$$

et

$$x^2 - 5 \text{ à un zéro dans } \mathbb{F}_p \Longleftrightarrow \left(\frac{5}{p}\right) = 1 \Longleftrightarrow \left(\frac{p}{5}\right) = 1 \Longleftrightarrow p \equiv 1, 4 \pmod 5$$

Donc

$$\begin{aligned} & \left(\frac{-5}{p}\right) = 1 \text{ et } x^2 - 5 \text{ a un zéro dans } \mathbb{F}_p \\ \Longleftrightarrow \quad & p \equiv 1, 9, 7, 3 \pmod{20} \text{ et } p \equiv 1, 4 \pmod 5 \\ \Longleftrightarrow \quad & p \equiv 1, 9 \pmod{20} \end{aligned}$$

Montrons maintenant que

$$\exists\, x, y \in \mathbb{Z} :\ p = x^2 + 5y^2 \Longleftrightarrow \left(\frac{-5}{p}\right) = 1 \text{ et } x^2 - 5 \text{ a un zéro dans } \mathbb{F}_p$$

On utilisera le fait que p s'écrit sous la forme x^2+5y^2 si et seulement si $\left(\frac{-5}{p}\right)=1$ et $f(x)$ a un zéro dans $\mathbb{F}_p$, où $f(x)$ est le polynôme minimal de $j(\sqrt{-5})$. Il faut donc déterminer $f(x)$.

On remarque d'abord que $K=\mathbb{Q}(\sqrt{-5})$ a nombre de classe 2. L'idéal $(2,1+\sqrt{-5})$ a norme 2, donc il n'est pas principal. On en déduit que $Cl(\mathcal{O}_K)=\{\mathcal{O}_K,(2,1+\sqrt{-5})\}$. On sait alors que le polynôme minimal de $j(\sqrt{-5})$ sur K est :

$$f(x)=(x-j(\sqrt{-5}))\left(x-j\left(\frac{1+\sqrt{-5}}{2}\right)\right)=x^2+ax+b$$

avec $a,b\in\mathbb{Z}$. On calcule maintenant ;

$$\begin{aligned} j(\sqrt{-5}) &= 1264538.9094751405\pm 10^{-10} \\ j\left(\frac{1+\sqrt{-5}}{2}\right) &= -\,538.9094751405\pm 10^{-10} \end{aligned}$$

Donc

$$\begin{aligned} -a=j\left(\frac{1+\sqrt{-5}}{2}\right)+j(\sqrt{-5}) &= 1264000.0000000000\pm 10^{-9} \\ b=j(\sqrt{-5})j\left(\frac{1+\sqrt{-5}}{2}\right) &= -\,681472000.0000000000\pm 10^{-2} \end{aligned}$$

Comme $f(x)$ a coefficients entiers, on en déduit que

$$f(x)=x^2-1264000x-681472000$$

Le discriminant de $f(x)$ vaut :

$$\Delta=1600421888000=2^{18}5^3 13^2 17^2$$

Donc $f(x)$ a un zéro dans $\mathbb{F}_p$ si et seulement si x^2-5 a un zéro dans $\mathbb{F}_p$.

On remarque que les calculs qu'on a fait nous permettent de conclure que

$$j(\sqrt{-5})=\frac{1264000+\sqrt{1600421888000}}{2}$$

et que le corps de classe de Hilbert de $K=\mathbb{Q}(\sqrt{-5})$ est $\mathcal{H}_K=K(\sqrt{5})$.

5.2 Division de la lemniscate

"Lemniscata geometrice in quinque partes dividitur."

Carl F. Gauss (1777-1855)

L'étude des corps cyclotomiques a permis à Gauss de démontrer le résultat classique suivant :

Théorème 5.2.1. *On peut diviser le cercle unitaire dans n parties égales à la règle et au compas si et seulement si n s'écrit sous la forme :*

$$n=2^a p_1 p_2\dots p_k$$

où les p_i sont premiers distincts de la forme $2^{2^{h_i}}+1$ (on les appelle premiers de Fermat*).*

Dans cette section, on va se servir de la théorie des courbes elliptiques à multiplication complexe qu'on a développé pour obtenir un résultat analogue pour la lemniscate.

Définition 5.2.2. *Soient $A, B \in \mathbb{R}^2$, et soit $c > 0$. On appelle* lemniscate *la courbe plane formée des points P tels que $|P - A||P - B| = c$.*

On choisit dans cette section $A = (-\sqrt{2}/2, 0)$, $B = (\sqrt{2}/2, 0)$ et $c = 1/2$. On trouve alors que l'équation de cette lemniscate est :

$$(x^2 + y^2)^2 = x^2 - y^2$$

qui s'écrit aussi $r^2 = \cos 2\theta$ en coordonnées polaires.
Pour $r \in [0, 1]$, on trouve que la longueur de l'arc de lemniscate contenu dans le premier quadrant et compris entre le point $(0, 0)$ et $(r\cos\theta(r), r\sin\theta(r))$ vaut

$$s(r) = \int_0^r \frac{1}{\sqrt{1 - r^4}} \mathrm{d}r$$

On note $\omega/2 = \int_0^1 \frac{1}{\sqrt{1-r^4}} \mathrm{d}r$ la longueur de l'arc de lemniscate contenu dans le premier quadrant. La longueur totale de la lemniscate est alors 2ω.
On remarque que l'application

$$\begin{aligned} s : [0, 1] &\longrightarrow [0, \omega/2] \\ r &\longmapsto \int_0^r \frac{1}{\sqrt{1 - r^4}} \mathrm{d}r \end{aligned}$$

est une bijection croissante. On note

$$\phi : [0, \omega/2] \to [0, 1]$$

son inverse. C'est un analogue pour la lemniscate de la fonction sinus pour le cercle. Le résultat suivant, du à Abel, décrit la propriété analytique cruciale de la fonction ϕ :

Proposition 5.2.3. *La fonction ϕ admet une extension à une fonction méromorphe sur $\mathbb{C}$, notée toujours ϕ.*

De plus, ϕ est une fonction elliptique pour le réseau $\Lambda = [(1 + i)\omega, (1 - i)\omega]$. Elle est donc L-périodique, pour $L = [2\omega, 2\omega i]$.

Les zéros de ϕ sont les points du réseau $[\omega, \omega i]$, et les pôles s'obtiennent en ajoutant $(\omega + \omega i)/2$ aux zéros. Les zéros et les pôles de ϕ sont simples.

Démonstration. Voir [2]. □

On peut formuler le problème de la division de la lemniscate en n parties égales de la façon suivante :

Pour quels valeurs de n les nombres $\phi(2k\omega/n)$, $k = 0, 1, \ldots, n - 1$ sont-ils constructibles à la règle et au compas ?

L'idée fondamentale pour répondre à cette question est d'utiliser la L-périodicité de la fonction ϕ pour la relier à la fonction de Weierstrass du réseau L, notée $\wp$.

Lemme 5.2.4. *Soit $L = [2\omega, 2\omega i]$.*

1. $g_2(L) = 1/4, g_3(L) = 0$
2. *$E := E_L = \mathbb{C}/L$ est isomorphe à la courbe projective lisse d'équation $y^2 = x^3 + x$*
3. *E est une courbe elliptique à multiplication complexe par l'anneau $\mathbb{Z}[i]$.*

Démonstration. 1. C'est un calcul. D'après 1. l'assertion 2. est triviale. Le dernier point découle du fait que le réseau L est homothétique au réseau $[1, i]$. □

Lemme 5.2.5. *1. On a les formules :*

$$\wp((1+i)z) = \frac{-i}{8}\frac{4\wp^2(z) - 1/4}{\wp(z)}$$

$$\wp((1-i)z) = \frac{i}{8}\frac{4\wp^2(z) - 1/4}{\wp(z)}$$

2. *si $\wp(\tau)$ est constructible, $\wp(\tau/2)$ l'est aussi.*
3. *Pour tout $a, b \in \mathbb{Z}$, $ab \neq 0$, pour tout $n \geq 1$, les nombres $\wp((2a\omega + 2bi\omega)/2^n)$ sont constructibles.*

Démonstration.
1. C'est un calcul direct, en utilisant la formule d'addition pour la fonction $\wp$ et les égalités $\wp(iz) = -\wp(z)$, qui découle de la définition de $\wp$, et $\wp'(iz) = i\wp(z)$, qui s'obtient par différentiation de l'égalité précédente.
2. Supposons $\wp(\tau)$ constructible. En posant $z = \tau/(1+i)$ dans la première égalité dans 1. on voit que $\wp(\tau/(1+i))$ satisfait une equation de degré 2 à coefficients constructibles, donc est constructible. Comme $\wp(\tau/(1+i)) = \wp((1-i)(\tau/2))$ la deuxième égalité dans 1., avec $z = \tau/2$, montre alors que $\wp(\tau/2)$ est constructible, comme c'est racine d'un polynôme quadratique à coefficients constructibles.
3. Les nombres $\wp(\omega), \wp(i\omega), \wp((1+i)\omega)$ sont les abscisses des points d'ordre 2 de la courbe $E : y^2 = 4x^3 - 1/4x$, donc il sont les racines du polynôme $4x^3 - 1/4x$, qui sont rationnelles donc constructibles. Ça montre le résultat pour $n = 1$. Le résultat général s'obtient par induction sur n à l'aide de 2.

□

Le résultat crucial suivant donne le lien entre la constructibilité des valeurs des fonctions ϕ et $\wp$.

Proposition 5.2.6. *$\phi(\tau)$ est constructible si et seulement si $\wp(\tau)$ l'est.*

Démonstration. Soit

$$g(z) = \frac{\wp'(z)}{(\wp(z) - \wp(z_0))(\wp(z) - \wp(z_1))}$$

avec $z_0 = (1+i)\omega/2$ et $z_1 = (3\omega + i\omega)/2$. Alors on vérifie que $g(z)$ a les mêmes zéros et pôles que $\phi(z)$, avec multiplicité. Il existe donc une constante c telle que $\phi(z) = cg(z)$. Comme $\phi(\omega/2) = 1$ et $g(\omega/2)$ est constructible d'après le lemme précédant, on trouve que c est constructible. Donc, si $\wp(\tau)$ est constructible $g(\tau)$ l'est, et $\phi(\tau)$ est aussi constructible.

Pour montrer la réciproque, on rappelle que ϕ est $\Lambda-$elliptique, avec $\Lambda = [(1+i)\omega, (1-i)\omega]$. Comme $(1+i)\Lambda = L$ on trouve que $\wp_\Lambda(z) = 2i\wp((1+i)z)$. On montre, par comparaison des zéros et pôles, qu'il existe une constante k telle que :

$$\phi(z) = k\frac{\wp_\Lambda(z) - \wp_\Lambda(\omega)}{\wp'_\Lambda(z)}$$

Cette identité, pour $z = \omega/2$, entraine que k est constructible.

Notons $u = (1+i)\omega/2$, $v = (1-i)\omega/2$. Comme les zéros de $\wp_\Lambda(z)$ sont u, v et ω, on trouve :

$$\phi(z)^2 = \frac{k^2}{4} \frac{\wp_\Lambda(z) - \wp_\Lambda(\omega)}{(\wp_\Lambda(z) - \wp_\Lambda(u))(\wp_\Lambda(z) - \wp_\Lambda(v))}$$

Donc si $\phi(\tau)$ est constructible $\wp_\Lambda(\tau)$ l'est. Comme

$$\wp_\Lambda(z) = 2i\wp((1+i)z) = \frac{1}{4}\frac{4\wp^2(z) - 1/4}{\wp(z)}$$

si $\wp_\Lambda(\tau)$ est constructible $\wp(\tau)$ est constructible, ce qui termine la preuve. □

En vue de cette proposition, le problème de la division de la lemniscate est réduit à la question suivante :

Pour quels valeurs de n les nombres $\wp(2k\omega/n)$, $k = 0, 1, \ldots, n-1$ sont-ils constructibles ?

L'énorme avantage de cette formulation est qu'elle porte sur les valeurs de la fonction $\wp$ du réseau L. La courbe elliptique correspondante $E = \mathbb{C}/L$ a multiplication complexe par l'anneau $\mathbb{Z}[i]$. On pourra alors utiliser les résultats de la section 4.3 pour répondre à la question.

Lemme 5.2.7. *1. On a un isomorphisme de $\mathbb{Z}[i]$-modules : $E[n] \cong \mathbb{Z}[i]/n\mathbb{Z}[i]$.*

2. Soit $K = \mathbb{Q}(i)$, F le corps obtenu en ajoutant à K les coordonnées des points dans $E[n]$. L'extension F/K est galoisienne, et on a un morphisme injectif :

$$Gal(F/K) \longrightarrow Aut_{\mathbb{Z}[i]}(E[n]) \cong (\mathbb{Z}[i]/n\mathbb{Z}[i])^*$$

3. Le groupe $(\mathbb{Z}[i]/n\mathbb{Z}[i])^*$ est un $2-$groupe si et seulement si n est de la forme $2^a p_1 \ldots p_k$, où les p_i sont premiers de Fermat.

Démonstration. 1. $E[n] \cong \frac{1}{n}L/L \cong L/nL \cong \mathbb{Z}[i]/n\mathbb{Z}[i]$

2. On a déjà observé dans la remarque 4.3.2 que F/K est galoisienne et qu'on a un morphisme injectif :

$$\rho : Gal(F/K) \longrightarrow Aut_{\mathbb{Z}}(E[n]) \cong Aut_{\mathbb{Z}}(\mathbb{Z}[i]/n\mathbb{Z}[i])$$

Le fait que E a multiplication complexe par $\mathbb{Z}[i]$ entraine que l'action de $Gal(F/K)$ sur $E[n]$ commute avec l'action de $\mathbb{Z}[i]$, c'est à dire, $\rho(\sigma) \in Aut_{\mathbb{Z}[i]}(E[n])$ pour tout $\sigma \in Gal(F/K)$.

3. C'est un calcul direct.

□

Grâce au lemme précédent, on peut donner une condition suffisante sur n pour la constructibilité des points $\phi(2k\omega/n)$.

Proposition 5.2.8. *Si $n = 2^a p_1 \ldots p_k$, où les p_i sont des premiers de Fermat distincts, alors les nombres $\phi(2k\omega/n), k = 0, \ldots, n-1$ sont constructibles.*

Démonstration. L'hypothèse sur n entraine que $(\mathbb{Z}[i]/n\mathbb{Z}[i])^*$ est un $2-$groupe, en conséquence $Gal(F/K)$ l'est, ce qui implique que $[F : \mathbb{Q}]$ est une puissance de 2, donc tout élément de F est constructible. En particulier, $\wp(2k\omega/n)$ est constructible pour $k = 0, \ldots n-1$, d'où le résultat. □

En effet, la réciproque de la proposition précédente est aussi vraie. Pour le montrer, on va utiliser le lemme suivant :

Lemme 5.2.9. *On note $K = \mathbb{Q}(i)$. Soit $M = K(\wp^2(2\omega/n))$. Alors M est le corps de classe de rayon n pour K, et on a un isomorphisme :*

$$Gal(M/K) \cong (\mathbb{Z}[i]/n\mathbb{Z}[i])^*/\{\pm 1, \pm i\}$$

Démonstration. Notons K_n le corps de classe de rayon n pour K. On a montré que $K_n = K(f_E(E[n]))$ où $f_E(z) = \frac{g_2(L)^2}{\Delta(L)}\wp^2(z)$. On a donc $K_n = K(\wp^2(E[n])) = K(\wp^2(2\omega/n))$. La dernière égalité découle du fait que pour tout $P, Q \in E[n]$ il existe $\tau \in \mathbb{Z}[i]$ tel que $Q = \tau P$, et alors $\wp(Q) = \wp(\tau P)$ est une fonction rationnelle de $\wp(P)$. Ceci montre que $M = K_n$. On sait que

$$\begin{aligned} Gal(K_n/K) &\cong \mathcal{I}_K(n)/\mathcal{P}_K(n) \\ &\cong \{\text{Idéaux de } \mathbb{Z}[i] \text{ premiers avec } n\}/\{(\alpha) : \alpha \in \mathbb{Z}[i], \alpha \equiv 1 \pmod{n}\} \end{aligned}$$

Comme $\mathbb{Z}[i]$ est principal, l'ensemble {Idéaux de $\mathbb{Z}[i]$ premiers avec n} s'identifie à $\{a \in \mathbb{Z}[i] : (a, n) = 1\}/\{\pm 1, \pm i\}$.

En plus, $(a) \in \mathcal{P}_K(n)$ si et seulement si $a \equiv 1 \pmod{n}$. On a donc un isomorphisme de groupes :

$$(\mathbb{Z}[i]/n\mathbb{Z}[i])^*/\{\pm 1, \pm i\} \cong \mathcal{I}_K(n)/\mathcal{P}_K(n)$$

ce qui termine la preuve. □

On peut finalement obtenir une caractérisation des entiers n tels que les nombres $\phi(2k\omega/n)$, $k = 0, \ldots, n-1$ soient constructibles, analogue au résultat de Gauss pour le cercle.

Théorème 5.2.10. *On peut diviser la lemniscate en n parties égales à la règle et au compas si et seulement si $n = 2^a p_1 \ldots p_k$, où les p_i sont premiers de Fermat distincts.*

Démonstration. On a déjà montré que la condition est suffisante. Montrons qu'elle est aussi nécessaire. Si $\phi(2\omega/n)$ est constructible, alors $\wp(2\omega/n)$ l'est. Le corps $M = K(\wp^2(2\omega/n))$ vérifie alors $[M : \mathbb{Q}] = 2^l$ pour un certain l, donc $Gal(M/K)$ est un $2-$groupe. Mais on a montré que $Gal(M/K) \cong (\mathbb{Z}[i]/n\mathbb{Z}[i])^*/\{\pm 1, \pm i\}$. On en déduit que $(\mathbb{Z}[i]/n\mathbb{Z}[i])^*$ est aussi un $2-$groupe, ce qui implique que n s'écrit comme dans l'énoncé du théorème. □

Conclusion

Nous avons donc, au terme de cet exposé, décrit de manière exhaustive les extensions abéliennes d'une extension quadratique imaginaire $K/\mathbb{Q}$ quelconque. D'une part grâce à la loi de réciprocité d'Artin qui classifie de manière intrinsèque les extensions abéliennes de K (on regarde un système de congruences relatif aux idéaux fractionnaires de $\mathcal{O}_K$), et d'autre part, grâce à la théorie de la multiplication complexe, qui, à l'instar du théorème de Kronecker-Weber pour $\mathbb{Q}$, nous a permis d'expliciter les corps de classe rayon N du corps K, en y ajoutant les abscisses des points de torsions de certaines courbes elliptiques.

Cette puissante théorie a des applications impressionnantes. Elle est à la base de la résolution d'un problème arithmétique sur lequel se sont penchés de nombreux mathématiciens du 17ème et 18ème siècle, parmi eux, Fermat, Euler, ou encore Legendre. Il s'agissait de déterminer les nombres premiers de la forme $x^2 + ny^2$, et nous avons résolu ce problème pour une infinité d'entiers n. Nous avons également pu determiner les valeurs de n pour lesquelles ils est possible de diviser la lemniscate en n parties égales à la règle et au compas, complétant ainsi les travaux de Gauss sur la construction des $n-$gones réguliers.

Remerciements

Nous tenons à remercier M. Nekovář, pour son aide précieuse, sa patience, et la motivation qu'il a su nous transmettre.

Références

[1] Conrad K., *Ostrowski's theorem*
http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/ostrowski.pdf

[2] Cox D., *Galois theory*, Wiley, 2012

[3] Cox D., *Primes of the form* $x^2 + ny^2$, Wiley, 2013

[4] Janusz G., *Algebraic number fields*, American Mathematical Society, 2005

[5] Lang S., *Elliptic functions*, Springer, 1987

[6] Milne J., *Algebraic number theory*
http://www.jmilne.org/math/CourseNotes/ant.html

[7] Milne J., *Modular functions and modular forms*
http://www.jmilne.org/math/CourseNotes/mf.html

[8] Nekovar J., *Algèbre 2* (notes de cours ENS 2015)
http://webusers.imj-prg.fr/~jan.nekovar/co/ens/

[9] Neukirch J., *Algebraic number theory*, Springer, 1999

[10] Rosen M., *Abel's theorem on the lemniscate*, American Mathematical Monthly, vol.88 **6**, 1981, 387-395

[11] Samuel P., *Théorie algébrique des nombres*, Hermann Paris, 1967

[12] A. Borel et al., *Seminar on complex multiplication*, Springer Lecture Notes in Mathematics 21, 1966

[13] Silverman J., *The arithmetic of elliptic curves*, Springer, 2009

[14] Silverman J., *Advanced topics in the arithmetic of elliptic curves*, Springer, 1999