Università degli Studi di Padova

DIPARTIMENTO DI MATEMATICA "TULLIO LEVI-CIVITA"
Corso di Laurea Magistrale in Matematica

Class Field Theory and Elliptic Curves with Complex Multiplication

Candidato:
Enrico Da Ronche
Matricola 2044683

Relatore:
Matteo Longo

Anno accademico 2022–2023
22/09/2023

Contents

Introduction **3**

1 Preliminaries **7**
1.1 Tate Cohomology of groups 7
1.1.1 G-modules 7
1.1.2 Definition of Tate groups 8
1.1.3 Maps between cohomology groups 11
1.1.4 The main results in Tate Cohomology 12
1.1.5 The Herbrand quotient 15
1.1.6 Galois Cohomology 15
1.1.7 Cohomology of profinite groups 16
1.2 Orders of number fields 17
1.3 Primes of number fields 19

2 Local Class Field Theory **23**
2.1 Statements of the main theorems 23
2.2 Proof of the local reciprocity law 26
2.2.1 Galois cohomology for local fields 26
2.2.2 The invariant map 28
2.2.3 The local Artin map 32
2.3 Proof of the local existence theorem 34
2.3.1 Lubin-Tate formal group laws 34
2.3.2 Newton polygon 35
2.3.3 Construction of K_π and ϕ_π 36
2.3.4 Local Kronecker-Weber Theorem: end of the proof . . 39
2.3.5 Uniqueness of the local Artin map 40
2.4 An example: cyclotomic extensions of $\mathbb{Q}_p$ 40

3 Global Class Field Theory **43**
3.1 Adele rings and Idele groups 43
3.2 Idelic class field theory 45
3.3 Proof of the global reciprocity law 47
3.3.1 Cohomology of ideles 47

3.3.2 The first inequality 49
3.3.3 The second inequality 50
3.3.4 End of the proof 56
3.4 Proof of the existence theorem 57
3.5 Global class field theory in terms of ideals 59
3.6 The principal ideal theorem 62
3.7 An example: the Hilbert class field of $\mathbb{Q}(\sqrt{-5})$ 66

4 Elliptic curves **67**
4.1 Weierstrass equations 67
4.2 The group law of an elliptic curve 69
4.3 Isogenies 71
4.4 Endomorphism rings and algebras 75
4.5 Elliptic curves over $\mathbb{C}$ 78

5 Complex Multiplication **87**
5.1 Proper ideals 87
5.2 Modular functions 88
5.3 Integrality of the j-invariant 92
5.4 The Chebotarev Density Theorem and other preliminaries . . 96
5.5 Ring class fields 96
5.6 The first main theorem of complex multiplication 99
5.7 The second main theorem of complex multiplication 103

Bibliography **105**

Introduction

Class Field Theory is an important branch of Algebraic Number Theory. Its main purpose is to study and classify the abelian extensions of local and global fields through objects defined in terms of the ground field. It started to be developed after 1850 and its main pioneers were David Hilbert, Helmut Hasse, Emil Artin and Claude Chevalley. The theory revolves around the notion of class field and it is strictly related to other important areas of Number Theory like Iwasawa Theory and the Birch and Swinnerton-Dyer conjecture. An explicit construction of class fields of number fields has not been fully developed yet and it is the main purpose of the Hilbert's twelfth problem. Anyway, it has been solved for the particular cases of $\mathbb{Q}$ and imaginary quadratic fields thanks to the theory of complex multiplication. The purpose of this thesis is to expose and prove the theorems of local and global class field theory and to use elliptic curves with complex multiplication to study the case of imaginary quadratic fields. The thesis is divided in five chapters which are connected according to the diagram at page 5.

In the first chapter we introduce the main definitions and results on Tate cohomology of groups, a branch of homological algebra that is crucial in the proofs of the main theorems of class field theory. Then, we define the basic notions of orders and primes of a number field which will be used in the study of global class field theory.

In the second chapter we study class field theory of local fields. It consists in two main results, the "local Artin reciprocity law" and the "local existence theorem", which lead to an elegant classification of finite abelian extensions of local fields. The proof of the first result is based on Tate cohomology, the proof of the second one uses the notion of Lubin-Tate formal group laws.

The next step is the exploration of global class field theory, i.e. of class field theory for global fields. We will especially consider the case of number fields. There are two possible formulations of the main theorems for this theory. The first one is based on the notion of idele, a group associated to any number field that permits to state the "global reciprocity law", the "global existence theorem" and the consequent corollaries in an elegant way. The second one is in terms of ideals. It is a less modern approach but it is useful for applications on the problem of splitting of primes. In this thesis we prove the results in terms of ideles and we only state those in terms

of ideals. We also define the Hilbert class field of a number field, i.e. its maximal abelian unramified extension, and we study its main properties. In particular, we prove the principal ideal theorem, which ensures that any ideal of a number field becomes principal in its Hilbert class field.

The chapter "Elliptic curves" introduces the basic notions for elliptic curves defined in the projective plane by a Weierstrass equation. We put on the set of points of any elliptic curve a structure of abelian group, we define and study isogenies and we state the existence and the uniqueness of the dual isogeny. Our main purpose is to study elliptic curves defined over $\mathbb{C}$ by using complex lattices and, in particular, to classify their endomorphism rings in order to give the definition of elliptic curves with complex multiplication.

Finally, the last chapter exposes the main results of the thesis. We use the theory of elliptic curves with complex multiplication to study global class field theory for imaginary quadratic fields. We will use different tools: modular functions and the Chebotarev Density Theorem. First, we prove the following central theorem:

Theorem 0.1. *If E is a complex elliptic curve with complex multiplication then the j-invariant $j(E)$ is an algebraic integer.*

Then we define the ring class fields $R_{\mathcal{O}}$ of an imaginary quadratic number field, a notion that extends the Hilbert class field to the case of non-maximal orders. The first main theorem of complex multiplication characterizes the ring class fields in terms of the j-invariant of suitable elliptic curves with complex multiplication.

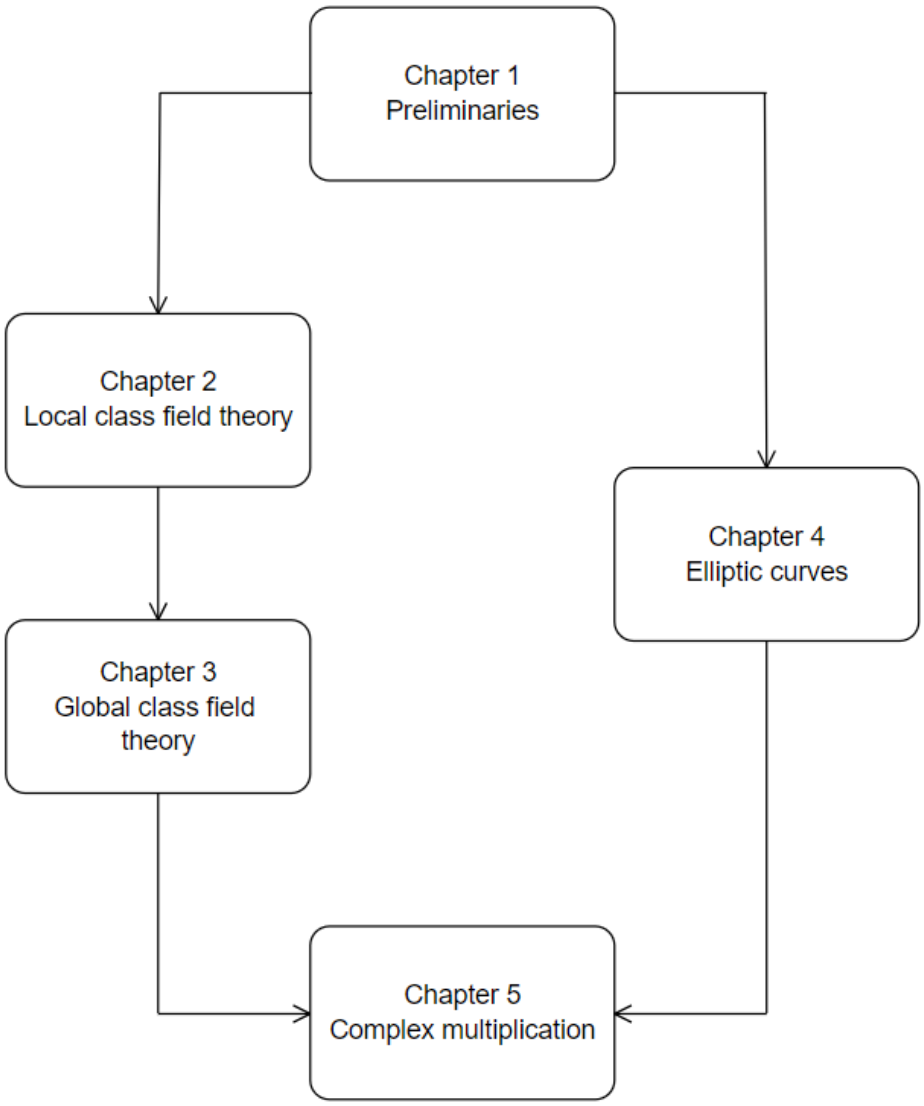
Theorem 0.2. *If E is a complex elliptic curve with $End(E) \cong \mathcal{O}$ where $\mathcal{O}$ is an order in an imaginary quadratic field K, then $R_{\mathcal{O}} = K(j(E))$.*

The second main theorem of complex multiplication characterizes ray class fields $K(\mathfrak{m})$ of an imaginary quadratic field K in terms of torsion points of an elliptic curve E and of a function $h : E \to \mathbb{C}$.

Theorem 0.3. *Let K be an imaginary quadratic field, $\mathfrak{m}$ a modulus for K and E a complex elliptic curve with complex multiplication such that $End(E) \cong \mathcal{O}_K$. Then*

$$K(\mathfrak{m}) = K(j(E), h(E[\mathfrak{m}]))$$

An interesting possibility to continue this work is to study the results found by Dasgupta and Kakde who gave a solution to the Hilbert's twelfth problem in more general situations.


Chapter 1
Preliminaries
Chapter 2
Local class field theory
Chapter 3
Global class field
theory
Chapter 4
Elliptic curves
Chapter 5
Complex multiplication

Chapter 1

Preliminaries

1.1 Tate Cohomology of groups

The purpose of this section is to introduce briefly the main definitions and results in Tate Cohomolgy. This theory will be fundamental for the proofs of the main theorems of local and global class field theory since we will study them with a cohomological approach.

1.1.1 G-modules

Definition 1.1. *Let G be a group. A **G-module** is an abelian group $(M,+)$ endowed with an action of G such that*

$$g(m_1+m_2)=gm_1+gm_2$$

for any $g\in G$, $m_1,m_2\in M$.
We also define

$$M^G:=\{m\in M: gm=m\,\forall\, g\in G\}$$

$$I_GM:=\langle gm-m: g\in G, m\in M\rangle$$

$$M_G:=M/I_GM$$

A homomorphism of groups $\phi: M_1\to M_2$ between two G-modules is a homomorphism of G-modules if

$$\phi(gm)=g\phi(m)$$

for any $g\in G, m\in M$.

For any G-module M over a finite group G we also introduce a norm map

$$Nm_G: M\to M, m\mapsto \sum_{g\in G} gm$$

It is immediate to observe that

$$Nm_G(M) \subset M^G$$

and

$$I_G M \subset Ker(Nm_G)$$

Another important notion is that of induced G-module.

Definition 1.2. *Let $H \leq G$ be groups and M an H-module. We define the G-module*

$$Ind_H^G M := \{\phi : G \to M : \phi(hg) = h\phi(g) \,\forall\, h \in H, g \in G\}$$

endowed with the operations

$$(\phi_1 + \phi_2)(x) = \phi_1(x) + \phi_2(x)$$

$$(g\phi)(x) = \phi(xg)$$

*A G-module M is called **induced** if there exists an abelian group M' such that*

$$M \cong Ind_{\{1\}}^G(M')$$

1.1.2 Definition of Tate groups

In this subsection we want to define homology and cohomology groups for a G-module M and, starting from them, to define Tate cohomology groups of M. We start with a series of definitions and results that come from the homological algebra.

Definition 1.3. *A G-module I is injective if for any pair of G-modules $N \subset M$, any homomorphism from N to I extends to M.*
A G-module P is projective if for any pair of G-modules $N \subset M$ and any homomorphism $f : P \to M/N$ there exists $g : P \to M$ which equals f when composed with the projection.
An injective resolution (I^i, f^i) for a G module M is an exact sequence

$$0 \longrightarrow M \longrightarrow I^0 \xrightarrow{f^0} I^1 \xrightarrow{f^1} \cdots$$

where I^i is an injective G-module for any i.
A projective resolution (P^i, g^i) for M is an exact sequence

$$\cdots \xrightarrow{g^1} P^1 \xrightarrow{g^0} P^0 \longrightarrow M \longrightarrow 0$$

where P^i is a projective G-module for any i.

Proposition 1.1. *The category of G-modules has enough injectives, i.e. every G-module can be embedded into an injective G-module, and enough projectives, i.e. any G-module is the image of a homomorphism whose domain is a projective G-module. Then any G-module admits both an injective and a projective resolution.*

Proof. See [8, Proposition 1.5, pag. 60]. □

Proposition 1.2. *The functor* $(\cdot)^G : G - Mod \to G - Mod$ *is left-exact. The functor* $(\cdot)_G : G - Mod \to G - Mod$ *is right-exact.*

Now, we use the previous definitions and propositions to define homology and cohomology groups. We fix a G-module M and we find an injective and a projective resolution for it:

$$0 \longrightarrow M \longrightarrow I^0 \xrightarrow{f^0} I^1 \xrightarrow{f^1} \cdots$$

$$\cdots \xrightarrow{g^1} P^1 \xrightarrow{g^0} P^0 \longrightarrow M \longrightarrow 0$$

The last proposition tells us that we can derive two complexes:

$$0 \xrightarrow{f^{-1}} (I^0)^G \xrightarrow{f^0} (I^1)^G \xrightarrow{f^1} \cdots$$

$$\cdots \xrightarrow{g^1} (P^1)_G \xrightarrow{g^0} (P^0)_G \xrightarrow{g^{-1}} 0$$

Definition 1.4. *The* ***r-th cohomology group*** *of the G-module M is defined as*

$$H^r(G, M) := \frac{Ker(f^r)}{Im(f^{r-1})}$$

The ***s-th homology group*** *of M is defined as*

$$H_s(G, M) := \frac{Ker(g^{s-1})}{Im(g^s)}$$

With the following proposition we want to prove that homology and cohomology groups are well-defined. In particular, they do not depend on the choice of the injective and projective resolutions. The proposition will be used also to define homomorphisms through the homology and cohomology groups.

Proposition 1.3. *Let* M, N *be G-modules,* $\phi : M \to N$ *a homomorphism of G-modules and* $(I^i, f^i), (J^j, g^j)$ *injective resolutions of, respectively, M and N. Then* ϕ *induces a morphism of complexes* (ϕ_i) *between* $((I^i)^G, f^i)$ *and* $((J^j)^G, g^j)$ *and the induced maps between the cohomology groups do not*

depend on the choice of the ϕ_i. The situation is described in the following commutative diagram:

$$\begin{array}{ccccccc} 0 & \xrightarrow{f^{-1}} & (I^0)^G & \xrightarrow{f^0} & (I^1)^G & \xrightarrow{f^1} & \cdots \\ & & \downarrow{\scriptstyle \phi_0} & & \downarrow{\scriptstyle \phi_1} & & \\ 0 & \xrightarrow{f^{-1}} & (J^0)^G & \xrightarrow{g^0} & (J^1)^G & \xrightarrow{g^1} & \cdots \end{array}$$

An analogous statement holds for homology groups.

Proof. See [8, Proposition A.8, pag. 93]. □

It is immediate from the definitions that

$$H^0(G, M) = M^G$$

$$H_0(G, M) = M_G$$

$$H^r(G, I) = 0$$

$$H_r(G, P) = 0$$

whenever I is injective and P is projective.
Finally, we can give the crucial definition of Tate groups.

Definition 1.5. *Let M be a G-module over a finite group G. Then the **r-th Tate group** of M is denoted $H^r_T(G, M)$ and it is defined as:*

- *$H^r(G, M)$ if $r > 0$;*
- *$M^G/Nm_G(M)$ if $r = 0$;*
- *$Ker(Nm_G)/I_G M$ if $r = -1$;*
- *$H_{-r-1}(G, M)$ if $r < -1$.*

Using the Snake lemma it is possible to prove the following.

Proposition 1.4. *Let*

$$0 \to M' \to M \to M'' \to 0$$

be a short exact sequence of G-modules.
Then for suitable boundary maps we have the following long exact sequences:

$$0 \to H^0(G, M') \to \cdots \to H^r(G, M'') \to H^{r+1}(G, M') \to \cdots$$

$$\cdots H_r(G, M'') \to H_{r-1}(G, M') \to \cdots \to H_0(G, M'') \to 0$$

$$\cdots \to H^r_T(G, M') \to H^r_T(G, M) \to H^r_T(G, M'') \to H^{r+1}_T(G, M') \to \cdots$$

For any G-module M we also have the exact sequence

$$0 \to H_T^{-1}(G,M) \to H_0(G,M) \to H^0(G,M) \to H_T^0(G,M) \to 0$$

where the middle map is the norm map.
In order to simplify some proofs and considerations we give another equivalent definition of cohomology groups which is more concrete than the previous one.

Definition 1.6. *Let G be a group, M a G-module and $r \geq 0$ an integer. Set $G^0 = \{1\}$.*
We define the sets of r-cochains as

$$C^r(G,M) := \{\phi : G^r \to M\}$$

and the maps

$$d^r : C^r(G,M) \to C^{r+1}(G,M)$$

$$(d^r\phi)(g_1,...,g_{r+1}) = g_1\phi(g_2,...,g_{r+1}) + \sum_{j=1}^{r}(-1)^j\phi(g_1,...,g_jg_{j+1},...,g_{r+1}) + (-1)^{r+1}\phi(g_1,...,g_r)$$

The sequence

$$C^0(G,M) \xrightarrow{d^0} C^1(G,M) \xrightarrow{d^1} C^2(G,M) \xrightarrow{d^2} \cdots$$

is a complex and so we can define:

- *the group of r-cocycles as $Z^r(G,M) := Ker(d^r)$;*
- *the group of r-coboundaries as $B^r(G,M) := Im(d^{r-1})$;*
- *the r-th cohomology group as $H^r(G,M) := Z^r(G,M)/B^r(G,M)$.*

1.1.3 Maps between cohomology groups

In this subsection we want to define some homomorphisms between cohomology groups that will be used in the sequel. If G_1 and G_2 are groups and M_1 and M_2 are, respectively, a G_1-module and a G_2-module, we say that two homomorphisms $\phi : G_2 \to G_1$ and $\psi : M_1 \to M_2$ are compatible if

$$\psi(\phi(g)m) = g\psi(m)$$

for any $g \in G_2$ and $m \in M_1$. Obviously, any pair of compatible homomorphisms induces homorphisms

$$H^r(G_1,M_1) \to H^r(G_2,M_2)$$

Using this technique we define the following maps:

- If $H \leq G$ are groups and M is a G-module, the inclusion $H \hookrightarrow G$ and the identity map on M are compatible and we call the induced homorphisms as the **restriction homomorphisms**

$$Res : H^r(G, M) \to H^r(H, M)$$

- If $H \trianglelefteq G$ are groups and M is a G-module, the quotient map $G \to G/H$ and the inclusion $M^H \hookrightarrow M$ are compatible and we call the induced homomorphisms as the **inflation homomorphisms**

$$Inf : H^r(G/H, M^H) \to H^r(G, M)$$

Proposition 1.5. *Let G be a group, $H \trianglelefteq G$, M a G-module and r a positive integer. Assume that $H^i(H, M) = 0$ for any $0 < i < r$. Then the sequence*

$$0 \longrightarrow H^r(G/H, M^H) \xrightarrow{Inf} H^r(G, M) \xrightarrow{Res} H^r(H, M)$$

is exact.

Proof. See [8, Proposition 1.34, pag. 71]. □

Proposition 1.6. *Let G be a finite group, $H \leq G$ a p-Sylow of G and M a G-module. Then the restriction homomorphisms*

$$H^r(G, M) \to H^r(H, M)$$

are injective on the p-primary components of $H^r(G, M)$.

Proof. See [8, Corollary 1.33, pag. 71]. □

1.1.4 The main results in Tate Cohomology

In this subsection we state some important facts in cohomology of groups which will be necessary in the sequel.

Proposition 1.7. *Let $H \leq G$ be groups, M an H-module and $r \geq 0$ an integer. Then*

$$H^r(G, Ind_H^G M) \cong H^r(H, M)$$

As a consequence, $H^r(G, M) = 0$ for any positive integer r and any induced G-module M.

Proof. See [8, Proposition 1.11, pag. 62]. □

Proposition 1.8. *Let G be a finite group and M an induced G-module. Then*

$$H_T^r(G, M) = 0$$

for any integer r.

Proof. See [8, Proposition 3.1, pag. 78]. □

Proposition 1.9. *Let G be a group, $\{M_i\}_i$ a family of G-modules and $r \geq 0$ an integer. Then*

$$H^r(G, \prod_i M_i) \cong \prod_i H^r(G, M_i)$$

Proof. See [8, Proposition 1.25, pag. 68]. □

Proposition 1.10. *If G is a group and we consider $\mathbb{Z}$ as a G-module with trivial action we have an isomorphism*

$$H_1(G, \mathbb{Z}) \cong G^{ab}$$

Proof. We consider the exact sequence

$$0 \to I_G \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$$

where the augmentation ideal I_G is the free $\mathbb{Z}$-submodule of $\mathbb{Z}[G]$ generated by $\{g-1 : g \in G^\times\}$ and the augmentation map $\mathbb{Z}[G] \to \mathbb{Z}$ is $\sum n_g g \mapsto \sum n_g$. Since $H_1(G, \mathbb{Z}[G]) = 0$ (because $\mathbb{Z}[G]$ is projective) we get the exact sequence

$$0 \to H_1(G, \mathbb{Z}) \to I_G/I_G^2 \to \mathbb{Z}[G]/I_G \to \mathbb{Z} \to 0$$

and, since the middle map is zero, we find an isomorphism

$$H_1(G, \mathbb{Z}) \cong I_G/I_G^2$$

The proof is concluded by composing the previous isomorphism with the inverse of the isomorphism

$$G/G' \to I_G/I_G^2,\ g \mapsto (g-1) + I_G^2$$

□

Proposition 1.11. *If G is a finite group and we consider $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{Q}/\mathbb{Z}$ as G-modules with trivial action, we have:*

- $H_T^0(G, \mathbb{Z}) = \mathbb{Z}/|G|\mathbb{Z}$ *and* $H^1(G, \mathbb{Z}) = 0$*;*
- $H_T^r(G, \mathbb{Q}) = 0$ *for any integer r;*
- $H^1(G, \mathbb{Q}/\mathbb{Z}) = Hom(G, \mathbb{Q}/\mathbb{Z})$.

Proof. See [8, Lemma 3.3, pag. 80]. □

Now, we state and prove Tate's Theorem which will be crucial in proving theorems of class field theory. During the proof we will need the following lemma.

Lemma 1.1. *If G is a finite group and M is a G-module such that*

$$H^1(H, M) = H^2(H, M) = 0$$

for any $H \leq G$, then for any $r \in \mathbb{Z}$ we have

$$H_T^r(G, M) = 0$$

Proof. See [8, Theorem 3.10, pag. 83]. □

Theorem 1.1. *Let G be a finite group and M a G-module. If for any $H \leq G$ we have $H^1(H, M) = 0$ and $H^2(H, M)$ cyclic of order equal to $|H|$ then $H_T^r(G, \mathbb{Z}) \cong H_T^{r+2}(G, M)$ for any integer r.*

Proof. We fix γ a generator of $H^2(G, M)$ and we consider a cocycle ϕ in the class of γ. We define the splitting G-module of ϕ as

$$M(\phi) := M \oplus (\bigoplus_{\sigma \in G^\times} \mathbb{Z}x_\sigma)$$

with the action

$$\sigma x_\tau := x_{\sigma\tau} - x_\sigma + \phi(\sigma\tau)$$

where x_σ is a formal symbol and $x_1 := \phi(1, 1)$. We define a homomorphism

$$\alpha : M(\phi) \to I_G,\ \alpha(m) = 0 \text{ on } M,\ \alpha(x_\sigma) = \sigma - 1$$

and we observe that we have the following exact sequences:

$$0 \to I_G \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$$

$$0 \to M \to M(\phi) \to I_G \to 0$$

The cohomology exact sequence of the second one over $H \leq G$ is

$$0 \to H^1(H, M(\phi)) \to H^1(H, I_G) \to H^2(H, M) \to H^2(H, M(\phi)) \to 0$$

because $H^1(H, M) = 0$ and

$$H^2(H, I_G) \cong H^1(H, \mathbb{Z}) = 0$$

(recall that $\mathbb{Z}[G]$ is an induced G-module). $Res(\gamma)$ generates $H^2(H, M)$ (it can be seen introducing the corestriction homomorphism) and, since ϕ is the coboundary of the cochain $\sigma \mapsto x_\sigma$, we discover that the fourth arrow in the previous diagram is just the zero map. Then the third arrow is surjective and hence an isomorphism because

$$H^1(H, I_G) \cong H_T^0(H, \mathbb{Z}) \cong \mathbb{Z}/|H|\mathbb{Z}$$

Then the last exact sequence tells us that

$$H^1(H, M(\phi)) = H^2(H, M(\phi)) = 0$$

The previous lemma implies that $H^r(H, M(\phi)) = 0$ for any integer r and so the cohomology sequences of the exact sequence

$$0 \to M \to M(\phi) \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$$

give the desired isomorphisms. □

1.1.5 The Herbrand quotient

The Herbrand quotient is a powerful instrument used to study cohomology of finite cyclic groups.

Proposition 1.12. *Let G be a finite cyclic group and M a G-module. Then for any $r \in \mathbb{Z}$ we have $H_T^r(G, M) \cong H_T^{r+2}(G, M)$.*

Proof. See [8, Proposition 3.4, pag. 81]. □

Definition 1.7. *Let G be a finite cyclic group and M a G-module such that its cohomology groups are finite. Then the **Herbrand quotient** of M is*

$$h(M) := \frac{|H_T^0(G, M)|}{|H_T^1(G, M)|}$$

The Herbrand quotient has the following properties.

Proposition 1.13. *Let G be a finite cyclic group. Then:*

1. *If $0 \to M' \to M \to M'' \to 0$ is a short exact sequence of G-modules then if two of their Herbrand quotients are defined so is the third and we have $h(M) = h(M')h(M'')$.*
2. *$h(M) = 1$ for any finite G-module M.*
3. *If $\phi : M \to N$ is a homomorphism of G-modules and $Ker(\phi)$ and $N/\phi(M)$ are finite, then $h(M)$ and $h(N)$ are both defined whenever one of them is so and in this case they are equal.*

Proof. See [8, Proposition 3.6, 3.8, Corollary 3.9, pag. 81,82]. □

1.1.6 Galois Cohomology

During the proofs of the theorems of class field theory we will mainly use Tate cohomology for modules over Galois groups, so now we prove some basic results in Galois cohomology that will be used in the sequel. First of all we observe that if L/K is a finite Galois extension of fields with Galois group G we have that both $(L^\times, \cdot)$ and $(L, +)$ are G-modules in a natural way.

Proposition 1.14. *$H^1(G, L^\times) = 0$ for any finite Galois extension L/K with Galois group G.*

Proof. We want to prove that any cocycle in $C^1(G, L^\times)$ is a coboundary, i.e. that for any map $\phi : G \to L^\times$ such that

$$\phi(\sigma\tau) = \sigma\phi(\tau)\phi(\sigma)$$

for any $\sigma, \tau \in G$ (it is called a cross homomorphism) there exists $x \in L^\times$ such that $\phi(\sigma) = \sigma(x)/x$ for any $\sigma \in G$. The well-known Theorem on the independence of the characters implies that the map

$$\sum_{\sigma \in G} \phi(\sigma)\sigma$$

is not everywhere zero and so there exists $a \in L^\times$ such that

$$b = \sum_{\sigma \in G} \phi(\sigma)\sigma(a) \neq 0$$

So for any $\tau \in G$ we have

$$\tau(b) = \sum_{\sigma \in G} \tau(\phi(\sigma))\tau(\sigma(a)) = \sum_{\sigma \in G} \phi(\tau)^{-1}\phi(\tau\sigma)\tau(\sigma(a)) = \phi(\tau)^{-1}(b)$$

$$\Rightarrow \phi(\tau) = b/\tau(b) = \tau(b^{-1})/b^{-1}$$

□

Proposition 1.15. *$H^r(G, L) = 0$ for any $r > 0$ and for any finite Galois extension L/K with Galois group G.*

Proof. We know that there exists $x \in K$ such that

$$\{\sigma(x) : \sigma \in G\}$$

is a normal basis for L over K. Then we have an isomorphism of G-modules

$$K[G] \to L, \sum_{\sigma \in G} a_\sigma \sigma \mapsto \sum_{\sigma \in G} a_\sigma \sigma(x)$$

Finally, $K[G] = Ind_{\{1\}}^G K$ implies

$$H^r(G, L) \cong H^r(\{1\}, K) = 0$$

□

1.1.7 Cohomology of profinite groups

During the proofs of theorems of class field theory we will work also with Galois groups of infinite Galois extensions and we know that they are profinite groups, i.e. Hausdorff, compact and totally disconnected topological groups. In order to work with them we introduce cohomology groups for profinite groups.

Definition 1.8. *Let G be a profinite group.*
We define a ***discrete G-module*** *as a G-module M such that the action*

$$G \times M \to M$$

is continuous if M is endowed with the discrete topology. As we did for ordinary G-modules, if $r \geq 0$ is an integer, the r-th cohomology group $H^r_{cts}(G, M)$ can be equivalently defined using injective resolutions of discrete G-modules or continuous cochains.

Proposition 1.16. *Let G be a profinite group, M a discrete G-module and $r \geq 0$ an integer. Then*

$$H^r_{cts}(G, M) = \bigcup_{H \trianglelefteq G,\ H \text{ open}} H^r(G/H, M^H)$$

where the inclusion

$$H^r(G/H, M^H) \hookrightarrow H^r_{cts}(G, M)$$

is given by the usual inflation homomorphism.

Proof. See [8, Proposition 4.2, pag. 87]. □

1.2 Orders of number fields

Definition 1.9. *Let K be a number field. An* ***order*** *$\mathcal{O}$ of K is a subring of K which is also a free $\mathbb{Z}$-module of rank equal to the dimension of K over $\mathbb{Q}$.*

Proposition 1.17. *The ring of integers $\mathcal{O}_K$ is the unique maximal order of a number field K.*

Proof. We already know that $\mathcal{O}_K$ is an order of K, so we just need to prove that any order is contained in it. Take $\mathcal{O}$ an order of K and $\alpha \in \mathcal{O}$. We consider the $\mathbb{Z}$-submodule of $\mathcal{O}$ generated by the powers of α and $\{\alpha_1, ..., \alpha_k\}$ a $\mathbb{Z}$-basis of it. Any α_i is a finite $\mathbb{Z}$-linear combination of powers of α, so we can take a positive integer N greater than all the exponents with which α appears in these combinations. Then,

$$\alpha^N = c_1\alpha_1 + ... + c_k\alpha_k$$

with $c_i \in \mathbb{Z}$ and it implies that α is an algebraic integer. □

As a first example, we can see that $\mathbb{Z}$ is the only order of $\mathbb{Q}$.

Proposition 1.18. *An order of a number field is a Noetherian integral domain of Krull dimension one.*

Proof. Let $\mathcal{O}$ be an order of K. Since it is a finitely generated $\mathbb{Z}$-module, all of its ideals are so and consequently they are also finitely generated $\mathcal{O}$-modules. Then $\mathcal{O}$ is Noetherian. Now, let $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}$ and take n a non-zero integer in $\mathfrak{p} \cap \mathbb{Z}$. Then, $n\mathcal{O} \subset \mathfrak{p} \subset \mathcal{O}$ and so $\mathfrak{p}$ and $\mathcal{O}$ are free $\mathbb{Z}$-modules of the same rank. Therefore, $\mathcal{O}/\mathfrak{p}$ is a finite integral domain, hence a field and so $\mathfrak{p}$ is maximal. □

Differently from the ring of integers $\mathcal{O}_K$, a generic order is not necessarily a Dedekind domain. Anyway, we can always define fractional ideals to be finitely generated submodules of K over the order and also the product of fractional ideals could be defined as usual. The main difference with the Dedekind case is that not all the fractional ideals are necessarily invertible and so we have to restrict our attention to fractional ideals that admit an inverse. We also observe that all the principal fractional ideals are trivially invertible. From these considerations we derive the following definitions.

Definition 1.10. *Let K be a number field and $\mathcal{O}$ an order in K. We denote as $I(\mathcal{O})$ and $P(\mathcal{O})$, respectively, the groups of invertible and principal fractional ideals of $\mathcal{O}$. Then we define the* ***Picard group*** *of $\mathcal{O}$ as*

$$Pic(\mathcal{O}) := I(\mathcal{O})/P(\mathcal{O})$$

Obviously, $Pic(\mathcal{O}_K)$ is just the ideal class group of K.
Now, we are mainly interested in studying orders of imaginary quadratic fields because they will be important in the development of theory of complex multiplication. First, we observe that all of them could be considered as $\mathbb{Z}$-modules generated by 1 and a suitable $\tau \in K$. We will denote an order of this kind as $[1, \tau]$.

Proposition 1.19. *All the orders of an imaginary quadratic field K could be written as*

$$\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$$

for a certain $f \in \mathbb{N}$ (which is called the conductor of the order and satisfies the equality $[\mathcal{O}_K : \mathcal{O}] = f$).

Proof. First of all we prove that $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$ is an order of K.
If $\mathcal{O}_K = [1, \tau]$ it is obvious that $\mathcal{O} = [1, f\tau]$ and so it is an additive subgroup and a free $\mathbb{Z}$-module of rank 2.
It is also a subring: if $n, m \in \mathbb{Z}$ and $a, b \in \mathcal{O}_K$, then

$$(n + fa)(m + fb) = nm + f(ma + nb + fab)$$

So it is an order and we also get the equality

$$[\mathcal{O}_K : \mathcal{O}] = [[1, \tau] : [1, f\tau]] = f$$

Now, let $\mathcal{O}$ be an order in an imaginary quadratic field K and assume $\mathcal{O}_K = [1, \tau]$. $\mathcal{O}$ is a $\mathbb{Z}$-submodule of rank 2 of $\mathcal{O}_K$ and it contains 1, so there exists $n \in \mathbb{N}$ such that $n\tau \in \mathcal{O}$. We take $f \in \mathbb{N}$ to be the smallest positive integer which satisfies this property. So $[1, f\tau] \subset \mathcal{O}$ and we prove the converse to conclude. If $\alpha \in \mathcal{O} \subset \mathcal{O}_K$, then $\alpha = a + b\tau$ for $a, b \in \mathbb{Z}$ and $b\tau = \alpha - a \in \mathcal{O}$. It implies that f divides b and so $\alpha \in [1, f\tau]$. □

Definition 1.11. *The **discriminant** $Disc(\mathcal{O})$ of an imaginary quadratic order $\mathcal{O} = [1, \tau]$ is the discriminant of the minimal polynomial of τ.*
*An **imaginary quadratic discriminant** is a negative integer which is a square modulo 4. It is also called **fundamental** if it is not the multiple of another imaginary quadratic discriminant by a non trivial square of an integer.*

It is just an exercise to show that the definition of discriminant of an imaginary quadratic order does not depend on the choice of τ and that it is compatible with the definition of discriminant of the ring of integers.
Now, we observe that by definition any discriminant of an imaginary quadratic order is an imaginary quadratic discriminant and also that fundamental discriminants coincide with discriminants of imaginary quadratic fields. Furthermore, the last proposition gives us the following corollary.

Corollary 1.1. *If D is an imaginary quadratic discriminant then there exists a unique imaginary quadratic order $\mathcal{O}$ of discriminant D and if K is the imaginary quadratic number field containing it we have that $D = f^2 D_K$ where D_K is the discriminant of the number field and f is the conductor of $\mathcal{O}$.*

Proof. Let $D = f^2 D'$, where $f \in \mathbb{N}$ and D' is a fundamental discriminant. Then there exists an imaginary quadratic field K such that $D_K = D'$ and we fix $\mathcal{O} := \mathbb{Z} + f\mathcal{O}_K$. In particular, if $\mathcal{O}_K = [1, \tau]$, then $\mathcal{O} = [1, f\tau]$. Now, if $x^2 + bx + c$ is the minimal polynomial of τ, $x^2 + fbx + f^2 c$ is the minimal polynomial of $f\tau$ and

$$Disc(\mathcal{O}) = f^2 b^2 - 4f^2 c = f^2(b^2 - 4c) = f^2 D_K$$

Uniqueness follows trivially from the last proposition because $f_1^2 D_1 = f_2^2 D_2$ if and only if $f_1 = f_2$ and $D_1 = D_2$ (where D_1 and D_2 are fundamental discriminants). □

1.3 Primes of number fields

Definition 1.12. *Let K be a field. A function $|\cdot| : K \to \mathbb{R}_{\geq 0}$ is called an **almost-absolute value** on K if the following conditions are satisfied:*

- $|x| = 0 \Leftrightarrow x = 0$ *for any* $x \in K$;

- $|xy| = |x||y|$ *for any* $x, y \in K$.

An almost-absolute value is called an ***absolute value*** *if also the triangular inequality is satisfied:*

$$|x + y| \leq |x| + |y| \; for \; any \; x, y \in K$$

An absolute value is called ***nonarchimedean*** *if we also have:*

$$|x + y| \leq max\{|x|, |y|\} \; for \; any \; x, y \in K$$

We say that two almost-absolute values $|\cdot|_1$ *and* $|\cdot|_2$ *are* ***equivalent*** *if there exists* $\lambda \in \mathbb{R}_{>0}$ *such that* $|\cdot|_2 = |\cdot|_1^{\lambda}$.

As a first example let $\mathfrak{p}$ be a prime ideal of a number field K and denote as $ord_{\mathfrak{p}}(x)$ the $\mathfrak{p}$-adic valuation for any $x \in K$ (i.e. the ramification index of $\mathfrak{p}$ in $x\mathcal{O}_K$). Then we choose $r > 1$ a real number and we define the $\mathfrak{p}$-adic absolute value as

$$|x| := \left(\frac{1}{r}\right)^{ord_{\mathfrak{p}}(x)}$$

Theorem 1.2. *Let* K *be a number field. Then every almost-absolute value of* K *is equivalent to exactly one of the following:*

- *the* $\mathfrak{p}$*-adic absolute value for a prime ideal* $\mathfrak{p}$ *of* K*;*
- *the absolute value* $x \mapsto |\sigma(x)|$ *for a real embedding* $\sigma : K \hookrightarrow \mathbb{R}$*;*
- *the absolute value* $x \mapsto |\sigma(x)|$ *for a pair of conjugate complex embeddings* $\{\sigma, \bar{\sigma}\}$ *with* $\sigma : K \hookrightarrow \mathbb{C}$.

The notion of prime of a number field will be crucial in global class field theory.

Definition 1.13. *Let* K *be a number field. A* ***prime*** *(or a place) of* K *is an equivalence class of almost-absolute values of* K*. We denote a generic prime by* v *and the completion of* K *with respect to one of its absolute values (there is at least one of them in every equivalence class) by* K_v*. We aslo denote by* $\mathcal{O}_v$ *the ring of integers of* K_v *and by* U_v *its group of units.*
We say that a prime v *is:*

- ***finite*** *if it associated to a prime ideal of* K *(and in this case we denote the ideal as* $\mathfrak{p}_v$*);*
- ***real*** *if it is associated to a real embedding (and we denote as* a_v *the image of* a *under the embedding for any* $a \in K$*);*
- ***complex*** *if it is associated to a pair of conjugate complex embeddings.*

We observe that the completion of a number field with respect to a real prime is $\mathbb{R}$ and with respect to a complex prime is $\mathbb{C}$. We want to choose a representative for any equivalence class and we call them **normalized almost-absolute values**. We make this choice in the following way:

- $|x|_v = \left(\frac{1}{N_{K/\mathbb{Q}}(\mathfrak{p})}\right)^{ord_{\mathfrak{p}}(x)}$ if v is a finite prime associated to $\mathfrak{p}$;
- $|x|_v = |\sigma(x)|$ if v is a real prime associated to σ;
- $|x|_v = |\sigma(x)|^2$ if v is a complex prime associated to σ.

In the end, we state two important results which will be crucial in the sequel. The first one is called the weak approximation theorem while the second is known as the product formula.

Theorem 1.3. *Let K be a field, $x_1, ..., x_n \in K$, $\epsilon > 0$ and $|\cdot|_1, ..., |\cdot|_n$ nontrivial inequivalent almost-absolute values on K. Then there exists $x \in K$ such that*

$$|x - x_i|_i < \epsilon$$

for any $i = 1, ..., n$.

Proof. See [7, Theorem 7.20, pag. 114]. □

Theorem 1.4. *Let K be a number field and $x \in K^\times$. Then*

$$\prod_{v \text{ prime of } K} |x|_v = 1$$

Proof. See [7, Theorem 8.8, pag. 138]. □

Chapter 2

Local Class Field Theory

The first step in the exploration of class field theory is the study of its local version. Local class field theory was introduced by Hasse in 1930 and its main purpose is the classification of abelian extensions of local fields.
We recall that a local field K must be one of the following:

- $\mathbb{R}$ or $\mathbb{C}$ (archimedean local field);
- a complete discrete valuation field with finite residue field (nonarchimedean local field).

First of all, we fix some notations for a nonarchimedean local field K. We will denote by:

- $\mathcal{O}_K$ the ring of integers of K;
- $\mathfrak{m}_K$ the maximal ideal of $\mathcal{O}_K$;
- U_K the group of units of $\mathcal{O}_K$;
- $k := \mathcal{O}_K/\mathfrak{m}_K$ the residue field of K.

2.1 Statements of the main theorems

In this first section we want to state the main theorems of local class field theory and to prove some corollaries. We recall that if L/K is a finite unramified extension of nonarchimedean local fields we have an isomorphism $Gal(L/K) \cong Gal(l/k)$ inherited from the action of $Gal(L/K)$ on $\mathcal{O}_L$ and we denote as $Frob_{L/K}$ the preimage of the map $x \mapsto x^{|k|}$ (which is a generator of $Gal(l/k)$ as a cyclic group). We also denote by K^{ab} the extension of K generated by all of its abelian extensions, by K^{un} the extension of K generated by all of its unramified extensions and by $Frob_K$ the generator of $Gal(K^{un}/K)$ which is just $Frob_{L/K}$ when restricted to a finite unramifed extension L/K. We start by stating the local reciprocity law.

Theorem 2.1. *If K is a local field, there exists a unique homomorphism*

$$\phi_K : K^\times \to Gal(K^{ab}/K)$$

such that:

- *if L/K is a finite abelian extension, ϕ_K induces an isomorphism*

$$\phi_{L/K} : K^\times/Nm_{L/K}(L^\times) \to Gal(L/K)$$

- *if K is nonarchimedean, $\phi_K(\pi)|_L = Frob_{L/K}$ for any finite unramified extension L/K and any prime element π of K.*

The maps ϕ_K and $\phi_{L/K}$ are called the **local Artin maps** for K and L/K respectively.
Now, we state the local existence theorem. We call **norm groups** of a local field K its subgroups of the form $Nm(L^\times) := Nm_{L/K}(L^\times)$ for a finite abelian extension L/K.

Theorem 2.2. *Let K be a local field. A subgroup of $K^\times$ is a norm group if and only if it is open of finte index.*

Finally, we prove some corollaries to the stated theorems. The first one is central in local class field theory because it gives an elegant classification of finite abelian extensions of a local field.

Corollary 2.1. *Let K be a local field. Then there is a one-to-one inclusion-reversing correspondence between the set of its finite abelian extensions and the set of the open subgroups of finte index of $K^\times$ (or, equivalently, the set of its norm subgroups) given by*

$$L \mapsto Nm(L^\times)$$

Proof. The defined map is trivially surjective thanks to the local existence theorem. In order to prove that it is injective and inclusion-reversing we need to show that for any finite abelian extensions L and L' of K we have

$$L \subset L' \Leftrightarrow Nm(L'^\times) \subset Nm(L^\times)$$

The first implication follows immediately from the transitivity of the norm. For the opposite direction we consider the following diagram:

$$\begin{array}{ccc} K^\times/Nm(L'^\times) & \xrightarrow{\phi_{L'/K}} & Gal(L'/K) \\ \downarrow{\scriptstyle id} & & \\ K^\times/Nm(L^\times) & \xrightarrow{\phi_{L/K}} & Gal(L/K) \end{array}$$

We recall that the map

$$Gal(LL'/K) \to Gal(L/K) \times Gal(L'/K), \sigma \mapsto (\sigma|_L, \sigma|_{L'})$$

is injective and it is immediate to see that its image is the set of couples $(\phi_{L/K} \circ id \circ \phi^{-1}_{L'/K}(\tau), \tau)$ for $\tau \in Gal(L'/K)$. Then $Gal(LL'/K) \cong Gal(L'/K)$ and so $L \subset L'$. □

Corollary 2.2. *Let K be a local field, L/K a finite abelian extension and $Nm(L^\times) \leq H \leq K^\times$. Then there exists a finite abelian extension M of K such that $H = Nm(M)$, i.e. H is a norm group.*

Proof. We call M the fixed field of $\phi_{L/K}(H \, mod \, Nm(L^\times))$ and we consider the following commutative diagram:

$$\begin{array}{ccc} K^\times & \xrightarrow{\phi_{L/K}} & Gal(L/K) \\ \downarrow{\scriptstyle id} & & \downarrow{\scriptstyle res} \\ K^\times & \xrightarrow{\phi_{M/K}} & Gal(M/K) \end{array}$$

It follows immediately that

$$\begin{aligned} Nm(M^\times) &= \phi^{-1}_{M/K}(1) = \phi^{-1}_{M/K}(res(Gal(L/M))) = \phi^{-1}_{M/K}(res(\phi_{L/K}(H))) \\ &= id(H) = H \end{aligned}$$

□

Corollary 2.3. *Let K be a local field and L_1/K and L_2/K finite abelian extensions. Then:*

- $Nm((L_1L_2)^\times) = Nm(L_1^\times) \cap Nm(L_2^\times)$;
- $Nm((L_1 \cap L_2)^\times) = Nm(L_1^\times)Nm(L_2^\times)$.

Proof. Both the results follow immediately from the fact that the defined bijection is inclusion-reversing, since:

- L_1L_2 is the smallest finite abelian extension of K that contains both L_1 and L_2;
- $Nm(L_1^\times) \cap Nm(L_2^\times)$ is the largest open subgroup of finite index of $K^\times$ which is contained in $Nm(L_1^\times)$ and in $Nm(L_2^\times)$;
- $L_1 \cap L_2$ is the largest finite abelian extension of K that is contained in L_1 and L_2;
- $Nm(L_1^\times)Nm(L_2^\times)$ is the smallest subgroup of $K^\times$ which contains both $Nm(L_1^\times)$ and $Nm(L_2^\times)$ and it is a norm group from the previous corollary.

□

2.2 Proof of the local reciprocity law

In this section we prove the existence of a local Artin map for any local field K and uniqueness in the archimedean case. Uniqueness in the nonarchimedean case will be proved at the end of the following section as a consequnce of the proof of local existence theorem.

Theorem 2.3. *If K is a local field, there exists a unique homomorphism*

$$\phi_K : K^\times \to Gal(K^{ab}/K)$$

such that:

- *if L/K is a finite abelian extension, ϕ_K induces an isomorphism*

$$\phi_{L/K} : K^\times / Nm_{L/K}(L^\times) \to Gal(L/K)$$

- *if K is nonarchimedean, $\phi_K(\pi)|_L = Frob_{L/K}$ for any finite unramified extension L/K and any prime element π of K.*

As a first step, we prove the theorem in the archimedean case.
If $K = \mathbb{C}$, we define

$$\phi_{\mathbb{C}} : \mathbb{C}^\times \to Gal(\mathbb{C}/\mathbb{C})$$

as the obvious trivial map. All the stated properties are obviously satisfied.
If $K = \mathbb{R}$, we define

$$\phi_{\mathbb{R}} : \mathbb{R}^\times \to Gal(\mathbb{C}/\mathbb{R})$$

as the map which sends the elements of $\mathbb{R}_{>0}$ to 1 and the others to the conjugation automorphism. Obviously it is the unique map which satisfies the stated properties.
Now, we prove the existence of ϕ_K for nonarchimedean local fields. In order to simplify the notation, from now on we denote by

$$H^2(L/K) := H^2(Gal(L/K), L^\times)$$

whenever L/K is a Galois extension.

2.2.1 Galois cohomology for local fields

Lemma 2.1. *Let L/K be a finite unramified extension of nonarchimedean local fields. Then the map*

$$Nm_{L/K} : U_L \to U_K$$

is surjective.

Proof. We denote by l and k the residue fields of L and K and by G the Galois group of L/K. Recall that

$$G \cong Gal(l/k)$$

First of all we observe that

$$1 = h(l^\times) = \frac{|H^0_T(G, l^\times)|}{|H^1_T(G, l^\times)|} = |H^0_T(G, l^\times)|$$

$$\Rightarrow H^0_T(G, l^\times) = 0$$

and

$$H^0_T(G, l) \cong H^2_T(G, l) = 0$$

Hence the maps

$$Nm : l^\times \to k^\times,\ Tr : l \to k$$

are surjective. Now, for a generic nonarchimedean local field E with residue field e, we consider the homorphisms

$$\alpha_E : U_E \to e^\times,\ u \mapsto u\, mod\, \mathfrak{m}_E$$

and

$$\beta_{E,m} : 1 + \mathfrak{m}^m_E \to e,\ 1 + a\pi^m \mapsto a\, mod\, \mathfrak{m}_E$$

and we observe that they are surjective and

$$ker(\alpha_E) = 1 + \mathfrak{m}_E,\ ker(\beta_{E,m}) = 1 + \mathfrak{m}^{m+1}_E$$

In order to conclude, we have to work with the following commutative diagrams:

$$\begin{array}{ccc} U_L & \xrightarrow{\alpha_L} & l^\times \\ \downarrow{\scriptstyle Nm} & & \downarrow{\scriptstyle Nm} \\ U_K & \xrightarrow{\alpha_K} & k^\times \end{array} \qquad \begin{array}{ccc} 1 + \mathfrak{m}^m_L & \xrightarrow{\beta_{L,m}} & l \\ \downarrow{\scriptstyle Nm} & & \downarrow{\scriptstyle Tr} \\ 1 + \mathfrak{m}^m_K & \xrightarrow{\beta_{K,m}} & k \end{array}$$

Finally, we take $u \in U_K$. The first commutative diagram tells us that there exists $v_0 \in U_L$ such that $\alpha_K(u) = \alpha_K(Nm(v_0))$ and then

$$u/Nm(v_0) \in 1 + \mathfrak{m}_K$$

With analogous considerations on the second diagram we find $v_1 \in 1 + \mathfrak{m}_L$ such that $u/Nm(v_0 v_1) \in 1 + \mathfrak{m}^2_K$. Proceeding in this way we can find a sequence $\{v_i\}_i$ such that $u/Nm(v_0 \cdots v_i) \in 1 + \mathfrak{m}^{i+1}_K$. If $v := \lim_{i \to +\infty} v_0 \cdots v_i$, we have $u/Nm(v) \in \bigcap 1 + \mathfrak{m}^m_K = \{1\}$ and we can conclude. □

Proposition 2.1. *$H^r_T(G, U_L) = 0$ for any integer r and for any finite unramified extension of local fields L/K with Galois group G.*

Proof. From the previous lemma we have that $H^0_T(G, U_L) = 0$ and, since G is cyclic, to conclude we just need to prove the proposition for $r = 1$. We fix a prime element $\pi \in K$ and we observe that, since

$$L^\times \cong U_L \times \pi^{\mathbb{Z}} \cong U_L \times \mathbb{Z}$$

we have

$$H^1(G, L^\times) \cong H^1(G, U_L) \times H^1(G, \mathbb{Z})$$

Since $H^1(G, L^\times) = 0$, the same holds for $H^1(G, U_L)$. □

2.2.2 The invariant map

Theorem 2.4. *Let K be a nonarchimedean local field. There exists an isomorphism*

$$inv_K : H^2(K^{un}/K) \to \mathbb{Q}/\mathbb{Z}$$

such that for any finite unramified extension L/K it induces an isomomorphism

$$inv_{L/K} : H^2(L/K) \to \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$$

Proof. First of all, we set L/K a finite unramified extension with Galois group G and we define the isomorphism $inv_{L/K}$. We consider the exact sequence

$$0 \to U_L \to L^\times \to \mathbb{Z} \to 0$$

and, since $H^2(G, U_L) = H^3(G, U_L) = 0$, we get an isomorphism

$$ord_L : H^2(L/K) \to H^2(G, \mathbb{Z})$$

Then we consider the exact sequence

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z}$$

and, since $H^1(G, \mathbb{Q}) = H^2(G, \mathbb{Q}) = 0$, we get an isomorphism

$$\delta : H^2(G, \mathbb{Z}) \to H^1(G, \mathbb{Q}/\mathbb{Z})$$

Now, we know that $H^1(G, \mathbb{Q}/\mathbb{Z}) \cong Hom(G, \mathbb{Q}/\mathbb{Z})$ and we consider the isomorphism

$$v : Hom(G, \mathbb{Q}/\mathbb{Z}) \to \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z},\ v(f) = f(Frob_{L/K})$$

Finally we can define

$$inv_{L/K} := v \circ \delta \circ ord_L$$

Now, inv_K can be defined starting from these isomorphisms. It is possible because, if $K \subset L \subset E$ is a tower of finite unramified extensions, the following diagram is commutative:

$$\begin{array}{ccc} H^2(L/K) & \xrightarrow{inv_{L/K}} & \mathbb{Q}/\mathbb{Z} \\ \downarrow Inf & & \downarrow id \\ H^2(E/K) & \xrightarrow{inv_{E/K}} & \mathbb{Q}/\mathbb{Z} \end{array}$$

□

The map inv_K is called the **invariant map** of K.
Now, our purpose is to extend the definition of the invariant map to $H^2(K^{sep}/K)$, where K^{sep} is the separable closure of K.

Lemma 2.2. *If L/K is a finite extension of nonarchimedean local fields of degree n, the following diagram is commutative.*

$$\begin{array}{ccc} H^2(K^{un}/K) & \xrightarrow{inv_K} & \mathbb{Q}/\mathbb{Z} \\ \downarrow Res & & \downarrow n \\ H^2(L^{un}/L) & \xrightarrow{inv_L} & \mathbb{Q}/\mathbb{Z} \end{array}$$

The restriction homomorphism is induced by the compatible homomorphisms

$$Gal(L^{un}/L) \to Gal(K^{un}/K)$$

$$K^{un\times} \hookrightarrow L^{un\times}$$

which are, respectively, the restriction and the natural inclusion.

Proof. The commutative diagram of the statement comes from the composition of the following commutative squares.

$$\begin{array}{ccccccc} H^2(K^{un}/K) & \xrightarrow{ord_K} & H^2(\Gamma_K, \mathbb{Z}) & \xrightarrow{\delta} & H^1(\Gamma_K, \mathbb{Q}/\mathbb{Z}) & \longrightarrow & \mathbb{Q}/\mathbb{Z} \\ \downarrow Res & & \downarrow e\,Res & & \downarrow e\,Res & & \downarrow fe \\ H^2(L^{un}/L) & \xrightarrow{ord_L} & H^2(\Gamma_L/\mathbb{Z}) & \xrightarrow{\delta} & H^1(\Gamma_L, \mathbb{Q}/\mathbb{Z}) & \longrightarrow & \mathbb{Q}/\mathbb{Z} \end{array}$$

The commutativity of the first square comes from the commutativity of

$$\begin{array}{ccc} K^{un\times} & \xrightarrow{ord_K} & \mathbb{Z} \\ \downarrow & & \downarrow e \\ L^{un\times} & \xrightarrow{ord_L} & \mathbb{Z} \end{array}$$

The commutativity of the second square comes from the fact that the boundary map commutes with the restriction homomorphism.
The commutativity of the third square comes from the fact that

$$Frob_L|_{K^{un}} = Frob_K^f$$

□

Now, we continue to consider a finite extension of nonarchimedean local fields L/K and we observe the following commutative diagram.

$$\begin{array}{ccccccc} 0 & \longrightarrow & \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} & \longrightarrow & H^2(K^{un}/K) & \xrightarrow{Res} & H^2(L^{un}/L) \\ & & \downarrow & & \downarrow Inf & & \downarrow Inf \\ 0 & \longrightarrow & H^2(L/K) & \longrightarrow & H^2(K^{sep}/K) & \xrightarrow{Res} & H^2(K^{sep}/L) \end{array}$$

Since the inflation homomorphisms are injective we find that the same holds for the left vertical arrow. We prove an important lemma.

Lemma 2.3. *If L/K is a finite Galois extension of nonarchimedean local fields with Galois group G, there exists an open subgroup V of U_L stable under G such that $H^r(G,V) = 0$ for any positive integer r.*

Proof. We choose a normal basis $\{\sigma(\alpha) : \sigma \in G\}$ of L over K (where $\alpha \in L$) and we define the free G-module

$$A := \sum_{\sigma \in G} \mathcal{O}_K \sigma(\alpha)$$

We can assume $A \subset \mathcal{O}_L$ and, since it is open in it, there exists a positive integer N such that $\pi^N \mathcal{O}_L \subset A$ where π is a prime element of K. Now we set

$$M := \pi^{N+1} A$$
$$V^i := 1 + \pi^i M$$
$$V := V^0$$

We observe that

$$M \cdot M = \pi^{2N+2} A \cdot A \subset \pi^{2N+2} \mathcal{O}_L \subset \pi \cdot \pi^{N+1} A \subset \pi M$$

From these considerations we find that V is an open subgroup of U_L stable under G and $\{V^i\}_{i \geq 1}$ is a descending family of open subgroups of V with trivial intersection, so we only have to prove that V has trivial cohomology. We observe that we have an isomorphism

$$M/\pi M \to V^i/V^{i+1},\ m \mapsto 1 + \pi^i m$$

and, since $M/\pi M$ is free over G, it implies that $H^r(G, V^i/V^{i+1}) = 0$ for any positive integer r. Now, if f is a r-cocycle with values in V, there exist a $(r-1)$-cochain g_1 with values in V and a r-cocycle f_1 with values in V^1 such that $f = d^{r-1}(g_1) + f_1$. Proceeding inductively we find that, for any $n > 0$, there exist a $(r-1)$-cochain g_{n+1} with values in V^n and a r-cocycle f_{n+1} with values in V^{n+1} such that $f_n = d^{r-1}(g_{n+1}) + f_{n+1}$. The product $g := \prod_{n=1}^{\infty} g_n$ is defined by a Cauchy sequence, so it converges and we get $f = d^{r-1}(g)$, which implies $H^r(G, V) = 0$ for any positive integer r. □

Now we can prove that $H^2(L/K)$ has order $[L : K]$ and so it is isomorphic to $\frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$. We just need to show that $|H^2(L/K)| \leq [L : K]$ and we do it by induction on $[L : K]$.

- For the base case we prove the claim for cyclic extensions. We consider V as in the previous lemma and we notice that U_L/V is finite because U_L is compact. Then

$$\begin{aligned} |H^2(L/K)| = \frac{|H^2(L/K)|}{|H^1(G, L^\times)|} = h(L^\times) = h(U_L)h(\mathbb{Z}) = h(V)\frac{|H^0_T(G, \mathbb{Z})|}{|H^1(G, \mathbb{Z})|} \\ = |\mathbb{Z}/[L : K]\mathbb{Z}| = [L : K] \end{aligned}$$

- We assume the claim is true for any positive integer $n < [L : K]$. It is possible to prove that $Gal(L/K)$ is solvable (see [7, Corollary 7.59, pag. 131]) and it implies that there exists a tower of Galois extensions $K \subsetneq E \subsetneq L$. The inflation-restriction exact sequence

$$0 \to H^2(E/K) \to H^2(L/K) \to H^2(L/E)$$

finally tells us that

$$|H^2(L/K)| \leq |H^2(L/E)||H^2(E/K)| = [L : K]$$

Finally, we can prove the existence of the invariant map for K^{sep}/K.

Theorem 2.5. *Let K be a nonarchimedean local field. There exists an isomorphism*

$$inv_K : H^2(K^{sep}/K) \to \mathbb{Q}/\mathbb{Z}$$

such that for any finite Galois extension L/K it induces an isomorphism

$$inv_{L/K} : H^2(L/K) \to \frac{1}{[L : K]}\mathbb{Z}/\mathbb{Z}$$

Proof. From the above discussions and results we have that

$$H^2(L/K) \subset H^2(K^{un}/K)$$

for every finite Galois extension L/K. Then, since

$$H^2(K^{sep}/K) = \bigcup_{L/K\ finite\ Galois} H^2(L/K)$$

we have that

$$Inf : H^2(K^{un}/K) \to H^2(K^{sep}/K)$$

is an isomorphism and we can conclude by composing its inverse with

$$inv_K : H^2(K^{un}/K) \to \mathbb{Q}/\mathbb{Z}$$

□

2.2.3 The local Artin map

Let L/K be a finite Galois extension of nonarchimedean local fields with Galois group G.
For any subgroup H of $Gal(L/K)$ there exists a field $K \subset E \subset L$ such that $H = Gal(L/E)$. We know that $H^1(Gal(L/E), L^\times) = 0$ and the properties of the invariant map tell us that $H^2(L/E)$ is cyclic of order equal to $[L : E]$. Then hypoteses of Tate's theorem are satisfied and we find an isomorphism

$$G^{ab} = H^{-2}(G, L^\times) \cong H^0(G, L^\times) = K^\times / Nm(L^\times)$$

When L/K is a finite abelian extension, we define the local Artin map of the extension as the inverse of the previous isomorphism

$$\phi_{L/K} : K^\times / Nm(L^\times) \to Gal(L/K)$$

Proposition 2.2. *Let $K \subset E \subset L$ be a tower of finite abelian extensions of nonarchimedean local fields. Then the following diagram commutes:*

$$\begin{array}{ccc} K^\times & \xrightarrow{\phi_{L/K}} & Gal(L/K) \\ \downarrow{\scriptstyle id} & & \downarrow \\ K^\times & \xrightarrow{\phi_{E/K}} & Gal(E/K) \end{array}$$

where the right vertical arrow is just the restriction homomorphism.

Proof. See [8, Proposition 3.3, pag. 107]. □

As a consequence of the previous proposition we can finally define the local Artin map of K

$$\phi_K : K^\times \to Gal(K^{ab}/K)$$

The last thing we have to prove is the following proposition.

Proposition 2.3. *If L/K is a finite unramified extension of nonarchimedean local fields and π is a prime element in K, we have that*

$$\phi_{L/K}(\pi) = Frob_{L/K}$$

Proof. We set $G := Gal(L/K)$, $n = [L : K]$ and $\sigma := Frob_{L/K}$. As a first claim we prove that the cochain

$$\phi : G^2 \to L^\times$$

$$\phi(\sigma^i, \sigma^j) = 1 \ \ if \ \ i + j \leq n - 1$$

$$\phi(\sigma^i, \sigma^j) = \pi \ \ if \ \ i + j > n - 1$$

represents a generator of $H^2(L/K)$.
In order to do it, we use the definition of $inv_{L/K}$. We choose $f \in H^1(G, \mathbb{Q}/\mathbb{Z})$, $f(\sigma^i) = \frac{i}{n} + \mathbb{Z}$ and we consider $\bar{f} : G \to \mathbb{Q}$, $\bar{f}(\sigma^i) = \frac{i}{n}$ as a lifting of f. Then

$$\delta^{-1}\bar{f}(\sigma^i, \sigma^j) = \sigma^i \bar{f}(\sigma^j) - \bar{f}(\sigma^{i+j}) + \bar{f}(\sigma^i)$$

and the claim follows from the identification of $\mathbb{Z}$ with $\pi^{\mathbb{Z}}$ because

$$\delta^{-1}\bar{f}(\sigma^i, \sigma^j) = 0 \ \ if \ \ i + j \leq n - 1$$

$$\delta^{-1}\bar{f}(\sigma^i, \sigma^j) = 1 \ \ if \ \ i + j > n - 1$$

Now we conclude the proof following the proof of Tate's Theorem, recalling that we have the following chain of isomorphisms:

$$G \cong H^{-2}(G, \mathbb{Z}) \cong H^{-1}(G, I) \cong H^0(G, L^\times) = K^\times / Nm(L^\times)$$

The definitions of the first two isomorphisms immediately imply that the image of σ in $H^{-1}(G, I)$ is $(\sigma - 1) + I^2$. Then, the boundary map defining the third isomorphism comes from the snake lemma applied to the diagram

$$\begin{array}{ccccccccc}
 & & & & & & H^{-1}(G,I) & & \\
 & & & & & & \downarrow & & \\
 & & & & (L^\times)_G & \longrightarrow & L^\times(\phi)_G & \longrightarrow & I_G & \longrightarrow & 0 \\
 & & & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & L^{\times G} & \longrightarrow & L^\times & \longrightarrow & L^\times(\phi)^G & \longrightarrow & I^G & & \\
 & & \downarrow & & & & & & & & \\
 & & H^0(G, L^\times) & & & & & & & &
\end{array}$$

We choose $x_\sigma + I_G L^\times(\phi) \in L^\times(\phi)_G$ as an element which sends to $\sigma - 1 + I^2 \in I_G$.
Finally, the image of $\sigma - 1 + I^2$ in $H^0(G, L^\times)$ is

$$\begin{aligned} Nm_G(x_\sigma) &= \sum_{i=0}^{n-1} \sigma^i x_\sigma \\ &= x_\sigma + \sum_{i=1}^{n-2} (x_{\sigma^{i+1}} - x_{\sigma^i} + \phi(\sigma, \sigma^{i+1})) + x_1 - x_{\sigma^{n-1}} + \phi(\sigma, \sigma^{n-1}) \\ &= \prod_{i=1}^{n-1} \phi(\sigma, \sigma^i) = \pi \end{aligned}$$

□

2.3 Proof of the local existence theorem

In this section we want to prove the local existence theorem.

Theorem 2.6. *Let K be a local field. A subgroup of $K^\times$ is a norm group if and only if it is open of finte index.*

As a first step, we prove it for archimedean local fields.
If $K = \mathbb{C}$, the only norm subgroup is $\mathbb{C}^\times = Nm(\mathbb{C}^\times)$ and it is open of finite index, so we just need to prove that it is the only one. If $H \leq \mathbb{C}^\times$ is open of finite index, there exists a positive integer n such that $\mathbb{C}^{\times n} \subset H$, but $\mathbb{C}^{\times n} = \mathbb{C}^\times$ for every n so $H = \mathbb{C}^\times$.
If $K = \mathbb{R}$, the only norm subgroups are $\mathbb{R}^\times = Nm(\mathbb{R}^\times)$ and $\mathbb{R}_{>0} = Nm(\mathbb{C}^\times)$ and they are open of finite index, so we just need to prove that there are no more. If $H \leq \mathbb{R}^\times$ is open of finite index, there exists a positive integer n such that $\mathbb{R}^{\times n} \subset H$, but $\mathbb{R}^{\times n}$ is $\mathbb{R}^\times$ if n is odd and $\mathbb{R}_{>0}$ if n is even, so H is one of them.
Then, we have to prove the theorem for nonarchimedean local fields, which is the most difficult part. First of all, we introduce the notion of Lubin-Tate formal group laws and we briefly recall the theory of Newton polygon.

2.3.1 Lubin-Tate formal group laws

Definition 2.1. *Let R be a commutative ring. A **commutative formal group law** is a power series $F \in R[[X, Y]]$ such that*

- *$F(X, Y) = X + Y +$ terms of degree ≥ 2;*
- *$F(X, F(Y, Z)) = F(F(X, Y), Z)$;*
- *$F(X, Y) = F(Y, X)$.*

A homomorphism $f : F \to G$ between commutative formal group laws is a power series $f \in TR[[T]]$ such that

$$f(F(X,Y)) = G(f(X), f(Y))$$

Let K be a nonarchimedean local field with $|k| = q$ and π a prime element in it. We define

$$LT(\pi) := \{f \in \mathcal{O}_K[[T]] : f \equiv \pi T \, mod \, T^2, \; f \equiv T^q \, mod \, \pi\}$$

Proposition 2.4. *For any $f \in LT(\pi)$ there exists a unique commutative formal group law F_f over $\mathcal{O}_K$ such that f is an endomorphism of F_f.*
*We call $\{F_f\}_{f \in LT(\pi)}$ as the family of the **Lubin-Tate formal group laws** associated to π.*

Proof. See [8, Proposition 2.12, pag. 33]. □

Proposition 2.5. *For any $f, g \in LT(\pi)$ and any $a \in \mathcal{O}_K$ there exists a unique homomorphism*

$$[a]_{g,f} : F_f \to F_g$$

such that:

- $[a]_{g,f} \equiv aT \, mod \, T^2$;
- $g \circ [a]_{g,f} = [a]_{g,f} \circ f$.

Furthermore, if we set

$$[a]_f := [a]_{f,f}$$

the inclusion

$$\mathcal{O}_K \hookrightarrow End(F_f), \; a \mapsto [a]_f$$

is a ring homomorphism.

Proof. See [8, Proposition 2.14, Corollary 2.17, pag. 34]. □

2.3.2 Newton polygon

Definition 2.2. *Let K be a local field and consider the polynomial*

$$p(x) = a_0 + \cdots + a_n x^n$$

*in $K[x]$ with $a_o a_n \neq 0$. We define the **Newton polygon** of p as the convex hull of the set of points*

$$\{(i, v_K(a_i)) : i = 0, ..., n\}$$

Theorem 2.7. *Let K be a local field and p a polynomial as the one considered in the previous definition. If $\{l_1, ..., l_r\}$ is the set of the slopes of the line segments of the Newton polygon of p, $\{j_1, ..., j_r\}$ is the set of the lenghts of their projections and $\{\alpha_1, ..., \alpha_s\}$ are the roots of p in K we have:*

- *$l_i \neq l_j$ whenever $i \neq j$;*
- *$-v_K(\alpha_i) \in \{l_1, ..., l_r\}$;*
- *the number of roots with valuation equal to $-l_i$ is, at most, j_i.*

Proof. See [7, Proposition 7.44, pag. 125]. □

2.3.3 Construction of K_π and ϕ_π

Let K be a nonarchimedean local field with $|k| = q$, π a prime element of $\mathcal{O}_K$ and f a polynomial of degree q in $LT(\pi)$. If n is a positive integer we set

$$\Lambda_f := \{x \in K^{sep} : |x| < 1\}$$
$$\Lambda_{f,n} := \{x \in \Lambda_f : [\pi]_f^n(x) = 0\}$$

where $\Lambda_{f,n} \subset \Lambda_f$ are two $\mathcal{O}_K$-modules with the operations defined by

$$x +_{\Lambda_f} y := F_f(x, y)$$
$$a * x := [a]_f(x)$$

We observe that $\Lambda_{f,n}$ is just the set of roots of $f^{(n)}$ because $[\pi]_f = f$ and because $f^{(n)}/T$ is a product of Eisenstein polynomials, i.e. its roots have positive valuations from the theory on Newton polygons. Now, for any positive integer n we set

$$K_{\pi,n} := K[\Lambda_{f,n}]$$

The previous considerations and the fact that $f^{(n)}$ is separable imply that $K_{\pi,n}/K$ is a Galois extension and it is independent of the choice of f. Indeed, if f and g are two different polynomials in $LT(\pi)$, the isomorphism $[1]_{g,f}$ induces an isomorphism of $\mathcal{O}_K$-modules $\Lambda_{f,n} \to \Lambda_{g,n}$. By induction, we choose

- π_1 a non-zero root of f;
- π_n a root of $f - \pi_{n-1}$.

Now, the polynomial f/T is Eisenstein, so the extension $K[\pi_1]/K$ is totally ramified of degree $q-1$. From the results about Newton polygons we know that $v_{K[\pi_1]}(\pi_1) = \frac{1}{q-1}$, so it is a prime element. Then the polynomial $f - \pi_1$ is Eisenstein and $K[\pi_2]/K[\pi_1]$ is a totally ramified extension of degree q. Proceeding in this way we find that $K[\pi_n]/K$ is a totally ramified extension of degree $(q-1)q^{n-1}$.
Obviously, $K[\pi_n] \subset K_{\pi,n}$ because $f^{(n)}(\pi_n) = 0$ and we want to prove that they are equal.

Proposition 2.6. *Let K be a nonarchimedean local field. Any K-automorphism of $K_{\pi,n}$ induces an $\mathcal{O}_K$-automorphism of $\Lambda_{f,n}$ and*

$$Aut_{\mathcal{O}_K}(\Lambda_{f,n}) \cong (\mathcal{O}_K/\mathfrak{m}^n)^\times$$

Proof.

- Obviously, if α is a root of $f^{(n)}$, the same holds for $\sigma(\alpha)$ where $\sigma \in Gal(K_{\pi,n}/K)$. Furthermore, if $\alpha \in \mathcal{O}_K$, we have

$$\begin{aligned}\sigma([a]_f(\alpha)) &= \sigma(\lim_{m\to+\infty}[a]_{f,m}(\alpha)) = \lim_{m\to+\infty}\sigma([a]_{f,m}(\alpha)) \\ &= \lim_{m\to+\infty}[a]_{f,m}(\sigma\alpha) = [a]_f(\sigma\alpha)\end{aligned}$$

  where $[a]_{f,m}$ is the sum of the terms of degree $\leq m$ of $[a]_f$.

- In order to prove that

$$Aut_{\mathcal{O}_K}(\Lambda_{f,n}) \cong (\mathcal{O}_K/\mathfrak{m}^n)^\times$$

  we just need to show that

$$\Lambda_{f,n} \cong \mathcal{O}_K/\mathfrak{m}^n$$

  and we will do it by induction. Since $\Lambda_{f,1}$ has q elements, the structure theorem for finitely generated modules over a PID implies that

$$\Lambda_{f,1} \cong \mathcal{O}_K/\mathfrak{m}$$

  Now, we assume the statement is true in the case $n-1$ and we prove it in the case n. Thanks to the results on the Newton polygon, we observe that if
  $\alpha \in \Lambda_{f,n-1}$, then the roots of the polynomial $f - \alpha$ stands in $\Lambda_{f,n}$, i.e. the map

$$\Lambda_{f,n} \to \Lambda_{f,n-1},\ x \mapsto [\pi]_f(x)$$

  is surjective. Then we have an exact sequence

$$0 \to \Lambda_{f,1} \to \Lambda_{f,n} \to \Lambda_{f,n-1} \to 0$$

  where the third arrow is the surjective map previously defined. Finally, $\Lambda_{f,n}$ has q^n elements and, since $\Lambda_{f,1}$ is a cyclic module, the same holds for $\Lambda_{f,n}$ and then

$$\Lambda_{f,n} \cong \mathcal{O}_K/\mathfrak{m}^n$$

□

Thanks to the previous proposition we have

$$(q-1)q^{n-1} = [K[\pi_n] : K] \leq [K_{\pi,n} : K] = |Gal(K_{\pi,n}/K)| \leq (q-1)q^{n-1}$$

and it implies that

$$K_{\pi,n} = K[\pi_n]$$

and

$$(\mathcal{O}_K/\mathfrak{m}^n)^\times \cong Gal(K_{\pi,n}/K)$$

Proposition 2.7. *π is a norm from $K_{\pi,n}$ for any positive integer n.*

Proof. We define

$$f_n(T) := (f/T) \circ f^{(n-1)} = \pi + \cdots + T^{(q-1)q^{n-1}}$$

and we observe that $f_n(\pi_n) = 0$. Then f_n is the minimum polynomial of π_n over K and then, if $n > 1$, we have

$$Nm_{K_{\pi,n}/K}(\pi_n) = (-1)^{(q-1)q^{n-1}}\pi = \pi$$

If $n = 1$ the statement follows from the transitivity of the norm. □

Finally, we set

$$K_\pi := \bigcup_{n \geq 1} K_{\pi,n}$$

We observe that K_π is a Galois extension of K since it is the union of an increasing sequence of Galois extensions of K. Now, using the fact that $K_\pi \cap K^{un} = K$ we define the map

$$\phi_\pi : K^\times \to Gal(K_\pi \cdot K^{un}/K)$$

in the following way: if $x = u\pi^m$ where $u \in U_K$, $\phi_\pi(x)$ acts on K^{un} as $Frob_K^m$ and on K_π according to

$$\phi_\pi(x)(\lambda) := [u^{-1}]_f(\lambda)$$

with $\lambda \in \Lambda_{f,n}$ for some n. It is immediate to see that ϕ_π is a group homomorphism. Another immediate consequence of the definition is that, if K_m is the unramified extension of K of degree m, $\phi_\pi(x)$ induces the identity on $K_{\pi,n} \cdot K_m$ whenever $x \in (1 + \mathfrak{m}^n) \cdot \langle \pi^m \rangle$. Indeed, $Frob_K^m$ is just the identity on K_m and if $u \in 1 + \mathfrak{m}^n$ the same holds for its inverse and $[u^{-1}]_f(\lambda) = \lambda$ for $\lambda \in \Lambda_{f,n}$ follows from the isomorphism

$$(\mathcal{O}_K/\mathfrak{m}^n)^\times \cong Gal(K_{\pi,n}/K)$$

Proposition 2.8. *Let K be a nonarchimedean local field. Then $K_\pi \cdot K^{un}$ and ϕ_π are independent of the choice of π.*

Proof. See [8, Theorem 3.9, pag. 40]. □

From now on we will denote $\phi' := \phi_\pi$ for any prime element π.

2.3.4 Local Kronecker-Weber Theorem: end of the proof

Lemma 2.4. *If L/K is a finte extension of nonarchimedean local fields and $Nm(L^\times)$ is of finite index in $K^\times$, then it is open.*

Proof. Since

$$Nm(L^\times) \cap U_K = Nm(U_L),$$

$U_K/Nm(U_L)$ injects into $K^\times/Nm(L^\times)$, so $Nm(U_L)$ is of finite index in U_K and it is also closed because continuous image of a compact set. Then it is open in U_K, which is open in $K^\times$, so $Nm(U_L)$ is open in $K^\times$ and it is contained in $Nm(L^\times)$. Then $Nm(L^\times)$ must be open too. □

Lemma 2.5. *Let K be a nonarchimedean local field. Then*

$$\phi_K(x)|_{K_\pi \cdot K^{un}} = \phi'(x)$$

Proof. Let π be a prime element of K. We know that $\phi_K(\pi)$ and $\phi'(\pi)$ act in the same way on K^{un}. Furthermore, $\pi \in Nm(K^\times_{\pi,n})$ and so $\phi_K(\pi)$ acts trivially on $K_{\pi,n}$ and the same holds for $\phi'(\pi) = \phi_\pi(\pi)$. The statement follows because the prime elements of K generate $K^\times$. □

The last step to prove the local existence theorem is the proof of the local Kronecker-Weber Theorem.

Theorem 2.8. *Let K be a nonarchimedean local field and π a prime element of $\mathcal{O}_K$. Then*

$$K^{ab} = K_\pi \cdot K^{un}$$

Proof. We denote as K_m the unramified extension of K of degree m and we set

$$K_{n,m} := K_{\pi,n} \cdot K_m$$
$$U_{n,m} := (1 + \mathfrak{m}^n) \cdot \langle \pi^m \rangle$$

We know that, if $x \in U_{n,m}$, $\phi_\pi(x)$ induces the identity on $K_{n,m}$ and then the same holds for $\phi_K(x)$. It implies that $U_{n,m} \subset Nm(K^\times_{n,m})$ and the following equality proves that they are equal:

$$\begin{aligned}(K^\times : U_{n,m}) &= (U_K : 1 + \mathfrak{m}^n)(\langle \pi \rangle : \langle \pi^m \rangle) = (q-1)q^{n-1}m \\ &= [K_{\pi,n} : K][K_m : K] = [K_{n,m} : K]\end{aligned}$$

where the last equality comes from the fact that $K_m \cap K_{\pi,n} = K$. If L/K is a finite abelian extension we know that $Nm(L^\times)$ is of finite index in $K^\times$, hence it is open and so there exist $n, m \geq 0$ such that $U_{n,m} \subset Nm(L^\times)$. Now, if $x \in K^\times$, we find that

$$\phi_K(x)\, fixes\, K_{n,m} \Rightarrow x \in Nm(K^\times_{n,m}) = U_{n,m} \subset Nm(L^\times) \Rightarrow \phi_K(x)\, fixes\, L$$

and, since any element of $Gal(L \cdot K_{n,m}/K)$ arises as the image of an element of $K^\times$ through ϕ_K, we have $L \subset K_{n,m}$. The statement follows. □

Finally, we can prove the local existence theorem for nonarchimedean local fields. The existence of the local Artin map implies that any norm subgroup of $K^\times$ is of finite index in $K^\times$, hence open. Conversely, for any open subgroup of finite index of $K^\times$ there exist $n, m \geq 0$ such that it contains $U_{n,m} = Nm(K^\times_{n,m})$. Since it contains a norm group, it is a norm group too.

2.3.5 Uniqueness of the local Artin map

Finally, we can also conclude the proof of the local reciprocity law by proving the uniqueness of the local Artin map.

Theorem 2.9. *If K is a nonarchimedean local field and ϕ_K is a local Artin map for K, then ϕ_K is unique.*

Proof. We assume that ϕ_K and ϕ are two local Artin maps for K and we fix a prime element π of $\mathcal{O}_K$. We know that the image of π under any local Artin map induces the identity on K_π and the Frobenius automorphism on K^{un}, hence we have that $\phi_K(\pi)$ and $\phi(\pi)$ induces the same automorphism on $K_\pi \cdot K^{un} = K^{ab}$, so they are equal. We can conclude because $K^\times$ is generated by its prime elements. □

2.4 An example: cyclotomic extensions of $\mathbb{Q}_p$

Let p be a prime positive integer, $n > 1$ a positive integer and ζ_n a primitive n-th root of 1 over $\mathbb{Q}_p$.
The Galois group of $\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p$ is cyclic, hence abelian, so we can study the action of elements of $\mathbb{Q}_p^\times$ on $\mathbb{Q}_p(\zeta_n)$ described by the local Artin map. We distinguish three cases.

First case: we assume n to be coprime with p. In this situation, the polynomial $X^n - 1$ is separable over $\mathbb{F}_p$ and its splitting field is $\mathbb{F}_{p^f}$, where f is the smallest positive integer such that n divides $p^f - 1$. Then, $\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p$ is an unramified extension of degree f and the action of the local Artin map is described in the following way: if $u \cdot p^t \in \mathbb{Q}_p^\times$ with $u \in \mathbb{Z}_p^\times$, its image under the local Artin map acts as the t power of the Frobenius automorphism.

Second case: we assume n to be a power of p. We set

$$f(T) = (T+1)^p - 1 \in LT(p)$$

and from the theory previously developed we immediately have that $\mathbb{Q}_p(\zeta_{p^r}) = (\mathbb{Q}_p)_{p,r}$. Then the extension is totally ramified of degree $(p-1)p^{r-1}$ and we can describe the action of $u \cdot p^t \in \mathbb{Q}_p^\times$ under the local Artin map as follows. We observe that $\zeta_{p^r} - 1$ is a root of $f^{(r)}$, so we just need to find the value $[u^{-1}]_f(\zeta_{p^r} - 1)$. Since $\mathbb{Z}_p/p^r\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$, there exists an integer v such

that $[u^{-1}]_f = [v]_f = (T+1)^v - 1$. Then $\zeta_{p^r} - 1$ is sent to $\zeta_{p^r}^v - 1$.

Third case: the general case is just an immediate consequence of the previous cases. Indeed, if $n = m \cdot p^r$ with p and m coprime, we have that

$$\mathbb{Q}_p(\zeta_n) = \mathbb{Q}_p(\zeta_m)\mathbb{Q}_p(\zeta_{p^r})$$

$$\mathbb{Q}_p(\zeta_m) \cap \mathbb{Q}_p(\zeta_{p^r}) = \mathbb{Q}_p$$

and the properties of the local Artin map tell us that we can describe it using the actions on $\mathbb{Q}_p(\zeta_m)$ and $\mathbb{Q}_p(\zeta_{p^r})$.

Chapter 3

Global Class Field Theory

The main purpose of global class field theory is to classify the abelian extensions of global fields. In this chapter we will put our attention on the particular case of number fields, i.e. on the finite extensions of $\mathbb{Q}$. There are two different ways to approach and to state the main theorems of global class field theory. The most modern and elegant formulation is based on the notion of ideles introduced by Chevalley. Otherwise, it is possible to formulate it in terms of ideals and the linked results are often more useful for applications. In this chapter we will state and prove the main theorems in terms of ideles and then we will only state the results given in terms of ideals.

3.1 Adele rings and Idele groups

In this section we want to introduce the notions of adele ring and idele group of a number field and to study their main properties. First of all we need to introduce the topological notion of restricted product.

Definition 3.1. *The* ***restricted product*** *of a family of topological spaces $(X_i)_i$ with respect to a family of open sets $(U_i)_i$ where $U_i \subset X_i$ for any i is the topological space*

$$\prod{}'(X_i, U_i) := \{(x_i)_i \in \prod X_i : x_i \in U_i \; for \; almost \; all \; i\}$$

The topology is defined by taking as a basis of open sets the family

$$\{\prod V_i : V_i \; is \; an \; open \; subset \; of \; X_i \; and \; V_i = U_i \; for \; almost \; all \; i\}$$

Definition 3.2. *Let K be a number field. The* ***adele ring*** *of K is the topological ring*

$$\mathbb{A}_K := \prod_{v \; prime \; of \; K}{}' (K_v, \mathcal{O}_v)$$

where K_v is the completion of K with respect to the prime v and $\mathcal{O}_v$ is its ring of integers. Addition and multiplication are defined componentwise.

Definition 3.3. *Let K be a number field. The **idele group** of K is the topological group*

$$\mathbb{I}_K := \prod_{v \, prime \, of \, K}' (K_v^\times, \mathcal{O}_v^\times)$$

Multiplication is defined componentwise.

We observe that as a set $\mathbb{I}_K$ is just $\mathbb{A}_K^\times$. Anyway, the topology of $\mathbb{I}_K$ is not the subspace topology inherited from $\mathbb{A}_K$ (but it injects continuosly inside it). If S is a finite set of primes of K, we define

$$\mathbb{I}_{K,S} := \prod_{v \in S} K_v^\times \times \prod_{v \notin S} \mathcal{O}_v^\times$$

Obviously, $\mathbb{I}_{K,S} \leq \mathbb{I}_K$. Now, we define some important functions involving $\mathbb{I}_K$ that will be useful in the sequel:

- The map
$$i_K : K^\times \to \mathbb{I}_K, a \mapsto (a, a, a, ...)$$
is an injective homomorphism. In particular, we can see $K^\times$ as a subgroup of $\mathbb{I}_K$. It is well-defined because any element of $K^\times$ is contained only in finitely many prime ideals of $\mathcal{O}_K$.

- The map
$$\alpha_K : \mathbb{I}_K \to I_K, (a_v)_v \mapsto \prod_{v \, finite \, prime} \mathfrak{p}_v^{ord_{\mathfrak{p}_v}(a_v)}$$
where $\mathfrak{p}_v$ is the prime ideal of $\mathcal{O}_K$ associated to v is a surjective homomorphism between the idele class group and the group of fractional ideals of K.

- The map
$$i_{K_v} : K_v^\times \to \mathbb{I}_K, a \mapsto (1, ..., 1, a, 1, ...1)$$
where a is in the position associated to K_v is an injective homomorphism.

The map i_K leads to the following fundamental definition.

Definition 3.4. *Let K be a number field. The **idele class group** of K is the topological group $C_K := \mathbb{I}_K / K^\times$.*

Now, we recall the notion of norm of ideals and we define norm of ideles.

Definition 3.5. *Let L/K be a finite extension of number fields with ideal groups I_K and I_L and idele groups $\mathbb{I}_K$ and $\mathbb{I}_L$.*
The map

$$Nm_{L/K} : I_L \to I_K$$

is defined by setting

$$Nm_{L/K}(\mathfrak{B}) = \mathfrak{p}^{f(\mathfrak{B}/\mathfrak{p})}$$

for any prime ideal $\mathfrak{B}$ of L where $\mathfrak{p} = \mathfrak{B} \cap \mathcal{O}_K$ and $f(\mathfrak{B}/\mathfrak{p})$ is the inertia degree of $\mathfrak{B}$ over $\mathfrak{p}$. Then the map is obtained with a multiplicative extension.
The map

$$Nm_{L/K} : \mathbb{I}_L \to \mathbb{I}_K$$

is defined by

$$(Nm_{L/K}((a_w)_w))_v = \prod_{w \text{ over } v} Nm_{L_w/K_v}(a_w)$$

The following proposition tells us that it is possible to extend norm maps to ideal and idele class groups and that they commute with the map α_K.

Proposition 3.1. *Let L/K be a finite extension of number fields. The following diagram is commutative:*

$$\begin{array}{ccccc} L^\times & \longrightarrow & \mathbb{I}_L & \xrightarrow{\alpha_L} & I_L \\ \downarrow{\scriptstyle Nm_{L/K}} & & \downarrow{\scriptstyle Nm_{L/K}} & & \downarrow{\scriptstyle Nm_{L/K}} \\ K^\times & \longrightarrow & \mathbb{I}_K & \xrightarrow{\alpha_K} & I_K \end{array}$$

Proof. For the commutativity of the left square see [7, Corollary 8.4, pag. 136]. The commutativity of the right square follows from the obvious equality

$$ord_{\mathfrak{B}}(l) = [L_w : K_v] ord_{\mathfrak{p}}(Nm_{L_w/K_v}(l))$$

for any prime v of K, any prime w of L which lies over v and any $l \in L_w$. □

3.2 Idelic class field theory

In this section we want to state the main theorems of global class field theory in terms of ideles. First of all we need to define a map which is central in this theory. We fix a finite abelian extension of number fields L/K and a prime v of K. We observe that for any prime w of L which lies over v the decomposition groups

$$D(w) = \{\sigma \in Gal(L/K) : \sigma w = w\}$$

and the local Artin maps

$$\phi_v : K_v^\times \to Gal(L_w/K_v)$$

coincide, i.e. $D(w)$ and ϕ_v are independent of the choice of w. Now, we define

$$\phi_{L/K} : \mathbb{I}_K \to Gal(L/K),\ \phi_{L/K}(a) = \prod_{v\ prime\ of\ K} \phi_v(a_v)|_L$$

We observe that the product is well-defined because if v is a finite prime and if we choose w in order to have L_w/K_v unramified, $\phi_v(a_v) = 1$ whenever $a_v \in U_v$. Properties of the local Artin maps imply that if $K \subset L_1 \subset L_2$ is a tower of finite abelian extensions of number fields we have

$$\phi_{L_2/K}(a)|_{L_1} = \phi_{L_1/K}(a)$$

and so if we vary L through the finite abelian extensions of K we get a homomorphism

$$\phi_K : \mathbb{I}_K \to Gal(K^{ab}/K)$$

Definition 3.6. *Let L/K be a finite abelian extension of number fields. ϕ_K and $\phi_{L/K}$ are called the (idelic) global Artin maps of K and L/K.*

Finally, we can state the global reciprocity law and the existence theorem.

Theorem 3.1. *Let K be a number field. Then the following properties hold:*

- $\phi_K(K^\times) = 1$;
- *if L/K is a finite abelian extension, ϕ_K induces an isomorphism*

$$\phi_{L/K} : \mathbb{I}_K/(K^\times \cdot Nm(\mathbb{I}_L)) \to Gal(L/K)$$

or, equivalently,

$$\phi_{L/K} : C_K/Nm(C_L) \to Gal(L/K)$$

Theorem 3.2. *Let K be a number field. If N is an open subgroup of finite index of C_K, then there exists a unique finite abelian extension L/K such that $Nm(C_L) = N$.*

As usual, class field theory is mainly interested in classifying abelian extensions of number fields. In this sense we give the following consequence of the previous theorems.

Corollary 3.1. *Let K be a number field. There is a one-to-one correspondence between finite abelian extensions of K and open subgroups of finite index of C_K given by the map*

$$L \mapsto Nm(C_L)$$

It also satisfies the following properties:

- $L_1 \subset L_2 \Leftrightarrow Nm(C_{L_2}) \subset Nm(C_{L_1})$;
- $Nm(C_{L_1 \cdot L_2}) = Nm(C_{L_1}) \cap Nm(C_{L_2})$;
- $Nm(C_{L_1 \cap L_2}) = Nm(C_{L_1}) \cdot Nm(C_{L_2})$.

The proof of this corollary just follows the same steps as the proof of the corollaries to the main theorems of local class field theory.
Open subgroups of finite index of C_K are called **norm groups**. If N is a norm group, we call the unique finite abelian extension L/K such that $Nm(C_L) = N$ as the **class field** of K belonging to N.

3.3 Proof of the global reciprocity law

In this section we prove the Artin global reciprocity law.

Theorem 3.3. *Let K be a number field. Then the following properties hold:*

- $\phi_K(K^\times) = 1$;
- *if L/K is a finite abelian extension, ϕ_K induces an isomorphism*

$$\phi_{L/K} : \mathbb{I}_K/(K^\times \cdot Nm(\mathbb{I}_L)) \to Gal(L/K)$$

or, equivalently,

$$\phi_{L/K} : C_K/Nm(C_L) \to Gal(L/K)$$

3.3.1 Cohomology of ideles

In this subsection we will give to $\mathbb{I}_L$ and C_L a structure of G-modules where $G = Gal(L/K)$ and we will study their properties under a cohomological point of view. First of all, if $a = (a_w)_w \in \mathbb{I}_L$ and $\sigma \in G$, we set

$$\sigma(a) := (\sigma(a_w))_{\sigma w}$$

The action on C_L is inherited from this one since $L^\times$ is G-invariant. It is immediate to observe that the norms on ideles and idele classes previously defined are exactly the norms given by the structures of G-modules. Furthermore, $\mathbb{I}_L^G = \mathbb{I}_K$ and $C_L^G = C_K$.

Definition 3.7. *Let K be a number field and S a finite set of primes of K which contains all the infinite ones. Then we define the set of **S-units** of K as*

$$U(S) := \{\alpha \in K^\times : ord_{\mathfrak{p}_v}(\alpha) = 0 \, \forall \, v \notin S\}$$

The set of T-units of L where T is a finite set of primes of L is invariant under the action of G, so it can be considered as a G-submodule of $L^\times$. Similarly, $\mathbb{I}_{L,T}$ is a G-submodule of $\mathbb{I}_L$. Furthermore, the usual unit theorem holds for S-units, i.e.

$$U(S) \cong \mathbb{Z}^{|S|-1} \times U(S)_{tors}$$

Now, we observe that if v is a prime of K, w_1 and w_2 are primes of L which lie over v sucht that $w_1 = \sigma w_2$ for $\sigma \in G$ and $G_{w_i} = Gal(L_{w_i}/K_v)$, then the isomorphisms

$$G_{w_2} \to G_{w_1},\ \tau \mapsto \sigma\tau\sigma^{-1}$$
$$L_{w_1} \to L_{w_2},\ x \mapsto \sigma^{-1}x$$

are compatible and they induce isomorphisms

$$H^r(G_{w_1}, L_{w_1}^\times) \cong H^r(G_{w_2}, L_{w_2}^\times)$$

Similarly

$$H^r(G_{w_1}, U_{w_1}) \cong H^r(G_{w_2}, U_{w_2})$$

From now one we will denote by $G^v := G_w$, $L^v := L_w$ and $U^v := U_w$ for any prime v of K and any prime w of L which lies over v.

Proposition 3.2. *Let L/K be a finite cyclic extension of number fields, S a finite set of primes of K and T the set of primes of L which lie over the primes in S. Then*

$$h(\mathbb{I}_{L,T}) = \prod_{v\in S}[L^v : K_v]$$

Proof. We have

$$\begin{aligned} h(G, \mathbb{I}_{L,T}) &= h(G, \prod_{v\in S}\prod_{w|v} L_w^\times) \cdot h(G, \prod_{v\notin S}\prod_{w|v} U_w) \\ &= \prod_{v\in S} h(G, \prod_{w|v} L_w^\times) = \prod_{v\in S} h(G^v, L^{v\times}) \\ &= \prod_{v\in S} |H^2(G^v, L^{v\times})| = \prod_{v\in S}[L^v : K_v] \end{aligned}$$

For the third equality see [8, Proposition 2.3, pag. 204].
For the fourth equality see [8, Proposition 2.5(b), pag. 205] and [8, Corollary 2.6(a), pag. 206].
The last equality comes from the isomorphism

$$H^2(G^v, L^{v\times}) \cong \frac{1}{[L^v : K_v]}\mathbb{Z}/\mathbb{Z}$$

given by the invariant map. □

Proposition 3.3. *Let L/K be a finite cyclic extension of number fields, S a set of primes of K which contain all the infinite ones and T the set of primes of L which lie over the primes in S. Then*

$$h(U(T)) = \frac{\prod_{v \in S} [L^v : K_v]}{[L : K]}$$

Proof. See [8, Proposition 3.1, pag. 208]. □

3.3.2 The first inequality

In this subsection we want to prove the following inequality, known as the first inequality.

Theorem 3.4. *Let L/K be a finite cyclic extension of number fields. Then*

$$(\mathbb{I}_K : K^\times \cdot Nm(\mathbb{I}_L)) \geq [L : K]$$

The proof is based on the following two lemmas.

Lemma 3.1. *If K is a number field and S is a finite set of primes which contains the infnte ones and a set of generators for the ideal class group $Cl(K)$, then*

$$\mathbb{I}_K = K^\times \cdot \mathbb{I}_{K,S}$$

Proof. Since S contains a set of generators for $Cl(K)$, any fractional ideal of K can be written as the product of ideals in S and a principal ideal, i.e.

$$I_K / \langle S \rangle \cdot K^\times = 0$$

Then, we can conclude because the map α_K defines an isomorphism

$$\mathbb{I}_K / \mathbb{I}_{K,S} \cdot K^\times \cong I_K / \langle S \rangle \cdot K^\times$$

□

Lemma 3.2. *$h(C_L) = [L : K]$ whenever L/K is a finite cyclic extension of number fields.*

Proof. We fix a finite set S of primes of K which contains:

- all the infinite primes;
- all the primes that ramify in L;
- the finite primes associated to a set of generators of $Cl(L)$;

and we denote by T the set of primes of L which lie over S.
Thanks to the previous lemma and to the fact that $L^\times \cap \mathbb{I}_{L,T} = U(T)$ we find

$$C_L = \mathbb{I}_L/L^\times = L^\times \cdot \mathbb{I}_{L,T}/L^\times \cong \mathbb{I}_{L,T}/L^\times \cap \mathbb{I}_{L,T} = \mathbb{I}_{L,T}/U(T)$$

and it implies

$$h(C_L) = \frac{h(\mathbb{I}_{L,T})}{h(U(T))} = [L:K]$$

where the last equality follows from the results on cohomology of ideles. □

The first inequality follows from the previous lemma because

$$\begin{aligned}(\mathbb{I}_K : K^\times \cdot Nm(\mathbb{I}_L)) &= |H^0_T(G, C_L)| \geq |H^0_T(G, C_L)|/|H^1_T(G, C_L)| \\ &= h(C_L) = [L:K]\end{aligned}$$

3.3.3 The second inequality

Now, we want to prove the opposite direction of the inequality. In order to do it we state a more general theorem.

Theorem 3.5. *Let L/K be a finite Galois extension of degree n of number fields with Galois group G. Then*

- $(\mathbb{I}_K : K^\times \cdot Nm(\mathbb{I}_L))$ *is finite and it divides n;*
- $H^1(G, C_L) = 0$*;*
- $H^2(G, C_L)$ *is finite and its order divides n.*

Lemma 3.3. *If the first point of the theorem holds in the case of finite cyclic extensions of prime degree p, then the theorem holds in general.*

Proof. We split the proof into three steps.
First step: we assume that the first point of the theorem holds for cyclic extensions of prime degree p and we prove that all the other points hold for cyclic extension of prime degree p. The third point of the theorem follows immediately because

$$\mathbb{I}_K/K^\times \cdot Nm(\mathbb{I}_L) \cong C_K/Nm(C_L) = H^0_T(G, C_L) \cong H^2(G, C_L)$$

while the second point follows from the fact that $h(C_L) = [L:K]$.
Second step: we assume that the theorem holds for cyclic extensions of prime degree p and we prove it holds for extensions L/K such that $Gal(L/K)$ is a p-group. Let $G := Gal(L/K)$, we will prove the claim by induction on $|G|$. Notice that, since it is a p-group, it has a normal subgroup H of finite index

p and set $K' := L^H$. We consider the following inflation-restriction exact sequences.

$$0 \to H^1(G/H, C_{K'}) \to H^1(G, C_L) \to H^1(H, C_L)$$

$$0 \to H^2(G/H, C_{K'}) \to H^2(G, C_L) \to H^2(H, C_L)$$

By induction, $H^1(G/H, C_{K'}) = 0$ and $H^1(H, C_L) = 0$, so
$H^1(G, C_L) = 0$.
Similarly, $|H^2(G/H, C_{K'})|$ divides p and $|H^2(H, C_L)|$ divides $\frac{[L:K]}{p}$, so
$|H^2(G, C_L)|$ divides $[L : K]$.
Finally, the first point follows from the equality

$$(C_K : Nm_{L/K}(C_L)) = (C_K : Nm_{K'/K}(C_{K'}))(Nm_{K'/K}(C_{K'}) : Nm_{L/K}(C_L))$$

and from the surjectivity of the obvious map

$$C_{K'}/Nm_{L/K'}(C_L) \to Nm_{K'/K}(C_{K'})/Nm_{L/K}(C_L)$$

Third step: we assume that the theorem holds for extensions L/K such that $Gal(L/K)$ is a p-group and we prove that it holds in general. If $G := Gal(L/K)$ and H is a p-Sylow of G, we know that the restriction homomorphisms $H^r_T(G, C_L) \to H^r_T(H, C_L)$ are injective on the p-primary components. Then the theorem follows since $H^1(H, C_L) = 0$ and $|H^0_T(H, C_L)|$ and $|H^2(H, C_L)|$ divide $[L : L^H]$. □

Lemma 3.4. *If the first point of the theorem holds in the case of finite cyclic extensions L/K of prime degree p such that K contains a p-th root of 1, then the theorem holds in general.*

Proof. Let ζ be a primitive p-th root of 1, $K' := K[\zeta]$, $L' := L \cdot K'$. Obviously, $[K' : K] = m < p$ and so $L \cap K' = K$. We consider the following diagram where the rows are exact and the squares commute.

$$\begin{array}{ccccccc}
C_L & \xrightarrow{Nm_{L/K}} & C_K & \longrightarrow & C_K/Nm(C_L) & \longrightarrow & 0 \\
\downarrow & & \downarrow & & \downarrow & & \\
C_{L'} & \xrightarrow{Nm_{L'/K'}} & C_{K'} & \longrightarrow & C_{K'}/Nm(C_{L'}) & \longrightarrow & 0 \\
\downarrow{\scriptstyle Nm_{L'/L}} & & \downarrow{\scriptstyle Nm_{K'/K}} & & \downarrow & & \\
C_L & \xrightarrow{Nm_{L/K}} & C_K & \longrightarrow & C_K/Nm(C_L) & \longrightarrow & 0
\end{array}$$

Now, the compositions of the maps in the first two columns are just exponentiations by m and so the same holds for the third column. $C_K/Nm(C_L)$ is killed by p and so, since it is coprime with m, the composition of the maps in the third column is an isomorphism. Finally it implies that $(C_K : Nm(C_L))$ divides $(C_{K'} : Nm(C_{L'}))$ and it divides $[L : K]$ by hypotesis. □

Thanks to the previous lemmas we only need to prove the second inequality in the case of finite cyclic extensions L/K of prime degree p such that K contains a p-th root of 1. We will prove it in a more general case, in particular we will consider L/K to be a finite abelian extension of exponent p. In particular $Gal(L/K) \cong (\mathbb{Z}/p\mathbb{Z})^r$ for a suitable positive integer r and Kummer theory tells us that $L = K[\sqrt[p]{\alpha_1}, ..., \sqrt[p]{\alpha_r}]$ for suitable $\alpha_i \in K$.
We also fix S to be a finite set of primes of K which contains:

- all the infinite primes;
- all the divisors of p;
- all the primes that ramify in L;
- a set of generators for $Cl(K)$;
- enough primes so that all α_i are in $U(S)$.

We set $M := K[U(S)^{\frac{1}{p}}]$, which is the Kummer extension corresponding to

$$U(S) \cdot K^{\times p}/K^{\times p} \cong U(S)/U(S) \cap K^{\times p} = U(S)/U(S)^p \cong (\mathbb{Z}/p\mathbb{Z})^s$$

where $s = |S|$ and the last isomorphism comes from the unit theorem and the fact that $\mu_p \subset U(S)_{tors}$. Then $K \subset L \subset M$ and $[M : L] = p^t$ where $t = s - r$.

Lemma 3.5. *If L/K is a finite abelian extension of number fields and A is a finite set of primes of K which contain the inifinite ones and those which ramify in L, the set*

$$\{\phi_v(\pi_v) : v \notin A\}$$

generates $Gal(L/K)$.

Proof. For any $v \notin A$ we denote by $(\mathfrak{p}_v, L/K) := \phi_v(\pi_v)$ seen as an element of $G := Gal(L/K)$. If H is the subgroup generated by the set considered in the statement and E is its fixed field we find that

$$(\mathfrak{p}_v, E/K) = (\mathfrak{p}_v, L/K)|_E = 1$$

for any $v \notin A$. Then all the primes of K which do not lie in A split in E. In order to prove that $H = G$ we claim that $E = K$. We define

$$D := \{(a_v)_v \in \mathbb{I}_K : a_v = 1 \, \forall \, v \in A\}$$

Obviously $D \subset Nm(\mathbb{I}_L)$ since $L_w = K_v$ whenever $w|v$, $v \notin A$.
Furthermore, if $a = (a_v)_v \in \mathbb{I}_K$, thanks to the weak approximation theorem we can find $b \in K^\times$ which is close to a_v for $v \in A$. Then there exists $\alpha \in D$ such that $(b\alpha)_v = a_v$ for any $v \notin A$ and it implies that $b\alpha$ is close to a. Then

$K^\times \cdot D$ is dense in $\mathbb{I}_K$. Now, we assume by contradiction that $E \neq K$ and so we can find a field K' such that $K \subset K' \subset L$, $K \neq K'$ and K'/K is cyclic. Then

$$D \subset Nm(\mathbb{I}_L) \subset Nm(\mathbb{I}_{K'})$$

which implies that $K^\times \cdot Nm(\mathbb{I}_{K'})$ is dense in $\mathbb{I}_K$. This subgroup must be open and, hence, closed and so

$$K^\times \cdot Nm(\mathbb{I}_{K'}) = \mathbb{I}_K$$

Then, thanks to the first inequality, we have $K' = K$, a contradiction, and the proof is concluded. □

Thanks to [8, Lemma 6.2, pag. 215], which is proved using the properties of S and the previous lemma, we can find a finite set of primes of K called T which is disjoint from S and such that

$$\{\phi_v(\pi_v) : v \in T\}$$

is a basis for $Gal(M/L)$ seen as a vector space over $\mathbb{F}_p$. Obviously $t = |T|$. Now we set

$$E := \prod_{v \in S} K_v^{\times p} \times \prod_{v \in T} K_v^\times \times \prod_{v \notin S \cup T} U_v$$

and we observe that it is a subgroup of $\mathbb{I}_K$ contained in $Nm(\mathbb{I}_L)$. Indeed, if $a = (a_v)_v \in E$, we can see that any component is a norm:

- if $v \in S$ the isomorphism

  $$K_v^\times / Nm(L_w^\times) \cong Gal(L_w/K_v)$$

  implies that the left group is killed by p and so $K_v^{\times p} \subset Nm(L_w^\times)$;
- if $v \in T$ it follows immediately from the fact that $L_w = K_v$;
- if $v \notin S \cup T$, L_w is unramified over K_v and so the norm map $U_w \to U_v$ is surjective.

Now we need to prove an auxiliary lemma.

Lemma 3.6. *Let K be a local field with $char(K) = 0$ and n a positive integer. Then*

$$(K^\times : K^{\times n}) = n\frac{|\mu_n|}{|n|}$$

and if K is nonarchimedean

$$(U_K : U_K^n) = \frac{|\mu_n|}{|n|}$$

where $|\mu_n|$ is the number of n-th roots of 1 in K and $|n|$ is the absolute value of n.

Proof. If $K = \mathbb{C}$, the first equation is just

$$1 = n\frac{n}{n^2}$$

If $K = \mathbb{R}$ and n is even, the first equation is just

$$2 = n\frac{2}{n}$$

If $K = \mathbb{R}$ and n is odd, the first equation is just

$$1 = n\frac{1}{n}$$

If K is nonarchimedean, the isomorphism $K^\times \cong U_K \times \mathbb{Z}$ tells us that we only need to prove the second equation. The exponential map defines an isomorphism from a subgroup of finite index of $\mathcal{O}_K$ to a subgroup of finite index of U_K and it implies

$$h(U_K) = h(\mathcal{O}_K) = (\mathcal{O}_K : n\mathcal{O}_K) = \frac{1}{|n|}$$

where the modules are considered over $\mathbb{Z}/n\mathbb{Z}$ and it acts trivially. Finally

$$(U_K : U_K^n) = \frac{|Ker(Nm_{\mathbb{Z}/n\mathbb{Z}}(U_K))|}{|n|} = \frac{|\mu_n|}{|n|}$$

□

The following two lemmas are crucial to conclude the proof of the second inequality.

Lemma 3.7. *It holds*

$$(\mathbb{I}_{K,S\cup T} : E) = p^{2s}$$

Proof. Since K contains a primitive p-th root of 1 and S contains all the primes with non-trivial valuation on p, we have

$$(\mathbb{I}_{K,S\cup T} : E) = \prod_{v\in S}(K_v^\times : K_v^{\times p}) = \prod_{v\in S} p\frac{|\mu_p|}{|p|_v} = \frac{p^{2s}}{\prod_{v\in S}|p|_v} = p^{2s}$$

thanks to the product formula. □

Lemma 3.8. *It holds*

$$(U(S \cup T) : K^\times \cap E) = p^{s+t}$$

Proof. The unit theorem implies that

$$(U(S \cup T) : U(S \cup T)^p) = p^{s+t}$$

and it is immediate to see that

$$U(S \cup T)^p \subset K^\times \cap E$$

so we only need to prove the opposite inclusion. Let $b \in K^\times \cap E$, $L := K[b^{\frac{1}{p}}]$ and

$$D := \prod_{v \in S} K_v^\times \times \prod_{v \in T} U_v^p \times \prod_{v \notin S \cup T} U_v$$

To conclude we need to show that $L = K$ and we split the proof into three steps.
First step: $D \subset Nm(\mathbb{I}_L)$. In order to prove the claim we take $(a_v)_v \in D$ and we prove that any component is a norm from $K_v[b^{\frac{1}{p}}]$.

- $v \in S$: it is obvious since $K_v[b^{\frac{1}{p}}] = K_v$;
- $v \in T$: it follows from the equality

  $$(K_v^\times : NmK_v[b^{\frac{1}{p}}]) = [K_v[b^{\frac{1}{p}}] : K_v]$$

  where the latter divides p;
- $v \notin S \cup T$: it follows from the fact that $K_v[b^{\frac{1}{p}}]/K_v$ is an unramified extension.

Second step: $D \cdot K^\times = \mathbb{I}_K$. We observe that

$$\mathbb{I}_{K,S}/D \cong \prod_{v \in T} U_v/U_v^p$$

and we consider the obvious map

$$U(S) \to \prod_{v \in T} U_v/U_v^p$$

Its kernel is $U(S) \cap L^{\times p}$ and thanks to Kummer theory the order of $U(S)/U(S) \cap L^{\times p}$ is p^t. Then, since $|p|_v = 1$ for $v \in T$, we have

$$(U(S) : U(S) \cap L^{\times p}) = \prod_{v \in T} (U_v : U_v^p)$$

and it implies that the considered map is surjective.
Consequently, $\mathbb{I}_{K,S} = D \cdot U(S)$ and finally

$$\mathbb{I}_K = \mathbb{I}_S \cdot K^\times = D \cdot U(S) \cdot K^\times = D \cdot K^\times$$

Third step: $L = K$. By contradiction, we assume $L \neq K$ and, since L/K is abelian and hence solvable, there exists a field K' such that $K \subset K' \subset L$ and K'/K is cyclic and non-trivial. Now

$$D \subset Nm(\mathbb{I}_L) \subset Nm(\mathbb{I}_{K'})$$

and so

$$\mathbb{I}_K = D \cdot K^\times = Nm(\mathbb{I}_{K'}) \cdot K^\times$$

Then the first inequality implies $K' = K$, a contradiction. □

Finally, we know that $(\mathbb{I}_K : K^\times \cdot Nm(\mathbb{I}_L))$ divides $(\mathbb{I}_K : K^\times \cdot E)$ and

$$(\mathbb{I}_K : K^\times \cdot E) = (K^\times \mathbb{I}_{K,S\cup T} : K^\times E) = \frac{(\mathbb{I}_{K,S\cup T} : E)}{(U(S \cup T) : K^\times \cap E)}$$
$$= \frac{p^{2s}}{p^{s+t}} = p^r = [L : K]$$

It concludes the proof of the second inequality.

3.3.4 End of the proof

Lemma 3.9. *If L/K is a finite abelian extension of number fields, $\phi_{L/K}(a) = 1$ for any $a \in K^\times$.*

Proof. We are going to prove the lemma only in the case of subfields of cyclotomic extensions. Then it can be proved in general thanks to [8, Lemma 8.5, pag. 222] and [8, Lemma 8.6, pag. 223]. First, we assume $L = \mathbb{Q}[\zeta_m]$ and $K = \mathbb{Q}$, where m is a positive integer and ζ_m is a primitive m-th root of 1. We can assume $m = l^r$ with l a prime positive integer.
Given $a \in \mathbb{R}^\times$ we have $\phi_\infty(a) = [sgn(a)]$.
Given $a = up^s \in \mathbb{Q}_p^\times$ we have $\phi_l(a) = [u^{-1}]$ if $p = l$ and $\phi_p(a) = [p^s]$ if $p \neq l$.
We observe that

$$\phi_\infty(-1) = [-1], \phi_l(-1) = [-1], \phi_p(-1) = [1]$$

$$\phi_l(l) = [1], \phi_p(l) = [1]$$

$$\phi_q(q) = [q], \phi_l(q) = [q^{-1}], \phi_p(q) = [1]$$

and thanks to these equalities we find that

$$\prod \phi_v(a) = 1$$

for any $a \in \mathbb{Q}^\times$. Then, the statement holds for any cyclotomic extension L/K where $L = K[\zeta_m]$ thanks to the commutativity of the diagram

$$\begin{array}{ccc} \mathbb{I}_K & \xrightarrow{\phi_{L/K}} & Gal(L/K) \\ \downarrow{\scriptstyle Nm_{K/\mathbb{Q}}} & & \downarrow \\ \mathbb{I}_\mathbb{Q} & \xrightarrow{\phi_{\mathbb{Q}[\zeta_m]/\mathbb{Q}}} & Gal(\mathbb{Q}[\zeta_m]/\mathbb{Q}) \end{array}$$

where the right vertical arrow is the restriction map. Now, if L/K is abelian and it is contained in a cyclotomic extension M of K, the statement follows from the fact that

$$\phi_{L/K} = res \circ \phi_{M/K}$$

where $res : Gal(M/K) \to Gal(L/K)$ is just the restriction homomorphism. □

Finally, we can conclude the proof. The first lemma of this subsection tells us that $K^\times \subset Ker(\phi_{L/K})$ and it is immediate to see that also $Nm(\mathbb{I}_L) \subset Ker(\phi_{L/K})$. Then $\phi_{L/K}$ is surjective and it induces a surjective homomorphism

$$\phi_{L/K} : \mathbb{I}_K/K^\times \cdot Nm(\mathbb{I}_L) \to Gal(L/K)$$

Thanks to the second inequality it is an isomorphism.

3.4 Proof of the existence theorem

In this section we prove the existence theorem.

Theorem 3.6. *Let K be a number field. If N is an open subgroup of finite index of C_K, then there exists a unique finite abelian extension L/K such that $Nm(C_L) = N$.*

First, we need to prove the following lemmas.

Lemma 3.10. *Let K be a number field. If $U \leq V$ is a norm group in C_K then so is V.*

Proof. If $U = Nm(C_L)$ for a suitable finite abelian extension L/K, the Reciprocity law gives the isomorphism

$$C_K/U \cong Gal(L/K)$$

The image of V/U is a subgroup of $Gal(L/K)$ and if M is its fixed field we get

$$C_K/V \cong Gal(M/K)$$

and it implies $V = Nm(C_M)$. □

Lemma 3.11. *If p is a prime positive integer and K is a number field which contains a primitive p-th root of 1, any open subgroup V of C_K such that C_K/V is finite and killed by p is a norm group.*

Proof. Let S a finite set of primes of K which contains

- all the infinite primes;
- all the primes dividing p;
- a set of generators for $Cl(K)$.

We fix also $L := K[U(S)^{\frac{1}{p}}]$ and

$$E := \prod_{v \in S} K_v^{\times p} \times \prod_{v \notin S} U_v$$

We claim that $K^\times \cdot E = K^\times \cdot Nm(\mathbb{I}_L)$. Obviously, $(\mathbb{I}_K : K^\times \cdot Nm(\mathbb{I}_L)) = p^{|S|}$ and

$$(\mathbb{I}_K : K^\times \cdot E) = (\mathbb{I}_{K,S} \cdot K^\times : E \cdot K^\times) = \frac{(\mathbb{I}_{K,S} : E)}{(\mathbb{I}_{K,S} \cap K^\times : E \cap K^\times)}$$
$$= \frac{\prod_{v \in S} (K_v^\times : K_v^{\times p})}{(U(S) : U(S)^p)} = \frac{p^{2|S|}}{p^{|S|}} = p^{|S|}$$

where the third equality follows from [8, Proposition 9.2, pag. 224]. Furthermore, $E \subset Nm(\mathbb{I}_L)$ because

- if $v \in S$, the isomorphism
$$K_v^\times / Nm(L_w^\times) \cong Gal(L_w/K_v)$$
implies $K_v^{\times p} \subset Nm(L_w^\times)$;
- if $v \notin S$, L_w is unramified over K_v and the norm map $U_w \to U_v$ is surjective.

Then the claim is true and we denote by U the inverse image of V in $\mathbb{I}_K$. Now, $\mathbb{I}_K^p \subset U$ and, since U is open, $\prod_{v \in S} 1 \times \prod_{v \notin S} U_v \subset U$ for a suitable finite set S of primes of K. Then $E \cdot K^\times \subset U$ and we can conclude because $E \cdot K^\times / K^\times$ is a norm group. □

Lemma 3.12. *If L/K is a finite cyclic extension of number fields, U is an open subgroup of finite index of C_K and $Nm_{L/K}^{-1}(U)$ is a norm group, then U is a norm group.*

Proof. We set $U' := Nm_{L/K}^{-1}(U)$ and, since it is a norm group, we fix M a suitable finite extension of L such that $U' = Nm_{M/L}(C_M)$. We claim that M/K is an abelian extension. Obviously M/K is Galois because U' is invariant. Since

$$Gal(L/K) \cong Gal(M/K)/Gal(M/L)$$

and $Gal(L/K)$ is cyclic, we just need to prove that $Gal(M/L)$ lies in the center of $Gal(M/K)$. We consider the Artin map

$$\phi_{M/L} : C_L \to Gal(M/L)$$

and, since it is surjective, we only have to show that

$$\phi_{M/L}(x) = \sigma\phi_{M/L}(x)\sigma^{-1} = \phi_{M/L}(\sigma x)$$

for any $x \in C_L$ and $\sigma \in Gal(M/K)$. It follows immediately from the facts that $Ker(\phi_{M/L}) = U'$ and $Nm_{L/K}(\sigma x/x) = 1$ and so M/K is abelian. Finally, $Nm_{M/K}(C_M) \subset U$ and so U is a norm group. □

Finally, we can conclude the proof of the existence theorem. We fix U an open subgroup of C_K of finite index and we prove by induction on its index that it is a norm group. The case $n = 1$ is obvious. For the inductive step, let p be a prime which divides $(C_K : U)$ and, thanks to the previous lemma, assume K contains a primitive p-th root of 1. There exists a subgroup V of C_K such that $U \subset V$ and $(C_K : V) = p$ and we know that it must be a norm group, i.e. $V = Nm(C_L)$ for a suitable finite abelian extension L/K. If $U' := Nm_{L/K}^{-1}(U)$, the norm map induces an isomorphism $C_L/U' \cong V/U$ which implies that U' is a norm group by induction. Finally, the previous lemma again implies that U is a norm group.

3.5 Global class field theory in terms of ideals

In this section we give a formulation of global class field theory in terms of ideals without proving the results. It will be useful for applications in the chapter about Complex Multiplication.

Definition 3.8. *Let K be a number field and S a finite set of primes of K. We denote by $I_{K,S}$ the free abelian group generated by the prime ideals that are not contained in S.*

Definition 3.9. *Let K be a number field. A* ***modulus*** *for K is a function*

$$\mathfrak{m} : \{primes\ of\ K\} \to \mathbb{Z}_{\geq 0}$$

which takes value 0 at complex primes, 0 or 1 at real primes and non-negative values at finite primes. We denote

$$\mathfrak{m} = \prod_{\mathfrak{p}\ prime\ of\ K} \mathfrak{p}^{\mathfrak{m}(\mathfrak{p})}$$

Given a modulus $\mathfrak{m}$ we denote as $S(\mathfrak{m})$ the set of primes which have a positive value under $\mathfrak{m}$.
Now, if K is a number field and $\mathfrak{m}$ is a modulus, we define

$$K_{\mathfrak{m},1} := \left\{ \begin{array}{lll} a \in K^\times : & ord_{\mathfrak{p}}(a-1) \geq \mathfrak{m}(\mathfrak{p}) & for\ all\ finite\ \mathfrak{p}\ dividing\ \mathfrak{m} \\ & a_{\mathfrak{p}} > 0 & for\ all\ real\ \mathfrak{p}\ dividing\ \mathfrak{m} \end{array} \right\}$$

It is easy to see that $K_{\mathfrak{m},1}$ injects into $I_{K,S(\mathfrak{m})}$ and it leads to the following definitions.

Definition 3.10. *Let K be a number field and $\mathfrak{m}$ a modulus for K.*
*A subgroup of $I_{K,S(\mathfrak{m})}$ which contains $K_{\mathfrak{m},1}$ is called a **congruence subgroup** modulo $\mathfrak{m}$.*
*The **ray class group** modulo $\mathfrak{m}$ is the quotient $Cl_K^{\mathfrak{m}} := I_{K,S(\mathfrak{m})}/K_{\mathfrak{m},1}$.*
*A finite abelian extension L/K which is unramified at all primes not in the support of $\mathfrak{m}$ and such that $Nm(I_{L,S(\mathfrak{m})_L}) \subset K_{\mathfrak{m},1}$ (where $S(\mathfrak{m})_L$ is the set of primes of L which lie over primes in $S(\mathfrak{m})$) is called a **ray class field** modulo $\mathfrak{m}$ and it is denoted as $K(\mathfrak{m})$.*

It is possible to prove the following.

Proposition 3.4. *Let K be a number field and $\mathfrak{m}$ a modulus for K. If a ray class field $K(\mathfrak{m})$ for K modulo $\mathfrak{m}$ exists, then it is unique.*

Now, we want to define the global Artin map for a finite abelian extension L/K. First of all, we recall that for any prime ideal $\mathfrak{B}$ of L we can define its decomposition group as

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

Furthermore, if $\mathfrak{B}$ lies over a prime ideal $\mathfrak{p}$ of K and it is unramified over it we have that

$$D(\mathfrak{B}) \cong Gal(L_{\mathfrak{B}}/K_{\mathfrak{p}}) \cong Gal(l/k)$$

where l and k are the residue fields of the completions, the first isomorphism is defined by extending the automorphisms and the second one by considering the action of the automorphisms on $\mathcal{O}_L$. We know that l and k are finte, hence $Gal(l/k)$ is a cyclic group generated by $x \mapsto x^{|k|}$. We denote its inverse image under the previous chain of isomorphisms as $(\mathfrak{p}, L/K)$. Finally, we can define the global Artin map.

Definition 3.11. *Let L/K be a finite abelian extension of number fields and S a finite set of primes of K that contains all those which ramify in L. We define the **global Artin map** of L/K with respect to S as*

$$\psi_{L/K,S} : I_{K,S} \to Gal(L/K), \prod \mathfrak{p}_i^{n_i} \mapsto \prod (\mathfrak{p}_i, L/K)^{n_i}$$

Now, we give the crucial notion of conductor for abelian extensions of local and global fields.

Definition 3.12. *If L/K is a finite abelian extension of local fields we define its* ***conductor*** $\mathfrak{c}(L/K)$ *as:*

- $\mathfrak{c}(L/K) = 0$ *if L and K are archimedean and equal;*
- $\mathfrak{c}(L/K) = 1$ *if $L = \mathbb{C}$ and $K = \mathbb{R}$;*
- $\mathfrak{c}(L/K) = min\{n \in \mathbb{N} : 1 + \mathfrak{m}_K^n \subset Nm(L^\times)\}$ *if L and K are nonarchimedean.*

If L/K is a finite abelian extension of number fields we define its conductor $\mathfrak{c}(L/K)$ as the modulus

$$\mathfrak{c}(L/K) : \{primes\, of\, K\} \to \mathbb{Z}_{\geq 0}, v \mapsto \mathfrak{c}(L_w/K_v)$$

It is well-defined because L/K is Galois and so the local conductors are independent of the choice of w.

It is possible to prove the following.

Proposition 3.5. *Prime ideals in the support of the conductor of a finite abelian extension of number fields L/K are exactly the prime ideals of K which ramify in L.*

Finally, we can state the main theorems of global class field theory in terms of ideals.

Theorem 3.7. *Let K be a number field and $\mathfrak{m}$ a modulus for K. If H is a congruence subgroup modulo $\mathfrak{m}$, then there exists a finite abelian extension L/K such that $H = K_{\mathfrak{m},1} \cdot Nm(I_{L,S(\mathfrak{m})})$. In particular, a ray class field $K(\mathfrak{m})$ for K modulo $\mathfrak{m}$ exists.*

Theorem 3.8. *Let K be a number field, $\mathfrak{m}$ a modulus for K and L/K a finite abelian extension. Then $\mathfrak{c}(L/K)$ divides $\mathfrak{m}$ if and only if L lies in $K(\mathfrak{m})$.*

Theorem 3.9. *Let K be a number field, $\mathfrak{m}$ a modulus for K and L/K a finite abelian extension contained in $K(\mathfrak{m})$. Then the global Artin map of L/K induces an isomorphism*

$$I_{K,S(\mathfrak{m})}/(K_{\mathfrak{m},1} \cdot Nm(I_{L,S(\mathfrak{m})_L})) \cong Gal(L/K)$$

where $S(\mathfrak{m})_L$ is the set of primes of L which lie over primes in $S(\mathfrak{m})$.

From the theorems we can deduce that we have an isomorphism

$$Cl_K^{\mathfrak{m}} \cong Gal(K(\mathfrak{m})/K)$$

and we can also derive the following corollary.

Corollary 3.2. *Let K be a number field, $\mathfrak{m}$ a modulus for K and set*

$$Nm(Cl_{L,\mathfrak{m}}) := K_{\mathfrak{m},1} \cdot Nm(I_{L,S(\mathfrak{m})_L}) \, mod \, K_{\mathfrak{m},1}$$

for any abelian extension L/K contained in $K(\mathfrak{m})$.
There is a one-to-one correspondence between the set of finite abelian extensions of K contained in $K(\mathfrak{m})$ and the set of subgroups of $Cl_K^{\mathfrak{m}}$ given by the map

$$L \mapsto Nm(Cl_{L,\mathfrak{m}})$$

It also has the following properties:

- $L_1 \subset L_2 \Leftrightarrow Nm(Cl_{L_2,\mathfrak{m}}) \subset Nm(Cl_{L_1,\mathfrak{m}})$;
- $Nm(Cl_{L_1 \cdot L_2,\mathfrak{m}}) = Nm(Cl_{L_1,\mathfrak{m}}) \cap Nm(Cl_{L_2,\mathfrak{m}})$;
- $Nm(Cl_{L_1 \cap L_2,\mathfrak{m}}) = Nm(Cl_{L_1,\mathfrak{m}}) \cdot Nm(Cl_{L_2,\mathfrak{m}})$.

Now, we can introduce the important definition of Hilbert class field.

Definition 3.13. *Let K be a number field. The **Hilbert class field** of K is the maximal abelian unramified extension of K. We denote it as H_K.*

It is immediate to see that the Hilbert class field is the ray class field of K with respect to the trivial module. It implies that we have an isomorphism

$$Cl_K \cong Gal(H_K/K)$$

and, in particular, $[H_K : K] = h_K$ where h_K is the class number of K.

3.6 The principal ideal theorem

In this section we want to prove an important result in class field theory: the principal ideal theorem. The statement is the following.

Theorem 3.10. *Let K be a number field and H_K its Hilbert class field. Then every ideal of $\mathcal{O}_K$ becomes principal in $\mathcal{O}_{H_K}$.*

First of all, we recall some notions from group theory. Given a group G, we denote by G' its commutator subgroup and by $G^{ab} := G/G'$ its abelianization.

Definition 3.14. *We fix a group G, a subgroup $H \leq G$ of finite index and a right transversal T for H in G. We define the **transfer map** as*

$$V_{G,H} : G^{ab} \to H^{ab}, g \, mod \, G' \mapsto \prod_{t \in T} tg(t \circ g)^{-1} \, mod \, H'$$

where $t \circ g$ is the only element of T such that $Htg = H(t \circ g)$.

Proposition 3.6. *If G is a group and $H \leq G$ is a subgroup of finite index, then $V_{G,H}$ is a well-defined group homomorphism and it is independent of the choice of a right transversal for H in G.*

Proof. Let T and S be two different right transversals for H in G. For any $t \in T$ there exists a unique $s \in S$ such that $Ht = Hs$, i.e. for any $t \in T$ there exists a unqiue $h_t \in H$ such that $h_t t \in S$. We also observe that $Hh_t tg = H(t \circ g)$, i.e. $(h_t t) \circ g = h_{t \circ g}(t \circ g)$. Then $V_{G,H}$ is independent of the choice of the right transversal because

$$\begin{aligned}\prod_{s\in S} sg(s\circ g)^{-1}\, mod\, H' &= \prod_{t\in T} h_t tg(h_{t\circ g}(t\circ g))^{-1}\, mod\, H'\\ &= \prod_{t\in T} h_t tg(t\circ g)^{-1}h_{t\circ g}^{-1}\, mod\, H'\\ &= \prod_{t\in T} tg(t\circ g)^{-1}\prod_{t\in T} h_t \prod_{t\in T} h_{t\circ g}^{-1}\, mod\, H'\\ &= \prod_{t\in T} tg(t\circ g)^{-1}\, mod\, H'\end{aligned}$$

Finally, $V_{G,H}$ is a group homomorphism:

$$\begin{aligned}V_{G,H}(xy) &= \prod_{t\in T} t(xy)(t\circ xy)^{-1}\, mod\, H'\\ &= \prod_{t\in T} tx(t\circ x)^{-1}\prod_{t\in T}(t\circ x)y((t\circ x)\circ y)^{-1}\, mod\, H'\\ &= \prod_{t\in T} tx(t\circ x)^{-1}\prod_{s\in T} sy(s\circ y)^{-1}\, mod\, H' = V_{G,H}(x)V_{G,H}(y)\end{aligned}$$

□

Proposition 3.7. *The transfer map $V_{G,G'} : G^{ab} \to (G')^{ab}$ is the zero homomorphism for any finitely generated group G such that $(G : G') < \infty$.*

Proof. We consider a more general setting: we fix $H \leq G$ a subgroup of finite index and we prove that the diagram

$$\begin{array}{ccc} G^{ab} & \xrightarrow{V_{G,H}} & H^{ab} \\ \downarrow{\scriptstyle \delta} & & \downarrow{\scriptstyle \delta} \\ I_G/I_G^2 & \xrightarrow{S} & (I_H + I_H I_G)/I_H I_G \end{array}$$

is commutative, where I_G (and, similarly, I_H) is the kernel of the augmentation map

$$\mathbb{Z}[G] \to \mathbb{Z}, \sum_{\sigma\in G} n_\sigma \sigma \mapsto \sum_{\sigma\in G} n_\sigma$$

the vertical isomorphisms are the maps

$$\delta(\sigma) = \sigma - 1$$

and, if T is a set of representatives of the right cosets of G/H containing 1, we define

$$S(x) = (\sum_{t \in T} t)x$$

First, we prove that the maps δ are isomorphisms. We observe that the set

$$\{(\delta\sigma)t : \sigma \in H, t \in T, t \neq 1\}$$

is a $\mathbb{Z}$-basis of $I_H + I_H I_G$ since it generates it and

$$0 = \sum_{\sigma,t} n_{\sigma,t}(\delta\sigma)t = \sum_{\sigma,t} n_{\sigma,t}\sigma t - \sum_{\sigma,t} n_{\sigma,t}t$$

implies that all the $n_{\sigma,t} = 0$. If we consider the map

$$I_H + I_H I_G \to H, (\delta\sigma)t \mapsto \sigma$$

it is immediate to see that it is surjective and a left inverse for δ. In the settings of the diagram it is also injective because the equality

$$\delta\sigma\delta(\sigma' t) = \delta(\sigma\sigma')t - \delta\sigma - (\delta\sigma')t$$

implies that $\delta\sigma\delta(\sigma' t)$ is sent to $\sigma\sigma'\sigma^{-1}\sigma'^{-1}$ which lies in the commutator subgroup.
Now, the diagram commutes if and only if

$$S(\delta\sigma \; mod \; I_G^2) = \sum_{t \in T} \delta\sigma_t \; mod \; I_H I_G$$

where $\sigma_t \in H$, $t\sigma = \sigma_t t'$ with $t' \in T$. Then the equality

$$\delta t + t\delta\sigma = \delta t' + \delta\sigma_t + \delta\sigma_t\delta t'$$

implies

$$S(\delta\sigma \; mod \; I_G^2) \equiv \sum_{t \in T} \delta\sigma_t \equiv \sum_{t \in T} t\delta\sigma \equiv (\sum_{t \in T} t)\delta\sigma \mod I_H I_G$$

and the claim is proved. Finally, to conclude the proof we need to prove that if $H = G'$ then S is the zero map. It is shown in [10, Theorem 7.6, pag. 412]. □

Proposition 3.8. *If $K \subset L \subset M$ is a tower of finite abelian unramified extensions of number fields such that $Gal(M/K)' = Gal(M/L)$, S_K is a finite set of primes of K and S_L is the set of primes of L that lie over them, then the following diagram is commutative:*

$$\begin{array}{ccc} I_{K,S_K} & \xrightarrow{\psi_{L/K}} & Gal(M/K)^{ab} \\ \downarrow & & \downarrow V \\ I_{L,S_L} & \xrightarrow{\psi_{M/L}} & Gal(M/L)^{ab} \end{array}$$

where the first vertical arrow is just extension of ideals and $V := V_{Gal(L/K),Gal(L/M)}$.

Proof. Let $\mathfrak{p}$ be a prime ideal in I_{K,S_K} and let $\mathfrak{q}_1, ..., \mathfrak{q}_r$ be the prime ideals of L which lie over $\mathfrak{p}$. We write

$$Gal(M/K) = \bigcup_{i,j} Gal(M/L)\tau_i g^j$$

where $g = (\mathfrak{r}, M/K)$ for a prime ideal $\mathfrak{r}$ of M which lies over $\mathfrak{p}$ and varying j from 0 to $m-1$ where m is the order of $(\mathfrak{p}, L/K)$. Then, if $\mathfrak{q}_i = L \cap \tau_i(\mathfrak{r})$, we have

$$(\mathfrak{q}_i, M/L) = (\tau_i(\mathfrak{r}), M/L) = \tau_i g^m \tau_i^{-1} = \prod_{j=0}^{m-1} \tau_i g^j g (\tau_i g^j \circ g)^{-1}$$

Finally,

$$V((\mathfrak{p}, L/K)) = \prod_i (\mathfrak{q}_i, M/L)$$

□

Finally, we consider a number field K and we call H_K its Hilbert class field and H_{H_K} the Hilbert class field of H_K. The extension H_{H_K}/K is unramified and Galois and, since H_K is the largest subextension of H_{H_K} that is abelian over K, we also have

$$Gal(H_{H_K}/K)' = Gal(H_{H_K}/H_K)$$

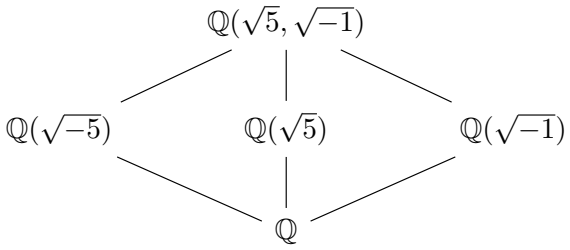
Then we get the following commutative diagram:

$$\begin{array}{ccc} Cl(K) & \xrightarrow{\psi_{H_K/K}} & Gal(H_K/K) \\ \downarrow & & \downarrow V \\ Cl(H_K) & \xrightarrow{\psi_{H_{H_K}/H_K}} & Gal(H_{H_K}/H_K) \end{array}$$

Horizontal arrows are isomorphisms and the map V is the zero map thanks to one of the previous propositions. Then also the left vertical map is the zero map and the proof of the theorem is concluded.

3.7 An example: the Hilbert class field of $\mathbb{Q}(\sqrt{-5})$

As an example of the developed theory we want to compute the Hilbert class field of the imaginary quadratic field $K := \mathbb{Q}(\sqrt{-5})$ and, in particular, we want to prove that it is $L := \mathbb{Q}(\sqrt{5}, \sqrt{-1})$. The situation is described in the following picture:



where all the extensions are Galois of degree 2. It is well-known that

$$h_K = 2 = [\mathbb{Q}(\sqrt{5}, \sqrt{-1}) : \mathbb{Q}(\sqrt{-5})]$$

and obviously any Galois extension of degree 2 is abelian, so we just need to prove that L/K is unramified. We know that the only rational primes which ramify in $\mathbb{Q}(\sqrt{-5})$ are 2 and 5, while 5 is the only rational prime which ramify in $\mathbb{Q}(\sqrt{5})$ and 2 is the only one which ramify in $\mathbb{Q}(\sqrt{-1})$. Now, we fix a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ and p a prime positive integer such that $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$ and we distinguish three cases to prove that $\mathfrak{p}$ is unramified in $\mathbb{Q}(\sqrt{5}, \sqrt{-1})$:

- $p = 2$: in this case, $\mathfrak{p} = (2, 1 + \sqrt{-5})$ and $p\mathcal{O}_K = \mathfrak{p}^2$. If

  $$p\mathcal{O}_L := (\prod_{i=1}^{g} \mathfrak{q}_i)^e$$

  where the $\mathfrak{q}_i$ are the primes of L which lie over $2\mathbb{Z}$ and their inertia degrees over it are f, we have $gef = 4$. Since $2\mathbb{Z}$ is ramified in K and it is unramified in $\mathbb{Q}(\sqrt{5})$, the only possibilities are

  $$g = 2, e = 2, f = 1$$

  or

  $$g = 1, e = 2, f = 2$$

  In both these two cases $\mathfrak{p}$ is unramified in L;

- $p = 5$: we just proceed with an argument similar to that of the previous case;

- $p \neq 2, 5$: in this case $p\mathbb{Z}$ is unramified in $\mathbb{Q}(\sqrt{-5})$ and in $\mathbb{Q}(\sqrt{-1})$. Then the subfield of $L/\mathbb{Q}$ fixed by the inertia sugroup of its Galois group relative to any prime ideal of L which lies over p contains them and, then, it is just L, so $p\mathbb{Z}$ is unramified in L and the same holds for $\mathfrak{p}$.

Chapter 4

Elliptic curves

Theory of elliptic curves is one of the most important branches of the modern mathematics. The theory is mainly developed in the field of algebraic geometry but it is strictly related and has a lot of consequences in number theory, complex analysis and many more research areas. The most famous example of application of the theory of elliptic curves is the proof of Fermat's Last Theorem, which states that if x, y, z, n are positive integers such that $x^n + y^n = z^n, xyz \neq 0$, then $n = 1, 2$. In this chapter we will see the main definitions and results related to elliptic curves in order to define elliptic curves with complex multiplication and to use them to study class field theory for imaginary quadratic fields. In order to simplify the exposition we will assume our curves to be defined over a field K with $char(K) \neq 2, 3$ and we will work only with plane projective curves defined by a Weierstrass equation.

4.1 Weierstrass equations

Definition 4.1. *Let K be a field. An **elliptic curve** E over K is a smooth plane projective curve in $\mathbb{P}^2(K)$ defined by a **Weierstrass equation**:*

$$y^2z = x^3 + axz^2 + bz^3, a, b \in K$$

We observe that, taking $\{z = 0\}$ as the hyperplane at infinity, the affine part of an elliptic curve is described by the equation $y^2 = x^3 + ax + b$ and the unique point at infinity is $(0, 1, 0)$. Furthermore, since elliptic curves are smooth by definition, the Weierstrass equation must satisfy the condition $4a^3 + 27b^2 \neq 0$.

Definition 4.2. *If E/K is an elliptic curve defined by a Weierstrass equation $y^2 = x^3 + ax + b$, we define*

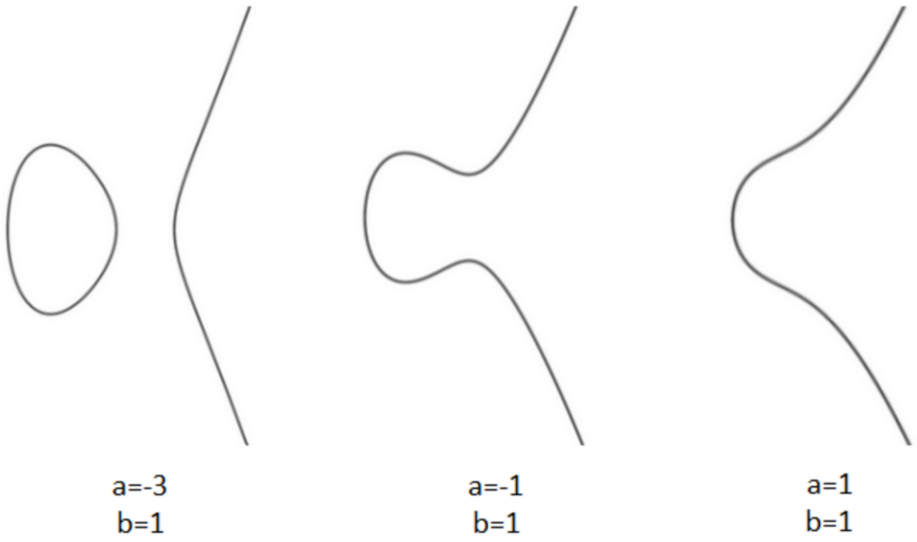
$$\Delta(E) := -16(4a^3 + 27b^2)$$

$$j(E) := -1728\frac{(4a)^3}{\Delta(E)}$$

The numbers $\Delta(E)$ and $j(E)$ are called respectively the **discriminant** and the **j-invariant** of E. Note that $j(E)$ is well-defined because $\Delta(E) \neq 0$. In order to have an idea of how elliptic curves look like over $\mathbb{R}$, we plot

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

varying the parameters:



Lemma 4.1. *Two elliptic curves*

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

and

$$y^2 = x^3 + a'x + b'$$

defined over a field K are isomorphic over K^{al} (an algebraic closure of K) if and only if there exists $\lambda \in (K^{al})^\times$ such that $a = \lambda^4 a'$ and $b = \lambda^6 b'$.

Proof. See [14, Lecture 13, Theorem 13.13, pag. 5]. □

The name and the importance of the j-invariant come from the following result.

Proposition 4.1. *Two elliptic curves E_1/K and E_2/K defined over a field K are isomorphic over K^{al} if and only if $j(E_1) = j(E_2)$.*

Proof. First, we prove that if $j(E_1) = j(E_2)$ then E_1 and E_2 are isomorphic. Assume that E_1 and E_2 are defined respectively by the equations $y^2 = x^3 + ax + b$ and $y^2 = x^3 + a'x + b'$. The equality $j(E_1) = j(E_2)$ implies that $a^3b'^2 = a'^3b^2$. The isomorphism $\phi : E_2 \to E_1$ wanted will be of the form $\phi(x', y') = (u^2x', u^3y')$ for a suitable $u \in K^{al}$. We distinguish the following cases:

- $a = 0 \Rightarrow b \neq 0 \Rightarrow a' = 0$, we take $u = (\frac{b}{b'})^{\frac{1}{6}}$;
- $b = 0 \Rightarrow a \neq 0 \Rightarrow b' = 0$, we take $u = (\frac{a}{a'})^{\frac{1}{4}}$;
- $ab \neq 0 \Rightarrow a'b' \neq 0$, we take $u = (\frac{a}{a'})^{\frac{1}{4}} = (\frac{b}{b'})^{\frac{1}{6}}$;

Conversely, we assume that E_1 and E_2 are isomorphic over K^{al}. From the previous lemma we know that there exists $\lambda \in (K^{al})^\times$ such that $a = \lambda^4 a'$ and $b = \lambda^6 b'$. Then:

$$j(E_1) = 1728\frac{(4a)^3}{16(4a^3 + 27b^2)} = 1728\frac{\lambda^{12}(4a')^3}{16\lambda^{12}(4a'^3 + 27b'^2)} = j(E_2)$$

□

4.2 The group law of an elliptic curve

The goal of this section is to define a group law on the points of an elliptic curve. In order to do so, we firstly recall the statement of the Bézout intersection theorem.

Theorem 4.1. *Given two plane projective curves over an algebraically closed field, the number of points of intersection counted with multiplicity is equal to the product of the degrees of the two curves.*

Proof. See [3, Corollary 4.6, pag. 31]. □

In particular, we are interested in the number of points of intersection between an elliptic curve and a line and the theorem tells us that they are three if counted with multiplicity. Now, let E/K be an elliptic curve over an algebraically closed field K and P and Q two points of E. We also set O to be the unique point of E in the hyperplane at infinity. We define $P * Q$ to be the third point of intersection of E with the line joining P and Q. Notice that if $P = Q$ the line joining them is just the tangent line at P. Then, we define

$$P + Q := (P * Q) * O$$

The most difficult part in proving that it defines a group law is to show that the operation is associative. We will prove it in a particular case and then we will give all the instruments to prove it in general. First we recall the Cayley-Bacharach Theorem.

Theorem 4.2. *Let K be an algebraically closed field and $P_1, ..., P_8$ distinct points in $\mathbb{P}^2(K)$ which belong to a non-singular cubic curve. Then there exists a unique point P_9 such that every cubic curve which contains $P_1, ..., P_8$ must contain also P_9.*

Proof. See [3, Exercise 4.13, pag. 32]. □

Lemma 4.2. *Addition of points of an elliptic curve is associative, i.e.*

$$(P + Q) + R = P + (Q + R)$$

for any $P, Q, R \in E$.

Proof. We take P, Q, R points of E and we set $P' := P * Q$ and $R' := Q * R$. We prove the lemma only in the case the set

$$S := \{P', Q, O, R', P' * O, Q * R', P' * Q, O * R'\}$$

contains eight distinct points. We define the following projective lines:

$$r := P' \vee Q, s := O \vee R', t := (P' * O) \vee (Q * R')$$

$$r' := P' \vee O, s' := Q \vee R', t' := (P' * Q) \vee (O * R')$$

Now, the points of S are eight distinct points of E and using the previous theorem we find that the ninth point is

$$(P' * O) * (Q * R') = (P' * Q) * (O * R')$$

This equality implies that

$$(O * (P * Q)) * R = P * (O * (Q * R))$$

which is just

$$(P + Q) * R = P * (Q + R)$$

and associativity follows. □

Proposition 4.2. *The set $(E, +)$ of points of an elliptic curve with addition is an abelian group with identity O.*

Proof. From the previous Lemma we already know that the addition is associative.
Addition is commmutative:

$$P + Q = (P * Q) * O = (Q * P) * O = Q + P$$

O is an identity for $(E, +)$:

$$P + O = (P * O) * O = P$$

Finally, if we define $-P := P * O$, we find that

$$P + (-P) = P + (P * O) = (P * (P * O)) * O = O * O = O$$

because the tangent line to E at O has multiplicity three in O. So any element has an opposite and hence $(E, +)$ is an abelian group. □

In order to help computations and to simplify some proofs in the next sections, we give explicit algebraic formulas for the additive group law.

Proposition 4.3. *Let E be an elliptic curve defined by an equation*

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

Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be points of E.
Then if $x_1 = x_2$ and $y_1 = -y_2$ we have $P_1 + P_2 = O$ (in particular, $-P_1 = (x_1, -y_1)$).
Otherwise we have $P_1 + P_2 = (m^2 - x_1 - x_2, 2mx_1 + mx_2 - m^3 - y_1)$, where m is calculated in the following way:

- *if $x_1 \neq x_2$, $m := \frac{y_2 - y_1}{x_2 - x_1}$;*
- *if $x_1 = x_2$ and $y_1 = y_2 \neq 0$, $m := \frac{3x_1^2 + a}{2y_1}$.*

Proof. See [11, Group Law Algorithm 2.3, pag. 53]. □

Notice that it is possible to prove the associativity of the group law by using these formulas and making computations in the various cases. The formulas also tell us that addition of points can be defined on elliptic curves over a generic field K.

4.3 Isogenies

In this section, we introduce the notion of isogenies and we study their main properties.

Definition 4.3. *Let E_1/K and E_2/K be two elliptic curves over a field K. An **isogeny** $\alpha : E_1 \to E_2$ is a projective morphism from E_1 to E_2 which sends the identity of E_1 to the identity of E_2.*

Obviously composition of isogenies is again an isogeny.
Given $\alpha, \beta : E_1 \to E_2$ isogenies, we define $(\alpha + \beta)(P) := \alpha(P) + \beta(P)$. We want to prove it is again an isogeny.

Proposition 4.4. *If $\alpha, \beta : E_1 \to E_2$ are isogenies, then $\alpha + \beta$ is an isogeny.*

Proof. Obviously, $(\alpha+\beta)(O) = \alpha(O)+\beta(O) = O+O = O$. In order to prove that it is a morphism we just need to prove that, for any elliptic curve E, the map

$$E \times E \to E,\ (P,Q) \mapsto P+Q$$

is a morphism. The formulas of the previous section tell us that it is everywhere a morphism except eventually for couple of points of the following kinds:

$$(P,P),\ (P,-P),\ (P,O),\ (O,P)$$

Then, if Q is any point of E, we define

$$\tau_Q : E \to E,\ \tau_Q(P) = P+Q$$

and we observe that it is a morphism. Given two points Q_1 and Q_2 of E, the map $\tau_{Q_2}^{-1} \circ \tau_{Q_1}^{-1} \circ + \circ (\tau_{Q_1} \times \tau_{Q_2})$ is again the addition map and it is everywhere a morphism except eventually for couple of points of the following kinds:

$$(P-Q_1, P-Q_2),\ (P-Q_1, -P-Q_2),\ (P-Q_1, -Q_2),\ (-Q_1, P-Q_2)$$

In this way we can find a finite number of maps that are the addition on $E \times E$ and such that for any point of E at least one of these maps is a morphism in it. Then the addition map is a morphism. □

Now, we state some important properties of isogenies.

Proposition 4.5. *Any non-zero isogeny is surjective.*

Proof. See [11, Theorem 2.3, pag. 20] □

Proposition 4.6. *Any isogeny is a group homomorphism.*

Proof. See [11, Theorem 4.8, pag. 71] □

Proposition 4.7. *Let E_0, E_1, E_2 and E_3 be elliptic curves and let*

$$\phi : E_0 \to E_1, \alpha, \beta : E_1 \to E_2, \psi : E_2 \to E_3$$

be non-zero isogenies. Then:

- $\alpha \circ \phi = \beta \circ \phi \Rightarrow \alpha = \beta$;
- $\psi \circ \alpha = \psi \circ \beta \Rightarrow \alpha = \beta$.

Proof. Since the involved isogenies are non-zero (and, hence, surjective) we have that

$$\alpha \circ \phi = \beta \circ \phi \Rightarrow (\alpha - \beta) \circ \phi = 0 \Rightarrow \alpha - \beta = 0 \Rightarrow \alpha = \beta$$

The second statement follows similarly. □

The most important example of isogeny is the multiplication by m map, with $m \in \mathbb{Z}$. In particular, given an elliptic curve E, we define

$$[m] : E \to E, [m](P) := mP$$

where mP is defined considering the group law on E.

Proposition 4.8. *If E/K is an elliptic curve and $m \in \mathbb{Z}$, $m \neq 0$, then $[m]$ is a non-zero isogeny.*

Proof. The statement is obvious for $m = 1$, since $[1]$ is just the identity map. Proceeding by induction we get that, if $m > 1$, $[m+1] = [m] + [1]$ is an isogeny because it is the sum of two isogenies. Furthermore, $[-1]$ is an isogeny because it is just the map $P \mapsto -P$, which is a morphism of varieties from the formulas in the previous section (and obviously $-O = O$). A similar induction argument will give us that $[m]$ is an isogeny for any $m < 0$. Now, we want to prove that $[m]$ is non-zero for any $m \neq 0$. It is obvious for $m = 1, -1$ and since $[mn] = [m] \circ [n]$ we just need to prove it for $m = 2$ and m odd. We consider $P_0 = (x_0, y_0)$ a generic point of E and we observe that $[2](P_0) = O$ if and only if $y_0 = -y_0$ if and only if $y_0 = 0$ if and only if $x_0^3 + ax_0 + b = 0$. So there are only finitely many points of E that are killed by $[2]$. It implies that $[2]$ is not constant and also that, if P is one of these points, $[m](P) = P$ if m is odd, and so these maps are not constant too. □

This result immediately implies that $[m] = [n]$ if and only if $m = n$ for any $m, n \in \mathbb{Z}$.
Now, we want to define the degree of an isogeny. In order to do so, we denote by $K(E)$ the function field of an elliptic curve over K and we observe that any non-zero isogeny $\alpha : E_1 \to E_2$ between elliptic curves over K induces a homomorphism of fields $\alpha^* : K(E_2) \to K(E_1)$ defined as $\alpha^*(\phi) = \phi \circ \alpha$. It is injective, so we can see $K(E_1)/K(E_2)$ as an extension of fields and it is possible to prove that it is finite (see [11, Theorem 2.4, pag. 20]). Then we have the following definition.

Definition 4.4. *Let E_1 and E_2 be elliptic curves defined over a field K and $\alpha : E_1 \to E_2$ an isogeny. The **degree** of α is denoted as $deg(\alpha)$ and it is just the degree of the field extension $K(E_1)/K(E_2)$ if α is non-zero. If α is constant we set $deg(\alpha) = 0$.*

It is an immediate consequence of this definition that the degree of the composition of two isogenies is the product of their degrees.
Finally, we can define the concept of dual isogeny which will be crucial in the study of endomorphism rings of elliptic curves.

Theorem 4.3. *For any isogeny $\alpha : E_1 \to E_2$ between two elliptic curves there exists a unique isogeny $\hat{\alpha} : E_2 \to E_1$ such that $\hat{\alpha} \circ \alpha = [deg(\alpha)]$.*
*The isogeny $\hat{\alpha}$ is called the **dual isogeny** of α.*

Proof. See [11, Theorem 6.1, pag. 81]. □

We observe that $\hat{0} = 0$. Furthermore, the dual isogeny has the following properties.

Proposition 4.9. *For any α and β isogenies between elliptic curves E_1 and E_2, γ isogeny between E_2 and E_3 and $m \in \mathbb{Z}$, the following properties hold:*

1. $[m] \circ \alpha = \alpha \circ [m]$;
2. $\alpha \circ \hat{\alpha} = [deg(\alpha)]$;
3. $\widehat{\alpha + \beta} = \hat{\alpha} + \hat{\beta}$;
4. $\widehat{\gamma \circ \alpha} = \hat{\alpha} \circ \hat{\gamma}$;
5. $\widehat{[m]} = [m]$;
6. $deg([m]) = m^2$;
7. $deg(\alpha) = deg(\hat{\alpha})$;
8. $\hat{\hat{\alpha}} = \alpha$.

Proof.

1. It follows trivially from the fact that α is a group homomorphism;
2. $\alpha \circ \hat{\alpha} \circ \alpha = \alpha \circ [deg(\alpha)] = [deg(\alpha)] \circ \alpha \Rightarrow \alpha \circ \hat{\alpha} = [deg(\alpha)]$;
3. See [11, Theorem 6.2, pag. 83];
4. $\hat{\alpha} \circ \hat{\gamma} \circ \gamma \circ \alpha = \hat{\alpha} \circ [deg(\gamma)] \circ \alpha = [deg(\gamma)] \circ [deg(\alpha)] = [deg(\gamma \circ \alpha)]$;
5. We proceed by induction. The statement is clear for $m = 0, 1$. If the statement is true for $m \geq 1$, then
$$\widehat{[m+1]} = \widehat{[m] + [1]} = \widehat{[m]} + \widehat{[1]} = [m] + [1] = [m+1]$$
A similar argument gives the proof for $m < 0$;
6. $[deg([m])] = \widehat{[m]} \circ [m] = [m] \circ [m] = [m^2] \Rightarrow deg([m]) = m^2$;
7. $$\begin{aligned}[deg(\alpha)] \circ [deg(\alpha)] = [deg(\alpha)^2] = [deg([deg(\alpha)])] = [deg(\alpha \circ \hat{\alpha})] \\ = [deg(\alpha) deg(\hat{\alpha})] = [deg(\alpha)] \circ [deg(\hat{\alpha})]\end{aligned}$$
$\Rightarrow deg(\alpha) = deg(\hat{\alpha})$;
8. $\alpha \circ \hat{\alpha} = [deg(\alpha)] = [deg(\hat{\alpha})]$.

□

4.4 Endomorphism rings and algebras

Definition 4.5. *Let K be a field and E_1/K, E_2/K two elliptic curves. The set $Hom(E_1, E_2)$ of isogenies from E_1 to E_2 is a group under addition.*
*If E/K is an elliptic curve, $End(E) := Hom(E, E)$ is the **endomorphism ring** of E (multiplication is given by composition of isogenies).*

We will consider $End(E)$ as a $\mathbb{Z}$-algebra. Recalling the results of the previous section we know that $charEnd(E) = 0$, since $\mathbb{Z}$ injects into it via the map $m \mapsto [m]$. The surjectivity of non-zero isogenies also tells us that $End(E)$ has no zero divisors. We observe that

$$\alpha\hat{\alpha} = [deg(\alpha)] \in \mathbb{Z}$$

and

$$\alpha + \hat{\alpha} = 1 - \alpha\hat{\alpha} - (1 - \alpha)(1 - \hat{\alpha}) \in \mathbb{Z}$$

so any enodomorphism α is a root of the polynomial

$$x^2 - (\alpha + \hat{\alpha})x + \alpha\hat{\alpha} \ \in \mathbb{Z}[x]$$

and then $End(E)$ is integral over $\mathbb{Z}$.
Furthermore, the map $\hat{\cdot} : End(E) \to End(E)$ is an involution of rings.

Definition 4.6. *Let E/K be an elliptic curve. The $\mathbb{Q}$-algebra*

$$End^0(E) := End(E) \otimes_{\mathbb{Z}} \mathbb{Q}$$

*is called the **endomorphism algebra** of E.*

From the properties of the tensor product we know that $End(E)$ and $\mathbb{Q}$ injects into $End^0(E)$ with intersection $\mathbb{Z}$. Since $\mathbb{Q}$ is the fraction field of $\mathbb{Z}$ all the elements of the endomorphism algebra can be written as pure tensors and so, with an abuse of notation, as $q\alpha$ with $q \in \mathbb{Q}$ and $\alpha \in End(E)$. We also have that $q\alpha = \alpha q$ for any $\alpha \in End^0(E)$ and $q \in \mathbb{Q}$. We can extend the map $\hat{\cdot}$ to $End^0(E)$ by setting $\widehat{q\alpha} := q\hat{\alpha}$. The map

$$\hat{\cdot} : End^0(E) \to End^0(E)$$

is called the **Rosati involution** of E. We also define the trace map

$$Tr(\alpha) := \alpha + \hat{\alpha}$$

and the norm map

$$Nm(\alpha) := \alpha\hat{\alpha}$$

Proposition 4.10. *The following properties hold:*

1. $\hat{\hat{\alpha}} = \alpha$, $\widehat{\alpha+\beta} = \hat{\alpha}+\hat{\beta}$, $\widehat{\alpha\beta} = \hat{\beta}\hat{\alpha}$, $\hat{q} = q$ *for any* $\alpha, \beta \in End^0(E)$, $q \in \mathbb{Q}$.

2. *The norm map is multiplicative and it takes values in* $\mathbb{Q}_{\geq 0}$. *It satisfies* $Nm(\alpha) = Nm(\hat{\alpha})$ *and* $Nm(\alpha) = 0$ *if and only if* $\alpha = 0$.

3. *The trace map is a* $\mathbb{Q}$*-linear map with values in* $\mathbb{Q}$ *and it satisfies* $Tr(\alpha) = Tr(\hat{\alpha})$. *Furthermore,* $Tr(\alpha) = 0 \Rightarrow \alpha^2 \in \mathbb{Q}_{\leq 0}$.

Proof.

1. We write $\alpha = q\phi$, $\beta = r\psi$ with $q, r \in \mathbb{Q}$ and $\phi, \psi \in End(E)$. Take $s \in \mathbb{Z}$ such that $sq, sr \in \mathbb{Z}$. Then:
$\hat{\alpha} = \widehat{q\phi} = q\hat{\phi} = q\phi = \alpha$;
$\widehat{\alpha+\beta} = \frac{1}{s}(\widehat{sq\phi + sr\psi}) = \frac{1}{s}(\widehat{sq\phi} + \widehat{sr\psi}) = \hat{\alpha}+\hat{\beta}$;
$\widehat{\alpha\beta} = \widehat{qr\phi\psi} = qr\widehat{\phi\psi} = qr\hat{\psi}\hat{\phi} = \hat{\beta}\hat{\alpha}$;
$\hat{q} = \widehat{q1} = q\hat{1} = q1 = q$.

2. In the same settings of the previous point we have:
$Nm(\alpha) = q\phi\widehat{q\phi} = q^2[deg(\phi)] \in \mathbb{Q}_{\geq 0}$;
$Nm(\alpha\beta) = \alpha\beta\widehat{\alpha\beta} = \alpha\beta\hat{\beta}\hat{\alpha} = \alpha Nm(\beta)\hat{\alpha} = Nm(\alpha)Nm(\beta)$;
$Nm(\hat{\alpha})\alpha = \alpha Nm(\hat{\alpha}) = \alpha\hat{\alpha}\hat{\hat{\alpha}} = \alpha\hat{\alpha}\alpha = Nm(\alpha)\alpha \Rightarrow Nm(\hat{\alpha}) = Nm(\alpha)$;
$Nm(\alpha) = 0 \Rightarrow q^2[deg(\phi)] = 0 \Rightarrow q = 0$ or $\phi = 0 \Rightarrow \alpha = 0$.

3. If $\alpha, \beta \in End^0(E)$ and $q, r \in \mathbb{Q}$, then:
$Tr(\alpha) = \alpha+\hat{\alpha} = 1-\alpha\hat{\alpha}-(1-\alpha)(1-\hat{\alpha}) = 1-Nm(\alpha)-Nm(1-\alpha) \in \mathbb{Q}$;
$Tr(q\alpha + r\beta) = q\alpha + r\beta + \widehat{q\alpha + r\beta} = q(\alpha+\hat{\alpha}) + r(\beta+\hat{\beta})$
$= qTr(\alpha) + rTr(\beta)$;
$Tr(\hat{\alpha}) = \hat{\alpha} + \hat{\hat{\alpha}} = \hat{\alpha} + \alpha = \alpha + \hat{\alpha} = Tr(\alpha)$;
$Tr(\alpha) = 0 \Rightarrow \hat{\alpha} = -\alpha \Rightarrow Nm(\alpha) = \alpha\hat{\alpha} = -\alpha^2$
$\Rightarrow \alpha^2 = -Nm(\alpha) \in \mathbb{Q}_{\leq 0}$.

□

Now, our purpose is to classify the endomorphism rings of elliptic curves. It is the starting point for the study of elliptic curves with complex multiplication. We start by classifying the endomorphism algebras of elliptic curves.

Theorem 4.4. *Let* E/K *be an elliptic curve over a field* K. *Then* $End^0(E)$ *is isomorphic to one of the following:*

- *the field of rationals* $\mathbb{Q}$;
- *an imaginary quadratic field;*

- *a quaternion algebra over $\mathbb{Q}$, i.e. a $\mathbb{Q}$-algebra which admits a $\mathbb{Q}$-basis $\{1, \alpha, \beta, \alpha\beta\}$ such that $\alpha^2, \beta^2 \neq 0$ and $\alpha\beta = -\beta\alpha$.*

Proof. If $End^0(E) = \mathbb{Q}$ there is nothing to prove.
Now, we assume there is $\alpha \in End^0(E)$ which is not in $\mathbb{Q}$. We can assume $Tr(\alpha) = 0$ (we can eventually substitute it with $\alpha - \frac{Tr(\alpha)}{2}$) and it implies that $\alpha^2 \in \mathbb{Q}_{\leq 0}$. So, if $End^0(E) = \mathbb{Q}(\alpha)$, then it is an imaginary quadratic field.
Finally, we assume there is β which is not in $\mathbb{Q}(\alpha)$. As we did before, we can assume $Tr(\beta) = 0$ and, by eventually replacing β with $\beta - \frac{Tr(\alpha\beta)}{2\alpha^2}\alpha$, also that $Tr(\alpha\beta) = 0$. Then $\alpha = -\hat{\alpha}$, $\beta = -\hat{\beta}$ and it implies

$$\alpha\beta = -\widehat{\alpha\beta} = -\hat{\beta}\hat{\alpha} = -\beta\alpha$$

It follows that $\mathbb{Q}(\alpha, \beta)$ is spanned by $\{1, \alpha, \beta, \alpha\beta\}$ and to prove that it is a quaternion algebra we just need to see that these elements are linearly independent. It is clear for $1, \alpha$ and β, so we assume by contradiction that $\alpha\beta = a + b\alpha + c\beta$ where the coefficients are in $\mathbb{Q}$. It implies that

$$(\alpha - c)\beta = a + b\alpha \Rightarrow \beta = \frac{a + b\alpha}{\alpha - c} \in \mathbb{Q}(\alpha)$$

but we know that it is not true.
The last thing to prove is that in the last case any $\gamma \in End^0(E)$ belongs to $\mathbb{Q}(\alpha, \beta)$. By contradiction we assume the opposite and, as we did before, we assume $Tr(\gamma) = Tr(\alpha\gamma) = 0$, which implies $\alpha\beta\gamma = -\beta\alpha\gamma = \beta\gamma\alpha$. So α commutes with $\beta\gamma$ and we claim that whenever $\delta \notin \mathbb{Q}$ and ρ are elements of the endomorphism algebra which commute, $\rho \in \mathbb{Q}(\delta)$. The statement will follow immediately.
As usual, we can assume $Tr(\delta) = Tr(\rho) = Tr(\delta\rho) = 0$ (we substitute α with $\alpha - a$ and β with $\beta - b - c\alpha$ for suitable $a, b, c \in \mathbb{Q}$) which implies
$\delta\rho = -\rho\delta$ and, since δ and ρ commute, we have $\delta\rho = 0$. So $\rho = 0 \in \mathbb{Q}(\delta)$. □

Corollary 4.1. *Let E/K be an elliptic curve over a field K. Then $End(E)$ is isomorphic to one of the following:*

- *the ring of integers $\mathbb{Z}$;*
- *an order in an imaginary quadratic field;*
- *an order in a quaternion algebra over $\mathbb{Q}$ (a subring which is also a free $\mathbb{Z}$-module of rank 4).*

Proof. We only need to prove that $End(E)$ is a free $\mathbb{Z}$-module of rank equal to the $\mathbb{Q}$-dimension of $End^0(E)$: the statement follows because $\mathbb{Z}$ is the only free $\mathbb{Z}$-module of rank 1 which is also a subring of $\mathbb{Q}$ and by definition in the other two cases. We observe that it is possible to choose a $\mathbb{Q}$-basis $\{e_1, ..., e_r\}$

of $End^0(E)$ (where r is its dimension) such that its elements are contained in $End(E)$ and $Tr(e_i e_j) = 0$ whenever $i \neq j$. Then, for any $\mathbb{Z}$-module A contained in $End^0(E)$ we set

$$A^* := \{\alpha \in End^0(E) : Tr(\alpha\phi) \in \mathbb{Z} \,\forall\, \phi \in A\}$$

It is easy to see that A^* is a $\mathbb{Z}$-module too and that $A \subset B \Rightarrow B^* \subset A^*$. Now, we take $A := \langle e_1, ..., e_r \rangle_{\mathbb{Z}}$ and we observe that

$$A \subset End(E) \subset End(E)^* \subset A^*$$

If we take $\alpha = a_1 e_1 + ... + a_r e_r \in A^*$ with $a_i \in \mathbb{Q}$, then

$$Tr(\alpha e_i) = a_i Tr(e_i^2) \in \mathbb{Z}$$

and this implies that a_i is an integer multiple of $\frac{1}{Tr(e_i^2)}$. Finally, we get that $\{\frac{e_1}{Tr(e_1^2)}, ..., \frac{e_r}{Tr(e_r^2)}\}$ is a $\mathbb{Z}$-basis of A^* and from the previous chain of inclusions we deduce that $End(E)$ is a free $\mathbb{Z}$-module of rank r. □

4.5 Elliptic curves over $\mathbb{C}$

The last section of this chapter is devoted to elliptic curves defined over $\mathbb{C}$. We start with some definitions.

Definition 4.7. *A **lattice** Λ in $\mathbb{C}$ is a discrete additive subgroup of $\mathbb{C}$ that is free of rank 2 as $\mathbb{Z}$-module. If ω_1 and ω_2 are two $\mathbb{Z}$-generators of Λ we can write $\Lambda = [\omega_1, \omega_2]$.*
*A **fundamental parallelogram** for a lattice Λ (related to a basis $\{\omega_1, \omega_2\}$) is a set of the form $\{x + t\omega_1 + r\omega_2 : t, r \in \mathbb{R}, 0 \leq t, r < 1\}$.*
*Two lattices Λ_1 and Λ_2 are said to be **homotetic** if there exists $\lambda \in \mathbb{C}$ different from zero such that $\Lambda_1 = \lambda\Lambda_2$.*

Definition 4.8. *A meromorphic function f on the complex plane is called an **elliptic function** for a lattice Λ if $f(z + \omega) = f(z)$ for any $\omega \in \Lambda$ and any $z \in \mathbb{C}$ where the function is defined.*
*The **order** of an elliptic function is the number of its poles in a fundamental parallelogram of Λ counted with multiplicity.*

We immediately observe that the well-known Liouville's Theorem implies that holomorphic elliptic functions are constant. It is also possible to prove that the order of an elliptic function also coincides with the number of zeros in a fundamental parallelogram counted with multiplicity (see [14, Lecture 14, Theorem 14.18, pag. 7]).

Definition 4.9. *If Λ is a lattice of $\mathbb{C}$ and $k \in \mathbb{Z}, k > 1$, we define:*

- *the Eisentstein series of weight* $2k$ *as*

$$G_{2k}(\Lambda) := \sum_{\omega\in\Lambda,\omega\neq 0} \frac{1}{\omega^{2k}}$$

- *the Weierstrass* $\wp$*-function as*

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

Proposition 4.11. *The following properties hold:*

1. $G_{2k}(\Lambda)$ *converges absolutely for all* $k > 1$*;*
2. $\wp(z;\Lambda)$ *is an even elliptic function of order 2 that is everywhere holomorphic outside* Λ*;*
3. $\wp'(z;\Lambda) = -2\sum_{\omega\in\Lambda} \frac{1}{(z-\omega)^3}$ *is an odd elliptic function of order 3 that is everywhere holomorphic outside* Λ*.*

Proof.

1. We fix d as the minimum distance between elements of Λ. We want to estimate the number of lattice points ω such that $r \leq |\omega| < r + \frac{d}{2}$ for r a positive real number. In order to do so, we observe that the radial projections of two distinct points of Λ on the circumference $|z| = r$ must be separated by an arch whose length is, at least, $\frac{d}{2}$. So we find that the number of lattice points we are interested in is bounded by $\frac{4\pi r}{d}$. Extending the argument to the case of an annulus of width 1, we immediately see that the number of lattice points ω such that $n \leq |\omega| < n+1$ for n a positive integer is bounded by $c(n+1) := \frac{8\pi}{d^2}(n+1)$.
   Then, $\sum_{\omega\in\Lambda,|\omega|\geq 1} \frac{1}{|\omega|^{2k}} \leq \sum_{n=1}^{\infty} \frac{c(n+1)}{n^{2k}} < \infty$.
   The statement follows because

$$\sum_{\omega\in\Lambda,\omega\neq 0} \frac{1}{\omega^{2k}} = \sum_{\omega\in\Lambda,|\omega|\geq 1} \frac{1}{|\omega|^{2k}} + \sum_{\omega\in\Lambda,0<|\omega|<1} \frac{1}{|\omega|^{2k}}$$

   and the second summation is finite.

2. First of all we prove that the series defining $\wp$ converges uniformly on every compact subset C of $\mathbb{C} \setminus \Lambda$. Since C is compact we can fix

$r > 0$ such that $|z| \leq r$ for any $z \in C$. Furthermore, for almost all the elements $\omega \in \Lambda$ we have $|\omega| \geq 2r$. Then,

$$\left|\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right| = \left|\frac{z(2\omega - z)}{\omega^2(z-\omega)^2}\right| \leq \frac{r(|2\omega| + |-z|)}{|\omega|^2(|\omega| - |z|)^2} \leq \frac{10r}{|\omega|^3}$$

and we see that it converges with an argument similar to that used in the previous point. The uniform convergence follows. Then, $\wp$ is holomorphic outside Λ and from the formula we see that it has poles of order 2 on points of Λ. It is easy to see that it is periodic: if $\omega_0 \in \Lambda$, then

$$\begin{aligned}\wp(z+\omega_0) &= \frac{1}{(z+\omega_0)^2} + \sum_{\omega\in\Lambda,\omega\neq 0}\left(\frac{1}{(z+\omega_0-\omega)^2} - \frac{1}{\omega^2}\right) \\ &= \frac{1}{z^2} + \sum_{\omega'\in\Lambda,\omega'\neq 0}\left(\frac{1}{(z-\omega')^2} - \frac{1}{\omega'^2}\right) = \wp(z)\end{aligned}$$

Finally, $\wp$ is even:

$$\begin{aligned}\wp(-z;\Lambda) &= \frac{1}{(-z)^2} + \sum_{\omega\in\Lambda,\omega\neq 0}\left(\frac{1}{(-z-\omega)^2} - \frac{1}{\omega^2}\right) \\ &= \frac{1}{z^2} + \sum_{-\omega\in\Lambda,\omega\neq 0}\left(\frac{1}{(-z+\omega)^2} - \frac{1}{\omega^2}\right) = \wp(z;\Lambda)\end{aligned}$$

3. The formula for $\wp'$ follows immediately from the defining formula for $\wp$. Since $\wp$ is an elliptic function that is holomorphic outside Λ, the same holds for its derivative and from the formula we see that it has poles of order 3 on points of Λ. Finally, $\wp'$ is odd:

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

□

Given a lattice Λ of $\mathbb{C}$, we define

$$g_2(\Lambda) := 60G_4(\Lambda)$$

$$g_3(\Lambda) := 140G_6(\Lambda)$$

$$\Delta(\Lambda) := g_2(\Lambda)^3 - 27g_3(\Lambda)^2$$

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

where $\Delta(\Lambda)$ and $j(\Lambda)$ are called respectively the **discriminant** and the **j-invariant** of the lattice. We will prove soon that the j-invariant is well-defined.
Then, we define E_Λ to be the elliptic curve over $\mathbb{C}$ defined by the equation:

$$y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$$

We see that this curve could be written in Weierstrass form as

$$y^2 = x^3 - \frac{g_2(\Lambda)}{4}x - \frac{g_3(\Lambda)}{4}$$

In particular, we see that $\Delta(E_\Lambda) = \Delta(\Lambda)$. These definitions are justified by the following results.

Lemma 4.3. *Given a lattice Λ, the function $\wp$ has the following Laurent series at $z = 0$:*

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

Proof. See [14, Lecture 14, Theorem 14.28, pag. 11]. □

Proposition 4.12. *For any $z \notin \Lambda$ we have that*

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

Proof. The Laurent expansion of $\wp$ at $z = 0$ gives the following:

- $\wp(z) = \frac{1}{z^2} + 3G_4(\Lambda)z^2 + 5G_6(\Lambda)z^4 + \cdots$
- $\wp'(z) = -\frac{2}{z^3} + 6G_4(\Lambda)z + 20G_6(\Lambda)z^3 + \cdots$
- $\wp(z)^3 = \frac{1}{z^6} + \frac{9G_4(\Lambda)}{z^2} + 15G_6(\Lambda) + \cdots$
- $\wp'(z)^2 = \frac{4}{z^6} - \frac{24G_4(\Lambda)}{z^2} - 80G_6(\Lambda) + \cdots$

We set $f(z) := \wp'(z)^2 - 4\wp(z)^3 + g_2(\Lambda)\wp(z) + g_3(\Lambda)$ and, using the previous formulas, we find that f is an elliptic function such that $f(0) = 0$, hence it is also holomorphic because $\wp$ and $\wp'$ have poles only on points of Λ. Then f is constant and so it is identically zero. □

Proposition 4.13. $\Delta(\Lambda) \neq 0$ *for any lattice Λ. In particular, E_Λ is smooth.*

Proof. First of all we observe that the discriminant of the polynomial

$$f(x) := 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$$

is equal to $16\Delta(\Lambda)$, so we just need to prove that $f(x)$ has three distinct roots. If $\Lambda = [\omega_1, \omega_2]$, $z_1 = \frac{\omega_1}{2}$, $z_2 = \frac{\omega_2}{2}$ and $z_3 = \frac{\omega_1+\omega_2}{2}$, then we have $f(\wp(z_i)) = 0$ for any i. Indeed,

$$f(\wp(z_i)) = 4\wp(z_i)^3 - g_2(\Lambda)\wp(z_i) - g_3(\Lambda) = \wp'(z_i)^2$$

and

$$\wp'(z_i) = \wp'(z_i - 2z_i) = \wp'(-z_i) = -\wp'(z_i) \Rightarrow \wp'(z_i) = 0$$

Now, the function $z \mapsto \wp(z) - \wp(z_i)$ is elliptic of order 2 and so it has two zeros counted with multiplicity. Its derivative in z_i is $\wp'(z_i) = 0$ so it is a double zero and in particular it is the only zero of the defined function. So the roots of f are distinct. □

Theorem 4.5. *The map $\Phi_\Lambda : \mathbb{C}/\Lambda \to E_\Lambda$ defined by $\Phi_\Lambda(z) = (\wp(z), \wp'(z))$ if $z \notin \Lambda$ and $\Phi_\Lambda(z) = O$ otherwise is an isomorphism of additive groups.*

Proof. The map is obviously well-defined. We only prove that the given function is a bijection.

- Φ_Λ is injective: assume $\Phi_\Lambda(z_1) = \Phi_\Lambda(z_2)$ with z_1, z_2 in a fundamental parallelogram. We have to distinguish two cases.
  If $\wp'(z_1) \neq 0$, we consider the function $z \mapsto \wp(z) - \wp(z_1) = \wp(z) - \wp(z_2)$. Since it is an elliptic function of order 2 its zeros are $\pm z_1$ and we find that $z_1 = z_2$ or $z_1 = -z_2$. If the latter holds,

  $$\wp'(z_1) = \wp'(-z_2) = -\wp'(z_2) = -\wp'(z_1) \Rightarrow \wp'(z_1) = 0$$

  contrary to our assumption, so $z_1 = z_2$.
  If $\wp'(z_1) = 0$, $\Phi_\Lambda(z_1)$ is a point of order 2 and from the proof of the previous proposition we know that the same holds for z_1. Since $\wp(z_1) = \wp(z_2)$, again the proof of the last proposition implies that $z_1 = z_2$.

- Φ_Λ is surjective: we fix $(x_0, y_0) \in E_\Lambda$ and we consider the map $z \mapsto \wp(z) - x_0$. It is an elliptic function of order 2, so we can fix $z_0 \in \mathbb{C}^\times$ such that $\wp(z_0) = x_0$. By eventually replacing z_0 with its opposite we find $\Phi_\Lambda(z_0) = (x_0, y_0)$.

For a complete proof see [14, Lecture 15, Theorem 15.1, pag. 1]. □

Finally, we state the Uniformization Theorem.

Theorem 4.6. *If $E/\mathbb{C}$ is a complex elliptic curve, then there exists a complex lattice Λ such that $E = E_\Lambda$.*

Proof. See [14, Lecture 15, Corollary 15.12, pag. 8]. □

Now, we put our attention on the j-invariant of a lattice. First we see that

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

Proposition 4.14. *Two lattices Λ_1 and Λ_2 are homotetic if and only if they have the same j-invariant. In particular, Λ_1 and Λ_2 are homotetic if and only if E_{Λ_1} and E_{Λ_2} are isomorphic.*

Proof. We assume $\Lambda_1 = \lambda\Lambda_2$ with $\lambda \in \mathbb{C}^\times$. Then

$$j(\Lambda_1) = j(\lambda\Lambda_2) = 1728\frac{g_2(\lambda\Lambda_2)^3}{\Delta(\lambda\Lambda_2)} = 1728\frac{\lambda^{12}g_2(\Lambda_2)^3}{\lambda^{12}\Delta(\Lambda_2)} = j(\Lambda_2)$$

Conversely, we assume $j(\Lambda_1) = j(\Lambda_2)$. The corresponding elliptic curves have the same j-invariant and so they are isomorphic. Then we know that there exists $\lambda \in \mathbb{C}^\times$ such that

$$g_2(\Lambda_2) = \frac{g_2(\Lambda_1)}{\lambda^4} = g_2(\lambda\Lambda_1),\ g_3(\Lambda_2) = \frac{g_3(\Lambda_1)}{\lambda^6} = g_3(\lambda\Lambda_1)$$

In order to conclude we just need to show that $\wp(z;\Lambda)$, and hence Λ because it is the set of poles of $\wp$, is completely determined by the values of $g_2(\Lambda)$ and $g_3(\Lambda)$ for any lattice Λ. We know that

$$\begin{aligned}\wp'(z)^2 = 4\wp(z)^3 - g_2(\Lambda)\wp(z) - g_3(\Lambda) &\Rightarrow 2\wp'(z)\wp''(z) = 12\wp(z)^2\wp'(z) - g_2(\Lambda)\wp'(z)\\ &\Rightarrow \wp''(z) = 6\wp(z)^2 - g_2(\Lambda)/2\end{aligned}$$

and, if we put $a_n := (2n+1)G_{n+2}$, the Laurent series of $\wp$ at $z = 0$ is

$$\wp(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty} a_n z^{2n}$$

Then, comparing the coefficients of z^{2n} we find that

$$(2n+2)(2n+1)a_{n+1} = 6(\sum_{k=1}^{n-1} a_k a_{n-k} + 2a_{n+1})$$

and it implies that any coefficient is determined by the previous ones. Since $a_1 = g_2(\Lambda)/20$ and $a_2 = g_3(\Lambda)/28$ our claim is proved. □

Now, we observe that $\mathbb{C}/\Lambda$ has a natural structure of complex torus if Λ is a lattice. We want to define what is a morphism of complex tori and to state a correspondence between them and isogenies between the associated elliptic curves.

Definition 4.10. *If Λ_1 and Λ_2 are complex lattices, we say that*

$$\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$$

is a morhpism of complex tori if $\phi(0) = 0$ and there exists a holomorphic function $f : \mathbb{C} \to \mathbb{C}$ such that $\pi_2 \circ f = \phi \circ \pi_1$ (where π_1 and π_2 are the natural projections, $\pi_i : \mathbb{C} \to \mathbb{C}/\Lambda_i$).

Proposition 4.15. *Let Λ_1 and Λ_2 be complex lattices. Then:*

1. *The map*

   $$\Phi : \{\alpha \in \mathbb{C} : \alpha\Lambda_1 \subset \Lambda_2\} \to \{morphisms\ from\ \mathbb{C}/\Lambda_1\ to\ \mathbb{C}/\Lambda_2\}, \alpha \mapsto \phi_\alpha$$

   where $\phi_\alpha(z+\Lambda_1) = \alpha z + \Lambda_2$ is an isomorphism of additive groups (and also of rings if $\Lambda_1 = \Lambda_2$).

2. *The map*

   $$\Psi : \{\alpha \in \mathbb{C} : \alpha\Lambda_1 \subset \Lambda_2\} \to Hom(E_{\Lambda_1}, E_{\Lambda_2}), \alpha \mapsto \psi_\alpha$$

   where $\psi_\alpha(P) = \Phi_{\Lambda_2} \circ \phi_\alpha \circ \Phi_{\Lambda_1}^{-1}(P)$ is an isomorphism of additive groups (and also of rings if $\Lambda_1 = \Lambda_2$).

Proof. We prove only the first statement.
Φ is well-defined: obviously ϕ_α is a morphism of complex tori because the multiplication by α is holomorphic in $\mathbb{C}$. Furthermore, $\phi_\alpha(0) = 0$ and it is well-defined because if $\omega \in \Lambda_1$, then $\alpha\omega \in \Lambda_2$.
Φ is a group homomorphism: for any $z \in \mathbb{C}$ we have

$$\phi_{\alpha+\beta}(\pi_1(z)) = \pi_2((\alpha+\beta)z) = \pi_2(\alpha z) + \pi_2(\beta z) = (\phi_\alpha + \phi_\beta)(\pi_1(z))$$

If $\Lambda_1 = \Lambda_2$, Φ is a ring homomorphism: for any $z \in \mathbb{C}$ we have

$$\phi_{\alpha\beta}(\pi(z)) = \pi(\alpha\beta z) = \phi_\alpha(\pi(\beta z)) = (\phi_\alpha\phi_\beta)(\pi(z))$$

Φ is injective: we assume that $\phi_\alpha = \phi_\beta$. Then $(\alpha-\beta)z \in \Lambda_2$ for any $z \in \mathbb{C}$ and so $\alpha - \beta = ((\alpha-\beta)z)' = 0$ because the map $z \mapsto (\alpha-\beta)z$ is continuous from a connected space ($\mathbb{C}$) to a discrete one (Λ_2) and so it is constant.
Φ is surjective: we fix $\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ a morphism of complex tori and $f : \mathbb{C} \to \mathbb{C}$ a holomorphic function such that $\pi_2 \circ f = \phi \circ \pi_1$. Now, for any $\omega \in \Lambda_1$ we define the holomorphic function $g_\omega(z) := f(z+\omega) - f(z)$. Since $\pi_2(g_\omega(z)) = \phi(\pi_1(z+\omega)) - \phi(\pi_1(z)) = 0$, the image of $g_\omega(z)$ is contained in Λ_2 and so it is constant. It implies $f'(z+\omega) = f'(z)$ for any $z \in \mathbb{C}$, $\omega \in \Lambda_1$, so f' is holomorphic and bounded, hence constant by Liouville's Theorem. Finally, we obtain that $f(z) = \alpha z + \beta$ with $\alpha, \beta \in \mathbb{C}$. We can conclude because $\pi_2(\beta) = \pi_2(f(0)) = \phi(\pi_1(0)) = \phi(0) = 0$ and so $\beta \in \Lambda_2$.
For a proof of the second statement see [14, Lecture 16, Theorem 16.4, pag. 4]. □

We can immediately see that ϕ_α is a group homomorphism for any $\alpha \in \mathbb{C}$ such that $\alpha\Lambda_1 \subset \Lambda_2$. Then the first point of the previous proposition immediately implies that every morphism of complex tori is also a group homomorphism.
Now we prove that conjugation in $\mathbb{C}$ and dualization in $End(E_\Lambda)$ have the same effects if we consider the isomorphism described in the previous proposition (in the case $\Lambda_1 = \Lambda_2$).

Proposition 4.16. *Let Λ be a complex lattice. Then for every $\psi \in End(E_\Lambda)$ we have that*

$$\Psi^{-1}(\psi) = \alpha \Rightarrow \Psi^{-1}(\hat{\psi}) = \bar{\alpha}$$

Proof. We consider the polynomial $p(x) := x^2 - Tr(\psi)x + Nm(\psi)$. We know that $p \in \mathbb{Z}[x]$ and $p(x) = (x - \psi)(x - \hat{\psi})$ in $End(E_\Lambda)$. Then, if we set $\beta = \Psi^{-1}(\hat{\psi})$, we get that α and β are the roots of p in $\mathbb{C}$. We distinguish two cases:

- $\alpha \in \mathbb{Z}$: it implies that also $\psi \in \mathbb{Z}$ and we know that $\hat{\psi} = \psi$. So $\beta = \alpha = \bar{\alpha}$;
- α is a complex algebraic integer in an imaginary quadratic field: it follows immediately that $\beta = \bar{\alpha}$.

□

From now on, when the endomorphism ring of a complex elliptic curve E is an order in an imaginary quadratic field, we will consider it as a subring of $\mathbb{C}$ via the inclusion

$$[\cdot] : End(E) \hookrightarrow \mathbb{C},\ [\psi] = \Psi^{-1}(\psi)$$

We say that the pair $(E, [\cdot])$ is normalized.
We conclude our treatment of complex elliptic curves with an useful corollary of the previous results.

Corollary 4.2. *If E is a complex elliptic curve then $End(E)$ is commutative.*

Proof. If E is a complex elliptic curve, the Uniformization Theorem tells us that there exists a complex lattice Λ such that $E = E_\Lambda$. Then, $End(E)$ is isomorphic to $\{\alpha \in \mathbb{C} : \alpha\Lambda \subset \Lambda\}$. The latter is a subring of $\mathbb{C}$, so it is commutative and the same holds for the former. □

So, for a complex elliptic curve $End(E)$ is isomorphic to $\mathbb{Z}$ or to an imaginary quadratic order. It will be the starting point for the theory of complex multiplication that we will see in the next chapter.

Chapter 5

Complex Multiplication

In the previous chapter we proved the classification Theorem for the endomorphism ring of an elliptic curve. In particular we saw that if E is an elliptic curve then $End(E)$ is isomorphic to $\mathbb{Z}$, an order in an imaginary quadratic field or an order in a quaternion algebra over $\mathbb{Q}$. We also proved that for a complex elliptic curve only the first two cases are possible. Starting from these results, we give the following important definition.

Definition 5.1. *Let E/K be an elliptic curve over a field K. Then we say that E has **complex multiplication** if $End(E) \supsetneq \mathbb{Z}$.*

In particular, a complex elliptic curve has complex multiplication if and only if its endomorphism ring is an order in an imaginary quadratic field. The main purpose of this chapter is to use the theory of elliptic curves with complex multiplication to study class field theory in detail for the case of an imaginary quadratic field.

5.1 Proper ideals

We observe that any fractional ideal of an order in an imaginary quadratic field is a lattice in $\mathbb{C}$.

Definition 5.2. *Let $\mathcal{O}$ be an order in an imaginary quadratic field and $\mathfrak{a}$ a fractional $\mathcal{O}$-ideal. We say that $\mathfrak{a}$ is **proper** if $\mathcal{O} = \{\alpha \in \mathbb{C} : \alpha\mathfrak{a} \subset \mathfrak{a}\}$.*

Since the inclusion $\mathcal{O} \subset \{\alpha \in \mathbb{C} : \alpha\mathfrak{a} \subset \mathfrak{a}\}$ always holds and the latter is an order we see that any fractional $\mathcal{O}_K$-ideal is proper.

Proposition 5.1. *Let K be an imaginary quadratic field, $\mathcal{O}$ an order of K and Λ a lattice in $\mathbb{C}$. Then $End(E_\Lambda) = \mathcal{O}$ if and only if Λ is homotetic to a (fractional) proper $\mathcal{O}$-ideal.*

Proof. If Λ is homotetic to a proper $\mathcal{O}$-ideal, obviously $End(E_\Lambda) = \mathcal{O}$.
In order to prove the converse, we assume $\Lambda = [1, \tau]$ and $\mathcal{O} = [1, \omega]$.

$End(E_\Lambda) = \mathcal{O}$ implies $\omega \in \Lambda$ and so there exist $a, b \in \mathbb{Z}, b \neq 0$ such that $\omega = a + b\tau$. Then $b\Lambda = [b, b\tau] = [b, \omega - a] \subset [1, \omega] = \mathcal{O}$, so Λ is homotetic to a sublattice of $\mathcal{O}$ and it is closed under multiplication by $\mathcal{O}$, i.e. it is an $\mathcal{O}$-ideal. Obviously, it is also proper. □

Proposition 5.2. *Let $\mathcal{O}$ be an order in an imaginary quadratic field. A (fractional) $\mathcal{O}$-ideal $\mathfrak{a}$ is proper if and only if it is invertible.*

Proof. If $\mathfrak{a}$ is invertible and $\lambda \in \mathbb{C}^\times$, then

$$\lambda\mathfrak{a} \subset \mathfrak{a} \Rightarrow \lambda\mathfrak{a}\mathfrak{a}^{-1} \subset \mathfrak{a}\mathfrak{a}^{-1} \Rightarrow \lambda\mathcal{O} \subset \mathcal{O} \Rightarrow \lambda \in \mathcal{O}$$

and so $\mathfrak{a}$ is proper. For the converse, we fix $\mathfrak{a} := \alpha[1, \tau]$ a proper $\mathcal{O}$-ideal, $\mathcal{O} := [1, \omega]$ and $ax^2 + bx + c \in \mathbb{Z}[x]$ to be the minimal polynomial of τ. Since $\mathfrak{a}$ and $[1, \tau]$ are homotetic we have that $\mathcal{O} = \{\lambda \in \mathbb{C} : \lambda[1, \tau] \subset [1, \tau]\}$ and it implies $\omega \in [1, \tau]$, so we can assume $\omega = n\tau$ with $n \in \mathbb{Z}$. Furthermore, $\omega\tau \in [1, \tau]$ and then $n\tau^2 \in [1, \tau]$ and $a|n$. Obviously $a\tau[1, \tau] \subset [1, \tau]$ and so $a\tau \in \mathcal{O} = [1, n\tau]$, which implies $a = n$ and $\mathcal{O} = [1, a\tau]$. Now, if we set $\bar{\mathfrak{a}} := \bar{\alpha}[1, \bar{\tau}]$ we find

$$\mathfrak{a}\bar{\mathfrak{a}} = N(\alpha)[1, \tau, \bar{\tau}, \tau\bar{\tau}] = \frac{N(\alpha)}{a}[a, a\tau, -b, c] = N(\mathfrak{a})[1, a\tau] = N(\mathfrak{a})$$

where the third equality follows from $gcd(a, b, c) = 1$ and

$$N(\mathfrak{a}) = [\mathcal{O} : \mathfrak{a}] = \frac{1}{a}[[1, a\tau] : \alpha[1, a\tau]] = \frac{1}{a}[\mathcal{O} : \alpha\mathcal{O}] = \frac{N(\alpha)}{a}$$

Finally, $\mathfrak{a}$ is an invertible $\mathcal{O}$-ideal with inverse $\frac{1}{N(\mathfrak{a})}\bar{\mathfrak{a}}$. □

Thanks to the previous results we can see that for any imaginary quadratic order $\mathcal{O}$, the Picard group $Pic(\mathcal{O})$ coincides with the set of (fractional) proper $\mathcal{O}$-ideals modulo homotety. Indeed, in any class of $Pic(\mathcal{O})$ we can find an invertible (and so proper) $\mathcal{O}$-ideal and it is easy to see that two $\mathcal{O}$-ideals lie in the same class if and only if they are homotetic.

5.2 Modular functions

In this section we introduce the definition of modular functions and we study their main properties. These notions will be crucial in the proofs of the main theorems of complex multiplication. First of all we denote by

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

the upper-half of the complex plane and by

$$SL_2(\mathbb{Z}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}) : ad - bc = 1 \right\}$$

the special linear group of degree 2 over $\mathbb{Z}$. Now, we let $SL_2(\mathbb{Z})$ act on $\mathbb{H}$ in the following way:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \tau := \frac{a\tau + b}{c\tau + d}$$

for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ and $\tau \in \mathbb{H}$. The action is well-defined thanks to the following lemma.

Lemma 5.1. *Let $\gamma \in SL_2(\mathbb{Z})$ and $\tau \in \mathbb{H}$. Then $\gamma \cdot \tau \in \mathbb{H}$.*

Proof. We set $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ and $\tau = x + iy$ with $x, y \in \mathbb{R}, y > 0$. We need to prove that $Im\left(\frac{a\tau+b}{c\tau+d}\right) > 0$. We have

$$\begin{aligned} \frac{a\tau + b}{c\tau + d} &= \frac{(ax + b + iay)(cx + d - icy)}{|c\tau + d|^2} \\ &= \frac{(ax + b)(cx + d) + acy^2 + i(ay(cx + d) - cy(ax + b))}{|c\tau + d|^2} \end{aligned}$$

and so

$$Im\left(\frac{a\tau + b}{c\tau + d}\right) = \frac{y(ad - bc)}{|c\tau + d|^2} > 0$$

□

Definition 5.3. *A **modular function** is a map*

$$f : \mathbb{H} \to \mathbb{C}$$

such that:

- *f is meromorphic;*
- *f is invariant under the action of $SL_2(\mathbb{Z})$, i.e. $f(\gamma \cdot \tau) = f(\tau)$ for all $\gamma \in SL_2(\mathbb{Z})$ and $\tau \in \mathbb{H}$;*
- *f is meromorphic at the cusps.*

What does it mean to be meromorphic at the cusps? Since f is invariant under the action of $SL_2(\mathbb{Z})$ we have, for any $\tau \in \mathbb{H}$,

$$f(\tau) = f\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \tau\right) = f(\tau + 1)$$

Furthermore, for every $z \in \mathbb{Z}$, the function $q = q(\tau) := e^{2\pi i \tau}$ defines a bijection between $\mathbb{H}_z := \{\tau \in \mathbb{H} : z \leq Re(\tau) < z + 1\}$ and the punctured unitary open disk $\mathbb{D}_0$.
Then there exists a meromorphic function $\bar{f} : \mathbb{D}_0 \to \mathbb{C}$ such that $\bar{f} \circ q = f$.

Obviously $\bar{f}$ admits a Laurent expansion and so f admits a so called q-expansion

$$f = \sum_{k=-\infty}^{+\infty} c_k q^k$$

with $c_k \in \mathbb{C}$ for any k. Finally, we say that f is meromorphic at the cusps if $\{c_k : k < 0, c_k \neq 0\}$ is finite.
Now, we recall that if $\Lambda = [u, v]$ is a complex lattice where $u = u_x + iu_y$ and $v = v_x + iv_y$, then the area $Vol(\Lambda)$ of any fundamental parallelogram of Λ is the absolute value of the determinant of $\begin{pmatrix} u_x & u_y \\ v_x & v_y \end{pmatrix}$. Thanks to this fact we can prove the following lemma.

Lemma 5.2. *If $\Lambda = [u, v]$ is a complex lattice and $\Lambda' = [s, t]$ is a sublattice of Λ with*

$$s = au + bv$$

$$t = cu + dv$$

where $a, b, c, d \in \mathbb{Z}$, then

$$[\Lambda : \Lambda'] = n \Leftrightarrow det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \pm n$$

Proof. We write $u = u_x + iu_y$, $v = v_x + iv_y$, $s = s_x + is_y$ and $t = t_x + it_y$. Then

$$\begin{pmatrix} s_x & s_y \\ t_x & t_y \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} u_x & u_y \\ v_x & v_y \end{pmatrix}$$

It follows that

$$[\Lambda : \Lambda'] = n \Leftrightarrow Vol(\Lambda') = nVol(\Lambda) \Leftrightarrow det \begin{pmatrix} s_x & s_y \\ t_x & t_y \end{pmatrix} = \pm n \, det \begin{pmatrix} u_x & u_y \\ v_x & v_y \end{pmatrix}$$
$$\Leftrightarrow det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \pm n$$

□

Definition 5.4. *The **j-function** is the map*

$$j : \mathbb{H} \to \mathbb{C}, \, \tau \mapsto j([1, \tau])$$

where $j([1, \tau])$ is the j-invariant of the complex lattice $[1, \tau]$.

Proposition 5.3. *The j-function is a holomorphic modular function.*

Proof. We need to prove that j satisifies the properties in the definition of modular function.

- j is holomorphic on $\mathbb{H}$. Since the discriminant of a lattice is always non-zero, we only have to prove that $g_i(\tau) := g_i([1,\tau])$ is holomorphic for $i = 2, 3$. We prove it for g_2, a similar argument works for g_3.
  We know that the series which define g_2 converges absolutely and to see that it is holomorphic we must prove that it converges uniformly on compact subsets of $\mathbb{H}$. Obviously, $g_2(\tau+1) = g_2(\tau)$ and so it is enough to prove it in the region $|Re(\tau)| \leq \frac{1}{2}$ and $Im(\tau) \geq \epsilon$ where ϵ is an arbitrary positive real number, $\epsilon < 1$. We claim that, under these conditions,
  $$|x + \tau y| \geq \frac{\epsilon}{2}\sqrt{x^2 + y^2}$$
  for any $x, y \in \mathbb{Z}$ and it concludes the proof.
  Let $\tau = a + ib$ with $a, b \in \mathbb{R}$. The claim is trivial if $|x + ay| \geq \frac{\epsilon}{2}|x|$. Instead, if $|x + ay| < \frac{\epsilon}{2}|x|$, then $|x| < |y|$ and the claim follows;
- j is invariant under the action of $SL_2(\mathbb{Z})$: it follows from the previous lemma;
- j is meromorphic at the cusps: it is a consequence of the following proposition.

□

Proposition 5.4. *The q-expansion of the j-function is*

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

with $c_n \in \mathbb{Z}$ for any n.

Proof. See [12, Proposition 7.4, pag. 59]. □

Proposition 5.5. *A holomorphic modular function is a polynomial in j. If the function is also holomorphic at infinity then it is constant.*

Proof. We assume that $f : \mathbb{H} \to \mathbb{C}$ is a holomorphic function which is also holomorphic at infinity. Then the limit

$$f(\infty) = \lim_{Im(\tau) \to \infty} f(\tau)$$

exists and it is finite in $\mathbb{C}$. Now, we consider a sequence $(\tau_k)_k$ of points in $\mathbb{H} \cup \infty$ and we study the sequence $f(\tau_k)$. We can assume $\tau_k \in D$ for any k where

$$D := \left\{\tau \in \mathbb{H} : |Re(\tau)| \leq \frac{1}{2},\ Im(\tau) > \frac{1}{2}\right\}$$

Indeed,

$$f(\tau + m) = f\left(\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \cdot \tau\right) = f(\tau)$$

for any $\tau \in \mathbb{H}$ and any $m \in \mathbb{Z}$ and if $Im(\tau) < \frac{1}{2}$ (and $|Re(\tau)| \leq \frac{1}{2}$) then

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

since $|\tau| < \frac{1}{\sqrt{2}}$ and

$$f\Big(\frac{-1}{\tau}\Big) = f\Big(\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \cdot \tau\Big) = f(\tau)$$

Now, if the imaginary parts of the τ_k are bounded, they lie in a compact set and so we can find a subsequence of $f(\tau_k)$ which converges. If they are unbounded, we can find a subsequence of τ_k such that the sequence of their images converges to $f(\infty)$. Then, $f(\mathbb{H} \cup \infty)$ is compact and, thanks to the Maximum Modulus Principle, we can conclude that f is constant.
If we only assume that f is holomorphic, then its q-expansion has only finitely many terms with a negative power of q and, thanks to the previous proposition, there exists a polynomial p such that $f - p \circ j$ is holomorphic at infinity. Then it is constant, i.e. f is a polynomial in j. □

5.3 Integrality of the j-invariant

In this section we want to prove that the j-invariant of a complex elliptic curve with complex multiplication is an algebraic integer. First of all, for any positive integer n we introduce the groups

$$D_n := \Big\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}) : ad - bc = n \Big\}$$

$$S_n := \Big\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in M_2(\mathbb{Z}) : ad = n, d > 0, 0 \leq b < d \Big\}$$

and, thanks to the fact that S_n is finite, the polynomial

$$F_n(X) := \prod_{\alpha \in S_n} (X - j \circ \alpha)$$

Lemma 5.3. *For any $\alpha \in D_n$ there exists a unique $\gamma \in SL_2(\mathbb{Z})$ such that $\gamma\alpha \in S_n$.*

Proof. See [12, Lemma 9.3, pag. 72]. □

Proposition 5.6. *The coefficients of $F_n(X)$ lie in $\mathbb{Z}[j]$.*

Proof. We write

$$F_n(X) = \sum_{m=0}^{|S_n|} s_m X^m$$

It is immediate to see that $s_m(\tau)$ is a holomorphic function on $\mathbb{H}$ which is symmetric on the $j \circ \alpha$'s for any m. We split the proof into four steps.
First step: $s_m(\tau)$ is invariant under the action of $SL_2(\mathbb{Z})$. We fix $\gamma \in SL_2(\mathbb{Z})$. We know that for any $\alpha \in S_n$ there exists a unique $\delta_\alpha \in SL_2(\mathbb{Z})$ such that $\delta_\alpha \alpha \gamma \in S_n$ and, since S_n is finite, it implies that the map

$$S_n \to S_n,\ \alpha \mapsto \delta_\alpha \alpha \gamma$$

is a bijection. The invariance of j under $SL_2(\mathbb{Z})$ implies

$$\{j \circ \alpha\gamma : \alpha \in S_n\} = \{j \circ \alpha : \alpha \in S_n\}$$

and it concludes the proof of the claim.
Second step: $s_m \in \mathbb{C}[j]$. From the previous step we have that, for any m, $s_m(\tau + 1) = s_m(\tau)$ and so s_m admits a q-expansion. If $\alpha = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in S_n$, we have

$$j \circ \alpha(\tau) = e^{-2\pi i \frac{a\tau+b}{d}} + \sum_{k=0}^{\infty} c_k e^{2\pi i k \frac{a\tau+b}{d}}$$

where the c_k are the coefficients of the q-expansion of j.
Then $q^{n+1}(j \circ \alpha)(\tau) \to 0$ as $q \to 0$ and so, for any m, there exists a positive integer N such that $q^N s_m(\tau) \to 0$ as $q \to 0$. Then, for any m, s_m is a holomorphic modular function and so $s_m \in \mathbb{C}[j]$.
Third step: $s_m \in \mathbb{Z}[[q, q^{-1}]]$. We fix a positive integer n, $\zeta_n = e^{\frac{2\pi i}{n}}$, $Q = q^{\frac{1}{n}}$ and $\alpha = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in S_n$. Then $j \circ \alpha$ admits a Q-expansion

$$j \circ \alpha = \zeta_n^{-ab} Q^{-a^2} + \sum_{k=0}^{\infty} c_k \zeta_n^{abk} Q^{a^2 k}$$

with coefficients in $\mathbb{Z}[\zeta_n]$. Now, if $\sigma \in Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ and $\sigma(\zeta_n) = \zeta_n^r$ with r and n coprime, from the comparison of the related Q-expansions we immediately find

$$\left(j \circ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\right)^\sigma = j \circ \begin{pmatrix} a & rb \\ 0 & d \end{pmatrix}$$

Furthermore, $j \circ \alpha$ only depends on $b \, (mod \, d)$ and, since r and d are coprime, we find

$$\left\{j \circ \begin{pmatrix} a & rb \\ 0 & d \end{pmatrix} : \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in S_n\right\} = \{j \circ \alpha : \alpha \in S_n\}$$

and it follows

$$\{(j \circ \alpha)^\sigma : \alpha \in S_n\} = \{j \circ \alpha : \alpha \in S_n\}$$

Finally, the Q-expansion of s_m lies in $\mathbb{Z}[\zeta_n] \cap \mathbb{Q} = \mathbb{Z}$ and, since we already know that it also admits a q-expansion, we find $s_m \in \mathbb{Z}[[q, q^{-1}]]$.

Fourth step: $s_m \in \mathbb{Z}[j]$. Thanks to the previous two steps we only need to prove that

$$\mathbb{C}[j] \cap \mathbb{Z}[[q, q^{-1}]] = \mathbb{Z}[j]$$

If f is an element of the former, we can write

$$f = a_d j^d + ... + a_0 \in \mathbb{C}[j]$$

Now, for any $k = 0, ..., d$, the polynomial $a_k j^k + ... + a_0$ belongs to $\mathbb{Z}[[q, q^{-1}]]$ and, thanks to the q-expansion of j, it implies that $a_k \in \mathbb{Z}$ for any $k = 0, ..., d$. □

Thanks to the proposition we find that there exists a polynomial

$$G_n(X, Y) \in \mathbb{Z}[X, Y]$$

such that $G_n(X, j) = F_n(X)$. We also set $H_n(X) := G_n(X, X)$. Before proving the main result we need two more lemmas.

Lemma 5.4. *$j \circ \beta$ is integral over $\mathbb{Z}[j]$ for any $\beta \in M_2(\mathbb{Z})$ of positive determinant.*

Proof. If $\beta \in D_n$, there exists $\gamma \in SL_2(\mathbb{Z})$ such that $\gamma\beta \in S_n$. Now

$$0 = F_n(j \circ \gamma\beta) = F_n(j \circ \beta)$$

and the statement follows because F_n is monic with coefficients in $\mathbb{Z}[j]$. □

Lemma 5.5. *H_n is non constant and with leading coefficient ± 1 whenever n is not a perfect square.*

Proof. We fix $\alpha = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in S_n$, $\zeta_n = e^{\frac{2\pi i}{n}}$ and $Q = q^{\frac{1}{n}}$. We observe that

$$j - j \circ \alpha = (Q^{-n} + \sum_{k=0}^{\infty} c_k Q^{nk}) - (\zeta_n^{-ab} Q^{-a^2} + \sum_{k=0}^{\infty} c_k \zeta_n^{abk} Q^{a^2 k})$$

By hypotesis n is not a perfect square and so the leading terms do not cancel. Then the Q-expansion of $F_n(j, j)$ has terms with negative powers of Q and the leading coefficient is a root of unity, hence ± 1 since we know it has coefficients in $\mathbb{Z}$. Anyway, $F_n(j, j)$ also admits a q-expansion and thanks to the form of the q-expansion of j we can conclude. □

Finally, we can prove the following.

Theorem 5.1. *If E is a complex elliptic curve with complex multiplication then the j-invariant $j(E)$ is an algebraic integer.*

Proof. We set $\mathcal{O} := End(E)$ and we assume it is an order of the imaginary quadratic field K. We distinguish two cases.
First case: $\mathcal{O} = \mathcal{O}_K$. We choose $\rho \in \mathcal{O}_K$ in the following way:

- $\rho = 1 + i$ if $K = \mathbb{Q}(i)$;
- $\rho = \sqrt{-D}$ if $K = \mathbb{Q}(\sqrt{-D})$ with D a positive square-free integer.

Then $n := |N_{K/\mathbb{Q}}(\rho)|$ is not a perfect square. Thanks to the Uniformization Theorem we can choose $\tau \in \mathbb{H}$ such that $j(\tau) = j(E)$. Now, $\rho[1, \tau] \subset [1, \tau]$ and, since

$$[[1,\tau] : [\rho, \rho\tau]] = \frac{Vol([\rho, \rho\tau])}{Vol([1,\tau])} = \frac{det\begin{pmatrix} \rho_x & \rho_x\tau_x - \rho_y\tau_y \\ \rho_y & \rho_x\tau_y + \rho_y\tau_x \end{pmatrix}}{det\begin{pmatrix} 1 & \tau_x \\ 0 & \tau_y \end{pmatrix}}$$

$$= \frac{\rho_x^2\tau_y + \rho_y^2\tau_y}{\tau_y} = |\rho|^2 = n$$

there exist $a, b, c, d \in \mathbb{Z}$ such that

$$\rho\tau = a\tau + b$$

$$\rho = c\tau + d$$

and $\alpha := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in D_n$. Finally

$$H_n(j(E)) = F_n(j(E), j(E)) = F_n(j(\alpha\tau), j(\tau)) = 0$$

and it proves the claim because H_n lies in $\mathbb{Z}[x]$ and its leading coefficient is ± 1.
Second case: $\mathcal{O}$ is a generic order of K.
If we write $\mathcal{O} = [\omega_1, \omega_2] \subset \mathcal{O}_K = [1, \tau]$, then there exist $a, b, c, d \in \mathbb{Z}$ such that

$$\omega_1 = a\tau + b$$

$$\omega_2 = c\tau + d$$

and $\alpha := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in D_n$ with $n > 0$. Finally, we know that $j(E) = j(\alpha\tau)$ is integral over $\mathbb{Z}[j(\tau)]$ and we can conclude since, from the previous case, $j(\tau)$ is integral over $\mathbb{Z}$. □

5.4 The Chebotarev Density Theorem and other preliminaries

For the following proofs we need to introduce the Dirichlet density of a set of finite primes.

Definition 5.5. *Let K be a number field and S a set of finite primes of K. Then the Dirichlet density of S is*

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

It is possible to prove that if S is finite then $\delta(S) = 0$ (see [2, pag. 169]). We will use the following result, known as Chebotarev Density Theorem.

Theorem 5.2. *If L/K is a Galois extension of number fields and*

$$S = \{\mathfrak{p} : \mathfrak{p}\ finite\ prime\ of\ K,\ \mathfrak{p}\ unramified\ in\ L,\ (\mathfrak{p}, L/K) = \langle\sigma\rangle\}$$

where $\langle\sigma\rangle$ is the conjugacy class of $\sigma \in Gal(L/K)$, then

$$\delta(S) = \frac{|\langle\sigma\rangle|}{[L:K]}$$

Proof. See [2, Theorem 8.17, pag. 170]. □

Two other important results that will be used in the sequel are stated in the following proposition.

Proposition 5.7. *Let K be a quadratic imaginary number field and $\mathcal{O}$ an order in it. Then:*

- *if $n \in \mathbb{N}$ then any class of $Pic(\mathcal{O})$ contains a proper $\mathcal{O}$-ideal with norm that is prime to n;*
- *any class of $Pic(\mathcal{O})$ contains infinitely many ideals of prime norm.*

Proof. For the first result see [2, Corollary 7.17, pag. 142]. For the second one see [14, Lecture 20, Theorem 20.11, pag. 6]. □

5.5 Ring class fields

In order to state the first main theorem of complex multiplication we need to introduce the notion of ring class field for imaginary quadratic fields. The idea behind this concept is to extend the definition of Hilbert class field, which is naturally associated to the ideal class group of $\mathcal{O}_K$, to non-maximal orders. We fix an imaginary quadratic field K. First of all, if $f \in \mathbb{Z}$, we

define $P_{K,\mathbb{Z}}(f)$ as the subgroup of $I_{K,(f)}$ generated by the principal ideals $\alpha\mathcal{O}_K$ such that there exists a positive integer a coprime with f which satisfies $\alpha \equiv amodf\mathcal{O}_K$. It is immediate to see that $P_{K,\mathbb{Z}}(f)$ is a congruence subgroup modulo (f), i.e. it contains $K_{(f),1}$.

Definition 5.6. *Let K be an imaginary quadratic field and $\mathcal{O}$ an order of conductor f in K. The **ring class field** of $\mathcal{O}$ is denoted by $R_{\mathcal{O}}$ and it is defined as the abelian extension associated to the congruence subgroup $P_{K,\mathbb{Z}}(f)$ by the existence theorem.*

It is immediate to observe that the ring class field of $\mathcal{O}_K$ is just the Hilbert class field, i.e. $R_{\mathcal{O}_K} = H_K$. We can also observe that the primes of K which ramify in $R_{\mathcal{O}}$ divide the conductor of $\mathcal{O}$.

Proposition 5.8. *Let K be an imaginary quadratic field and $\mathcal{O}$ an order of conductor f in K. Then we have an isomorphism*

$$Pic(\mathcal{O}) \cong I_{K,(f)}/P_{K,\mathbb{Z}}(f)$$

Proof. We say that an $\mathcal{O}$-ideal $\mathfrak{a}$ is coprime with f if $\mathfrak{a} + f\mathcal{O} = \mathcal{O}$ and we observe that it implies that $\mathfrak{a}$ is proper. Indeed, if $\alpha \in K$ and $\alpha\mathfrak{a} \subset \mathfrak{a}$ we have

$$\alpha\mathcal{O} = \alpha(\mathfrak{a} + f\mathcal{O}) = \alpha\mathfrak{a} + \alpha f\mathcal{O} \subset \mathfrak{a} + f\mathcal{O}_K \subset \mathcal{O}$$

We denote by $I(\mathcal{O}, f)$ the subgroup of $I(\mathcal{O})$ generated by the $\mathcal{O}$-ideals that are coprime with f and by $P(\mathcal{O}, f)$ its subgroup of principal fractional $\mathcal{O}$-ideals. We will prove the statement through a chain of isomorphisms

$$I_{K,(f)}/P_{K,\mathbb{Z}}(f) \cong I(\mathcal{O}, f)/P(\mathcal{O}, f) \cong I(\mathcal{O})/P(\mathcal{O}) = Pic(\mathcal{O})$$

We define

$$A := \{\mathcal{O}_K - ideals\, prime\, to\, f\}$$

$$B := \{\mathcal{O} - ideals\, prime\, to\, f\}$$

$$F : A \to B,\ F(\mathfrak{a}) = \mathfrak{a} \cap \mathcal{O}$$

$$G : B \to A,\ G(\mathfrak{a}) = \mathfrak{a}\mathcal{O}_K$$

We prove that:

- F is well-defined. If $\mathfrak{a} \in B$, we observe that $\mathfrak{a} + f\mathcal{O} = \mathcal{O}$ if and only if the multiplication by f from $\mathcal{O}/\mathfrak{a}$ to itself is an isomorphism, i.e. if and only if f and $N(\mathfrak{a})$ are coprime. Then, if $\mathfrak{a} \in A$, the obvious injection

  $$\mathcal{O}/\mathcal{O} \cap \mathfrak{a} \hookrightarrow \mathcal{O}_K/\mathfrak{a}$$

  tells us that $\mathfrak{a} \cap \mathcal{O} \in B$.

- G is well-defined. If $\mathfrak{a} \in B$, then

$$\mathfrak{a}\mathcal{O}_K + f = (\mathfrak{a} + f\mathcal{O})\mathcal{O}_K = \mathcal{O}\mathcal{O}_K = \mathcal{O}_K$$

- $G \circ F = id_A$. If $\mathfrak{a} \in A$ we have

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

  The other inclusion is trivial.

- $F \circ G = id_B$. If $\mathfrak{a} \in B$ we have

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

  The other inclusion is trivial.

- G is multiplicative: it is obvious.

Then, the map F can be extended to an isomorphism

$$\bar{F} : I_{K,(f)} \to I(\mathcal{O}, f)$$

In order to get the first isomorphism we just need to prove that

$$\bar{F}(P_{K,\mathbb{Z}}) = P(\mathcal{O}, f)$$

or, equivalently,

$$\alpha\mathcal{O}_K \in P_{K,\mathbb{Z}}(f) \Leftrightarrow \alpha \in \mathcal{O},\ N(\alpha)\ prime\ to\ f$$

If $\alpha \in \mathcal{O}_K$, $\alpha \equiv a\ mod\ f\mathcal{O}_K$, $a \in \mathbb{Z}$ coprime with f, then $N(\alpha) \equiv a^2\ mod\ f$ and it implies $gcd(N(\alpha), f) = gcd(a^2, f) = 1$. The implication ($\Rightarrow$) is proved since we have also $f\mathcal{O}_K \subset \mathcal{O}$ and so $\alpha \in \mathcal{O}$. For the converse we assume $\mathcal{O} = [1, fw]$ and so there exists $a \in \mathbb{Z}$ such that $\alpha \equiv a\ mod\ f\mathcal{O}_K$. Then $gcd(a, f) = 1$ because $gcd(N(\alpha), f) = 1$ and $N(\alpha) \equiv a^2\ mod\ f$, so the claim is proved.
Now, we define

$$H : I(\mathcal{O}, f)/P(\mathcal{O}, f) \to I(\mathcal{O})/P(\mathcal{O}),\ H([\mathfrak{a}]) = [\mathfrak{a}]$$

We prove that:

- H is a well-defined group homomorphism. It is obviously a group homomorphism and it is well-defined since $P(\mathcal{O}, f) \subset P(\mathcal{O})$.

- H is injective. It follows from the equality

$$P(\mathcal{O}, f) = I(\mathcal{O}, f) \cap P(\mathcal{O})$$

The inclusion ($\subset$) is trivial. For the opposite direction we consider $\alpha\mathcal{O} = \mathfrak{a}\mathfrak{b}^{-1} \in I(\mathcal{O}, f) \cap P(\mathcal{O}, f)$ where $\alpha \in K$ and $\mathfrak{a}$ and $\mathfrak{b}$ are $\mathcal{O}$-ideals prime to f. If $m = N(\mathfrak{b})$ we have

$$m\alpha\mathcal{O} = m\mathfrak{a}\mathfrak{b}^{-1} = \mathfrak{a} \cdot m\mathfrak{b}^{-1} = \mathfrak{a}\bar{\mathfrak{b}} \subset \mathcal{O}$$

which implies $m\alpha\mathcal{O} \in P(\mathcal{O}, f)$. Then the same holds for

$$\alpha\mathcal{O} = (m\alpha\mathcal{O})(m\mathcal{O})^{-1}$$

- H is surjective. It follows from the fact that any class of $Pic(\mathcal{O})$ contains an ideal with norm that is prime to f.

□

5.6 The first main theorem of complex multiplication

The purpose of this section is to prove the first main theorem of complex multiplication which gives a concrete construction of ring class fields of imaginary quadratic fields in terms of the j-invariants of suitable elliptic curves.

Theorem 5.3. *If E is a complex elliptic curve with $End(E) \cong \mathcal{O}$ where $\mathcal{O}$ is an order in an imaginary quadratic field K, then $R_{\mathcal{O}} = K(j(E))$.*

Corollary 5.1. *If E is a complex elliptic curve with $End(E) \cong \mathcal{O}_K$ where K is an imaginary quadratic field, then $H_K = K(j(E))$.*

We fix an imaginary quadratic field K and an order $\mathcal{O}$ in it. We set

$$Ell_{\mathcal{O}}(\mathbb{C}) := \{j(E) : E/\mathbb{C}\, elliptic\, curve,\ End(E) \cong \mathcal{O}\}$$

Now, we want to define an action of $Pic(\mathcal{O})$ on $Ell_{\mathcal{O}}(\mathbb{C})$ in the following way: from the Uniformization Theorem and the results on proper ideals we know that if E is an elliptic curve over $\mathbb{C}$ with $End(E) \cong \mathcal{O}$ then there exists a proper fractional $\mathcal{O}$-ideal $\mathfrak{b}$ such that $E = E_{\mathfrak{b}}$. Now, if $\mathfrak{a}$ is a proper fractional $\mathcal{O}$-ideal, we set

$$[\mathfrak{a}] \cdot j(E_{\mathfrak{b}}) := j(E_{\mathfrak{a}^{-1}\mathfrak{b}})$$

where we use the square brackets to indicate classes. Obviously, it is a well-defined group action thanks to the fact that homotetic lattices defines isomorphic elliptic curves. We prove some important properties of this action.

Proposition 5.9. *The action of $Pic(\mathcal{O})$ on $Ell_{\mathcal{O}}(\mathbb{C})$ is free and transitive.*

Proof. The action is free because

$$[\mathfrak{a}] \cdot j(E_{\mathfrak{b}}) = j(E_{\mathfrak{b}}) \Leftrightarrow \mathfrak{a}^{-1}\mathfrak{b} = \lambda\mathfrak{b}, \lambda \in \mathbb{C}^{\times} \Leftrightarrow [\mathfrak{a}] = 1$$

Furthermore, the finite sets $Pic(\mathcal{O})$ and $Ell_{\mathcal{O}}(\mathbb{C})$ have the same cardinality because the map

$$Pic(\mathcal{O}) \to Ell_{\mathcal{O}}(\mathbb{C}),\ [\mathfrak{a}] \mapsto j(E_{\mathfrak{a}})$$

is a bijection thanks to the properties we studied. Then the action is also transitive. □

Before proceeding, we need also to prove the following.

Proposition 5.10. *If E is a complex elliptic curve with complex multiplication by $\mathcal{O}$ and $\sigma \in Aut(\mathbb{C})$, then $j(E^{\sigma}) = j(E)^{\sigma}$ and $End(E^{\sigma}) \cong \mathcal{O}$.*

Proof. The first equality follows immediately from the fact that the j-invariant of E is a rational combination of the coefficients of a Weierstrass equation for E. For the other equality, we observe that for any $\sigma \in Aut(\mathbb{C})$ and if $E = E_{\Lambda}$ for a suitable complex lattice Λ we have $\sigma(E_{\Lambda}) = E_{\sigma(\Lambda)}$. Indeed,

$$g_2(\sigma(\Lambda)) = 60G_4(\sigma(\Lambda)) = \sigma(60)\sigma(G_4(\Lambda)) = \sigma(g_2(\Lambda))$$

and the same holds for g_3. Then

$$\begin{aligned} End(E_{\Lambda}^{\sigma}) &= End(E_{\sigma(\Lambda)}) = \{\alpha \in \mathbb{C} : \alpha\sigma(\Lambda) \subset \sigma(\Lambda)\} \\ &\cong \{\alpha \in \mathbb{C} : \alpha\Lambda \subset \Lambda\} = End(E_{\Lambda}) = \mathcal{O} \end{aligned}$$

□

Now, we define a group homomorphism

$$F : Gal(K^{al}/K) \to Pic(\mathcal{O})$$

in the following way:

$$F(\sigma) \cdot j(E) = j(E^{\sigma})$$

for any $\sigma \in Gal(K^{al}/K)$ and any complex elliptic curve E with $End(E) \cong \mathcal{O}$.

Proposition 5.11. *The function F is well-defined.*

Proof. Thanks to the properties of the action of $Pic(\mathcal{O})$ on $Ell_{\mathcal{O}}(\mathbb{C})$, the values of F are uniquely determined by the given condition. Then we only need to prove that for any two complex elliptic curves E_1 and E_2 with complex multiplication by $\mathcal{O}$ and any proper fractional $\mathcal{O}$-ideal $\mathfrak{a}$ we have

$$j(E_1^{\sigma}) = [\mathfrak{a}] \cdot j(E_1) \Rightarrow j(E_2^{\sigma}) = [a] \cdot j(E_2)$$

We assume that $j(E_2) = [\mathfrak{b}] \cdot j(E_1)$ for a suitable proper fractional $\mathcal{O}$-ideal $\mathfrak{b}$. Then

$$\begin{aligned} j(E_2^\sigma) = j(E_2)^\sigma = ([\mathfrak{b}] \cdot j(E_1))^\sigma = [\mathfrak{b}]^\sigma \cdot j(E_1)^\sigma = [\mathfrak{b}] \cdot j(E_1^\sigma) = [\mathfrak{b}][\mathfrak{a}] \cdot j(E_1) \\ = [\mathfrak{a}][\mathfrak{b}] \cdot j(E_1) = [\mathfrak{a}] \cdot j(E_2) \end{aligned}$$

For a proof of the third equality see [12, Proposition 2.5, pag. 113]. □

We fix a complex elliptic curve E with $End(E) \cong \mathcal{O}$ and we compute

$$\begin{aligned} ker(F) &= \{\sigma \in Gal(K^{al}/K) : F(\sigma) = 1\} \\ &= \{\sigma \in Gal(K^{al}/K) : F(\sigma) \cdot j(E) = j(E)\} \\ &= \{\sigma \in Gal(K^{al}/K) : j(E) = j(E^\sigma)\} \\ &= \{\sigma \in Gal(K^{al}/K) : j(E) = j(E)^\sigma\} = Gal(K^{al}/K(j(E))) \end{aligned}$$

Then, $K(j(E))/K$ is Galois and we can consider F as an injective homomorphism

$$F : Gal(K(j(E))/K) \to Pic(\mathcal{O})$$

In particular, since $Pic(\mathcal{O})$ is an abelian group, we can observe that $K(j(E))/K$ is an abelian extension.

Lemma 5.6. *If $\mathfrak{p}$ is a prime of K which satisfies:*

- *$\mathfrak{p} \cap \mathcal{O}$ is a proper $\mathcal{O}$-ideal of norm p, where p is a prime integer;*
- *p is unramified in K and $\mathfrak{p}$ is unramified in $K(j(E))$;*
- *any element of $Ell_{\mathcal{O}}(\mathbb{C})$ is the j-invariant of an elliptic curve defined by a Weierstrass equation with coefficients in $\mathcal{O}_{K(j(E))}$ and with discriminant that is not divided by any prime $\mathfrak{q}$ of $K(j(E))$ which lies over $\mathfrak{p}$ (i.e., E has good reduction modulo $\mathfrak{q}$);*
- *for every prime $\mathfrak{q}$ of $K(j(E))$ which lies over $\mathfrak{p}$, the elements of $Ell_{\mathcal{O}}(\mathbb{C})$ are distinct modulo $\mathfrak{q}$.*

then $F(\sigma_{\mathfrak{p}}) = [\mathfrak{p} \cap \mathcal{O}]$.

Proof. See [14, Lecture 21, Theorem 21.1, pag. 3]. □

Proposition 5.12. *The map F is surjective.*

Proof. If α is a class in $Pic(\mathcal{O})$, we know that there are infinitely many primes of K such that the first condition of the previous lemma is satisfied and $[\mathfrak{p} \cap \mathcal{O}] = \alpha$. The other conditions of the lemma excludes only finitely many primes, so there exists a prime $\mathfrak{p}$ of K such that

$$F(\sigma_{\mathfrak{p}}) = [\mathfrak{p} \cap \mathcal{O}] = \alpha$$

Then F is surjective. □

Finally we have an isomorphism

$$Gal(K(j(E))/K) \cong Pic(\mathcal{O})$$

In particular, we have that

$$[K(j(E)) : K] = [R_{\mathcal{O}} : K]$$

The next step in the proof is to show that $R_{\mathcal{O}} \subset K(j(E))$ and it will be enough to conclude.
Given a finite extension of number fields L/K we denote by

$$S_{L/K} := \{\mathfrak{p} : \mathfrak{p} \textit{ prime ideal of } K \textit{ which splits completely in } L\}$$

Given two sets A and B we write $A \dot{\subset} B$ if there exists a finite set C such that $A \subset B \cup C$.
We want to prove the following proposition.

Proposition 5.13. *If M/K and L/K are finite extensions of number fields and M/K is Galois, then*

$$S_{M/K} \dot{\subset} S_{L/K} \Rightarrow L \subset M$$

Proof. We denote by L' the Galois closure of L and by N a Galois extension of K which contains M and L'. We also fix $\sigma \in Gal(N/M)$. Thanks to the Chebotarev Density Theorem we can find infinitely many primes $\mathfrak{p}$ of K which are unramified in N and such that there exists a prime $\mathfrak{B}$ of N which lies over $\mathfrak{p}$ and satisfies $(\mathfrak{B}, N/K) = \sigma$. If $\mathfrak{B}' = \mathfrak{B} \cap \mathcal{O}_M$, we have

$$(\mathfrak{B}', M/K) = (\mathfrak{B}, N/K)|_M = \sigma|_M = 1$$

and so $\mathfrak{p} \in S_{M/K}$. Since there are infinitely many primes which satisfy these properties and $S_{M/K} \dot{\subset} S_{L/K} = S_{L'/K}$ (the last equality is a well-known fact), we can assume $\mathfrak{p} \in S_{L'/K}$. It implies

$$\sigma|_{L'} = (\mathfrak{B}, N/K)|_{L'} = (\mathfrak{p}, L'/K) = 1$$

Then $\sigma \in Gal(N/L')$ and it implies $Gal(N/M) \subset Gal(N/L')$. Then $L' \subset M$ and the statement follows. □

Now, we want to use the previous proposition to conclude. We need the following two lemmas.

Lemma 5.7. *It holds*

$$S_{K(j(E))/\mathbb{Q}} \dot{\subset} \{p \in \mathbb{Z} : p \textit{ prime}, \exists \alpha \in \mathcal{O} \textit{ s.t. } p = N(\alpha)\}$$

Proof. Let $p \in S_{K(j(E))/\mathbb{Q}}$ such that it does not divide the conductor of $\mathcal{O}$, it is unramified in $K(j(E))$ and there is a prime $\mathfrak{p}$ of K which lies over p such that $F(\sigma_{\mathfrak{p}}) = [\mathfrak{p} \cap \mathcal{O}]$. With these restrictions we exclude only finitely many primes. Now, since p splits completely in $K(j(E))$, the same holds for $\mathfrak{p}$ and so $\sigma_{\mathfrak{p}} = 1$. Then

$$[\mathfrak{p} \cap \mathcal{O}] = F(\sigma_{\mathfrak{p}}) = F(1) = 1$$

and it implies that $\mathfrak{p} \cap \mathcal{O}$ is a principal $\mathcal{O}$-ideal. Furthermore, since $\mathcal{O}/\mathfrak{p}\cap\mathcal{O}$ injects into $\mathcal{O}_K/\mathfrak{p}$, then

$$N(\mathfrak{p} \cap \mathcal{O}) = [\mathcal{O} : \mathfrak{p} \cap \mathcal{O}] = [\mathcal{O}_K : \mathfrak{p}] = p$$

and the statement is proved. □

Lemma 5.8. *It holds*

$$\{p \in \mathbb{Z} : p \, prime, \, \exists \alpha \in \mathcal{O} \, s.t. \, p = N(\alpha)\} \dot{\subset} S_{R_{\mathcal{O}}/\mathbb{Q}}$$

Proof. Let f be the conductor of $\mathcal{O}$ and fix a prime $p \in \mathbb{Z}$ such that it does not divide f and it is unramified in K. If $p = N(\alpha)$ for a suitable $\alpha \in \mathcal{O}$, then $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$ with $\mathfrak{p} \neq \bar{\mathfrak{p}}$ and $\mathfrak{p} = \alpha\mathcal{O}_K$. It implies $\mathfrak{p} \in P_{K,\mathbb{Z}}(f)$, so $(\mathfrak{p}, R_{\mathcal{O}}/K) = 1$ and $\mathfrak{p}$ splits completely in $R_{\mathcal{O}}$. If τ is the complex conjugation we have that

$$\begin{aligned} ker(\phi_{\tau(R_{\mathcal{O}})/K,f}) &= \tau(ker(\phi_{R_{\mathcal{O}}/K,f})) = \tau(P_{K,\mathbb{Z}}(f)) \\ &= P_{K,\mathbb{Z}}(f) = ker(\phi_{R_{\mathcal{O}}/K,f}) \end{aligned}$$

and so $\tau(R_{\mathcal{O}}) = R_{\mathcal{O}}$ (see [2, Corollary 8.7, pag. 163]). Finally, $R_{\mathcal{O}}/\mathbb{Q}$ is Galois and so p splits completely in $R_{\mathcal{O}}$. □

Thanks to the previous two lemmas we have

$$S_{K(j(E))/\mathbb{Q}} \dot{\subset} S_{R_{\mathcal{O}}/\mathbb{Q}}$$

The extension $K(j(E))/\mathbb{Q}$ is Galois. Indeed, if τ is the complex conjugation, we have $End(E^{\tau}) \cong End(E) \cong \mathcal{O}$ and it implies that

$$j(E)^{\tau} = j(E^{\tau}) \in K(j(E))$$

Finally, we can conclude that $R_{\mathcal{O}} \subset K(j(E))$.

5.7 The second main theorem of complex multiplication

The purpose of the second main theorem of complex multiplication is to describe ray class fields of imaginary quadratic fields. In order to state it we

need to introduce some terminology. If E is a complex elliptic curve with complex multiplication by $\mathcal{O}_K$ we define the set of its torsion points as

$$E_{tors} = \{P \in E : [\alpha](P) = 0,\ \exists\, \alpha \in \mathcal{O}_K\}$$

and, if $\mathfrak{m}$ is an integral ideal of $\mathcal{O}_K$, the set of its $\mathfrak{m}$-torsion points is

$$E[\mathfrak{m}] = \{P \in E : [\alpha](P) = 0\, \forall\, \alpha \in \mathfrak{m}\}$$

Furthermore, if Λ is a complex lattice such that $E = E_\Lambda$ and $\Phi_\Lambda : \mathbb{C}/\Lambda \to E$ is the usual isomorphism, we define the function

$$h : E \to \mathbb{C}$$

in the following way:

- if $j(E) \neq 0, 1728$, $h(\Phi_\Lambda(z)) = \frac{g_2(\Lambda)g_3(\Lambda)}{\Delta(\Lambda)}\wp(z;\Lambda)$
- if $j(E) = 1728$, $h(\Phi_\Lambda(z)) = \frac{g_2(\Lambda)^2}{\Delta(\Lambda)}\wp(z;\Lambda)^2$
- if $j(E) = 0$, $h(\Phi_\Lambda(z)) = \frac{g_3(\Lambda)}{\Delta(\Lambda)}\wp(z;\Lambda)^3$

where $z \in \mathbb{C}$. It is easy to see that h is independent of the choice of Λ.

Theorem 5.4. *Let K be an imaginary quadratic field, $\mathfrak{m}$ a modulus for K and E a complex elliptic curve with complex multiplication such that $End(E) \cong \mathcal{O}_K$. Then*

$$K(\mathfrak{m}) = K(j(E), h(E[\mathfrak{m}]))$$

Proof. See [12, Theorem 5.6, pag. 135]. □

It is immediate to deduce the following computation of the maximal abelian extension of an imaginary quadratic field.

Corollary 5.2. *Let K be an imaginary quadratic field and E a complex elliptic curve with complex multiplication such that $End(E) \cong \mathcal{O}_K$. Then*

$$K^{ab} = K(j(E), h(E_{tors}))$$

Bibliography

[1] J. W. S. Cassels and A. Fröhlich. *Algebraic Number Theory.* Thompson Book Company, 1967.

[2] D. A. Cox. *Primes of the form $x^2 + ny^2$.* Wiley, 1989.

[3] A. Gathmann. *Plain Algebraic Curves.* 2018.

[4] D. Harari. *Galois Cohomology and Class Field Theory.* Springer, 2020.

[5] D. Husemöller. *Elliptic Curves.* Springer, 2004.

[6] J. S. Milne. *Elliptic Curves.* 2006.

[7] J. S. Milne. *Algebraic Number Theory.* 2020.

[8] J. S. Milne. *Class Field Theory.* 2020.

[9] J.S. Milne. *Fields and Galois Theory.* 2022.

[10] J. Neukirch. *Algebraic Number Theory.* Springer, 1967.

[11] J. H. Silverman. *The Arithmetic of Elliptic Curves.* Springer, 1986.

[12] J. H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves.* Springer, 1994.

[13] J.H. Silverman. *Rational Points on Elliptic Curves.* Springer, 2015.

[14] A. Sutherland. Elliptic curves, 2021. MIT course.

[15] A. Sutherland. Number theory 1, 2021. MIT course.