Multiplication complexe et corps de classe de Hilbert

Alexandre Demoulin sous la tutelle de Konstantin Ardakov

1er Avril au 10 Août 2023 à Oxford

Table des matières

0.1 Déroulé du stage

Mon stage s'est déroulé à Oxford au Mathematical Institut (M.I.) sous la tutelle de Konstantin Ardakov du 1er Avril au 10 Août 2023. Le stage s'est constitué de rendez-vous hebdomadaire consitstant à échanger sur les livres que j'avais à étudier :

1. Le premier mois était consacré à l'étude des fondations de la géométrie algébrique et de la théorie des schémas.
2. Le deuxième mois était consacré à l'étude des fondements de la théorie des corps locaux notament avec [Ser62].
3. Le troisième mois était consacré à l'étude de la théorie de Lubin-Tate.
4. Le dernier mois s'est dévoué à l'étude du résultat que je présente dans ce mémoire. Il a cru bon de présenter ce résultat car il utilise presque tout ce qui a été abordé durant ce stage.

J'ai aussi assisté à de nombreuses conférences de mathématiques que proposait le M.I. mais aussi un cycle de conférences de combinatoire à Londre où j'ai pu parler plus en détails avec certains chercheurs.

0.2 Contexte mathématique

Mon stage aura été une introduction à la théorie algébrique des nombres. Cette dernière étudie les extensions finies de $\mathbf{Q}$ contenues dans $\mathbf{C}$. Un des points de départ de cette théorie est par exemple la question suivante appelé problème de Galois inverse :

Question 0.2.1 Étant donné un groupe fini G, peut-on trouver un corps de nombre $\mathbf{K}$ tel que $\mathrm{Gal}(\mathbf{K}/\mathbf{Q}) = G$?

On peut décliner cette question sous plusieurs aspects notamment en remplaçant le corps $\mathbf{Q}$ par un autre corps ou en ne s'interressant qu'à une certaine catégorie de groupe pour G. La théorie de Lubin-Tate élucide la question pour $\mathbf{Q}_p$ (corps des nombres p-adiques) pour p premier et G un groupe abélien en calculant explicitement $\mathbf{Q}_p^{ab}$ la plus grande extension abélienne de $\mathbf{Q}_p$ et son groupe de galois.

Résultat 0.2.2 Soit p un nombre premier alors $\mathrm{Gal}(\mathbf{Q}_p^{ab}/\mathbf{Q}) \simeq \hat{\mathbf{Z}} \times \mathbf{Q}_p^{\times}$

Nous n'expliquerons pas ce que siginifie $\hat{\mathbf{Z}}$, on notera simplement que nous avons explicitement calculé $\mathrm{Gal}(\mathbf{Q}_p^{ab}/\mathbf{Q})$. Par la correspondance de Galois, la question est entièrement résolue : les sous-groupes abéliens solution du problème inverse de Galois pour $\mathbf{Q}_p$ sont les sous-groupes finis de $\mathrm{Gal}(\mathbf{Q}_p^{ab}/\mathbf{Q})$. Ce résultat a été mentionné en premier car il a été longuement étudié durant le stage mais on peut plus simplement citer le théorème de Konecker-Weber qui offre une solution explicite au problème **0.2.1** dans le cas où G est abélien.

Résultat 0.2.3 On note $\mathbf{Q}^{cyc} = \mathrm{Vect}_{\mathbf{Q}}\{\zeta \in \mathbf{C}, \exists n \in \mathbf{N} \quad \zeta^n = 1\}$ alors $\mathbf{Q}^{ab} = \mathbf{Q}^{cyc}$ et $\mathrm{Gal}(\mathbf{Q}^{cyc}/\mathbf{Q}) \simeq \hat{\mathbf{Z}}$.

Pour aboutir à ce résultat il a été nécessaire de faire de la théorie de la ramification que nous expliquerons dans la section **2.** Pour caricaturer le processus, certaines extensions de corps de nombres présentent des ramifiactions et d'autre non. Lorsqu'elles en ont, cette ramification constitue un point d'attaque à l'étude de l'extension. Lorsqu'elle n'en présente pas, la situation est plus délicate. Par exemple le résultat **0.2.3** assure que chaque extension abélienne de $\mathbf{Q}$ est ramifiée. En revanche si l'on remplace $\mathbf{Q}$ par un corps de nombre plus gros cette propriété n'est plus vraie. On appelle le corps de classe de Hilbert d'un corps de nombre la plus grande extension abélienne non ramifiée. Ainsi le corps de classe de Hilbert de $\mathbf{Q}$ est $\mathbf{Q}$. L'objet d'une partie de ce stage a été de calculer ce corps de classe de Hilbert pour une certaine catégorie de corps de nombre.

Théorème 0.2.4 Soit $\mathbf{K}$ un corps quadratique complexe (i.e. de la forme $\mathbf{Q}(\sqrt{d})$ où d est un entier négatif) alors le corps de classe de Hilbert de $\mathbf{K}$ est égale à $\mathbf{K}(j(\mathcal{O}_{\mathbf{K}}))$.

Dans une première partie nous introduirons les outils cruciaux de la théorie algébrique des nombres. Nous détaillerons ensuite ce que signifie "être ramifié". Enfin, nous ferons un détour par les courbes elliptiques (ceci précisera quel est la quantité $j(\mathcal{O}_{\mathbf{K}})$). Pour finir, nous préciserons ce qu'est le corps de classe de Hilbert et nous fournirons la démonstration du théorème **0.2.4.**

1 Le groupe des idéaux

Le but de cette section de fournir une démonstration partielle de l'existence et l'unicité de la décompositon des idéaux fractionnaires dans un anneau de Dedekind en idéaux premiers. Nous introduirons également les groupes $\mathfrak{I}(\mathcal{O}_{\mathbf{K}})$ et $\mathcal{CL}(\mathcal{O}_{\mathbf{K}})$ qui s'avèreront cruciaux par la suite.

1.1 Anneaux de Dedekind

Définition 1.1.1

1. Un *corps de nombre* $\mathbf{K}$ est un sous-corps de $\mathbf{C}$ de degré fini sur $\mathbf{Q}$.
2. Un *entier est algébrique* s'il est racine d'un polynôme unitaire à coeficients entiers. Si $\mathbf{K}$ est un corps, on note $\mathcal{O}_{\mathbf{K}}$ l'anneau des entiers algébriques de $\mathbf{K}$.
3. Un anneau R est dit *intégralement clos* si $\mathcal{O}_{\mathbf{K}} = R$ où $\mathbf{K}$ est le corps des fractions de R.

Par exemple, l'anneau des entiers de $\mathbf{Q}$ est $\mathbf{Z}$ et l'anneau des entiers du corps de nombre $\mathbf{Q}[\sqrt{2}]$ est $\mathbf{Z}[\sqrt{2}]$.

Définition 1.1.2 Soit $\mathbf{K}$ un corps de nombre de degré n sur $\mathbf{Q}$. On note $\sigma_1, \sigma_2, \dots \sigma_n$ les n plongement de $\mathbf{K}$ dans $\mathbf{C}$. On appelle *norme* d'un élément $x \in \mathbf{K}$ la quantité $N_{\mathbf{K}}(x) = \sigma_1(x)\sigma_2(x)\dots\sigma_n(x)$.

On rappelle que si $x \in \mathcal{O}_{\mathbf{K}}$ alors $N_{\mathbf{K}}(x) \in \mathbf{Z}$. Par exemple $N_{\mathbf{Q}[i]}(i) = 1$ et $N_{\mathbf{Q}[\sqrt{2}]}(\sqrt{2}) = -2$.

Définition 1.1.3 Soit R un anneau. Il est dit *de Dedekind* si les conditions suivantes sont vérifiées :

1. Tout les idéaux premiers non nuls de R sont maximaux.
2. R est intègre.
3. R est intégralement clos.
4. R est Noethérien.

1.2 Anneaux à valuation discrète

Le but de cette section est de donner une caractérisation locale des anneaux de Dedekind.

Définition 1.2.1 Soit A un anneau, on dit que A est un *anneau à valuation* discrète si les conditions suivantes sont vérifiés :

1. A est principal.
2. A possède un unique idéal premier non nul.

Ainsi, si on note π un élément tel que $\mathfrak{m} = \pi A$ où $\mathfrak{m}$ est l'unique idéal premier non nul de A, alors, par factorialité de A, tout éléments est de la forme $\pi^n u$ où $n \in \mathbf{N}$ et u est une unité. Ainsi, le corps des fractions $\mathbf{K}$ de A est exactement égale à $A[\pi^{-1}]$.

Exemple 1.2.2 L'anneau $\mathbf{Z}_{(p)}$ pour p un nombre premier est un anneau à valuation discrète de même que l'anneau $\mathbf{Z}_p$ des entiers p-adiques. Dans les deux cas on peut prendre $\pi = p$.

Proposition 1.2.3 Si R est un anneau intègre et Noethérien alors les propriétés suuivantes sont équivalentes :

1. R est un anneau de Dedekind.
2. Pour chaque idéal premier non nul $\mathfrak{p}$, l'anneau local $R_\mathfrak{p}$ est un anneau à valuation discrète.

On pourra trouver la démonstration de ce théorème dans [Ser62] (**1.3.4**).

Définition 1.2.4 Soit A un anneau intègre et $\mathbf{K}$ son corps des fractions. Un *idéal fractionnaire* de A est un sous A-module de type fini de $\mathbf{K}$.

Si $\mathfrak{a}$ est un tel idéal fractionnaire alors on pourra toujours réduire au même dénominateur les générateurs de $\mathfrak{a}$. Si α est un tel dénominateur alors il existe $\mathfrak{i}$ un idéal de A tel que $\mathfrak{a} = \frac{1}{\alpha}\mathfrak{i}$

Exemple 1.2.5 Les ensembles $2\mathbf{Z}$ et $\frac{5}{3}\mathbf{Z}$ sont deux idéaux fractionnaires de $\mathbf{Z}$

Remarque. Les idéaux fractionnaires d'un anneau à valuation discrète A sont les $\pi^k A$ où $k \in \mathbf{Z}$.

1.3 Unicité de la décomposition en idéaux premiers

Le but de cette section est de montrer que les idéaux d'un anneau de Dedekind peuvent se décomposer uniquement comme le produit d'idéaux premiers.

Définition 1.3.1 Soit $\mathfrak{a}$ un idéal fractionnaire de A. On dit que $\mathfrak{a}$ est inversible si $\mathfrak{a}\mathfrak{a}^{-1} = A$ où l'idéal fractionnaire $\mathfrak{a}^{-1}$ désigne :

$$\mathfrak{a}^{-1} = \{x \in \mathbf{K} | x\mathfrak{a} \subset A\}$$

Remarque. L'ensemble $\mathfrak{a}^{-1}$ est bien un idéal fractionnaire en effet, si $\alpha \in \mathfrak{a}$ est non nul, $\mathfrak{a}^{-1} \subset \frac{1}{\alpha}A$.

Soit $\mathfrak{p}$ un idéal premier et $\mathfrak{a}, \mathfrak{b}$ des idéaux fractionnaires d'un anneau intègre R. On notera alors $\mathfrak{a}_\mathfrak{p} = \mathfrak{a} \cdot R_\mathfrak{p}$ et on vérfie que l'on dispose de :

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

$$(\mathfrak{a}\mathfrak{b})_\mathfrak{p} = \mathfrak{a}_\mathfrak{p}\mathfrak{b}_\mathfrak{p}$$

Théorème 1.3.2 Dans un anneau de Dedekind R, tout idéal fractionnaire non nul est inversible. On note alors $\mathfrak{I}(R)$ le groupe des idéaux non nuls de R.

Démonstration. Soit $\mathfrak{a}$ un idéal fractionnaire de R. On suppose, par l'absurde que l'idéal $\mathfrak{i} := \mathfrak{a}\mathfrak{a}^{-1}$ ne soit pas égal à R. Ainsi, il est contenu dans un idéal premier $\mathfrak{p}$ non nul. Ainsi :

$$\mathfrak{i}_\mathfrak{p} = \mathfrak{a}_\mathfrak{p}\mathfrak{a}_\mathfrak{p}^{-1}$$

Comme $\mathfrak{i} \subset \mathfrak{p}$, $\mathfrak{i}_\mathfrak{p} \subsetneq \pi R_\mathfrak{p}$. Mais si $\mathfrak{a}_\mathfrak{p} = \pi^k R_\mathfrak{p}$ alors on peut montrer que $\mathfrak{a}_\mathfrak{p}^{-1} = \pi^{-k} R_\mathfrak{p}$. On obtient donc $\mathfrak{i}_\mathfrak{p} = R_\mathfrak{p}$ ce qui est une contradiction. □

On note $\mathcal{CL}(R)$ le groupe quotient de $\mathfrak{I}(R)$ par le sous-groupe engendré par les idéaux principaux non nuls.

Théorème 1.3.3 Soit $\mathfrak{i}$ un idéal non nul de R un anneau de Dedekind. Alors il existe un unique entier naturel $n \in \mathbf{N}$ et des uniques idéaux premiers non nuls $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n$ tel que $\mathfrak{i} = \mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_n$.

Démonstration. ***Existence :*** On note E l'ensemble des idéaux ne vérifiant pas le théorème, par l'absurde supposons E non vide. Alors, comme R est Noethérien, on peut prendre $\mathfrak{j}$ un élément maximal pour l'inclusion ($\mathfrak{j} \neq R$ car $R \notin E$ comme étant un produit vide d'idéaux premiers).
On peut ainsi écrire $\mathfrak{j} = \mathfrak{i}\mathfrak{p}$, $\mathfrak{i}$ désignant un idéal et $\mathfrak{p}$ désignant un idéal premier non nul. On dispose, par essence, de $\mathfrak{i} \subset \mathfrak{j}$. Si $\mathfrak{j} = \mathfrak{i}$ alors $\mathfrak{j} = \mathfrak{j}\mathfrak{p}$ d'où $\mathfrak{p} = R$ ce qui est absurde. Ainsi $\mathfrak{i} \subsetneq \mathfrak{j}$ et donc $\mathfrak{i} \notin E$. On en déduit ainsi une décomposition pour $\mathfrak{i}$ et donc une décomposition pour $\mathfrak{j}$ ce qui est absurde.
Unicité : Prenons deux écriture différentes : $\mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_n = \mathfrak{q}_1\mathfrak{q}_2 \ldots \mathfrak{q}_m$. Alors $\mathfrak{q}_1\mathfrak{q}_2 \ldots \mathfrak{q}_m \subset \mathfrak{p}_1$ et aisni l'un des $\mathfrak{q}_i$, disons $\mathfrak{q}_1$ est contenu dans $\mathfrak{p}_1$. Comme tout idéal premier est maximal dans un anneau de Dedekind, $\mathfrak{p}_1 = \mathfrak{q}_1$. Ainsi en simplifiant de part et d'autre et en itérant on obtient $n = m$ et $\mathfrak{p}_i = \mathfrak{q}_i$. □

1.4 Application aux corps de nombres

Le but de cette partie est de montrer que $\mathcal{O}_\mathbf{K}$ est un anneau de Dedekind pour $\mathbf{K}$ un corps de nombre.

lemme 1.4.1 Soit $\mathfrak{i}$ un idéal de $\mathcal{O}_\mathbf{K}$ alors $\mathcal{O}_\mathbf{K}/\mathfrak{i}$ est un corps fini. On notera $\|i\|$ son cardinal.

Démonstration. Prenons $x \in \mathfrak{i}$ non nul et posons $r = N_\mathbf{K}(x) \in \mathbf{Z}$. On a alors $r \in \mathfrak{i}$ car $r/x \in \mathbf{K}$. Le nombre r/x est un entier algébrique, étant produit de conjugués de x. Si on écrit $\mathcal{O}_\mathbf{K} = \bigoplus \alpha_i \mathbf{Z}$ alors comme $(r) \subset \mathfrak{i}$, $\mathcal{O}_\mathbf{K}/\mathfrak{i} \subset \mathcal{O}_\mathbf{K}/(r) = \bigoplus \alpha_i \mathbf{Z}/r\mathbf{Z}$. Le dernier ensemble est fini de cardinal r^n. □

Théorème 1.4.2 Si $\mathbf{K}$ est un corps de nombre, $\mathcal{O}_\mathbf{K}$ est un anneau de Dedekind.

Démonstration.
1. Si $\mathfrak{p}$ est un idéal premier de $\mathcal{O}_\mathbf{K}$ alors l'anneau intègre $\mathcal{O}_\mathbf{K}/\mathfrak{p}$ étant fini c'est donc un corps. Dès lors $\mathfrak{p}$ est maximal.
2. $\mathcal{O}_\mathbf{K}$ est intègre.
3. $\mathcal{O}_\mathbf{K}$ est intégralement clos par essence.

4. Les idéaux de $\mathcal{O}_{\mathbf{K}}$ sont des sous-groupe de $\mathcal{O}_{\mathbf{K}}$ qui est finiement engendré. Ainsi les idéaux de $\mathcal{O}_{\mathbf{K}}$ sont finiement engendrés et donc $\mathcal{O}_{\mathbf{K}}$ est Noethérien.

□

2 Théorie de la ramifiaction

Le but de cette section est d'introduire les objets nécessaires pour expliquer ce qu'est l'application d'Artin et le conducteur d'une extension.

2.1 Décomposition des idéaux premiers dans les extensions

On fixe $\mathbf{K} \subset \mathbf{L}$ deux corps de nombres.

Définition-Propriété 2.1.1 Soit $\mathfrak{p}$ un idéal premier non nul de $\mathcal{O}_{\mathbf{K}}$ et $\mathfrak{P}$ un idéal premier non nul de $\mathcal{O}_{\mathbf{L}}$ alors on dit que $\mathfrak{P}$ est *au-dessus* de $\mathfrak{p}$ si l'une des conditions suivantes équivalentes ci-dessous est vérifée :

1. $\mathfrak{P} | \mathfrak{p}\mathcal{O}_{\mathbf{L}}$
2. $\mathfrak{P} \supset \mathfrak{p}\mathcal{O}_{\mathbf{L}}$
3. $\mathfrak{P} \supset \mathfrak{p}$
4. $\mathfrak{P} \cap \mathcal{O}_{\mathbf{K}} = \mathfrak{p}$
5. $\mathfrak{P} \cap \mathbf{K} = \mathfrak{p}$

Démonstration. En effet,

— $1 \Leftrightarrow 2$ est une conséquence de **1.3.3.**

— $2 \Leftrightarrow 3$ est clair

— $4 \Rightarrow 3$

— $4 \Leftrightarrow 5$ car les éléments de $\mathfrak{P}$ sont des entiers algébriques.

— Montrons $3 \Leftrightarrow 4$, $\mathfrak{P} \cap \mathcal{O}_{\mathbf{K}}$ étant un idéal premier non nul de $\mathcal{O}_{\mathbf{K}}$ vérifiant $\mathfrak{P} \cap \mathcal{O}_{\mathbf{K}} \supset \mathfrak{p}$ alors ou bien $\mathfrak{P} \cap \mathcal{O}_{\mathbf{K}} = \mathcal{O}_{\mathbf{K}}$ ou bien $\mathfrak{P} \cap \mathcal{O}_{\mathbf{K}} = \mathfrak{p}$ car $\mathcal{O}_{\mathbf{K}}$ est un anneau de Dedekind. Le premier cas est impossible car dès lors $1 \in \mathfrak{P}$.

□

Théorème 2.1.2 Pour tout idéal premier non nul $\mathfrak{p}$ de $\mathcal{O}_{\mathbf{K}}$, il existe $\mathfrak{P}$ un idéal premier non nul de $\mathcal{O}_{\mathbf{L}}$ tel que $\mathfrak{P}$ soit au-dessus de $\mathfrak{p}$. Tout idéal premier $\mathfrak{P}$ de $\mathcal{O}_{\mathbf{L}}$ est au-dessus d'un unique idéal de $\mathcal{O}_{\mathbf{K}}$.

Démonstration. Pour la première partie il suffit de prendre un divieur premier de $\mathfrak{p}\mathcal{O}_{\mathbf{L}}$, sauf si ce dernier est égal à $\mathcal{O}_{\mathbf{L}}$. Le cas échéant prenons $\gamma \in \mathfrak{p}^{-1} \backslash \mathcal{O}_{\mathbf{K}}$ de tel sorte que $\gamma\mathfrak{p} \subset \mathcal{O}_{\mathbf{K}}$. On obtient alors $\gamma\mathfrak{p}\mathcal{O}_{\mathbf{L}} \subset \mathcal{O}_{\mathbf{K}}\mathcal{O}_{\mathbf{L}} \subset \mathcal{O}_{\mathbf{L}}$. Si $\mathfrak{p}\mathcal{O}_{\mathbf{L}} = \mathcal{O}_{\mathbf{L}} \ni 1$ alors $\gamma \in \mathcal{O}_{\mathbf{L}}$ est un entier algébrique et donc $\gamma \in \mathcal{O}_{\mathbf{K}}$ fournissant une contradiction. Pour la deuxième partie du théorème l'idéal $\mathfrak{P}$ est au-dessus de $\mathfrak{P} \cap \mathcal{O}_{\mathbf{K}}$, non nul car contenant la norme des éléments de $\mathfrak{P}$. □

2.2 Les nombres e, g et f

Pour cette partie, on fixe $\mathfrak{p}$ un idéal premier non nul de $\mathcal{O}_\mathbf{K}$ et $\mathfrak{P}$ un idéal premier non nul de $\mathcal{O}_\mathbf{L}$ au-dessus de $\mathfrak{p}$.

Définition 2.2.1 On appelle *indice de ramification* de $\mathfrak{P}$ au dessus l'unique entier naturel $e_{\mathbf{L}/\mathbf{K}}(\mathfrak{P}|\mathfrak{p}) = e$ tel que $\mathfrak{P}^e$ divise $\mathfrak{p}\mathcal{O}_\mathbf{L}$ et e maximale.

Définition 2.2.2 On note $g_{\mathbf{L}/\mathbf{K}}(\mathfrak{p})$ le nombre de facteurs premiers de $\mathfrak{p}\mathcal{O}_\mathbf{L}$.

Définition-Propriété 2.2.3 Le corps fini $\mathcal{O}_\mathbf{K}/\mathfrak{p}$ s'injecte canoniquement dans $\mathcal{O}_\mathbf{L}/\mathfrak{P}$. On note $f_{\mathbf{L}/\mathbf{K}}(\mathfrak{P}|\mathfrak{p})$ et on appelle *degré d'inertie* la dimension de $\mathcal{O}_\mathbf{L}/\mathfrak{P}$ comme $\mathcal{O}_\mathbf{K}/\mathfrak{p}$-espace vectoriel.

Théorème 2.2.4 La $\mathcal{O}_\mathbf{K}/\mathfrak{p}$-algèbre $\mathcal{O}_\mathbf{L}/\mathfrak{p}\mathcal{O}_\mathbf{L}$ est de dimension $n = [\mathbf{L} : \mathbf{K}]$ et on dispose de :

$$n = \sum_{\mathfrak{q}|\mathfrak{p}} f(\mathfrak{q}|\mathfrak{p})e(\mathfrak{q}|\mathfrak{p})$$

Démonstration. L'essence de la preuve consiste à montrer que $\mathcal{O}_\mathbf{L}$ est un $\mathcal{O}_\mathbf{K}$-module libre de rang n, cela montre la première assertion. Pour la seconde on prouve l'isomorphisme $\mathcal{O}_\mathbf{L}/\mathfrak{p}\mathcal{O}_\mathbf{L} \simeq \prod_{\mathfrak{P}|\mathfrak{p}} \mathcal{O}_\mathbf{K}/\mathfrak{P}^{e(\mathfrak{P}|\mathfrak{p})}\mathcal{O}_\mathbf{K}$ puis on calcule la dimension de chacun des facteurs . On trouvera la preuve complète dans [Ser62] (**1.5.10.**). □

Définition 2.2.5 On dit que :

— $\mathfrak{p}$ est *ramifié* si $e(\mathfrak{P}|\mathfrak{p}) > 1$ pour un $\mathfrak{P}$ au dessus de $\mathfrak{p}$.

— $\mathfrak{p}$ est *inerte* si $g(\mathfrak{p}) = 1$ et $e(\mathfrak{P}|\mathfrak{p}) = 1$ pour tout $\mathfrak{P}$ au dessus de $\mathfrak{p}$.

Exemple 2.2.6 Par exemple prenons l'extension $\mathbf{Q} \subset \mathbf{Q}(\sqrt{2})$. L'idéal $2\mathbf{Z}[\sqrt{2}]$ se décompose en $(\sqrt{2}\mathbf{Z}[\sqrt{2}])^2$. Dès lors :

1. $e(\sqrt{2}\mathbf{Z}[\sqrt{2}]|2\mathbf{Z}) = 2$.
2. $f(\sqrt{2}\mathbf{Z}[\sqrt{2}]|2\mathbf{Z}) = 1 (car \mathbf{Z}/2\mathbf{Z} \simeq \mathbf{Z}[\sqrt{2}]/\sqrt{2}\mathbf{Z}[\sqrt{2}])$. On retrouve bien la formule de **2.2.5.**
3. L'idéal $2\mathbf{Z}$ est ramifié, mais $3\mathbf{Z}$ ne l'est pas pour cette extension.

2.3 Théorie de Galois et ramification

On conserve les notations de la partie précédentes. On notera $\overline{\mathbf{L}} = \mathcal{O}_\mathbf{L}/\mathfrak{P}$ et $\overline{\mathbf{K}} = \mathcal{O}_\mathbf{K}/\mathfrak{p}$. Les démonstrations des théorèmes **2.3.1** et **2.3.4** sont présentes dans [Ser62].

Théorème 2.3.1 Le groupe $\mathrm{Gal}(\mathbf{L}/\mathbf{K})$ agit transitivement sur les idéaux premiers non nuls $\mathfrak{P}$ de $\mathcal{O}_\mathbf{L}$ au-dessus de $\mathfrak{p}$.

Définition 2.3.2 On pose :

— Le groupe de décomposition $D_{\mathbf{L}/\mathbf{K}}(\mathfrak{P}) = \{\sigma \in \mathrm{Gal}(\mathbf{L}/\mathbf{K}) \mid \sigma(\mathfrak{P}) = \sigma\}$

— Le groupe d'inertie $T_{\mathbf{L}/\mathbf{K}}(\mathfrak{P}) = \{\sigma \in \mathrm{Gal}(\mathbf{L}/\mathbf{K}) \mid \sigma(\alpha) \equiv \alpha \bmod \mathfrak{P}\ \forall \alpha \in \mathcal{O}_\mathbf{L}\}$

Proposition 2.3.3 Le cardinal de D est égale à ef.

Démonstration. L'action étant transitive, il suffit d'utiliser la formule orbite-stabilisateur. □

Remarque. Le groupe T est inclus dans le groupe D. Pour chaque éléments de $\sigma \in D$, on peut définir $\overline{\sigma} \in \mathrm{Gal}(\overline{\mathbf{L}}/\overline{\mathbf{K}})$ par $\sigma(\overline{\alpha}) = \overline{\sigma(\alpha)}$. Ainsi T est le noyau de $\overline{\cdot}$.

Théorème 2.3.4 L'application

$$\begin{aligned} \phi \ : \ D/T &\longrightarrow \mathrm{Gal}(\overline{\mathbf{L}}/\overline{\mathbf{K}}) \\ [\sigma] &\longmapsto \overline{\sigma} \end{aligned}$$

est un isomorphisme.

2.4 Morphisme et théorème d'Artin

On se place ici dans le cas où l'idéal $\mathfrak{P}$ est non-ramifié au-dessus de $\mathfrak{p}$. Dans ce cas un simple calcul assure que le cardinal de T est égale à $e = 1$. Dès lors l'application $\overline{\cdot}$ est un isomorphisme. Il existe alors un unique élément $\sigma_{\mathfrak{P}}$ tel que $\overline{\sigma_{\mathfrak{P}}}$ soit le morphisme de Frobenius de l'extension $\mathrm{Gal}(\overline{\mathbf{L}}/\overline{\mathbf{K}})$.

Proposition 2.4.1 Soit $s \in \mathrm{Gal}(\mathbf{L}/\mathbf{K})$, on dipose des égalités suivantes :

$$D(s\mathfrak{P}) = sD(\mathfrak{P})s^{-1} \quad \sigma_{s\mathfrak{P}} = s\sigma_{\mathfrak{P}}s^{-1}$$

Remarque. Si l'extension $\mathbf{L}/\mathbf{K}$ est abélienne, on notera que les groupes et éléments $D(\mathfrak{P}), \sigma_{\mathfrak{P}}$ ne dépendent uniquement que de $\mathfrak{p}$. On les notera, dans ce cas, $D(\mathfrak{p})$ et $\sigma_{\mathfrak{p}}$. On se placera dans l'hypothèse que $\mathbf{L}/\mathbf{K}$ est abélienne.

Définition 2.4.1

- Soit $\mathfrak{a}$ un idéal de $\mathcal{O}_{\mathbf{K}}$. On note $\mathfrak{I}(\mathfrak{a})$ le sous-groupe de $\mathfrak{I}(\mathcal{O}_{\mathbf{K}})$ des idéaux premiers avec $\mathfrak{a}$.
- Soit $\mathfrak{d}$ un idéal tel que si $\mathfrak{p}$ est ramifié, alors $\mathfrak{p}|\mathfrak{d}$. Alors on définit *l'application d'Artin* comme :

$$\begin{aligned} (\cdot, \mathbf{L}/\mathbf{K}) \ : \ \mathfrak{I}(\mathfrak{d}) &\longrightarrow \mathrm{Gal}(\mathbf{L}/\mathbf{K}) \\ \mathfrak{p} &\longmapsto \sigma_{\mathfrak{p}} \end{aligned}$$

Théorème 2.4.3 Il existe un idéal $\mathfrak{d}$ tel que chaque premiers ramifié le divise et tel que si $\alpha \equiv 1 \bmod \mathfrak{d}$ alors $((\alpha), \mathbf{L}/\mathbf{K}) = 1$.

Remarque. Parmi tout les idéaux vérifiant cette propriété, on appelera *conducteur* tout idéal maximal pour cette propriété.

3 Courbe Elliptiques

Nous reviendrons plus tard sur l'utilité du théorème **2.4.3.**, on peut déjà souligner qu'il permet d'obtenir des informations sur $\mathrm{Gal}(\mathbf{L}/\mathbf{K})$ dans le cas où l'extension est abélienne. Cette section aura pour but de présenter brièvement les courbes elliptiques et leurs liens avec les deux parties précédentes via la multiplication complexe. Cette présentation ne saurait faire guise d'une pédagogie redoutable par manque d'espace. Tout·e lecteur·ice étranger·ère au vaste concept des courbes elliptiques pourra se référer à [Rei88] et [Sil08] puis [Sil94] pour les sujets plus pointus abordé en la fin de cette section. On pourra trouver dans ces mêmes références toutes les démonstrations omises et les rappels présents dans cette section.

3.1 Introduction aux courbes elliptiques

Définition 3.1.1 Soit $\mathbf{K}$ un corps et n un entier naturel.

- On nomme *ensemble algébrique projectif* tout sous-ensemble V de $\mathbb{P}^n(\mathbf{K})$ étant le lieu d'annulation d'un idéal I homogène de $\mathbf{K}[X_0, X_1, \ldots, X_n]$.
- Pour un tel ensemble V on note $I(V)$ l'idéal engendré par les polynômes homogènes s'annulant sur tout V. L'ensemble V est une *variété algébrique projective* si $I(V)$ est un idéal premier.
- On désigne par l'anneau $\mathbf{K}(V)$ l'ensemble des fractions f/g quotienté par $\sim$ où $f, g \in \mathbf{K}[X_0, X_1, \ldots, X_n]$ mais $g \notin I(V)$ tel que f et g sont homogènes de même degrés et $f/g \sim f'/g'$ si et seulement si f et f' ont le même degré et $f - f' \in I(V)$.
- Un élément $f \in K(V)$ est régulier en $P \in V$ dès lors que f a un représentant de la forme g/h où $h(P) \neq 0$.
- Lorsque V est une variété alors on appelle *dimension* de V le degré de transcendance de $\mathbf{K}(V)$ par rapport à $\mathbf{K}$.
- Une *courbe algébrique* est une variété de dimension 1.

Remarque. Un idéal homogène est un idéal engendré par des polynômes homogènes. Le degré de transcendance d'une $\mathbf{K}$-algèbre est le cardinal de la plus grande famille algébriquement indépendante, par exemple, le degré de transcendance de $\mathbf{K}[X_1, \ldots, X_n]$ est n et le degré de transcendance de $\mathbf{R}$ comme $\mathbf{Q}$-algèbre est infini.

Exemple 3.1.2 Le sous-ensemble V de $\mathbb{P}^2$ défini par l'équation $Z = Y$ est une variété projective de dimension 1 avec $I(V) =$ idéal homogène engendré par $Z - Y$ et $\mathbf{K}(V) \simeq \mathbf{K}(t)$.

Définition 3.1.3 On nomme *courbe elliptique* un couple constitué d'une courbe algébrique de $\mathbb{P}^2$ de genre 1 et d'un point O de cette même courbe. Par abus de language on omettra souvent le point O.

Remarque. Nous ne définirons pas ici ce que désigne le genre d'une courbe algébrique car nous n'utiliserons pas cet aspect des courbes elliptique par la suite. De plus, cette notion coïncide avec le genre topologique lorsque $\mathbf{K} = \mathbf{C}$ ce qui sera le cas par la suite.

Exemple 3.1.4 La courbe définie par l'équation $Y^2Z = X^3 - 3XZ^2 + 3Z^3$ dans $\mathbb{P}^2(\mathbf{C})$ est une courbe elliptique.

Definition 3.1.5 Soit $\mathbf{K}$ un corps.

- Si $V_1, V_2 \subset \mathbb{P}^n(\mathbf{K})$ sont deux variétés alors une *fonction rationnelle* f entre V_1 et V_2 est une application partielle de la forme $f(P) = [f_0(P), \ldots, f_n(P)]$ tel que $f(P) \in V_2$ et $f_i \in K(V_1)$.
- Une fonction rationnelle $f = [\phi_0, \ldots, \phi_n]$ est *définie* en $P \in V_1$ s'il existe $g \in \mathbf{K}(V_1)$ dès lors que chaque $\phi_i g$ est *régulier* en P et que $\phi_i g(P) \neq 0$ pour un certain i.
- f est un morphisme dès lors qu'il est défini en tout point.
- Une *isogénie* entre deux courbes elliptiques (E_1, O_1), (E_2, O_2) est un morphisme f entre les courbes E_1 et E_2 vérifiant $f(O_1) = O_2$. On note $\mathrm{End}(E)$ les isogénies d'une courbe elliptique E sur elle-même.

Proposition 3.1.6 Soit E une courbe elliptique sur un corps K. Alors il existe $x, y \in \mathbf{K}(E)$ tel que l'application :

$$\begin{aligned} \phi : \ & E \longrightarrow \mathbb{P}^2(K) \\ & P \longmapsto [x(P), y(P), 1] \end{aligned}$$

est un isomorphisme de E sur une courbe, lieu d'annulation d'une *équation de Wierstrass* :

$$C : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6$$

Où $a_1, \ldots a_6 \in K$ et $\phi(O) = [0, 1, 0]$. Lorsque la caractéristique de K est différente de 2 ou 3 on peut simplifier l'équation en :

$$Y^2Z = X^3 + AXZ^2 + BZ^3$$

Définition-Proposition 3.1.7 Soit E une courbe elliptique sur un corps de caractéristique $\neq 2, 3$ alors la quantité j définie ci-dessous caractérise entièrement la courbe E à isomorphisme près.

$$\Delta = -16(4A^3 + 27B^2) \qquad j = -1728\frac{(4A)^3}{\Delta}$$

Réciproquement, si $j \in \mathbf{K}^{ca}$, $\mathbf{K}^{ca}$ étant la clôture algébrique de $\mathbf{K}$ alors il existe une courbe elliptique ayant comme invariant j et étant le lieu d'annulation d'un équation de Wierstrass à coefficients dans $\mathbf{K}(j)$.

3.2 Réseaux et courbes elliptiques

Définition 3.2.1 On désigne par *réseau* tout sous-groupe discret Λ de $\mathbf{C}$ tel que $\mathrm{Vect}_{\mathbf{C}}(\Lambda) = \mathbf{C}$. On dit que deux réseaux Λ_1 et Λ_2 sont *homothétiques* s'il existe $\alpha \in \mathbf{C}^*$ tel que $\Lambda_1 = \alpha\Lambda_2$.

Exemple 3.2.2 Les sous-groupes $\mathbf{Z} + i\pi\mathbf{Z}$ et $\mathbf{Z}[i]$ sont tout deux des réseaux, le deuxième est d'ailleurs stable par multiplication et l'autre non.

Définition-Proposition 3.2.3 Soit Λ un réseau. Alors on note $\mathcal{P}$ la fonction $\mathcal{P}$ de Weierstrass holomorphe et Λ périodique définie par :

$$\mathcal{P}(z) = \frac{1}{z^2} + \sum_{\lambda \in \Lambda *} \frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2}$$

Rappel 3.2.4 On ne détaillera pas ici comment toute courbe elliptique E peut être munie d'une structure de groupe abélien. Ce qui nous importe c'est que cette loi de groupe munit E d'une structure de groupe de Lie complexe. En particulier, toute isogénie induit un morphisme de groupe entre courbes elliptiques et $(\mathrm{End}(E), +, \circ)$ est un anneau.

Proposition 3.2.5 Soit E une courbe elliptique sur $\mathbf{C}$. Alors il existe un unique réseau Λ à homothétie près tel que $\mathbf{C}/\Lambda$ et E soit isomorphes en tant que groupe de Lie complexe et variété algébrique. On donne ici explicitement l'isomorphisme :

$$\begin{aligned} \Phi : \mathbf{C}/\Lambda &\longrightarrow E \\ z &\longmapsto [\mathcal{P}(z), \mathcal{P}'(z), 1] \end{aligned}$$

De manière générale si Λ est un réseau alors on note E_Λ la courbe elliptique associée.

Definition 3.2.6 Soit Λ un réseau, alors pour tout $k \in \mathbf{N}$ la quantité suivante est bien définie :

$$G_{2k}(\Lambda) = \sum_{\lambda \in \Lambda *} \frac{1}{\lambda^{2k}}$$

On notera aussi :

$$g_2(\Lambda) = 60 G_4(\Lambda) \quad g_3(\Lambda) = 140 G_6(\Lambda) \quad \Delta(\Lambda) = g_2(\Lambda)^3 - 27 g_3(\Lambda)^2$$

$$j(\Lambda) = 1728 \frac{g_2(\Lambda)^3}{\Delta(\Lambda)}$$

Proposition 3.2.7 Avec les notations précédentes : $j(\Lambda) = j(\Phi(C/\Lambda))$.

Proposition 3.2.8 Soit Λ un réseau et $E = \Phi(C/\Lambda)$. Alors, $\mathrm{End}(E) \simeq \{\alpha \in \mathbf{C} | \alpha\Lambda \subset \Lambda\}$.

3.3 Multiplication complexe

Définition 3.3.1 Soit E une courbe elliptique complexe et R un sous-anneau de $\mathbf{C}$. On dit que E a pour multiplication complexe R si $\mathrm{End}(E) \simeq R$. On désignera par $\mathcal{ELL}(R)$ les classes d'isomorphismes des courbes elliptiques avec multiplication complexe R.

Remarque. Une telle appellation est motivé par le fait que l'on munit les courbes de $\mathcal{ELL}(R)$ d'une multiplication par les éléments de R.

Pour le reste de ce cette sous-section, on fixera $\mathbf{K}$ un corps de nombre. On notera

que lorsque K est un corps quadratique imaginaire, $\mathcal{O}_{\mathbf{K}}$ est un réseau de $\mathbf{C}$ et d'après la proposition précédente, $E_{\mathcal{O}_{\mathbf{K}}} \in \mathcal{ELL}(\mathcal{O}_{\mathbf{K}})$

Soit $\mathfrak{a}$ un idéal fractionnaire non nul de $\mathcal{O}_{\mathbf{K}}$ et Λ un réseau tel que $E_\Lambda \in \mathcal{ELL}(\mathcal{O}_{\mathbf{K}})$. Alors on peut définir le sous-groupe de $\mathbf{C}$:

$$\mathfrak{a}\Lambda = \{\alpha_1\lambda_1 + \alpha_2\lambda_2 + \cdots + \alpha_r\lambda_r | \alpha_i \in \mathfrak{a}, \lambda_i \in \Lambda, r \in \mathbf{N}\}$$

Proposition 3.3.2 Soit Λ un réseau vérifiant $E_\Lambda \in \mathcal{ELL}(\mathcal{O}_{\mathbf{K}})$, et soit $\mathfrak{a}$ et $\mathfrak{b}$ deux idéaux fractionnaires de $\mathcal{O}_{\mathbf{K}}$. Alors,

1. $\mathfrak{a}\Lambda$ est un réseau de $\mathbf{C}$
2. La courbe elliptique $E_{\mathfrak{a}\Lambda}$ satisfait $\mathrm{End}(E_{\mathfrak{a}\Lambda}) \simeq \mathcal{O}_{\mathbf{K}}$
3. $E_{\mathfrak{a}\Lambda} \simeq E_{\mathfrak{b}\Lambda}$ si et seulement si $\overline{\mathfrak{a}} = \overline{\mathfrak{b}}$ dans $\mathcal{CL}(\mathcal{O}_{\mathbf{K}})$

Démonstration.

1. Par hypothèse et le théorème **3.2.8.** on dispose $\mathrm{End}(E_\Lambda) \simeq \mathcal{O}_{\mathbf{K}}$ d'où $\mathcal{O}_{\mathbf{K}}\Lambda = \Lambda$. Prenons un entiers d tel que $d\mathfrak{a} \subset \mathcal{O}_{\mathbf{K}}$. On obtient alors $d\mathfrak{a}\Lambda \subset \Lambda$ donc $\mathfrak{a}\Lambda \subset \frac{1}{d}\Lambda$ et $\mathfrak{a}\Lambda$ est un sous-groupe discret de Λ. Soit maintenant d' un entier tel que $d'\mathcal{O}_{\mathbf{K}} \subset \mathfrak{a}$. On dispose ainsi de $d'\Lambda \subset \mathfrak{a}\Lambda$. Ainsi $\mathfrak{a}\Lambda$ engendre linéairement $\mathbf{C}$ c'est donc bien un réseau.
2. Soit $\alpha \in \mathbf{C}$ alors :

$$\alpha\mathfrak{a}\Lambda \subset \mathfrak{a}\Lambda \Longleftrightarrow \alpha\mathfrak{a}\mathfrak{a}^{-1}\Lambda \subset \mathfrak{a}\mathfrak{a}^{-1}\Lambda \Longleftrightarrow \alpha\Lambda \subset \Lambda$$

Dès lors,

$$\mathrm{End}(E_{\mathfrak{a}\Lambda}) \simeq \{\alpha \in \mathbf{C} \mid \alpha\mathfrak{a}\Lambda \ \subset \mathfrak{a}\Lambda\} = \{\alpha \in \mathbf{C} \mid \alpha\Lambda \ \subset \Lambda\} \simeq \mathrm{End}(E_\Lambda) \simeq \mathcal{O}_{\mathbf{K}}$$

3. Le théorème **3.2.5** assure que $E_{\mathfrak{a}\Lambda} \simeq E_{\mathfrak{b}\Lambda}$ si et seulement si les deux réseaux $\mathfrak{a}\Lambda$ et $\mathfrak{b}\Lambda$ sont homothétiques. C'est-à-dire qu'il existe $u \in \mathbf{C}^*$ tel que :

$$\mathfrak{a}\Lambda = u\mathfrak{b}\Lambda \Longleftrightarrow \Lambda = u\mathfrak{b}\mathfrak{a}^{-1}\Lambda \Longleftrightarrow \Lambda = u\mathfrak{a}\mathfrak{b}^{-1}\Lambda$$

Dès lors, les idéaux fractionnaires $\mathfrak{a}\mathfrak{b}^{-1}$ et $\mathfrak{b}\mathfrak{a}^{-1}$ sont inclus dans $\mathcal{O}_{\mathbf{K}}$ et ainsi on dispose de :

$$\mathfrak{a} = u\mathfrak{b}$$

□

Théorème 3.3.3 Le groupe $\mathcal{CL}(\mathcal{O}_{\mathbf{K}})$ agit simplement transitivement sur $\mathcal{ELL}(\mathcal{O}_{\mathbf{K}})$via l'action $\mathfrak{a} \cdot E_\Lambda = E_{\mathfrak{a}^{-1}\Lambda}$

Corollaire 3.3.4 L'ensemble $\mathcal{ELL}(\mathcal{O}_{\mathbf{K}})$ est fini de cardinal $\#\mathcal{CL}(\mathcal{O}_{\mathbf{K}})$.

3.4 Action de $\mathrm{Gal}(\mathbf{K}^{ca}/\mathbf{K})$ sur $\mathcal{ELL}(\mathcal{O}_\mathbf{K})$

Soit $\sigma \in \mathrm{Aut}(\mathbf{C})$ et E une courbe elliptique complexe. Alors E^σ désignera la nouvelle courbe dont les points sont les images des points de E par σ. C'est bien une courbe elliptique et si E possédait une équation de Wiertrass alors E^σ aussi et ses coefficients sont l'images des précédents par σ.

Proposition 3.4.1 Soit $\sigma \in \mathrm{Aut}(\mathbf{C})$ et E une courbe elliptique complexe.

1. $\mathrm{End}(E) \simeq \mathrm{End}(E^\sigma)$
2. $j(\mathcal{O}_\mathbf{K})$ est un nombre algébrique dès lors que $\mathbf{K}$ est un corps quadratique imaginaire.
3. $\mathcal{ELL}(\mathcal{O}_\mathbf{K}) = \mathcal{ELL}_{\mathbf{Q}^{ca}}(\mathcal{O}_\mathbf{K})$ où ce dernier ensemble désigne les courbes elliptiques sur $\mathbf{Q}^{ca}$ à $\mathbf{Q}^{ca}$-isomorphisme de variétés près tel que $\mathrm{End}(E) \simeq \mathcal{O}_\mathbf{K}$.

Démonstration.

1. L'application θ : $\mathrm{End}(E) \longrightarrow \mathrm{End}(E^\sigma)$ est un isomorphisme.
$$\varphi \longmapsto \sigma\varphi\sigma^{-1}$$
2. L'action de $\mathrm{Aut}(\mathbf{C})$ sur les courbes elliptiques induit une action de $\mathrm{Aut}(\mathbf{C})$ sur $\mathcal{ELL}(\mathcal{O}_\mathbf{K})$. Ainsi si σ parcourt $\mathrm{Aut}(\mathbf{C})$, $E_{\mathcal{O}_\mathbf{K}} \in \mathcal{ELL}(\mathcal{O}_\mathbf{K})$. Cependant, comme l'invanriant j est déduit des coefficients de l'équation de Wiertrass d'une courbe elliptique à l'aide de fractions, multiplications et additions, on peut prétendre que $j(E^\sigma) = j(E)^\sigma$. Dès lors $j(\mathcal{O}_\mathbf{K})^\sigma = j(\mathcal{O}_\mathbf{K}^\sigma)$. Mais les classes d'isomorphismes de $\mathcal{O}_\mathbf{K}$ sont finies d'après le corollaire **3.3.4** donc $j(\mathcal{O}_\mathbf{K})^\sigma$ ne prend qu'un nombre fini de valeurs, aisni $[\mathbf{Q}(j(\mathcal{O}_\mathbf{K})), \mathbf{Q}]$ est fini. Donc j est algébrique.
3. Soit E une courbe elliptique de $\mathcal{ELL}(\mathcal{O}_\mathbf{K})$, on veut montrer qu'elle admet un repésentant dans $\mathcal{ELL}_{\mathbf{Q}^{ca}}(\mathcal{O}_\mathbf{K})$. On sait dès lors que $j(E)$ est un nombre algébrique ainsi on peut définir une courbe elliptique d'invariant $j(E)$ et dont les coefficients de son équation de Wiertrass sont dans $\mathbf{Q}(j(E)) \subset \overline{\mathbf{Q}}$. Cela nous fourni bien un tel représentant.

□

En particulier si $\mathbf{K}$ est un corps de nombre on peut restreindre l'action de $\mathrm{Aut}(\mathbf{C})$ sur $\mathcal{ELL}(\mathcal{O}_\mathbf{K})$ à une action de $\mathrm{Gal}(\mathbf{K}^{ca}/\mathbf{K})$ sur $\mathcal{ELL}(\mathcal{O}_\mathbf{K})$.

Résumons ainsi tout le travail que nous avons fourni. Nous avons construit deux actions sur $\mathcal{ELL}(\mathcal{O}_\mathbf{K})$:

1. L'action de $\mathrm{Gal}(\mathbf{K}^{ca}/\mathbf{K})$.
2. L'action simplement transitive de $\mathcal{CL}(\mathcal{O}_\mathbf{K})$.

Ainsi la deuxième étant simplement transitive, on peut définir un morphisme F de la sorte :

$$\begin{aligned} F \ : \ \mathrm{Gal}(\mathbf{K}^{ca}/\mathbf{K}) &\longrightarrow \mathcal{CL}(\mathcal{O}_\mathbf{K}) \\ \sigma &\longmapsto F(\sigma) \end{aligned}$$

tel que si E est une courbe elliptique, $E^\sigma = F(\sigma) \cdot E$. Nous ôtons ici plusieurs étapes, il faudrait notamment prouver que cette relation ne dépende pas de la courbe elliptique E choisie.

4 Corps de classe de Hilbert

4.1 Définitions

Pour rappel, nous avons défini la notion de *conducteur* pour toute extension abélienne de corps de nombres. Pour définir le corps de classe de Hilbert d'un corps de nombre $\mathbf{K}$ nous devons introduire la notion de *ray class field*. Les démonstrations de cette section sont toutes dues à [Sil94].

Définition 4.1.1 Soit $\mathbf{K}$ un corps de nombre et $\mathfrak{c}$ un idéal de $\mathcal{O}_\mathbf{K}$. le corps $\mathbf{K}_\mathfrak{c}$ est un *ray class field* de $\mathbf{K}$ (modulo $\mathfrak{c}$) si, pour toute extension abélienne $\mathbf{L}$ de $\mathbf{K}$ on dipose de :

$$\mathfrak{c}_{\mathbf{L}/\mathbf{K}} | \mathfrak{c} \Longrightarrow \mathbf{L} \subset \mathbf{K}_\mathfrak{c}$$

Définition 4.1.2 Soit $\mathfrak{a}$ un idéal de $\mathcal{O}_\mathbf{K}$ alors on note par $\mathrm{P}(\mathfrak{a})$ l'ensemble :

$$\mathrm{P}(\mathfrak{a}) = \{(\alpha) | \alpha \in \mathbf{K}^*, \alpha \equiv 1 \mod \mathfrak{a}\}$$

Pour rappel, avec ces notations, $\mathfrak{c}_{\mathbf{L}/\mathbf{K}}$ est le plus grand idéal tel que $\mathrm{P}(\mathfrak{c}_{\mathbf{L}/\mathbf{K}}) \subset \ker(\cdot, \mathbf{L}/\mathbf{K})$.

Définition 4.1.3 Si $\mathbf{K} \subset \mathbf{L}$ est une extension de corps de nombres, alors on définit l'application *norme* :

$$\begin{aligned} N_L \ : \ \mathfrak{I}(\mathcal{O}_\mathbf{L}) &\longrightarrow \mathfrak{I}(\mathcal{O}_\mathbf{K}) \\ \mathfrak{P} &\longmapsto \mathfrak{p}^{f(\mathfrak{P}|\mathfrak{p})} \end{aligned}$$

Où $\mathfrak{p} = \mathfrak{P}_{\mathcal{O}_\mathbf{K}}$.

La propriété suivante assure l'existence et l'unicité du *ray class field*.

Proposition 4.1.4 Soit $\mathbf{K} \subset \mathbf{L}$ une extension abélienne de corps de nombre. Soit $\mathfrak{c}$ un idéal de $\mathcal{O}_\mathbf{K}$

1. Le morphisme d'Artin :

$$(\cdot, \mathbf{L}/\mathbf{K} \ : \ ) \longrightarrow \mathfrak{I}(\mathfrak{c}_{\mathbf{L}/\mathbf{K}})\mathrm{Gal}(\mathbf{L}/\mathbf{K})$$

   est surjectif.

2. Le noyau du morhisme d'Artin est $(N_L\mathfrak{I}(\mathcal{O}_\mathbf{L}))\mathrm{P}(\mathfrak{c}_{\mathbf{L}/\mathbf{K}})$.
3. Il existe un unique *ray class field* de $\mathbf{K}$ modulo $\mathfrak{c}$. Le conducteur de $\mathbf{K}_\mathfrak{c}/\mathbf{K}$ divise $\mathfrak{c}$

Le *corps de classe de Hilbert* de $\mathbf{K}$ est simplement le corps $\mathbf{K}_{(1)}$ que l'on notera $\mathbf{H}$. Son conducteur est donc (1) d'après le point 3 et aucun idéal premier de $\mathcal{O}_\mathbf{K}$ n'est ramifié. De plus, $\mathrm{P}((1)) = \{$idéaux principaux fractionnaires de $\mathcal{O}_\mathbf{K}\}$ et $\mathfrak{I}((1)) = \{$idéaux fractionnaires de $\mathcal{O}_\mathbf{K}\}$. Dès lors, le morphisme d'Artin induit un isomorphisme :

$$(\cdot, \mathbf{H}/\mathbf{K}) \ : \ \mathcal{CL}(\mathcal{O}_\mathbf{K}) \longrightarrow \mathrm{Gal}(\mathbf{H}/\mathbf{K})$$

4.2 Calcul du corps de classe de Hilbert

Pour assurer la démonstration du théorème annoncé en introduction, nous allons admettre deux lemmes :

Lemme 4.2.1 Il existe un ensemble fini de nombre premiers $S \subset \mathbf{Z}$ tel que si $p \notin S$ est un nombre premier qui se décompose dans $\mathcal{O}_{\mathbf{K}}$ disons $p\mathcal{O}_{\mathbf{K}} = \mathfrak{p}\mathfrak{p}'$ alors :

$$F(\sigma_{\mathfrak{p}}) = \overline{\mathfrak{p}} \in \mathcal{CL}(\mathcal{O}_{\mathbf{K}})$$

Lemme 4.2.2 Soit $\mathbf{K}$ un corps de nombre et $\mathfrak{c}$ un idéal de $\mathcal{O}_{\mathbf{K}}$. Alors toute classe d'idéaux de $\mathfrak{I}(\mathfrak{c})/\mathrm{P}(\mathfrak{c})$ contient une inifinité de représentant.

Théorème 4.2.3 Soit $\mathbf{K}$ un corps quadratique imaginaire. Alors $\mathbf{K}(j(\mathcal{O}_{\mathbf{K}}))$ est une extension abélienne de $\mathbf{K}$.

Démonstration. Rappellons que l'on dispose d'un morphisme $F :\ \mathrm{Gal}(\mathbf{K}^{ca}/\mathbf{K}) \longrightarrow \mathcal{CL}(\mathcal{O}_{\mathbf{K}})$. Soit $\mathbf{L}$ l'unique corps, d'après la correspondance de Galois, tel que $\ker F = \mathrm{Gal}(\mathbf{K}^{ca}/\mathbf{L})$. Dès lors :

$$\begin{aligned}
\mathrm{Gal}(\mathbf{K}^{ca}/\mathbf{L}) &= \ker F \\
&= \{\sigma \in \mathrm{Gal}(\mathbf{K}^{ca}/\mathbf{K}) \mid F(\sigma) = 1\} \\
&= \{\sigma \in \mathrm{Gal}(\mathbf{K}^{ca}/\mathbf{K}) \mid F(\sigma) \cdot E = E\} \\
&= \{\sigma \in \mathrm{Gal}(\mathbf{K}^{ca}/\mathbf{K}) \mid E^{\sigma} = E\} \\
&= \{\sigma \in \mathrm{Gal}(\mathbf{K}^{ca}/\mathbf{K}) \mid j(E^{\sigma}) = j(E)\} \\
&= \{\sigma \in \mathrm{Gal}(\mathbf{K}^{ca}/\mathbf{K}) \mid j(E)^{\sigma} = j(E)\} \\
&= \mathrm{Gal}(\mathbf{K}^{ca}/\mathbf{K}(j(\mathcal{O}_{\mathbf{K}})))
\end{aligned}$$

Dès lors $\mathbf{L} = \mathbf{K}(j(\mathcal{O}_{\mathbf{K}}))$ et $\mathrm{Gal}(\mathbf{L}/\mathbf{K}^{ca}))$ s'injecte dans $\mathcal{CL}(\mathcal{O}_{\mathbf{K}})$ donc c'est un groupe abélien. Nous avons donc montré que $\mathbf{L}$ était une extension abélienne de $\mathbf{K}$. □

Lemme 4.2.4 La composition des deux flèches suivantes :

$$I(\mathfrak{c}_{\mathbf{L}/\mathbf{K}}) \xrightarrow{(\cdot,\mathbf{L}/K)} \mathrm{Gal}(\mathbf{L}/\mathbf{K})) \xrightarrow{F} \mathcal{CL}(\mathcal{O}_{\mathbf{K}})$$

est égale à la projection naturelle de $I(\mathfrak{c}_{\mathbf{L}/\mathbf{K}})$ sur $\mathcal{CL}(\mathcal{O}_{\mathbf{K}})$ c'est à dire que pour tout idéal fractionnaire $\mathfrak{a} \in \mathfrak{I}(\mathfrak{c}_{\mathbf{L}/\mathbf{K}})$ on dispose de $F((\mathfrak{a}, \mathbf{L}/\mathbf{K})) = \overline{\mathfrak{a}}$.

Démonstration. Prenons $\mathfrak{a}$ un idéal fractionnaire de $\mathfrak{I}(\mathfrak{c}_{\mathbf{L}/\mathbf{K}})$ et notons S l'ensemble décrit par le lemme **4.2.1**. D'après le lemme **4.2.2.** il existe un idéal premier $\mathfrak{p} \in \mathfrak{I}(\mathfrak{c}_{\mathbf{L}/\mathbf{K}})$ dans la même $P(\mathfrak{c}_{\mathbf{L}/\mathbf{K}})$-classe que $\mathfrak{a}$ et n'étant pas dans S. En d'autre termes, on peut trouver $\alpha \in \mathbf{K}^*$ tel que :

$$\alpha \equiv 1 \mod \mathfrak{c}_{\mathbf{L}/\mathbf{K}} \quad \text{et} \quad \mathfrak{a} = (\alpha)\mathfrak{p}$$

Calculons alors :

$$\begin{aligned} F((\mathfrak{a},\mathbf{L}/\mathbf{K})) &= F(((\alpha)\mathfrak{p},\mathbf{L}/\mathbf{K})) && \text{car } \mathfrak{a}=(\alpha)\mathfrak{p} \\ &= F((\mathfrak{p},\mathbf{L}/\mathbf{K})) && \text{car } \alpha\equiv 1 \mod \mathfrak{c}_{\mathbf{L}/\mathbf{K}} \\ &= \overline{\mathfrak{p}} && \text{d'après le lemme } \mathbf{4.2.1} \\ &= \overline{\mathfrak{a}} && \text{car } \mathfrak{a}=(\alpha)\mathfrak{p} \end{aligned}$$

□

Théorème 4.2.5 Le corps de classe Hilbert de $\mathbf{K}$ est $\mathbf{L}$.

Démonstration. La conséquence immédiate du lemme **4.2.4.** est que pour tout idéal principal $(\alpha) \in I(\mathfrak{c}_{\mathbf{L}/\mathbf{K}})$ on dispose de

$$F(((\alpha),\mathbf{L}/\mathbf{K})) = 1$$

Nous savons également que l'application F : $\mathrm{Gal}(\mathbf{L}/\mathbf{K}) \longrightarrow \mathcal{CL}(\mathcal{O}_{\mathbf{K}})$ est injective. alors on dispose de :

$$((\alpha),\mathbf{L}/\mathbf{K}) = 1 \quad \text{pour} \quad (\alpha) \in I(\mathfrak{c}_{\mathbf{L}/\mathbf{K}})$$

Cependant, l'idéal $\mathfrak{c}_{\mathbf{L}/\mathbf{K}}$ est le plus petit idéal $\mathfrak{c}$ vérifiant :

$$\alpha \equiv 1 \mod \mathfrak{c} \Longrightarrow ((\alpha),\mathbf{L}/\mathbf{K}) = 1$$

Dans notre cas, $\mathfrak{c}_{\mathbf{L}/\mathbf{K}} = 1$ nécessairement. Le conducteur est divisible par tout les idéaux premiers qui sont ramifiés. Dès lors l'extension $\mathbf{L}/\mathbf{K}$ n'est pas ramifiée. Ainsi, le corps $\mathbf{L}$ est contenu dans le corps de classe de Hilbert $\mathbf{H}$ de $\mathbf{L}$.
De plus, L'application naturelle $I(\mathfrak{c}_{\mathbf{L}/\mathbf{K}}) = I((1)) \longrightarrow \mathcal{CL}(\mathcal{O}_{\mathbf{K}})$ est clairement surjective. Dès lors le lemme **4.2.4.** assure que F : $\mathrm{Gal}(\mathbf{L}/\mathbf{K}) \longrightarrow \mathcal{CL}(\mathcal{O}_{\mathbf{K}})$ est aussi surjective et donc c'est un isomorphisme. Dès lors :

$$[\mathbf{L}:\mathbf{K}] = \#\mathrm{Gal}(\mathbf{L}/\mathbf{K}) = \#\mathcal{CL}(\mathcal{O}_{\mathbf{K}}) = \#\mathrm{Gal}(\mathbf{H}/\mathbf{K}) = [\mathbf{H}:\mathbf{K}]$$

Ceci combiné avec l'inclusion $\mathbf{L} \subset \mathbf{H}$ prouve $\mathbf{L} = \mathbf{H}$. Et puique $\mathbf{L} = \mathbf{K}(j(\mathcal{O}_{\mathbf{K}}))$ alors nous avons prouvé le théorème annoncé en introduction. □

Références

[Rei88] Miles Reid. *Undergraduate Algebraic Geometry.* London Mathematical Society Student Text. Press Syndicate of the University of Cambridge, 1988.

[Ser62] Jean-Pierre Serre. *Coprs locaux.* Springer. 1962.

[Sil94] Joseph H. Silvermann. *Advanced topic in the Arithmetic of Elliptic Curve.* Springer. 1994.

[Sil08] Joseph H. Silvermann. *The Arithmetic of Elliptic Curve.* Springer. 2008.