INVERSE GALOIS PROBLEM

by

Eda Kırımlı

B.S., Mathematics, Mimar Sinan Fine Arts University, 2015

Submitted to the Institute for Graduate Studies in
Science and Engineering in partial fulfillment of
the requirements for the degree of
Master of Science

Graduate Program in Mathematics

Boğaziçi University

2018

ACKNOWLEDGEMENTS

In the first place, I would like to express my sincere appreciation to my advisor Assoc. Prof. Ekin Özman. I am deeply grateful for all the time she has devoted me and for all the help and insight she has given me. This thesis would not have been possible without her advice, her perspective, and our weekly meetings. I would also like to thank my jury members Prof. İlhan İkeda and Assist. Prof. Özer Öztürk.

I am deeply thankful my great friends Neslihan Girgin, Melissa Nalbandiyan and Harun Kır for the time we spent together at Boğaziçi University in the last two years. It would be much harder for me to write this thesis without their endless support and encouragement. Also, I would also like to thank the numerous friends and colleagues who have encouraged and guided me over the years. There are too many of these people for me to name. My best friend Tuğçe Nalçakan deserves special thanks with her perfect personality. In addition, I would like express my thanks to my B.Sc. advisor Prof. Ayşe Berkman for enlightening advices and her constant encouragement.

Finally, I wish to express my gratitude to my mother and my twin sister Seda Kırımlı for the love and encouragement they have given me throughout these years. I also would like to emphasize my special thanks to my father since he showed me the beauty of mathematics even when I was a little girl, and I know that he will live in my heart forever.

ABSTRACT

INVERSE GALOIS PROBLEM

The main focus of this thesis is so called Inverse Galois Problem. The statement of the problem is that given a finite group G, does there exist a finite Galois extension $L/\mathbb{Q}$ whose Galois group is G? There has been a great process in the problem, but it is still open. Galois theory is the study of the structure and symmetry of a polynomials or associated field extensions. According to the Fundamental Theorem of Galois Theory, there exists a correspondence between a finite algebraic field extension and its Galois group. But, this correspondence is very complicated in general. Inverse Galois Problem deals with this complexity. We will give an introduction to the Inverse Galois Problem and present some different approaches to construct an extension of $\mathbb{Q}$ that gives a desired Galois group. In particular, we will realize some specific groups as Galois groups, these groups are finite abelian groups, symmetric groups S_n, the general linear group $\mathbb{GL}_2(\mathbb{F}_p)$, and the projective special linear group $\mathbb{PSL}_2(\mathbb{F}_p)$. Finally, we will give a short survey about known results on Inverse Galois Problem.

ÖZET

KARŞIT GALOIS PROBLEMİ

Bu tezde Karşıt Galois Problemini inceleyeceğiz. Karşıt Galois problemi şu soruyu sorar: Verilen bir sonlu grup için öyle bir Galois genişlemesi var mıdır ki bu Galois genişlemesine karşılık gelen Galois grubu verilen sonlu grup olsun? Problemle ilgili birçok sonuç elde edilmesine rağmen hala açık bir problemdir. Galois teori, polinomların ve cisim genişlemelerin simetrileri ve yapılarını inceler. Galois'in Temel Teoremine göre sonlu cebirsel cisim genişlemeleri ile bu genişlemeye karşılık gelen Galois grup arasında bir karşılıklılık vardır. Fakat, bu karşılıklılık genelde çok karışıktır. Karşıt Galois Problemi bu zorlukla ilgilenir. Bu tezde Karşıt Galois Problemini tanıtacağız ve Galois genişlemesi inşa etmek için farklı çözüm metodlarını vermeye çalışacağız. Galois grubu olarak elde edeceğimiz gruplar şunlardır; sonlu değişmeli gruplar, simetrik gruplar S_n, genel lineer gruplar $\mathbb{GL}_2(\mathbb{F}_p)$ ve projektif özel liner gruplar $\mathbb{PSL}_2(\mathbb{F}_p)$. Son olarak problem hakkında bilinen sonuçları derleyeceğiz.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF SYMBOLS

$Aut(E)$	Automorphism group of an elliptic curve E
$\mathcal{B}$	A basis of L over K
C	A curve C
C/K	A curve C defined over a field K
CM	Complex multiplication
$\hat{\mathbb{C}}$	$\mathbb{C} \cup \{\infty\}$
$\mathbb{C}(\Lambda)$	The set of elliptic functions
$Cl(\mathcal{O})$	The ideal class group of an order $\mathcal{O}$
D	Fundamental domain
$D_{\mathfrak{q}/\mathfrak{p}}$	Decomposition group of $\mathfrak{q}$ over $\mathfrak{p}$
$deg(\phi)$	Degree of the map ϕ
e_i	The ramification index of $\mathfrak{q}_i$ over the ideal $\mathfrak{p}$
E	Elliptic curve
$E(K)$	The group of K-rational points of an elliptic curve E over K
E_Λ	The complex elliptic curve isomorphic to $\mathbb{C}/\Lambda$
E_{tors}	The torsion subgroup of an elliptic curve E
$Ell_{\mathbb{C}}(\mathcal{O})$	Isomorphism class of elliptic curves over $\mathbb{C}$ with $End(E) \simeq \mathcal{O}$
$E[m]$	m-torsion subgroup of the elliptic curve E
$End(E)$	Endomorphism ring of the elliptic curve E
f_i	The resudial degree (or inertia degree) of $\mathfrak{q}_i$ over the ideal $\mathfrak{p}$
$\mathbb{F}_p$	The finite field of p elements
$G_{2k}(\Lambda)$	The Eisenstein series of weight $2k$
$h(\mathcal{O})$	The class number of $\mathcal{O}$
$H^0(Gal(\overline{K}/K), M)$	The 0-th cohomology group of a $Gal(\overline{K}/K)$-module M
$H^1(Gal(\overline{K}/K), M)$	The 1-th cohomology group of a $Gal(\overline{K}/K)$-module M
$Isom(C)$	The group of $\overline{K}$-isomorphisms from C to itself
$I_{\mathfrak{q}/\mathfrak{p}}$	Inertia group of $\mathfrak{q}$ over $\mathfrak{p}$
$\mathcal{H}$	Upper half plane

j	The j-invariant of an elliptic curve E
$\overline{K}$	Algebraic closure of a field K
K^*	Multiplicative group of a field K
$K(E)$	Function field of an elliptic curve E
$\mathcal{R}(z)$	Real part of a complex number z
$[m]$	Multiplication-by-m map
$N(I)$	Norm of an ideal I
O	The identity element of an elliptic curve
$\mathcal{O}$	An order in a quadratic field K
$\mathcal{O}_K$	The ring of integers of a field K
$\mathbb{P}^2$	Projective 2-space
$\mathfrak{p}$	An ideal of a field K
$\mathfrak{q}$	An ideal of a field L
$S_0(N)$	Moduli space for $\Gamma_0(N)$
$\mathbb{SL}_2(\mathbb{Z})$	Modular group
w_N	Atkin-Lehner involution
$X_0(N)$	Compact modular curve for $\Gamma_0(N)$
$X_1(N)$	Compact modular curve for $\Gamma_1(N)$
$X(N)$	Compact modular curve for $\Gamma(N)$
Δ	Discriminant of Weierstrass equation
$\Gamma_0(N)$	Congruence subgroup of level N
$\Gamma_1(N)$	Congruence subgroup of level N
$\Gamma(N)$	Principal congruence subgroup of level N
Λ	Lattice
$\wp(z;\Lambda)$	The Weierstrass $\wp$-function
μ_n	The group of n-th roots of unity
ξ	1-cocycle
ξ_n	Primitive n-th roots of unity
ρ_n	Galois representation
$\hat{\phi}$	The dual isogeny of ϕ

$\varphi(n)$	Euler φ-function
ψ	Division polynomial
ω	The invariant differential of E
$\left(\frac{\cdot}{\cdot}\right)$	Legendre symbol

1. INTRODUCTION

Galois theory demonstrates the connection between polynomials, field extensions and groups. Galois groups were first explored by their namesake Evariste Galois in the early 1800's. If we are interested in polynomials over a field K, any separable polynomial can be associated with its splitting field L and its Galois group $Gal(L/K)$ formed by the field automorphisms that permute the roots of the polynomial. Then, the Fundamental Theorem of Galois Theory states that subfields of the field extension L/K correspond bijectively with subgroups the Galois group $Gal(L/K)$. The Fundamental Theorem of Galois Theory was published in the 1840's after Galois' death.

Galois theory has a variety of applications from coding theory to differential equations. Many of these applications show the benefit to study the action of one object on another object in order to get information about the structure of both of these objects. The most well-known application of Galois Theory is the solvability of polynomials by radicals. It shows that a polynomial of degree 5 or higher is not solvable by radicals in general, which was proved by Galois. To be precise, he showed that a polynomial is solvable by radicals if and only if its Galois group is solvable.

According to the Fundamental Theorem of Galois Theory, there exists a correspondence between a finite algebraic field extension and its Galois group. Unfortunately, this correspondence is mostly very complicated. Mathematicians can solely compute the Galois group of a separable polynomial up to degree 15 by using today's powerful computer algebra softwares. The Galois group of a separable polynomial can be identified with the permutation group of the roots of the polynomial. This means that a Galois group of a polynomial of degree n can be seen as a subgroup of S_n. But, a correspondence between a polynomial of degree n and subgroups of its Galois group can be understood completely only for small integers n.

The Inverse Galois Problem deals with this complexity. Since it is very difficult to consider a general separable polynomial of degree n, for a large integer n, Inverse Galois Problem asks the converse of the question for specific base field: Is it possible to realize any finite group as a Galois group of a Galois extension of $\mathbb{Q}$?

The main focus of this thesis is Inverse Galois Problem. More precisely, given a finite group G, does there exist a finite Galois extension $L/\mathbb{Q}$ whose Galois group is G? It is a very natural question, even an undergraduate student who has studied Galois theory can ask Inverse Galois problem. David Hilbert considered this problem firstly, and he gave a solution in his paper [1] when the group G is S_n or A_n for any integer n. In general, it is simpler to construct a field extension which gives a desired Galois group. On the other hand, if we require a specific base field of an extension, like $\mathbb{Q}$, the problem becomes much harder.

In this thesis, we will not only introduce the Inverse Galois Problem in a comprehensible manner, but also present different approaches to construct Galois extensions whose Galois groups give a desired finite group. The thesis is organized as follows:

In Chapter 2, we will summarize Galois theory briefly, and give main definitions and theorems of Galois theory which are cited from the book [2].

In Chapter 3, we will realize finite abelian groups as Galois groups. For this aim, some basic definitions and tools about cyclotomic extensions will be given in the first section, and the main result will be proven in the second section.

In Chapter 4, symmetric group S_n for any integer n will be constructed as a Galois group of a Galois extension. We will firstly summarize algebraic number theory by using the books [3] and [4]. Then, we will prove that S_n can be seen as a Galois group by using given algebraic number theory tools in the second section.

In Chapter 5, our aim is to express the general linear group $\mathbb{GL}_2(\mathbb{F}_p)$ with entries in the finite field $\mathbb{F}_p$ as a Galois group. We will focus on elliptic curves and give all necessary definitions and theorems about elliptic curves in the first section, most of them are cited from the book [5]. In the second section, we will use the paper of Nuria Vila [6] in order to realize $\mathbb{GL}_2(\mathbb{F}_p)$ as a Galois group.

In Chapter 6, the projective special linear group $\mathbb{PSL}_2(\mathbb{F}_p)$ with entries in the finite field $\mathbb{F}_p$ will be seen as a Galois group. We need to define twists of curves, modular curves, orders, complex multiplication etc. in order to prove the main theorem. In the first section, we will define these objects and tools, they are mostly cited from the books [5], [7], and [8]. Then, we will use the paper [9] of Pete L. Clark to obtain $\mathbb{PSL}_2(\mathbb{F}_p)$ as a Galois group.

In Chapter 7, we will give a short survey of known results on Inverse Galois Problem, and present some significant methods that are frequently used on the problem.

2. PRELIMINARIES

In this chapter, our aim is to summarize Galois theory briefly. For this reason, we will give main definitions and theorems of Galois theory which will be used frequently in the following chapters. For more detailed explanations of these results and their proofs, we will refer the reader to Chapters 13 and 14 in [2].

2.1. Algebraic Extensions

Definition 2.1. *An element $\alpha \in L$ is said to be algebraic over K if $f(\alpha) = 0$ for some nonzero polynomial $f(x) \in K[x]$. If α is not algebraic over K, then α is called transcendental over K.*

Proposition 2.2. [2, Proposition 13.2.9.] *There exists a polynomial $m_\alpha(x) \in K[x]$ for any algebraic element α satisfying the following conditions:*

(i) $m_\alpha(x)$ *is a monic polynomial in* $K[x]$.
(ii) α *is a root of* $m_\alpha(x)$, *i.e.* $m_\alpha(\alpha) = 0$.
(iii) If $p(x)$ *is another polynomial in* $K[x]$ *satisfying* $p(\alpha) = 0$, *then* $deg(p(x)) \geq deg(m_\alpha(x))$. *In particular, we obtain* $m_\alpha(x) \mid p(x)$.

Definition 2.3. *Let $\alpha \in L$. If α is an algebraic element over K, the polynomial $m_\alpha(x)$ in Proposition 2.2 is called the minimal polynomial of α.*

Definition 2.4. *A field extension L/K is said to be algebraic, if each element of L is algebraic over K.*

Theorem 2.5. [2, Proposition 13.2.12.] *Any finite algebraic field extension is simple.*

Definition 2.6. *A field F is called algebraically closed if every nonconstant polynomial $f(x) \in F[x]$ has a root in F. In other words, a field F is algebraically closed if and only if every polynomial in $F[x]$ factors completely into linear polynomials.*
An extension field L of K is an algebraic closure of K when L is an algebraically closed field.

Proposition 2.7. [2, PROPOSITION 13.4.30.] *Every field F has an algebraic closure.*

Theorem 2.8. [2, THEOREM 14.6.35.] *The field of complex number $\mathbb{C}$ is algebraically closed.*

We will denote an algebraic closure of K by $\overline{K}$. In this thesis, we will only consider finite extensions L/K. Thus, any extension field L of K is a subfield of $\overline{K}$.

2.2. Normal Extensions, Separable Extensions, and Perfect Fields

Definition 2.9. *Let L/K be a field extension and let $f(x)$ be a nonconstant polynomial in $K[x]$. The polynomial $f(x)$ splits in L, if $f(x)$ factors completely into linear factors in $L[x]$.*
A field L is called the splitting field of $f(x)$ if $f(x)$ splits in L and it does not split completely in any proper subfield of L.

Theorem 2.10. [2, THEOREM 13.4.25.] *Let F be a field and let $f(x)$ be a polynomial in $F[x]$, i.e. $f(x) \in F[x]$. There exists an extension K of F which is a splitting field of $f(x)$.*

Definition 2.11. *Let L/K be an algebraic field extension and let L be a splitting field of a polynomial $f(x) \in K[x]$. Then L is called a normal extension of K.*

Definition 2.12. *Let F be a field. A polynomial $f(x) \in F[x]$ is separable if it has no multiple roots. A polynomial is called nonseparable if it is not separable.*

Proposition 2.13. [2, PROPOSITION 13.5.33.] *A polynomial $f(x)$ is separable if and only if it is relatively prime to its derivative $f'(x)$, i.e. $gcd(f(x), f'(x)) = 1$.*

Definition 2.14. *Let L/K be an algebraic field extension. An element β of L is a separable element if its minimal polynomial is a separable.*
Let L/K be an algebraic field extension. The field L is said to be separable over K if each element of L is a root of a separable polynomial in $K[x]$.
Let F be a field. The field K is called a perfect field if every algebraic extension of F is a separable extension.

2.3. Galois Extensions

Definition 2.15. *Let F be a field. An isomorphism σ from F to F is called an automorphism of F. The set of all automorphisms of F is denoted by $Aut(F)$.*
Let L be a field. An automorphism σ is said to fix a subset K of L, if all the elements of K are fixed by σ, i.e. $\sigma(a) = a$ for all $a \in K$. The set of automorphisms fixing K is generally denoted by $Aut(L/K)$.

Definition 2.16. *Let L be a field and let $Aut(L)$ be the set of automorphisms of L. Let H be a subgroup of automorphism group $Aut(L)$. Then the subfield of L which is fixed by elements of H is called the fixed field of H. Precisely, the fixed field of H is given by*

$$L^H := Fix(H) := \{k \in L \mid \sigma(k) = k \text{ for all } \sigma \in H\}.$$

Definition 2.17. *Let L be an algebraic extension of K. The field L is said to be a Galois extension of K if $\mid Aut(L/K) \mid = [L : K]$.*

Definition 2.18. *A Galois group is a group of field automorphisms under composition, that is, the set of automorphisms σ of L such that $\sigma(x) = x$ for every $x \in K$. It is denoted by $Gal(L/K)$.*

Theorem 2.19. [2, Theorem 14.2.13.] *Let L/K be a finite field extension. Then the following statements are equivalent.*

(i) *L/K is a Galois extension.*
(ii) *L/K is a normal and separable field extension.*
(iii) *L is the splitting field of a separable polynomial $f(x) \in K[x]$.*

Before moving on the next theorem, let us give a new notation about the Galois group. If $f(x)$ is a separable polynomial in $K[x]$, then $Gal(f(x))$ is defined as the Galois group of the splitting field of the polynomial $f(x)$.

Theorem 2.20. [2, THEOREM 14.2.14.] *Let L/K be a finite Galois extension and let G be the Galois group of the Galois extension L/K. Then,*

(i) There is a one-to-one correspondence between intermediate fields M of the extension L/K, $K \subseteq M \subseteq L$ and subgroups H of the Galois group G, $\{Id\} \subseteq H \subseteq G$ given by

$$M = Fix(H) = L^H.$$

(ii) H is a normal subgroup of G if and only if an intermediate field $K \subseteq M \subseteq L$ is a normal extension of K. This case happens if and only if M/K is a Galois extension. In particular, we obtain an isomorphism of groups in this case given by $Gal(M/K) = G/H$.

(iii) We obtain $[M : K] = [G : H]$ and $[L : M] =\mid H \mid$ for each subfield $K \subseteq M \subseteq L$.

Finally, we introduce Galois Theory generalized to infinite extensions.

Definition 2.21. *A field extension L/K is said to be Galois if it is algebraic, normal and separable. In this case, $Aut(L/K)$ is said to be the Galois group of the extension and is denoted by $Gal(L/K)$.*

Definition 2.22. *Let G be a group. The group G is called a topological group if G has a topology in which the following maps $(g, h) \mapsto gh$ and $g \mapsto g^{-1}$ are continuous maps.*

Let L/K be a finite Galois extension. We can give a topological structure to the Galois group $Gal(L/K)$, namely the discrete topology. As we have seen in Theorem 2.20, there exists a bijective correspondence between intermediate fields of L/K and subgroups of $Gal(L/K)$. Unfortunately, this theorem does not hold for infinite Galois extensions in general.

Now, let L/K be a field extension (not necessarily finite). In this case, the group $Gal(L/K)$ is just the group of automorphisms $\sigma : L \to L$ fixing the field K. We should define a topology on infinite Galois groups in order to give Fundamental Theorem of Galois Theory for infinite Galois extensions.

Theorem 2.23. [2, KRULL] *Let L/K be a Galois extension with Galois group $Gal(L/K)$. In order to topologize G, a base is taken for the closed sets such that the subgroups of G which are fixing subgroups of the finite extensions of K in L. This topology is called Krull topology on $Gal(L/K)$. The closed subgroups of $Gal(L/K)$ correspond bijectively with the subfields of L containing K with the Krull topology. Also, closed normal subgroups of $Gal(L/K)$ correspond to normal extensions of K in L.*

3. REALIZATION OF ABELIAN GROUPS AS GALOIS GROUPS

The main purpose of this chapter is to see that any abelian group can be realized as a Galois group of a Galois field extension over rational numbers $\mathbb{Q}$. In order to reach our aim, we need to understand structure of the cyclotomic extensions $\mathbb{Q}(\xi_n)$ over rational numbers, where ξ_n is a primitive n-th root of unity for a positive integer n. For this reason, we will study the cyclotomic extension $\mathbb{Q}(\xi_n)$ in detail in the first section of this chapter. Then, we will use cyclotomic extensions in the second section of this chapter to realize any abelian group G as a Galois group over $\mathbb{Q}$.

From now on, we fix an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. Every algebraic field extension K/L is a subfield of $\overline{\mathbb{Q}}$.

Definition 3.1. *Let L, K be fields and let L be a Galois extension field of K. Then L is said to be an abelian extension of K if its Galois group $Gal(L/K)$ is an abelian group.*

3.1. Cyclotomic Extensions

Let us fix a positive integer $n > 0$. We will denote by ξ_n a primitive n-th root of unity in $\overline{\mathbb{Q}}$, i.e. $\xi_n^n = 1$ and $\xi_n^m \neq 1$ for $0 < m < n$. The purpose of this section is to prove that any cyclotomic extension $\mathbb{Q}(\xi_n)$ is a Galois extension. Firstly, we need to verify the existence of n-th roots of unity for any positive integer n. Then, we are going to present some features of the cyclotomic fields $\mathbb{Q}(\xi_n)$.

Definition 3.2. *Let us consider the splitting field of the polynomial $x^n - 1$ over $\mathbb{Q}$. The roots of the polynomial $x^n - 1$ are called the n-th roots of unity.*

We know that every nonzero complex number $a + bi \in \mathbb{C}$ can be written in a unique way of the form $r.e^{i\theta} = r(\cos(\theta) + i\sin(\theta))$ where $r > 0$, $0 \leq \theta < 2\pi$. This formula simply represents the point $a + bi$ of the complex plane in terms of polar coordinates where r is the distance of (a, b) from the origin and θ is the angle with the real positive axis.

There are n distinct solutions of the equation $x^n - 1$ in $\mathbb{C}$. These are the elements $e^{2\pi ki/n} = \cos(2\pi k/n) + i.\sin(2\pi k/n)$ for $k = 0, 1, ...n - 1$. Geometrically, these points are n equally spaced points with starting point $(1, 0)$ on a unit circle in $\mathbb{C}$. All of these points are the n-th roots of unity since $(e^{2\pi ki/n})^n = e^{(2\pi ki/n)n} = e^{2\pi ki} = 1$.

The n-th roots of unity in any field form a group under multiplication. It is easy to see that this group in $\mathbb{C}$ is cyclic due to the analytic formula of them, with generator $e^{2\pi i/n}$. In any field there is no formula, but these roots of unity still form a cyclic group.

Let $K/\mathbb{Q}$ be a field extension such that K is the splitting field of a polynomial $x^n - 1 \in \mathbb{Q}[x]$. Let $a, b \in K$ be the n-th roots of unity. If $a^n = 1$ and $b^n = 1$, then $(ab)^n = a^n b^n = 1$. Also we have $a^{-1} = a^{n-1}$ satisfying $(a^{n-1})^n = (a^n)^{n-1} = 1$. These prove that the collection of n-th roots of unity is a group under multiplication and this subset of K^* is closed under multiplication. Therefore, the n-th roots of unity form a cyclic group. The group of the n-th roots of unity is denoted by μ_n. A generator of the cyclic group of the n-th roots of unity is said to be a *primitive n-th root of unity*.

Fact 3.3. Let ξ_n be a primitive n-th root of unity. The others primitive n-th roots of unity are given by ξ_n^a where a is an integer coprime to n between $1 \leq a < n$ due to the fact that these are the other generators for a cyclic group of order n. In fact, it will be proved in Theorem 3.10 that there are exactly $\varphi(n)$-many primitive n-th roots of unity, where $\varphi(n)$ is the Euler φ-function.

Example 3.4. Let us consider the primitive roots of unity in $\mathbb{C}$ for some small values of n:

$$\xi_1 = 1$$
$$\xi_2 = -1$$
$$\xi_3 = (-1 + i\sqrt{3})/2$$
$$\xi_4 = i$$
$$\xi_6 = (1 + i\sqrt{3})/2$$
$$\xi_8 = \sqrt{2}/2 + i\sqrt{2}$$

Definition 3.5. *The splitting field of the polynomial $x^n - 1$ over $\mathbb{Q}$ is the field $\mathbb{Q}(\xi_n)$. The field $\mathbb{Q}(\xi_n)$ is said to be the cyclotomic field of n-th roots of unity.*

In order to determine the degree of the extension $\mathbb{Q}(\xi_n)$, we need to look at the minimal polynomial of ξ_n over $\mathbb{Q}$. A special case is obtained when $n = p$ is a prime. Consider the factorization of the polynomial $x^p - 1$ as follows;

$$x^p - 1 = (x - 1)(x^{p-1} + x^{p-2} + ... + x + 1)$$

and since $\xi_p \neq 1$, then ξ_p is a root of the following polynomial;

$$\phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + ... + x + 1.$$

The following polynomial is obtained by letting $\phi_p(x) = \phi_p(x + 1)$

$$\begin{aligned}\phi_p(x) = \phi_p(x + 1) &= \frac{\binom{p}{0}x^p + \binom{p}{1}x^{p-1} + ... + px^0 + 1 - 1}{x} \\ &= \frac{x^p + px^{p-1} + \frac{p(p-1)}{2}x^{p-1} + ... + px}{x} \\ &= x^{p-1} + px^{p-2} + ... + p.\end{aligned}$$

Every term in the polynomial $\phi_p(x)$ has p factor. Since p does not divide the leading term, and p^2 does not divide p, we can use Einstein criterion at p. Then, $\phi_p(x)$ is irreducible polynomial. Thus, we get that $\phi_p(x)$ is the minimal polynomial of ξ_p over $\mathbb{Q}$. So, $[\mathbb{Q}(\xi_p) : \mathbb{Q}] = p - 1$.

Definition 3.6. *Let $n \in \mathbb{Z}$ and let μ_n denote the group of n-th roots of unity of the polynomial $\phi(x) = x^n - 1$ over $\mathbb{Q}$. The cyclotomic polynomial $\phi_n(x)$ is defined as a polynomial whose roots are primitive n-th roots of unity;*

$$\phi_n(x) = \prod_{primitive\ \xi\ \in\ \mu_n} (x - \xi) = \prod_{\substack{1 \le a < n \\ (a,n)=1}} (x - \xi_n^a)$$

Let us assume that d is a divisor of n and ξ_d is a d-th root of unity, then ξ_d is also an n-th root of unity since $\xi_d^n = (\xi_d)^{d\frac{n}{d}} = 1$. Thus $\mu_d \subset \mu_n$ for all $d|n$.

Let us consider the factorization of the polynomial $\phi(x) = x^n - 1$ into irreducible factors. In fact, $x^d - 1 \mid x^n - 1$ for all $d|n$. By using Definition 3.6, we obtain $\phi(x) = x^n - 1 = \prod_{d|n} \phi_d(x)$ since every n-th root of unity is actually a primitive d-th root of unity.

Lemma 3.7. [2, Theorem 13.6.41.] *Let n be a positive integer. The cyclotomic polynomial $\phi_n(x)$ is an irreducible monic polynomial in $\mathbb{Z}[x]$ having degree $\varphi(n)$.*

Corollary 3.8. *Let $\mathbb{Q}(\xi_n)/\mathbb{Q}$ be the cyclotomic field of n-th roots of unity. The degree of the extension $\mathbb{Q}(\xi_n)/\mathbb{Q}$ is*

$$[\mathbb{Q}(\xi_n) : \mathbb{Q}] = \varphi(n).$$

Corollary 3.9. *The cyclotomic field $\mathbb{Q}(\xi_n)$ is a Galois extension over $\mathbb{Q}$.*

Proof. We need to show that $f(x) = x^n - 1$ is separable. If it was not, any multiple root of $f(x)$ would be also a root of $f'(x) = n.x^{n-1}$. The only root of $f'(x)$ is 0 since $n \neq 0$ in $\mathbb{Q}$, but 0 is not a root of $f(x)$. This implies that $f(x)$ has n distinct roots, so it is a separable polynomial. Thus, $\mathbb{Q}(\xi_n)$ is a splitting field of a separable polynomial over $\mathbb{Q}$. Therefore, $\mathbb{Q}(\xi_n)/\mathbb{Q}$ is a Galois extension.

□

Theorem 3.10. [2, Theorem 14.5.26.] *Let ξ_n be a primitive n-th root of unity. Let $\mathbb{Q}(\xi_n)/\mathbb{Q}$ be the cyclotomic field of n-th roots of unity. The Galois group of the cyclotomic field $\mathbb{Q}(\xi_n)/\mathbb{Q}$ of n-th roots of unity is isomorphic to the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^*$. The isomorphism is determined explicitly as follows;*

$$\begin{aligned} \psi : &(\mathbb{Z}/n\mathbb{Z})^* \longrightarrow Gal(\mathbb{Q}(\xi_n)/\mathbb{Q}) \\ &a \ mod \ n \mapsto \sigma_a \end{aligned}$$

where $\sigma_a(\xi_n) = \xi_n^a$.

Proof. Any automorphism σ of the cyclotomic field $\mathbb{Q}(\xi_n)/\mathbb{Q}$ is determined by its action on the primitive n-th roots of unity. Indeed, the element ξ_n has to be mapped to another primitive n-th roots of unity. Let σ_a be an automorphism such that $\sigma_a(\xi_n) = \xi_n^a$ for some integer a, $1 \leq a \leq n$, relatively prime to n. Since there are $\varphi(n)$-many such integers a, it shows that every such map is an automorphism of $\mathbb{Q}(\xi_n)/\mathbb{Q}$. Since σ_a is an automorphism, this means that the map ψ is well-defined. Also, the map ψ is a homomorphism as follows

$$(\sigma_a\sigma_b)(\xi_n) = \sigma_a(\xi_n^b) = (\xi_n^b)^a = \xi^{ab} = \sigma_{ab}.$$

The map ψ is bijective since every Galois automorphism has the form of σ_a for a unique a (mod n). Therefore, the map ψ is an isomorphism. □

The degree of the cyclotomic field $\mathbb{Q}(\xi_n)$ of n-th roots of unity over $\mathbb{Q}$ is $\varphi(n)$, i.e. $[\mathbb{Q}(\xi_n) : \mathbb{Q}] = \varphi(n)$. Thus, the following isomorphism is obtained

$$Gal(\mathbb{Q}(\xi_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*.$$

3.2. Abelian Groups as Galois Groups

Theorem 3.11. [2, Theorem 5.2.3.] *(Fundamental Theorem of Finitely Generated Abelian Groups) Let G be a finitely generated abelian group. Then,*
$G \cong \mathbb{Z}^r \times \mathbb{Z}_{n_1} \times ..... \times \mathbb{Z}_{n_k}$ for some integers $r, n_1, n_2, ...n_k$ satisyfing the following conditions:

(i) $r \geq 0$ and $n_j \geq 2$ for all j,
(ii) $n_{i+1} \mid n_i$ for $1 \leq j \leq k-1$.

In other words, every finitely generated abelian group is a direct product of cyclic groups.

Theorem 3.12. [10, Theorem 4.1.2.] *(Dirichlet Theorem) Let $a, N \in \mathbb{Z}$ be relatively prime integers i.e. $gcd(a, N) = 1$. Then, there are infinitely many prime numbers p such that $p \equiv a \ (mod\ N)$ or equivalently $p = a + tN$ for some $t \in \mathbb{N}$.*

Recall that two ideals I, J of a ring A are said to be prime each other, or *coprime*, if $I + J = A$.

Theorem 3.13. [2, Theorem 7.6.17.] *(Chinese Remainder Theorem) Let R be a ring. Let $I_1, ..., I_s$ be ideals of R. The map $R \to R/I_1 \times R/I_2 \times ... \times R/I_s$*
with $r \to (r + I_1, r + I_2, ..., r + I_s)$ is a ring homomorphism with kernel $I_1 \cap I_2 \cap ... \cap I_s$. If for each $i, j \in \{1, 2, ..., k\}$ with $i \neq j$ the ideals I_i and I_j are coprime, then this map is surjective and $I_1 \cap I_2 \cap ... \cap I_s$=$I_1.I_2...I_s$. Therefore,
$R/I_1 \times R/I_2 \times ... \times R/I_s = R/(I_1 \cap I_2 \cap ... \cap I_s) = R/I_1.I_2...I_s$

Corollary 3.14. *Let $m_1, ..., m_r$ be pairwise coprime integers, and let m be an integer such that $m = \prod_{i=1}^{r} m_i$. Then $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/m_1\mathbb{Z} \times ... \times \mathbb{Z}/m_r\mathbb{Z}$.*

Theorem 3.15. [2, PAGE 599-600] *Let G be a finite abelian group. Then G is a Galois group of a Galois extension over $\mathbb{Q}$.*

Proof. Firstly, we will prove that G is isomorphic to a quotient subgroup of $(\mathbb{Z}/M\mathbb{Z})^*$ for some $M \in \mathbb{Z}$. According to Fundamental Theorem of Finitely Generated Abelian Groups, any finite abelian group is isomorphic to a product of cyclic groups such that

$$G = \prod_{i=1}^{s} \mathbb{Z}/m_i\mathbb{Z}.$$

It is known that $(p_i - 1)\mathbb{Z}$ is a normal subgroup of $m_i\mathbb{Z}$ when $m_i|(p_i - 1)$. Let us take a quotient of groups $\mathbb{Z}/(p_i - 1)\mathbb{Z}$ and $m_i\mathbb{Z}/(p_i - 1)\mathbb{Z}$ in order to get
$\mathbb{Z}/(p_i - 1)\mathbb{Z} \ / \ m_i\mathbb{Z}/(p_i - 1)\mathbb{Z}$.

By using Third Isomorphism Theorem, we obtain the following group
$\mathbb{Z}/(p_i - 1)\mathbb{Z} \ /m_i\mathbb{Z}/(p_i - 1)\mathbb{Z} \cong \mathbb{Z}/m_i\mathbb{Z}$. Hence, every cyclic group $\mathbb{Z}/m_i\mathbb{Z}$ is a quotient subgroup of $\mathbb{Z}/(p_i - 1)\mathbb{Z}$. Recall that there exist infinitely many primes such that $p_i \equiv 1 \pmod{m_i}$ by Dirichlet theorem. This implies that we can choose s distinct primes p_i's satisfying $p_i \equiv 1 \pmod{m_i}$ for $1 \leq i \leq s$.

The canonical projection $\mathbb{Z}/(p_i - 1)\mathbb{Z} \to \mathbb{Z}/m_i\mathbb{Z}$ for $1 \leq i \leq s$ gives us the following surjective homomorphism:

$$\pi : \prod_{i=1}^{s} \mathbb{Z}/(p_i - 1)\mathbb{Z} \to G = \prod_{i=1}^{s} \mathbb{Z}/m_i\mathbb{Z}$$

Let us define $M := \prod_{i=1}^{s} p_i$. Since $\mathbb{Z}/p_i\mathbb{Z}$ is a field, we have $(\mathbb{Z}/p_i\mathbb{Z})^*$=$\mathbb{Z}/p_i\mathbb{Z} - \{0\}$. Since both groups are cyclic and have the same cardinality, the multiplicative group $((\mathbb{Z}/p_i\mathbb{Z})^*,.)$ and the additive group $(\mathbb{Z}/(p_i - 1)\mathbb{Z}, +)$ are isomorphic. Then we get the following group isomorphism:

$$\prod_{i=1}^{s} \mathbb{Z}/(p_i - 1)\mathbb{Z} \cong \prod_{i=1}^{s} (\mathbb{Z}/p_i\mathbb{Z})^*.$$

Since all p_i's are distinct prime numbers, they are pairwise relatively prime to each other. Thus, we may apply Chinese Remainder Theorem to deduce the following isomorphism:

$$\prod_{i=1}^{s}(\mathbb{Z}/p_i\mathbb{Z})^* \cong (\mathbb{Z}/M\mathbb{Z})^*.$$

By using the last two isomorphisms and the surjective map π, we conclude that we have constructed a surjective map from $\mathbb{Z}/M\mathbb{Z}$ to the group $G = \prod_{i=1}^{s}\mathbb{Z}/m_i\mathbb{Z}$.

We also know the existence of the isomorphism $Gal(\mathbb{Q}(\xi_M)/\mathbb{Q}) \cong \mathbb{Z}/M\mathbb{Z}$ where ξ_M is the primitive M-th root of unity. By combining all the results above, we get that there exists a surjective homomorphism, namely ψ as follows,

$$\psi : Gal(\mathbb{Q}(\xi_M)/\mathbb{Q}) \to G$$

In particular, we have the following new isomorphism by applying First Isomorphism Theorem

$$Gal(\mathbb{Q}(\xi_M)/\mathbb{Q})\big/ker(\psi) \cong G.$$

By using Fundamental Theorem of Galois Theory, we will finish the proof as below. Let us denote $H = ker(\psi)$ and $F = Fix(H)$. Since $H = ker(\psi)$, H is a normal subgroup of G. According to Theorem 1.34, $F/\mathbb{Q}$ is a Galois extension with Galois group given by

$$Gal(F/\mathbb{Q}) \cong Gal(\mathbb{Q}(\xi_M)/\mathbb{Q})\big/H \cong G.$$

These isomorphisms finish the proof, we have found a Galois extension of $\mathbb{Q}$ with Galois group G as desired. □

Finally, we will state Kronecker-Weber theorem which is one of the earliest results in class field theory. We will omit the proof of Kronecker-Weber theorem since more developed tools of class field theory are needed and this is beyond the scope of this thesis.

Theorem 3.16. [8, THEOREM 2.8.8.] *(Kronecker-Weber Theorem) Every finite abelian extension of* $\mathbb{Q}$ *is contained in a cyclotomic field.*

Notice that Kronecker-Weber Theorem is the converse of Theorem 3.15. These two theorems seem very similar at first sight, but the difference between them is subtle. The first theorem shows that there exists an abelian extension of $\mathbb{Q}$ for a given finite abelian group and this extension is contained in a cyclotomic extension. In other words, the former theorem solely assures existence, but it does not give aany information about other field extensions also giving desired Galois group. This means that there may exist some other extensions of $\mathbb{Q}$ realizing the same Galois group, but not contained in a cyclotomic extension of $\mathbb{Q}$. In fact, Kronecker-Weber theorem guaarantees that this is not possible.

To sum up, combining Theorem 3.15 of this chapter and Kronecker-Weber Theorem, it is concluded that every finite abelian group G can be realized as a Galois group of a Galois extension over $\mathbb{Q}$.

4. SYMMETRIC GROUPS S_n AS GALOIS GROUPS

Our aim in this chapter is to prove that the symmetric group S_n for each positive integer n can be seen as a Galois group. Indeed, we will find a polynomial which will be used to construct a Galois extension over $\mathbb{Q}$ possessing a Galois group isomorphic to S_n. In order to achieve our aim, we need to use some objects and tools in algebraic number theory. In the first section of this chapter, we will examine these necessary objects and tools in detail. Then, we will prove the main theorem in the second section of this chapter.

4.1. Algebraic Number Theory Tools

In what follows, there is a brief summary of number fields and its properties. Before proving the main theorem, we need to define features of ring of integers and ramification theory of field extensions. Proofs of many statements in this section are not given, we refer the reader to [3] and [4] for proofs of theorems and more detailed explanations of statements.

Definition 4.1. *A number field is a subfield of* $\mathbb{C}$ *which has finite degree over* $\mathbb{Q}$.

Example 4.2.

(i) Quadratic number field $\mathbb{Q}(\sqrt{m})$ is a number field of degree 2 over $\mathbb{Q}$ where $m \in \mathbb{Z} - \{0, 1\}$ and m is squarefree.

(ii) Cylotomic field $\mathbb{Q}(\xi_n)$ is a number field of degree $\phi(n)$ where ξ_n is a primitive n-th root of unity and $\varphi(n)$ is an Euler-φ function.

Definition 4.3. *A complex number is said to be an algebraic integer if it is a root of a monic polynomial with coefficients in* $\mathbb{Z}$.
Equivalently, a complex number is called an algebraic integer if it has a minimal polynomial with coefficients in $\mathbb{Z}$.

Example 4.4. Let ξ_n be an n-th root of unity. Since it is a root of the polynomial $x^n - 1 \in \mathbb{Z}[x]$, it is an algebraic integer.

Definition 4.5. *The set of algebraic numbers in $\mathbb{C}$ forms a ring and it is denoted by $\mathbb{A}$. When K is a number field, $K \cap \mathbb{A}$ is called the ring of integers of K, and it is usually denoted by $\mathcal{O}_K$.*

In this chapter, we will denote the ring of integers by A or B instead of $\mathcal{O}_K$ for simplicity.

Definition 4.6. *Let A, B be rings and let A be a subring of B. An element α of B is said to be integral over A if it is a root of a monic polynomial $f(x) \in A[y]$.*
The ring B is said to be an integral extension of A, if each element of B is integral over A.

Definition 4.7. *Let K be a field and let A be a subring of the field K. The integral closure B of A is defined as the ring of elements of K which are integral over A.*
An integral domain is called integrally closed if it is equal to its integral closure in its field of fractions.

4.1.1. Dedekind Domains

Definition 4.8. *An integral domain R is said to be a Dedekind domain if it satisfies the following conditions:*

(i) Every ideal of R is finitely generated.
(ii) Every nonzero prime ideal of R is a maximal ideal.
(iii) R is integrally closed in its field of fractions.

Equivalently, one can define a Dedekind domain as a noetherian integral domain of dimension 1 which is integrally closed in its field of fractions.

Let $S = \{\alpha/\beta : \alpha, \beta \in R,\ \beta \neq 0\ \}$. The last condition in Definition 4.8 asserts that if α/β is a root of a polynomial with coefficients in R, then $\alpha/\beta \in R$, meaning that $\beta \mid \alpha$ in R.

Theorem 4.9. [3, Theorem 3.14.] *Every number field is a Dedekind domain.*

Theorem 4.10. [4, Theorem 6.2.] *Let A be a Dedekind domain with the field of fractions K. Let L/K be a finite separable extension of K. Then the integral closure B of A in L is a Dedekind domain.*

Definition 4.11. *Let A be an integral domain and let K be the field of fractions of A. Let I be an A-submodule of K. Then, I is a fractional ideal of A if $aI \subset A$ for some $a \in A - \{0\}$ and a is said to be the denominator of I. An integral ideal is a fractional ideal with the property $a = 1$.*

Proposition 4.12. [2, Proposition 16.2.9.] *Let A be an integral domain and let K be the field of fractions of A.*

(i) Any finitely generated A-submodule of K is a fractional ideal of A.

(ii) If A is a noetherian domain and I is a fractional ideal of A, then I is a finitely generated A-submodule of K.

(iii) Let I and J be fractional ideals with denominators r and s, respectively. Then $I \cap J$ is also a fractional ideal with denominator r or s, $I.J$ and $I+J$ are fractional ideals with denominator rs.

Proposition 4.13. [3, Theorem 3.15.] *Let A be an integral domain and let K be the field of fractions of A. Let I be a prime ideal of A. Let $J = \{x \in K : xI \subseteq A\}$. Then J is a fractional ideal of A and $IJ = A$. This means that a prime ideal in a Dedekind domain is invertible.*

Theorem 4.14. [4, Theorem 2.8.] *Let A be a Dedekind domain and let $Spec(A)$ be the set of prime ideals of A. Then any nonzero fractional ideal of A can be written uniquely as a product of prime ideals:*

$$I = \prod_{P_i \in Spec(A)} P_i^{e_i}$$

where e_i's are integers and all but finitely many of them are zero.

4.1.2. Trace, Norm and Characteristic Polynomial

Definition 4.15. *Let K be a field. Let L be a K algebra of dimension n. Let $r \in L$ and let multiplication by r map be m_r such that*

$$m_r : \quad L \to L \text{ with } x \to rx.$$

The map m_r is clearly a homomorphism of K-vector spaces. Let M_r denote the matrix of the map m_r for fixed basis $\mathcal{B}$ of L over K.
The map $Norm_{L/K}$: $L \to K$ with $r \to det(m_r) = det(M_r)$ is called norm map from L to K. In particular, the norm map is multiplicative:

$$Norm_{L/K}(rs) = Norm_{L/K}(r)Norm_{L/K}(s) \text{ for all } r, s \in L.$$

The map $Tr_{L/K}$: $L \to K$ with $r \to trace(m_r) = trace(M_r)$ is called trace map from L to K. In particular, the trace map is additive:

$$Tr_{L/K}(r + s) = Tr_{L/K}(r) + Tr_{L/K}(s) \text{ for all } r, s \in L.$$

Also, if $r \in \mathbb{Q}$, then $Tr_{L/K}(r) = n.r$ and $Norm_{L/K}(r) = r^n$. Let $char_r(x) \in K[x]$ denote the characteristic polynomial of linear map m_r. Then,

$$char_r(x) = x^n - Tr_{L/K}(r)x^{n-1} + ... + (-1)^n Norm_{L/K}(r).$$

When we have a field extension L/K, the following equivalent definitions of trace, norm and characteristic polynomial are much more useful.

Lemma 4.16. [4, LEMMA 4.2.5.] *Let L/K be a separable extension of degree n. Let $\sigma_1, ..., \sigma_n$ be n distinct embeddings of L into $\overline{K}$ algebraic closure of K. Then,*

(i) $Tr_{L/K}(\alpha) = \sigma_1(\alpha) + ... + \sigma_n(\alpha)$ *for all* $\alpha \in L$.
(ii) $Norm_{L/K}(\alpha) = \sigma_1(\alpha)...\sigma_n(\alpha)$ *for all* $\alpha \in L$.
(iii) The characteristic polynomial of α *over* L *is* $char_\alpha(x) = (x-\sigma_1(\alpha))...(x-\sigma_n(\alpha))$.

Definition 4.17. *Let K be a number field of degree n. Let $\sigma_1, ..., \sigma_n$ be n embeddings of K into $\mathbb{C}$. The discriminant of n-tuple $\alpha_1, ..., \alpha_n \in K$ is defined by*

$$disc(\alpha_1, ..., \alpha_n) = \mid \sigma_i(\alpha_j) \mid^2$$

i.e., the square of the determinant of the matrix which has $\sigma_i(\alpha_j)$ in the i-th row and the j-th column.

Alternatively, the discriminant of n-tuple is defined in terms of trace as follows

$$disc(\alpha_1, ..., \alpha_n) = \mid Tr(\alpha_i\alpha_j) \mid .$$

This is immediate from matrix equation

$$[\sigma_j(\alpha_i)] = [\sigma_1(\alpha_i\alpha_j) + ... + \sigma_n(\alpha_i\alpha_j)]$$

and properties of the discriminant such that $\mid a_{ij} \mid = \mid a_{ji} \mid$ and $|MN| = |M||N|$ for any two matrix A and B.

Definition 4.18. *Let K be a number field. A set of algebraic integers $\beta_1, ..., \beta_k$ in K is said to be an integral basis of K if every algebraic integer α in K can be expressed uniquely as $\alpha = a_1\beta_1 + ... + a_k\beta_s$ where $a_1, ..., a_k \in \mathbb{Z}$.*

If the set of n-tuple $\mathcal{B} = \{\alpha_1, ..., \alpha_n\}$ is an integral basis of a field K, the discriminant of n-tuple $disc(\alpha_1, ..., \alpha_n)$ is defined as the discriminant of the field K, and it is denoted by $disc(K)$.

4.1.3. Norm of an Ideal

Definition 4.19. *Let K be a number field and let A be the ring of integers of the number field K. Let I be a nonzero ideal of A. The norm of an ideal is defined as $N(I) = |A/I|$.*

Theorem 4.20. [2, THEOREM 12.1.4] *Let M be a free $\mathbb{Z}$-module of rank n, where n is finite. Let A be a submodule of M. Then,*

(i) A is also a free $\mathbb{Z}$-module of rank less than n.

(ii) There exists a basis $\{e_1, ..., e_n\}$ of M and there exist nonzero elements $a_1, ..., a_r \in \mathbb{Z}$ satisfying that the set $\{a_1e_1, ..., a_ne_n\}$ forms a basis of A and $a_i|a_{i+1}$ for $1 \leq i \leq r-1$.

Proposition 4.21. *Let K be a number field and let A be the ring of integers of K. Let I be an ideal of A. Then A/I is finite, i.e., the norm of ideal I in number field K is finite.*

Proof. Firstly, let I be a principal ideal such that $I = (a)A$ for some $a \in A - \{0\}$. Let m_a be a multiplication map by a

$$m_a : A \to aA \text{ with } x \mapsto ax.$$

Clearly, the map m_a is surjective. Since A is an integral domain, the map m_a is also injective. We know that A is a free $\mathbb{Z}$-module of rank $r = [K : \mathbb{Q}]$. By using previous Theorem 4.20, we obtain $(a)A$ is also a free $\mathbb{Z}$-module.

By using Theorem 4.20, we obtain that there exist nonzero elements $a_1, ..., a_r \in \mathbb{Z}$ and a basis $\{a_1e_1, ..., a_re_r\}$ such that

$$aA \cong a_1e_1\mathbb{Z} \oplus ... \oplus a_re_r\mathbb{Z} \quad \text{and} \quad A \cong e_1\mathbb{Z} \oplus ... \oplus e_r\mathbb{Z}.$$

Thus , we get

$$A/I = A/aA \cong (e_1\mathbb{Z} \oplus ... \oplus e_r\mathbb{Z})\big/(a_1e_1\mathbb{Z} \oplus ... \oplus a_re_r\mathbb{Z}) \cong \mathbb{Z}/a_1\mathbb{Z} \oplus ... \oplus \mathbb{Z}/a_r\mathbb{Z} \ .$$

The last isomorphism above implies that A/I is finite and it has cardinality $a_1...a_r$. Secondly, let us now assume that I is any ideal of A. We know that $(a) = aA \subseteq I$ for any $a \in I - \{0\}$. Also I/aA is an ideal of of A/aA. By taking quotient, we get

$$(A/aA)\big/(I/aA) \cong A/I.$$

Then, we have $|A/I| = |(A/aA)\big/(I/aA)| \leq |A/aA|$. From the first part of this proof, we conclude that $|A/aA|$ is finite, so $|A/I|$ as well. □

Theorem 4.22. [3, Theorem 3.22.] *Let L/K be a field extension of number fields with degree n and let A, B be the rings of integers of K, L respectively.*

(i) The norm of ideals of A is multiplicative, i.e., for some ideals I, J of A we have $N(IJ) = N(I)N(J)$.

(ii) Let I be an ideal in A and let IB be an ideal in B. Then $N(IB) = N(I)^n$.

(iii) The norm of a principal ideal (α) of A is $N((\alpha)) = |Norm_{L/K}(\alpha)|$.

4.1.4. Properties of Number Fields

Let K, L be number fields and let L/K be a extension field. Let A, B be the rings of integers of K, L respectively. It can be easily seen that $\mathbb{Z} \subseteq A$. Let $\mathfrak{p}$ be an ideal in A, and consider an ideal $\mathfrak{p}B$ generated by prime ideal $\mathfrak{p}$. By using Theorem 4.14, the following product of prime ideals is obtained,

$$\mathfrak{p}B = \prod_{i=1}^{s} \mathfrak{q}_i^{e_i}$$

where $\mathfrak{q}_1, ..., \mathfrak{q}_s$ are prime ideals of $\mathfrak{p}B$.

Definition 4.23. *The integer e_i is called the ramification index of $\mathfrak{q}_i$ over the ideal $\mathfrak{p}$. The field $A/\mathfrak{p}_i$ is called residue field of A at $\mathfrak{p}_i$. Let $f_i = [B/\mathfrak{q}_i : A/\mathfrak{p}]$. The degree f_i is called the residual degree (or inertia degree) of $\mathfrak{q}_i$ over $\mathfrak{p}$.*

Remark 4.24. *Notice that $B/\mathfrak{q}_i$ forms a vector space over $A/\mathfrak{p}_i$.*

Theorem 4.25. [3, Theorem 3.19.] *With the same notation L, K, A, B as above, let us fix $\mathfrak{q}_i = \mathfrak{q}$ for some i, $1 \leq i \leq s$. The following statements are equivalent.*

(i) $\mathfrak{q} \mid \mathfrak{p}B$
(ii) $\mathfrak{q} \subset \mathfrak{p}B$
(iii) $\mathfrak{q} \subset \mathfrak{p}$
(iv) $\mathfrak{q} \cap A = \mathfrak{p}$
(v) $\mathfrak{q} \cap K = \mathfrak{p}$.

If one of these conditions holds, the prime $\mathfrak{q}$ is said to be lying over $\mathfrak{p}$, or said to be $\mathfrak{p}$ lying under $\mathfrak{q}$.

Theorem 4.26. [3, Theorem 3.20.] *Every prime ideal $\mathfrak{q}$ in B lies over a unique prime ideal $\mathfrak{p}$ of A. Moreover, every prime ideal $\mathfrak{p}$ in A lies under at least one prime ideal $\mathfrak{q}$ of B.*

Theorem 4.27. [3, Theorem 3.21] *Let L/K be a field extension of degree n. Let A and B be the rings of integers of fields K and L, respectively. Let $\mathfrak{p}$ be a prime ideal in A and let $\mathfrak{q}_1,\ldots,\mathfrak{q}_s$ be prime ideals of B lying over $\mathfrak{p}$ such that $\mathfrak{p}B = \prod_{i=1}^{s} \mathfrak{q}_i^{e_i}$ where e_i is the ramification index of $\mathfrak{q}_i$ over $\mathfrak{p}$ and f_i is the residue degree of $\mathfrak{q}$ over $\mathfrak{p}$. Then,*

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

Proof. The proof will be done for the special case $K = \mathbb{Q}$. Let $p \in \mathbb{Z}$ be a prime number. Since every ideal can be written as the product of prime ideals according to Theorem 4.14, we have

$$pB = \prod_{i=1}^{s} \mathfrak{q}_i^{e_i}.$$

By taking the norm of an ideals, we get

$$N(pB) = \prod_{i=1}^{s} N(\mathfrak{q}_i)^{e_i} = \prod_{i=1}^{s} (p^{f_i})^{e_i}.$$

Also, it is known that $N(pB) = p^n$ from Proposition 4.22. Thus, $n = \sum_{i=1}^{s} e_i f_i$. □

Definition 4.28. *Let L, K, A, B be as usual, a prime ideal $\mathfrak{p}$ is said to be ramified in B (or in L) if and only if the ramification index is greater than 1, i.e. $e > 1$ for a prime ideal $\mathfrak{q}$ of B lying over $\mathfrak{p}$.*
If a prime ideal $\mathfrak{p}$ is not ramified in B, it is said to be unramified in B.

Theorem 4.29. [3, Theorem 3.24.] *Let K be a number field. Let A be the ring of integers of K. Let us suppose that $p \in \mathbb{Z}$ is a prime such that p is ramified in A. Then, p divides $disc(A)$.*

Definition 4.30. *Let K, L be number fields and let A, B be the rings integers of K, L respectively. An extension L of a number field K is called unramified over K if there is no prime ideal in A that ramifies in B.*

Theorem 4.31. *[4, Corollary 5.4.6.] Let K be a number field and A be the ring of integers of K. Then there exists a prime $p \in \mathbb{Z}$ which ramifies in A.*

4.1.5. Ramification Theory of Galois Extensions

Proposition 4.32. [4, Proposition 1.2.19] *Let A be an integral domain with the field of fractions K and let L/K be a field extension. If L/K is a Galois extension with Galois group G, then $\tau(B) = B$ for all $\tau \in G$.*

Proof. Let $\alpha \in B$. Let $f(x) \in A[x]$ be a monic polynomial satisfying $f(\alpha) = 0$. Since τ is identity when it is restricted to K, we get $\tau \restriction_K = Id_K$ for any $\tau \in G$. Let $f(x) = a_n x^n + ... + a_1 x + a_0$ with $a_i \in A$ for all $i = 1, ..., n$. We know that $f(\alpha) = 0$. Applying τ to $f(x)$, we get $\tau(f(x)) = a_n \tau(x)^n + ... + a_1 \tau(x) + a_0 = f(\tau(x))$. So $f(\tau(x)) = \tau(f(x))$ and $\tau(x)$ is a root of $f(x)$ for any $\tau \in G$. Thus $\tau(x)$ is integral over A. This implies that $\tau(x)$ is an element of B, i.e. $\tau(B) \subset B$. Since G is a group, $\tau^{-1} \in G$. By using previous part of the proof, we obtain $\tau^{-1}(B) \subset B$. Applying τ again, we get $B = \tau\tau^{-1}(B) \subset \tau(B)$. Therefore, we have $\tau(B) = B$. □

Theorem 4.33. [3, Theorem 3.23.] *Let L/K be a Galois extension of number fields and let A, B be rings of integers of K, L, respectively. Let $\mathfrak{p}$ be a prime ideal in A. If L is a Galois extension of K, the Galois group $Gal(L/K)$ acts on the prime ideals over $\mathfrak{p}$ transitively, i.e., if $\mathfrak{q}_1$ and $\mathfrak{q}_2$ are primes lying over $\mathfrak{p}$, there exists an element $\sigma \in Gal(L/K)$ such that $\sigma(\mathfrak{q}_1) = \mathfrak{q}_2$.*

Corollary 4.34. *Let L/K be a Galois extension with the same notation above. Let $\mathfrak{q}_1$ and $\mathfrak{q}_2$ be prime ideals lying over $\mathfrak{p}$ with ramification index e_1, e_2 and inertia degrees f_1, f_2, respectively. Then ramification and inertia degrees are equal, i.e. $e_1 = e_2$ and $f_1 = f_2$.*

Corollary 4.35. *The Corollary 4.34 shows that a prime ideal $\mathfrak{p}$ in A splits in B such that $\mathfrak{p}B = (\mathfrak{q}_1, ..., \mathfrak{q}_s)^e$ where $\mathfrak{q}_i$'s are distinct prime ideals and all of them have the same inertia degree f over $\mathfrak{p}$ in the case of Galois extension L/K. By using Theorem 4.27, it is concluded that $n = efs$.*

Definition 4.36. *Let L/K be a Galois extension of degree n with the Galois group $G = Gal(L/K)$. Let A, B be the rings of integers of K, L respectively. Let $\mathfrak{p}$ be a prime ideal in A and let $\mathfrak{q}$ be a prime ideal of B lying over $\mathfrak{p}$.*
The decomposition group of $\mathfrak{q}$ over $\mathfrak{p}$ is defined as

$$D_{\mathfrak{q}/\mathfrak{p}} = \{\sigma \in G : \sigma(\mathfrak{q}) = \mathfrak{q}\} \qquad \text{or equivalently}$$
$$D_{\mathfrak{q}/\mathfrak{p}} = \{\sigma \in G : \sigma(\alpha) = 0 \ (mod\ \mathfrak{q}) \text{ for all } \alpha \in \mathfrak{q}\}.$$

The inertia group of $\mathfrak{q}$ over $\mathfrak{p}$ is defined as

$$I_{\mathfrak{q}/\mathfrak{p}} = \{\sigma \in G : \sigma(\alpha) \equiv \alpha \ (mod\ \mathfrak{q}) \text{ for all } \alpha \in B\}.$$

Remark 4.37. *The inertia group of $\mathfrak{q}$ over $\mathfrak{p}$ is a subgroup of the decomposition group of $\mathfrak{q}$ over $\mathfrak{p}$, i.e. $I_{\mathfrak{q}/\mathfrak{p}} \leqslant D_{\mathfrak{q}/\mathfrak{p}} \leqslant G$. In fact, the inertia group is normal in the decomposition group, $I_{\mathfrak{q}/\mathfrak{p}} \trianglelefteq D_{\mathfrak{q}/\mathfrak{p}}$. Furthermore the group $D_{\mathfrak{q}/\mathfrak{p}}/I_{\mathfrak{q}/\mathfrak{p}}$ is a cyclic group of order f where f is the residue degree of $\mathfrak{q}$ over $\mathfrak{p}$.*

Definition 4.38. *Let L/K be a Galois extension with the Galois group G. Let A, B be the rings of integers of K, L respectively. Let $\mathfrak{p}$ be a prime ideal in A and let $\mathfrak{q}$ be a prime ideal of B lying over $\mathfrak{p}$. Let $I_{\mathfrak{q}/\mathfrak{p}}$ be the inertia group of $\mathfrak{q}$ over $\mathfrak{p}$ and let $D_{\mathfrak{q}/\mathfrak{p}}$ be the decomposition group of $\mathfrak{q}$ over $\mathfrak{p}$.*
The inertia field $L^{I_{\mathfrak{q}/\mathfrak{p}}}$ is defined as the fixed field of $I_{\mathfrak{q}/\mathfrak{p}}$ in L, and the decomposition field $L^{D_{\mathfrak{q}/\mathfrak{p}}}$ is defined as the fixed field of $D_{\mathfrak{q}/\mathfrak{p}}$ in L.

Lemma 4.39. [4, Lemma 3.8.5.] *Let L/K be a Galois extension with the Galois group G. Let A, B be the rings of integers of K, L respectively. Let us consider residue fields $B/\mathfrak{q}$ and $A/\mathfrak{p}$. The residue field extension $B/\mathfrak{q}/A/\mathfrak{p}$ is a Galois extension of degree f with Galois group $\mathcal{G}$, where $f = [B/\mathfrak{q}_i : A/\mathfrak{p}]$.*

Corollary 4.40. *A prime ideal* $\mathfrak{q}$ *lying over* $\mathfrak{p}$ *has no ramification if and only if the inertia group* $I_{\mathfrak{q}/\mathfrak{p}}$ *is trivial. It follows that* $\mathfrak{q}$ *is ramified in* A *if and only if* $I_{\mathfrak{q}/\mathfrak{p}} \neq \{id\}$.

Theorem 4.41. [3, Theorem 4.29.] *Let* L/K *be a Galois extension with Galois group* G. *Let* A, B *be the rings of integers of* K, L *respectively. Let* $\mathfrak{p}$ *be a prime ideal in* A *and let* $\mathfrak{q}$ *be a prime ideal of* B *lying over* $\mathfrak{p}$. *Let* $I_{\mathfrak{q}/\mathfrak{p}}$ *be the inertia group of* $\mathfrak{q}$ *over* $\mathfrak{p}$. *Then, the inertia field* $L^{I_{\mathfrak{q}/\mathfrak{p}}}$ *is the largest intermediate field such that* $e = 1$, *where* e *is the ramification degree of* $\mathfrak{q}$ *over* $\mathfrak{p}$.

Remark 4.42. In this thesis, we will consider only number fields, not the case of function fields. All definitions, theorems and tools of this chapter can be generalized to function fields, which is another important object of algebraic number theory.

4.2. Realization of The Group S_n

All the necessary statements are produced in the previous section in order to prove that the polynomial

$$f(x) = x^n - x - 1$$

is an irreducible polynomial which gives a Galois extension with Galois group S_n. First of all, we will show that the polynomial $f(x)$ is irreducible.

Proposition 4.43. [11, Theorem 1.] *The polynomial* $f(x) = x^n - x - 1$ *with* $n > 1$ *is irreducible over rational numbers* $\mathbb{Q}$.

Proof. Since this proof leads to the main result in this section, we will prove it in detail by dividing into steps.

(i) Firstly, we show that the polynomial $f(x)$ does not have any roots in $\mathbb{Q}$. Let $c = a/b$ be a fraction satisfying $f(c) = 0$ where $a, b \in \mathbb{Z}$ and $gcd(a, b) = 1$.

Then,

$$f(c) = \frac{a^n}{b^n} - \frac{a}{b} - 1 = 0 \leftrightarrow a^n - ab^{n-1} = b^n \leftrightarrow a(a^{n-1} - b^{n-1}) = b^n.$$

It can be easily seen that a divides b. Since $gcd(a, b) = 1$ by hypothesis, then $a = 1$. By plugging $a = 1$ in the above argument, we get $1 - b^{n-1} = b^n$. Since $1 - b^{n-1} = b^n$ can be written as $(1 + b)b^{n-1} = 1$, we conclude that b is invertible. By hypothesis $b \in \mathbb{Z}$, thus $b = \pm 1$. So we get $c = \frac{a}{b} = \pm 1$. But, this gives a contradiction because of the fact that 1 and -1 are not roots of the polynomial $f(x)$. Therefore, the polynomial $f(x)$ does not have roots in rational numbers $\mathbb{Q}$.

(ii) We now prove that the polynomial $f(x)$ is a separable. In other words, we prove that the polynomial $f(x)$ has no multiple roots in $\mathbb{C}$. Let us assume that $z \in \mathbb{C}$ be a multiple root of the polynomial $f(x)$. Then, z would also be root of the derivative $f^{'}(x)$ of the polynomial $f(x)$. Since $f^{'}(x) = nx^{n-1} = 1$, we would have $nz^{n-1} = 1$ and $nz^n = z$ by multiplying by z. Then, we have the following calculation;

$$f(z) = 0 \rightarrow nf(z) = nz^n - nz - 1 = z - nz - n = 0 \rightarrow (1 - n)z = n.$$

Thus, $z = \frac{n}{1-n} \in \mathbb{Q}$ since $n > 1$. Since we have seen that the polynomial $f(x)$ has no roots in $\mathbb{Q}$ in the first part of the proof, we get a contradiction. Therefore, $f(x)$ is a separable polynomial.

(iii) We obtained that if $f(x)$ is reducible, it splits into factors of degree at least 2, meaning that $f(x)$ can be reducible for $n \geq 4$.

Let $q(x)$ be a monic factor of degree t of the polynomial $f(x)$. Let us denote the set of all the roots of the factor $q(x)$ by $R(q(x))$ and consider the following sum:

$$S(q(x)) = \sum_{z \in R(q(x))} (z - \frac{1}{z}).$$

Let us now recall the definition of the elementary symmetric functions of a polynomial. Let $F(x) = \prod_{i=1}^{t}(x - z_i)$ be a polynomial. The elementary symmetric functions of the polynomial $F(x)$ are defined by the evaluations of the elementary symmetric functions in the roots of the polynomial $F(x)$, i.e.

$$s_i = \sum_{(r_1,...,r_i)\in S_i} z_{r_1}...z_{r_i}.$$

where S_i is the set of all distinct i-tuples. Indeed, s_i's are exactly the coefficients of the polynomial $F(x)$ where $i = 1, ..., t$. The reader is referred to Section 4.3 in [12] for detailed explanation of elementary symmetric functions.
Let $\{s_i\}_{1\leq i\leq t}$ denote the elementary symmetric functions of the factor $q(x)$ of $f(x)$. Let us notice the following equality:

$$\frac{s_{d-1}}{s_d} = \frac{1}{z_1} + ... + \frac{1}{z_t}.$$

Thus, it is obtained that

$$S(q(x)) = s_1 - \frac{s_{d-1}}{s_d}.$$

Since $\{s_i\}_{1\leq i\leq t}$ are the set of coefficients of the factor $q(x)$, one has $s_i \in \mathbb{Z}$ for each $i = 1, ..., t$. Furthermore, we need to evaluate the constant term s_d of the factor $q(x)$, namely $s_d = \pm q(0)$. Since $q(x)$ is the factor of $f(x)$, there exists a nonzero polynomial $g(x)$ such that $f(x) = q(x)g(x)$. Thus, $f(0) = q(0)g(0) = -1$. Since the factor $q(x)$ has coefficients in $\mathbb{Z}$, it is proved $q(0) = \pm 1$, so $S(q(x))$ is in $\mathbb{Z}$ as well. Since all the coefficients of the polynomial $f(x)$ is already known, we have $S(f(x)) = 1$.
Let $z = re^{i\varphi}$ be a root of the factor $q(x)$. Since $f(z) = z^n - z - 1$, we obtain

$$r^{2n} = |z - 1|^2 = r^2 + 1 + 2r\cos(\varphi). \tag{4.1}$$

Let us assume that $r = 1$, then $\cos(\varphi) = -1/2$ and $\varphi = \frac{\pi}{3}$. Thus, z is a cubic root of unity and z is not a root of $f(x)$. Therefore, $r \neq 1$. We now take the real part of the complex number z to verify the following inequality:

$$2\mathcal{R}(z - \frac{1}{z}) > \frac{1}{r^2} - 1.$$

Firstly, we get the following equality since $\frac{1}{z} = \frac{1}{r}\mathrm{e}^{-i\varphi}$

$$2\mathcal{R}(z - \frac{1}{z}) = 2\cos(\varphi)(r - \frac{1}{r})$$

and we get $2\cos(\varphi) = (r^{2n} - r^2 - 1)/2r$ by equation 4.1, so we get

$$\begin{aligned} 2\mathcal{R}(z - \frac{1}{z}) &= \frac{(r^2-1)(r^{2n} - r^2 - 1)}{r^2} \\ &= \frac{(r^2-1)(r^{2n} - r^2)}{r^2} - \frac{r^2-1}{r^2}. \end{aligned}$$

Notice that the term $\frac{(r^2-1)(r^{2n}-r^2)}{r^2}$ is positive for all r since both factors in the term are positive for $r > 1$ and they are negative for $r < 1$. Thus, the following inequality is obtained easily,

$$2\mathcal{R}(z - \frac{1}{z}) > \frac{1}{r^2} - 1.$$

Let z_i be a root of every possible factor $q(x)$ of $f(x)$ and let us denote the norm of z_i by r_i. Since we know $q(0) = \pm 1$, the following equality is obtained

$$1 = |q(0)|^2 = \prod_{i=1}^{t} r_i^2 \quad \rightarrow \quad 1 = \frac{1}{\prod_{i=1}^{t} r_i^2} = \prod_{i=1}^{t} \frac{1}{r_i^2}. \tag{4.2}$$

By using inequality between geometric mean and arithmetic mean, we have

$$\frac{1}{d}\sum_{i=1}^{t} \frac{1}{r_i^2} \geq (\prod_{i=1}^{t} \frac{1}{r_i^2})^{1/d} = 1. \tag{4.3}$$

In particular $\sum_{i=1}^{t} \frac{1}{r_i^2} \geq d$. Since $S(q(x)) \in \mathbb{Z}$ and by using above Equations 4.2 and 4.3, one can conclude

$$2S(q(x)) = 2\sum_{i=1}^{t} \mathcal{R}(z_i - \frac{1}{z_i}) > \sum_{i=1}^{t} (\frac{1}{r_i^2} - 1) \geq 0.$$

This means that $S(q(x)) > 0$, also we know $S(q(x)) \in \mathbb{Z}$, which is equivalent to $S(q(x)) \geq 1$. Then $S(q(x)) + S(g(x)) \geq 2$, which gives a contradiction. Therefore, the polynomial $f(x) = x^n - x - 1$ is irreducible over $\mathbb{Q}$ for each positive integer n.

□

From now on, let K be the splitting field of the polynomial $f(x) = x^n - x - 1$ in $\mathbb{Q}[x]$. The polynomial $f(x)$ is a separable polynomial over $\mathbb{Q}$ as we have seen in Proposition 4.43. Then, $K/\mathbb{Q}$ is a Galois extension by the Theorem 2.19. Let G be the Galois group of the Galois extension $K/\mathbb{Q}$ and let A be the ring of integers of the field K. Let $\{\alpha_i\}_{1 \leq i \leq n}$ be the set of the roots of $f(x)$. Also, the Galois group G acts on the set of roots transitively by Theorem 4.33. It follows that every $\sigma \in G$ can be associated with a permutation of the n roots. Thus G is seen as a subgroup of S_n naturally.

Lemma 4.44. *Let K be a number field and A be the ring of integers of K. Let $K/\mathbb{Q}$ be a Galois extension with the Galois group G. The Galois group G is generated by the inertia groups $I_{\mathfrak{q}_{ij}/p_i}$'s, where p_i ranges over all the prime numbers and $\mathfrak{q}_{ij}$ ranges over all the prime ideals $\mathfrak{q}_{ij}$ of A lying over p_i.*

Proof. It is known every inertia group $I_{\mathfrak{q}_{ij}/p_i}$ is a subgroup of G by definition. Let us now assume that H is a subgroup of G generated by all the inertia groups, i.e. $H = \langle I_{\mathfrak{q}_{ij}/p_i} \rangle$, where p_i ranges over prime numbers and $\mathfrak{q}_{ij}$ ranges over prime ideals $\mathfrak{q}_{ij}$ of A lying over p. Let i and j be fixed integers and consider the related inertia group $I_{\mathfrak{q}_{ij}/p_i}$ and set $I = I_{\mathfrak{q}_{ij}/p_i}$ for simplicity. Since $I = I_{\mathfrak{q}_{ij}/p_i}$ is a subgroup of H, the corresponding fixed fields satisfy $K^H \subset K^I$.

According to Theorem 4.41, the inertia field K^I is the largest intermediate field such that ramification degree e of $\mathfrak{q}_{ij}$ over p_i is 1. It follows that the extension $K^H/\mathbb{Q}$ is unramified at every prime p. Since there is no unramified extension of rational numbers $\mathbb{Q}$ as given in Theorem 4.31, we have $K = \mathbb{Q}$. By Fundamental Theorem of Galois (Theorem 2.20), we conclude that $H = G$. □

Lemma 4.45. [13, Lemma 3.] *Let K be a number field and let A be its ring of integers. Let p be a prime number and let $\mathfrak{p}$ be a prime ideal of A lying over p. Let $I_\mathfrak{p}$ be the inertia group corresponding to prime ideal $\mathfrak{p}$ lying over p. Then, the order of the inertia group $I_\mathfrak{p}$ is less than or equal to 2, i.e. $I_\mathfrak{p} \leq 2$. In particular, if $I_\mathfrak{p}$ is not trivial, then it is generated by a transposition.*

Proof. Let us denote the reduction of an element a of A in $A/\mathfrak{p}$ by $\overline{a}$. Consider the reduction of $f(x)$ mod $\mathfrak{p}$ as follows

$$\overline{f(x)} = \prod_{i=1}^{n}(x - \overline{a_i}) = x^n - x - 1 \in A/\mathfrak{p}[x]$$

where a_1,..., a_n are the roots of $f(x)$. Furthermore, we have $\overline{f'(x)} = nx^{n-1} - 1$. Then we get the following equality $x\overline{f'(x)} - n\overline{f(x)} = nx^n - x - nx^n + nx + n = (n-1)x + n$. Since p can not divide both n and $n-1$, the equality is nonzero. Let us denote the greatest common divisor of the polynomials $\overline{f(x)}$ and $\overline{f'(x)}$ by $h(x)$. Then $h(x)$ has to divide $x\overline{f'(x)} - n\overline{f(x)}$ as well. Let us assume $\overline{f(x)} = h(x)r(x)$ and $\overline{f'(x)} = h(x)s(x)$, then we have

$$(n-1)x + n = h(x)(xs(x) - nr(x))$$

This implies that $h(x)$ has degree at most 1. Since every multiple root x_i of the polynomial $f(x)$ forms a factor of $h(x)$, $\overline{f(x)}$ has at most one double root. Let us now suppose that the inertia group $I_\mathfrak{p}$ correspond to prime ideal $\mathfrak{p}$ is not trivial. This means that there exists an element $g \in I_\mathfrak{p}$ which is not the identity element. Thus, there exist roots x_i and x_j with $i \neq j$ such that $g(x_i) = x_j$.

The element g of $I_{\mathfrak{p}}$ also satisfies $g(x) = x \bmod \mathfrak{p}$. Thus, we get the following relation

$$x_i = g(x_i) = x_j \bmod \mathfrak{p}$$
$$\text{equivalently} \quad \overline{x_i} = \overline{g(x_i)} = \overline{x_j}$$

Then $\overline{x_i}$ is a double root of $\overline{f(x)}$. That is to say, for every root x_i such that $g(x_i) = x_j$ with $i \neq j$, we get a double root of $\overline{f(x)}$. Since $\overline{f(x)}$ has at most one double root, we obtain $g(x_k) = x_k$ for any $k \neq i, j$ in the set $\{1, ..., n\}$. This means that g is the transposition of the roots x_i, x_j, i.e. $s = (x_i, x_j)$. Furthermore, $I_{\mathfrak{p}}$ can not have another nontrivial element because of the fact that we will find another multiple root again. Thus, $I_{\mathfrak{p}} = \{Id, g\}$.

□

Lemma 4.44 and Lemma 4.45 have shown that the Galois group G of the polynomial $f(x) = x^n - x - 1$ is generated by transpositions of the roots of the polynomial $f(x)$. Furthermore, since $f(x)$ is an irreducible polynomial, the Galois group G acts transitively on the set of roots of $f(x)$. In the next lemma, we will show that any subgroup of S_n satisfying these features gives the whole group S_n.

Lemma 4.46. [13, Lemma 5.] *Let n be a positive integer and let G be a transitive subgroup of S_n. Let us assume that G is generated by transpositions. Then G is equal to S_n.*

Proof. Let A be the set of transpositions in the subgroup G and let (x, y) be a transposition in S_n. We are going to prove that (x, y) belongs to G. Since G is a transitive subgroup of S_n, there exists an element $g \in G$ satisfying $g(x) = y$. We can write $g \in G$ as $g = \prod_{i=1}^{s} a_i$ for some $a_1, ..., a_s \in A$ because of the fact that G is generated by transpositions.

We can choose $a_1, ..., a_s$ such that s is minimal in the lengths of product of elements of A which are equal to g. Let us show that y is not fixed by a_1. If it was fixed, we would get $a_1 g(x) = a_1(y) = y$. Since a_1 is a transposition, it follows that $a_2....a_s(x) = y$ which gives a contradiction with the fact that s is minimal. Likewise, we can show that none of the a_j's fixes y, i.e. $a_j(y) = y$ for $j = 2, ..., s-1$. Let us denote $a_i^{'} = a_j^{-1} a_i a_j$ for a fixed j and for all $i = 1, ..., s-1$. It is easy to see that every $a_i^{'}$ is belong to A. We can write g as

$$g = a_j(\prod_{i=1}^{j-1} a_j^{'})(\prod_{i=j+1}^{r} a_i).$$

Then, we apply the same argument used above for a_1 in order to show that none of the a_j's satisfies $a_j(y) = y$. Particularly, this is true for a_s. Furthermore, a_s does not fix x. If it was, i.e. $a_s(x) = x$, then we would get $a_1....a_s(x) = a_1....a_{s-1} = y$. This gives a contradiction with the minimality of s. Thus, we have proved the result as desired. To be more precise, any transposition permutes two elements and fixes all the other elements. Since x and y are not fixed by a_s, we obtain $a_s = (x, y)$. Therefore, $(x, y) \in G$ and $G = S_n$.

□

To conclude, we have constructed S_n as a Galois group of a Galois extension K over $\mathbb{Q}$, where K is the splitting field of the polynomial $f(x) = x^n - x - 1 \in \mathbb{Q}[x]$.

There are many other methods to realize S_n as a Galois group, this method is not the only possibility. Let n be a fixed integer. We have seen that the splitting of the polynomial $f(x) = x^n - x - 1 \in \mathbb{Q}[x]$ has Galois group $G = S_n$. One can find another irreducible polynomial $g(x) \in \mathbb{Q}[x]$ whose Galois extension has Galois group isomorphic to S_n for a fixed n. Then, it can be checked by PARI/GP that these two extensions are not the same. To illustrate this with an example, let $g(x) = x^5 - 6x + 3$ be a polynomial over $\mathbb{Q}$. It is an irreducible polynomial by using Eisenstein criterion at 3 and the polynomial $g(x)$ has two nonreal roots. Let us recall the following lemma.

Lemma 4.47. *Let p be a prime number and let $h(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of degree p with exactly two nonreal zeros in $\mathbb{C}$. Thus, the Galois group of $h(x)$ over $\mathbb{Q}$ is the symmetric group S_p.*

By using Lemma 4.47, it can be seen that the splitting field of $g(x)$ has Galois group S_5. On the other and, we know that the splitting field of $f(x) = x^5 - x - 1$ has also Galois group S_5. If we check in PARI/GP, these two extensions are not isomorphic to each other.

5. THE GROUP $\mathbb{GL}_2(\mathbb{F}_p)$ AS A GALOIS GROUP

Let p be a prime number and let $\mathbb{GL}_2(\mathbb{F}_p)$ be the general linear group with entries in the finite field $\mathbb{F}_p$. In this chapter, our main purpose is to construct $\mathbb{GL}_2(\mathbb{F}_p)$ as a Galois group of a Galois extension over $\mathbb{Q}$. For this aim, we will use a geometric method via elliptic curves by using the paper [14]. This is different from previous chapters. This chapter is divided into two sections. In the first section, we will summarize the theory of elliptic curves as much as possible, since elliptic curves will be used widely in the following chapter as well. In the second section, we will explain the method we used, and then apply the method in order to realize $\mathbb{GL}_2(\mathbb{F}_p)$ as a Galois group of a Galois extension over $\mathbb{Q}$.

5.1. Elliptic Curves

In this section, we will give all the necessary definitions, theorems and tools in the theory of elliptic curves. These objects are not studied in depth here, we refer the reader to [5] for more detailed explanations.

A projective variety of dimension 1 is called a *curve*.

Definition 5.1. *Let K be a field and let C be a projective curve in $\mathbb{P}^2(K)$ given by a homogeneous polynomial $F(X,Y,Z)$. A point $P=[a,b,c]$ is said to be singular if and only if*

$$\frac{\partial F}{\partial X}(P)=\frac{\partial F}{\partial Y}(P)=\frac{\partial F}{\partial Z}(P)=0.$$

The projective curve C given by the homogeneous polynomial $F(X,Y,Z)$ is called non-singular or smooth if every point P of the curve C is nonsingular.

Nonsingularity of a curve gives rise to a well-defined tangent line for each point of the curve.

Definition 5.2. *The equation of the tangent line of a curve C given by the equation $F(X,Y,Z)=0$ at the point $P=[a,b,c]$ has the following form*

$$\frac{\partial F}{\partial x}(P)(X-a)+\frac{\partial F}{\partial Y}(P)(Y-b)+\frac{\partial F}{\partial Z}(P)(Z-c)=0.$$

Definition 5.3. *An elliptic curve E is a smooth projective curve of genus 1 with a specified base point O.*

Definition 5.4. *Let E be an elliptic curve. The elliptic curve E is defined over K if E is defined over K as a curve and $O \in E(K)$, where $E(K)$ is the set of K-rational points of the elliptic curve E.*

5.1.1. Weierstrass Equations

In this subsection, we will define elliptic curves by cubic equations, called Weierstrass equations.

Definition 5.5. *A Weierstrass equation is an equation of the form*

$$Y^2Z+a_1XYZ+a_3YZ^3=X^3+a_2X^2Z+a_4XZ^2+a_6Z^3$$

with coefficients $a_1,...,a_6 \in \bar{K}$. Furthermore, a curve is said to be a Weierstrass curve, if it is given by a Weierstrass equation.

Moreover, we oftenly switch to nonhomogeneous (or affine) coordinates in this thesis, meaning that we substitute the points of our curve by $x=X/Z$ and $y=Y/Z$ in order to express a Weierstrass equation by the zero set of the following polynomial

$$y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6.$$

If $char(K) \neq 2$, then we can give a simpler form of a Weierstrass equation by completing the square. Then, replacing y with $\frac{1}{2}(y - a_1x - a_3)$ gives an equation of the form

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$$

where

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, \\ b_4 &= 2a_4 + a_1a_3, \\ b_6 &= a_3^2 + 4a_6. \end{aligned}$$

Additionally, we define the following quantities:

$$\begin{aligned} b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2, \\ c_4 &= b_2^2 - 24b_4, \\ c_6 &= b_2^3 + 36b_2b_4 - 216b_6, \\ \Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6, \\ j &= c_4^3/\Delta, \\ \omega &= \frac{dx}{2y + a_1x + a_3} = \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y} \end{aligned}$$

Definition 5.6. *The quantity Δ given above is said to be the discriminant of the Weierstrass equation. The quantity j is called the j-invariant of the elliptic curve E. The quantity ω is said to be the invariant differential related to the Weierstrass equation.*

Proposition 5.7. [5, Proposition 3.1.4.] *Two elliptic curves are isomorphic over $\overline{K}$ if and only if they both have the same j-invariant.*

Remark 5.8. Notice that we have seen that an elliptic curve E is given by a Weierstrass equation of the form $Y^2Z + a_1XYZ + a_3YZ^3 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$. If $char(K) \neq 2$, we can simplify the Weierstrass equation to the form $y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$. Furthermore, if $char(K) \neq 2, 3$, the elliptic curve E can be given by a Weierstrass equation of the form $y^2 = x^3 + Ax + B$ for some $A, B \in K$.

Theorem 5.9. [5, PROPOSITION 3.3.1.] *Let E be an elliptic curve defined over K and let $K(E)$ be the function field of the elliptic curve E.*

(i) There exist functions $x, y \in K(E)$ such that the following map

$$\phi : E \to \mathbb{P}^2$$
$$\phi = [x, y, 1]$$

gives an isomorphism of E/K to a curve C given by a Weierstrass equation

$$C : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

where coefficients $a_1, ..., a_6 \in K$ and $\phi(O) = [0, 1, 0]$.

(ii) Conversely, every smooth cubic curve C is given by a Weierstrass equation as in (i) above is an elliptic curve defined over K with a distinguished point $O = [0, 1, 0]$.

(iii) Any two Weierstrass equations for the elliptic curve E differ by a linear change of variables of the form

$$X = u^2X' + r \quad and \quad Y = u^3Y' + su^2X' + t \quad where \quad u, r, s, t \in K, u \neq 0.$$

Fact 5.10. Let K be a field with $char(K) \neq 2$. Let us consider a Weierstrass equation $f(x,y) = y^2 - x^3 - ax^2 - bx - c = y^2 - g(x)$ where $a, b, c \in K$. Let $P = (x_0, y_0)$ be the point of the curve given by $f(x,y) = y^2 - x^3 - ax^2 - bx - c$. We know that $P = (x_0, y_0)$ is a singular point if and only if

$$\frac{\partial f}{\partial x}(x_0, y_0) = -g'(x_0) = 0 \quad \text{and} \quad \frac{\partial f}{\partial y}(x_0, y_0) = 2y_0 = 0.$$

Equivalently, the curve given by $f(x,y) = y^2 - x^3 - ax^2 - bx - c = y^2 - g(x)$ has a singular point if and only if $g(x)$ has a multiple root. Indeed, let us assume that (x_0, y_0) is a point on the curve given by $f(x,y)$ and x_0 is a multiple root of the polynomial $g(x)$. Thus, x_0 is also a root of $g'(x)$, i.e. $\frac{\partial f}{\partial x}(x_0, y_0) = 0$. Furthermore, we have

$$f(x_0, y_0) = 0 \rightarrow y_0^2 - g(x_0) = 0 \rightarrow y_0 = 0.$$

Thus, $\frac{\partial f}{\partial y}(x_0, y_0) = 0$ and (x_0, y_0) is a singular point. In a similar way, if (x_0, y_0) is a singular point, we have $\frac{\partial f}{\partial y}(x_0, y_0) = 0$, so $y_0 = 0$ since $char(K) \neq 2$. Thus, we obtain

$$f(x_0, y_0) = 0 \rightarrow -g(x_0) = 0 \rightarrow x_0 \text{ is a root of } g(x).$$

Also, we have $\frac{\partial f}{\partial x}(x_0, y_0) = 0$, i.e. $g'(x) = 0$. Thus, x_0 is a multiple root of $g(x)$. Eventually, we have obtained that the curve given by $f(x,y) = y^2 - g(x)$ is a non-singular curve if and only if $g(x)$ has no multiple roots.

We can also see that a polynomial $g(x)$ has no multiple roots by considering its discriminant D_g. The discriminant of a polynomial $g(x)$ can be found by using discriminant formula of a cubic polynomial.

On the other hand, the discriminant of a polynomial $g(x)$ gives information about geometric features of the curve given by $f(x,y) = y^2 - g(x)$ as follows.

(i) If $D_g(x) = 0$, the curve related to polynomial $y^2 = g(x)$ has a singular point. This implies that one can not obtain an elliptic curve in this case.

(ii) If $D_g(x) < 0$, the polynomial $g(x)$ has one real zero and a pair of complex conjugate roots. This implies that one can have an elliptic curve in this case. Furthermore, the elliptic curve given by $y^2 = g(x)$ has a unique component.

(iii) If $D_g(x) > 0$, the polynomial $g(x)$ has three real zeros. Moreover, the elliptic curve associated to $y^2 = g(x)$ has two components.

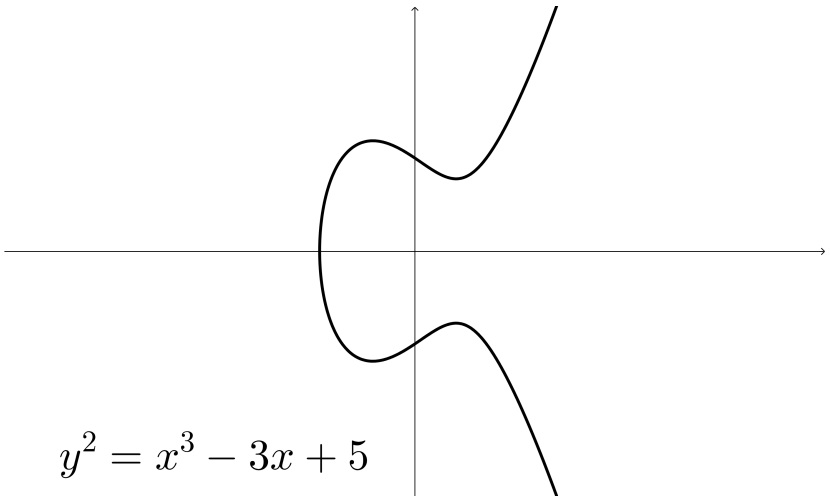

Figure 5.1. Elliptic curve with one component

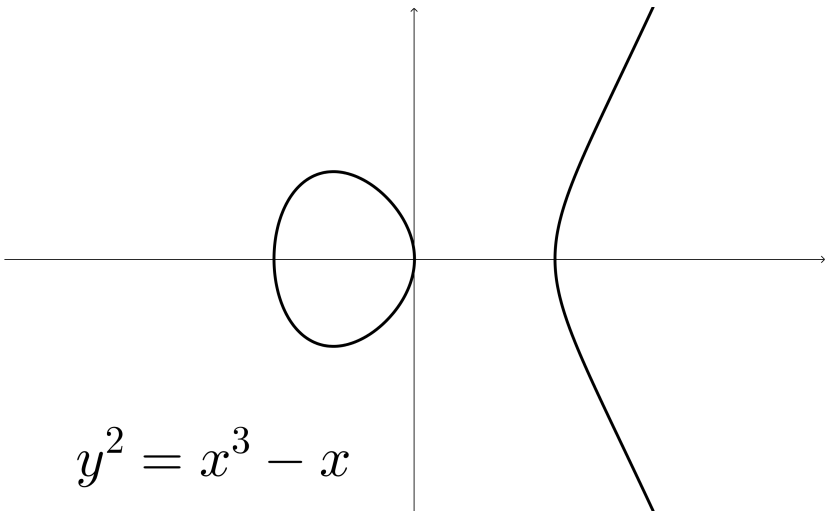

Figure 5.2. Elliptic curve with two component

5.1.2. Group Structure of an Elliptic Curve

Let E be an elliptic curve given by a Weierstrass equation and let L be a line in the projective space $\mathbb{P}^2$. Since Weierstrass equation of an elliptic curve has degree 3, the line L intersects with the elliptic curve E at exactly 3 points, namely P, Q, R. (If L is a tangent line of E, the points P, Q, R may be not be distinct.) Let us now define composition law $+$ on a elliptic curve E as follows.

Composition Law: Let E be an elliptic curve. Let P and Q be the points on the elliptic curve E. Let L be the line connecting points P and Q (L is tangent line if $P = Q$), and let R be the third point of intersection of L with E. Let L' be the line connecting points R and O. Then, $P + Q$ is the third intersection point of L' with E.

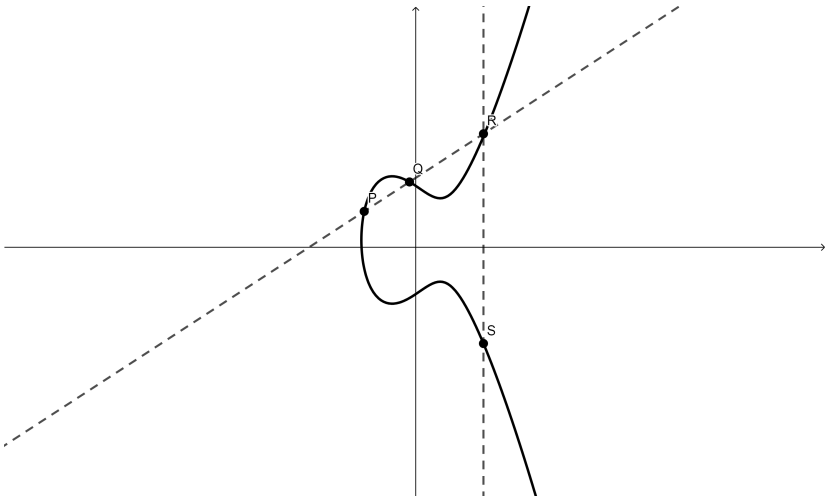

Figure 5.3. Adding two points on an elliptic curve

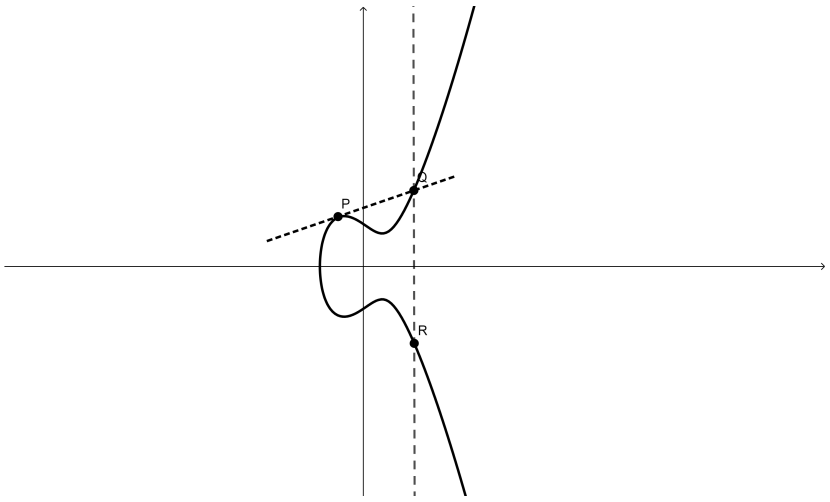

Figure 5.4. Adding a point to itself on an elliptic curve

Proposition 5.11. [5, PROPOSITION 3.2.2.] *Let E be an elliptic curve. The composition law $+$ on an elliptic curve satisfies the following conditions:*

(i) If a line L intersects with E at the points P,Q,R (not necessarily to be distinct points), then

$$(P + Q) + R = O.$$

(ii) $P + O = P$ for all $P \in E$.

(iii) $P + Q = Q + P$ for all $P, Q \in E$.

(iv) Let $P \in E$. There exists a point of E, denoted by $-P$, such that

$$P + (-P) = O.$$

(v) Let $P, Q, R \in E$. Then, we have $(P + Q) + R = P + (Q + R)$.

In other words, the composition law $+$ turns an elliptic curve E into an abelian group with identity element O.

Example 5.12. Let E be an elliptic curve given by $y^2 = x^3 + ax^2 + bx + c$. Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be points on the elliptic curve E and let L be the line passing through P_1 and P_2. We are going to find the third intersection point $P_3 = (x_3, y_3)$ of the elliptic curve E. The line L has the following equation

$$y = \lambda x + v \text{ where } \lambda = \frac{y_2 - y_1}{x_2 - x_1} \text{ and } v = y_1 - \lambda x_1 = y_2 - \lambda x_2.$$

The line L intersects the elliptic curve E in the two points P_1 and P_2 by construction. By substituting $y = \lambda x + v$ in the equation of the elliptic curve E, we get

$$\begin{aligned} & y^2 = (\lambda x + v)^2 = x^3 + ax^2 + bx + c \\ \rightarrow \quad & 0 = x^3 + (a - \lambda^2)x^2 + (b - 2\lambda v)x + (c - v^2). \end{aligned}$$

Since a cubic equation in x is found, its three roots x_1, x_2, x_3 give the x-coordinates of the three intersection points. Then,

$$x^3 + (a - \lambda^2)x^2 + (b - 2\lambda v)x + (c - v^2) = (x - x_1)(x - x_2)(x - x_3).$$

By equating the coefficients of the x^2 term on both side, we obtain

$$a - \lambda^2 = -x_1 - x_2 - x_3.$$

Thus, $x_3 = \lambda^2 - a - x_1 - x_2$ and $y_3 = \lambda x_3 + v$.

Proposition 5.13. [5, Proposition 3.2.2.] *Let E be an elliptic curve defined over K. Then*

$$E(K) = \{(x, y) \in K^2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{O\}$$

is a subgroup of the elliptic curve E.

5.1.3. Isogenies

Definition 5.14. *Let E_1 and E_2 be elliptic curves. The isogeny ϕ from E_1 to E_2 is defined as a morphism such that*

$$\phi : E_1 \to E_2, \qquad \phi(O_{E_1}) = O_{E_2}$$

where O_{E_1} and O_{E_2} are the identity elements of E_1 and E_2 as abelian groups, respectively. The elliptic curves E_1 and E_2 are called isogenous if there exists a nonconstant isogeny ϕ from E_1 to E_2.

A morphism between two curves is either constant or surjective. For proof of this statement, we refer the reader to Theorem 2.2.3 in [5]. Thus, an isogeny between the elliptic curves E_1 and E_2 satisfies either

$$\phi(E_1) = \{O_{E_2}\} \quad \textit{or} \quad \phi(E_1) = E_2.$$

Remark 5.15. Since it can be understood from the content, the identity of an elliptic curve E will be denoted simply by O instead of O_E.

We also define the zero isogeny as $[0](P) = O$ for all $P \in E_1$. Thus, it can be concluded that every isogeny is a finite map of curves, except for the zero isogeny.

Definition 5.16. *The degree of an isogeny ϕ is defined as the degree of the finite extension $\overline{K}(E_1)/\phi^*\overline{K}(E_2)$, where $\phi^* : \overline{K}(E_2) \longrightarrow \overline{K}(E_1)$ is usual injection of function fields corresponding to E_2 and E_1, respectively.*

We have seen that elliptic curves form abelian groups, thus the maps between elliptic curves also form a group. We will denote isogenies from an elliptic curve E_1 to an elliptic curve E_2 by the following set

$$Hom(E_1, E_2)=\{\phi : E_1 \to E_2 : \phi \text{ is an isonegy}\}.$$

The sum of two isogenies is defined as follows

$$(\phi + \psi)(P) = \phi(P) + \psi(P)$$

where $\phi, \psi \in Hom(E_1, E_2)$. Since the equations giving group law on E are morphisms, the sum of two isogeny $\phi + \psi$ is still an isogeny. Thus $Hom(E_1, E_2)$ forms a group.

If we consider the set of isogenies from a elliptic curve E to itself, i.e. $Hom(E, E)$, we can also compose two isogenies. Let us denote the set of isogenies from E to E by $End(E)$, namely $Hom(E, E) = End(E)$. Then $End(E)$ forms a ring whose addition law is given as above and multiplication is given by the composition law as follows,

$$(\phi\psi)(P) = (\phi(\psi(P))$$

where $\phi, \psi \in End(E)$.

Definition 5.17. *Let E be an elliptic curve. The ring $End(E)$ is said to be the endomorphism ring of E. The invertible elements in $End(E)$ form the automorphism group of the elliptic curve E, it is denoted by $Aut(E)$.*

Example 5.18. The multiplication by m isogeny for each $m \in \mathbb{Z}$ is defined by

$$[m](P) = \underbrace{P + P + ... + P}_{\text{m times}}.$$

Let us set $[m](P) = [-m](-P)$ for $m < 0$. When $m = 0$, it is already defined as $[0](P) = O$, i.e. zero isogeny.

Definition 5.19. *Let E be an elliptic curve and let $m \in \mathbb{Z}$, $m > 1$. The m-torsion subgroup of the elliptic curve E is defined as the set of points of order m in E, which is given by*

$$E[m]=\{P \in E : [m](P) = O\}.$$

The torsion subgroup of the elliptic curve E is defined as the set of points of finite order in E as follows:

$$E_{tors} = \bigcup_{m=1}^{\infty} E[m].$$

Let K be a field. When the elliptic curve E is defined over K, the set of points of finite order in $E(K)$ is denoted by $E_{tors}(K)$.

Remark 5.20. Let K be a field and let $char(K) = 0$. Let us consider the following map

$$[\quad] : \mathbb{Z} \longrightarrow End(E).$$

It is injective since multiplication-by-n isogenies are always in $End(E)$. The map gives information about the structure of the elliptic curve E.

Definition 5.21. *Let E be an elliptic curve and let $End(E)$ be the endomorphism ring of E. If $End(E)$ is strictly larger than $\mathbb{Z}$, we say that the elliptic curve E has complex multiplication, or shortly CM.*

Elliptic curves with complex multiplication have many interesting properties, we will examine them in detail later. Now, we will give an example of elliptic curve having complex multiplication.

Example 5.22. Let K be a field with $char(K) \neq 2$ and let $i \in \overline{K}$ be a primitive fourth root of unity, i.e. $i^2 = -1$. The elliptic curve E/K determined by the equation

$$E : y^2 = x^3 - x$$

has the endomorphism ring $End(E)$ strictly larger than $\mathbb{Z}$, since $End(E)$ contains a map which is not a multiplication-by-n map, denoted by $[i]$

$$\begin{aligned}[i] :& E \longrightarrow E \\ & (x, y) \mapsto (-x, iy).\end{aligned}$$

Thus the elliptic curve E has complex multiplication. Let us note that

$$[i] \circ [i](x, y) = [i](-x, iy) = (x, -y) = -(x, y).$$

This means that $[i] \circ [i] = [-1]$. Thus, there exists a ring homomorphism such that

$$\begin{aligned}&\mathbb{Z}[i] \longrightarrow End(E) \\ &m + ni \mapsto [m] + [n] \circ [i].\end{aligned}$$

In fact, this map is an isomorphism if $char(K) = 0$. In this case, we get the automorphism group

$$Aut(E) \cong \mathbb{Z}[i]^* = \{\pm 1, \pm i\}$$

is a cyclic group of order 4.

Proposition 5.23. [5, Proposition 3.4.12.] *Let E be an elliptic curve and Φ be a finite subgroup of E. There exists a unique elliptic curve E' and a separable isogeny*

$$\phi : E \longrightarrow E' \quad \textit{satisfying} \quad ker(\phi) = \Phi.$$

5.1.4. Group of Rational Points of an Elliptic Curve

Let K be a number field and let E/K be an elliptic curve defined over K. Our main goal in this subsection is to give two important results about the structure of the group $(E(K), +)$.

Theorem 5.24. [5, THEOREM 8.4.1] *(Mordell-Weil) Let K be a number field and let E be an elliptic curve defined over K. The group $E(K)$ of K-rational points of E is a finitely generated abelian group and it has the following form*

$$E(K) \cong E(K)_{tors} \times \mathbb{Z}^r$$

where $E(K)_{tors}$ is the torsion subgroup containing all elements of finite order and $\mathbb{Z}^r$ is a free group of the rank r with nonnegative integer r.

In particular, the case of $K = \mathbb{Q}$ is obtained by Theorem 5.24

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{tors} \times \mathbb{Z}^r.$$

The structure of $E(\mathbb{Q})_{tors}$ is well-known. Mazur presented a list of all the possible torsion subgroups $E(\mathbb{Q})_{tors}$. On the other hand, the free group $\mathbb{Z}^r$ is mysterious and there are less results about the rank r, and also the rank r is difficult to compute. Since we are interested in the base field $K = \mathbb{Q}$ in this thesis, Mordel-Weil theorem is much more useful when $K = \mathbb{Q}$.

Theorem 5.25. [5, THEOREM 8.7.5.] *(Mazur) Let $E/\mathbb{Q}$ be an elliptic curve over $\mathbb{Q}$. Then, the torsion subgroup $E(\mathbb{Q})_{tors}$ of $E(\mathbb{Q})$ is isomorphic to one of the following fifteen finite groups:*

$$\mathbb{Z}/N\mathbb{Z} \text{ when } 1 \leq N \leq 10 \text{ or } N = 12,$$
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z} \text{ when } 1 \leq N \leq 4.$$

Moreover, each one of these groups occurs as a torsion subgroup $E(\mathbb{Q})_{tors}$ for some elliptic curve $E/\mathbb{Q}$ over $\mathbb{Q}$.

5.1.5. Elliptic Curves over $\mathbb{C}$

Definition 5.26. *Let ω and ω' be $\mathbb{R}$-linearly independent complex numbers. A complex lattice defined by ω, ω' is the following set:*

$$\Lambda = \{a\omega + b\omega' : a, b \in \mathbb{Z}\}.$$

Fact 5.27. A lattice is a free $\mathbb{Z}$-module of rank 2. The set $\{\omega, \omega'\}$ forms a basis of the lattice defined by ω, ω' as a $\mathbb{Z}$-module. Every element $\lambda \in \Lambda$ is written uniquely as $\lambda = a\omega + b\omega'$ for some $a, b \in \mathbb{Z}$. The basis $\{\omega, \omega'\}$ is not unique, and the basis is independent of a choice of a basis.

Definition 5.28. *Let Λ_1 and Λ_2 be lattices. The lattices Λ_1 and Λ_2 are said to be homothetic if there exists a complex number $c \in \mathbb{C}^*$ such that $\Lambda_1 = c\Lambda_2$.*

Definition 5.29. *Let Λ be a lattice. A fundamental parallelogram for the lattice Λ is the following set*

$$D = \{a + k_1\omega_1 + k_2\omega_2 : 0 \leq k_1, k_2 < 1\}$$

where $a \in \mathbb{C}$ and $\{\omega_1, \omega_2\}$ is a basis of the lattice Λ.

Definition 5.30. *Let Λ be a lattice. An elliptic function f relative to the lattice Λ is defined as a meromorphic function on $\mathbb{C}$ satisfying the following condition*

$$f(z+\omega) = f(z) \text{ for all } \omega \in \Lambda, z \in \mathbb{C}.$$

Remark 5.31. Liouville's Theorem says that every holomorphic bounded entire function f is constant.

Proposition 5.32. [5, Proposition 6.2.1] *An elliptic function which has no poles (or no zeros) is constant.*

Proof. Let f be a holomorphic function on $\mathbb{C}$ and let D be a fundamental parallelogram for Λ. Since f is periodic,

$$\sup_{z\in\mathbb{C}} |f(z)| = \sup_{z\in\bar{D}} |f(z)|.$$

It is known that f is continuous and $\bar{D}$ is compact, then $|f(z)|$ is bounded on entire $\mathbb{C}$. By using Liouville's theorem, f is constant. Moreover, if f has no zero, look at $1/f$ and proceed similarly. □

Definition 5.33. *Let $\Lambda \in \mathbb{C}$ be a lattice. The Weierstrass $\wp(z)$-function is defined for each $z \in \mathbb{C} \setminus \Lambda$ by the series*

$$\wp(z) = \frac{1}{z^2} + \sum_{\substack{\omega\neq 0 \\ \omega\in\Lambda}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right) \quad \text{for } z \in \mathbb{C} \text{ and } z \notin \Lambda.$$

The Eisenstein series of weight $2k$ for Λ is given by the series

$$G_{2k}(\Lambda) = \sum_{\substack{\omega\neq 0 \\ \omega\in\Lambda}} \omega^{-2k}.$$

Theorem 5.34. [5, THEOREM 6.3.1] *Let $\Lambda \subset \mathbb{C}$ be a lattice with a basis $\{\omega_1, \omega_2\}$ and let $\wp$ be the Weierstrass function relative to Λ.*

(i) The Eisenstein series $G_{2k}(\Lambda)$ is absolutely convergent for $k > 1$.

(ii) The series defining $\wp$ converges absolutely and uniformly in every compact set which does not contain an element of Λ.

(iii) The Weierstrass $\wp$-function is an even elliptic function.

Theorem 5.35. [5, THEOREM 6.3.2] *Let $\Lambda \in \mathbb{C}$ be a lattice and let $\mathbb{C}(\Lambda)$ be the set of all elliptic functions. Then, every elliptic function is a combination of the Weierstrass $\wp$-function and its derivative $\wp'$. Hence,*

$$\mathbb{C}(\Lambda) = \mathbb{C}(\wp(z), \wp'(z)).$$

Theorem 5.36. [5, THEOREM 6.3.5.]

(i) The Laurent series of the Weierstrass $\wp(z)$ function around $z = 0$ is

$$\wp(z) = \frac{1}{z^2} + \sum_{k=1}^{\infty} (2k+1) G_{2k+2} z^{2k}.$$

(ii) Let $z \in \mathbb{C} \setminus \Lambda$. The Weierstrass $\wp(z)$ function and its derivative $\wp'(z)$ satisfy the following relation

$$\wp'(z)^2 = 4\wp(z)^3 - 60G_4\wp(z) - 140G_6. \tag{5.1}$$

Remark 5.37. The standard notation is given as follows

$$g_2 = g_2(\Lambda) = 60G_4(\Lambda) \quad \textit{and} \quad g_3 = g_3(\Lambda) = 140G_6.$$

Thus, the relation between $\wp(z)$ and $\wp'(z)$ turns into the following form

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3.$$

Proposition 5.38. [5, PROPOSITION 6.3.6.] *Let $\Lambda \in \mathbb{C}$ be a lattice. Let $g_2 = g_2(\Lambda)$ and $g_3 = g_3(\Lambda)$ be quantaties related to the lattice Λ.*

(i) The polynomial $f(x) = 4x^2 - g_2x - g_3$ has distinct roots. The discriminant of $f(x)$ is given by $\Delta(\Lambda) = g_2^3 - 27g_3^3$, which is nonzero.

(ii) Let $E/\mathbb{C}$ be an elliptic curve given by

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

which is an elliptic curve due to (i). Then, the following map

$$\begin{aligned} \phi :& \mathbb{C}/\Lambda \longrightarrow E(\mathbb{C}) \\ & z \mapsto [\wp(z), \wp'(z), 1] \end{aligned}$$

is a complex analytic isomorphism, i.e., it is an isomorphism of Riemann surfaces which is also a group homomorphism.

Definition 5.39. *The j-invariant of the lattice Λ is defined as*

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

Remark 5.40. Notice that $\Delta(\Lambda)$ is not equal to 0, so the j-invariant of a lattice Λ is always well-defined.

Theorem 5.41. [5, THEOREM 6.4.1.] *Let $\alpha \in \mathbb{C}$ and $\Lambda_1, \Lambda_2 \subset \mathbb{C}$ be lattices such that $\alpha\Lambda_1 \subset \Lambda_2$. Let ϕ_α be a holomorphic homomorphism satisfying*

$$\begin{aligned} \phi_\alpha :& \mathbb{C}/\Lambda_1 \longrightarrow \mathbb{C}/\Lambda_2 \\ & \phi_\alpha(z) = \alpha z \ mod\ \Lambda \ . \end{aligned}$$

(i) The association

$$\{\alpha \in \mathbb{C} : \alpha\Lambda_1 \subset \Lambda_2\} \longrightarrow \left\{ \begin{array}{c} holomorphic\ maps \\ \phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2 \\ with\ \phi(0) = 0 \end{array} \right\} \tag{5.2}$$

$$\alpha \qquad \longmapsto \qquad \phi_\alpha \tag{5.3}$$

is a bijection.

(ii) Let E_1 and E_2 be elliptic curves corresponding to lattices Λ_1 and Λ_2, respectively. They are given by $E_1 : y^2 = 4x^3 - g_2(\Lambda_1)x - g_3(\Lambda_1)$ and $E_2 : y^2 = 4x^3 - g_2(\Lambda_2)x - g_3(\Lambda_2)$. Then the natural inclusion

$$\{isogenies\ \phi : E_1 \to E_2\} \longrightarrow \left\{ \begin{array}{c} holomorphic\ maps \\ \phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2 \\ with\ \phi(0) = 0 \end{array} \right\}$$

is bijection.

This theorem gives the only holomorphic maps from $\mathbb{C}/\Lambda_1$ to $\mathbb{C}/\Lambda_2$.

Corollary 5.42. [5, COROLLARY 6.4.1.1.] *Let $E_1/\mathbb{C}$ and $E_2/\mathbb{C}$ be elliptic curves corresponding to lattices Λ_1 and Λ_2, respectively. Then E_1 and E_2 are isomorphic over $\mathbb{C}$ if and only if Λ_1 and Λ_2 are homothetic, it means that there exists some $\alpha \in \mathbb{C}^*$ such that $\Lambda_1 = \alpha\Lambda_2$.*

Proof. Firstly, let us suppose that Λ_1 and Λ_2 are homothetic lattices. This means that there exists an $\alpha \in \mathbb{C}^*$ such that $\Lambda_2 = \alpha\Lambda_1$. Then

$$g_2(\Lambda_2) = g_2(\alpha\Lambda_1) = 60G_4(\alpha\Lambda_1) = 60 \sum_{\substack{w\in\alpha\Lambda_1 \\ w\neq 0}} w^{-4} = 60\alpha^{-4} \sum_{\substack{w\in\Lambda_1 \\ w\neq 0}} w^{-4} = \alpha^{-4} g_2(\Lambda_1)$$

and

$$g_3(\Lambda_2) = g_3(\alpha\Lambda_1) = 140G_6(\alpha\Lambda_1) = 140 \sum_{\substack{w\in\alpha\Lambda_1 \\ w\neq 0}} w^{-6} = 140\alpha^{-4} \sum_{\substack{w\in\Lambda_1 \\ w\neq 0}} w^{-6} = \alpha^{-6} g_2(\Lambda_1).$$

Thus

$$j(\Lambda_2) = 1728\frac{g_2(\Lambda_2)^3}{g_2(\Lambda_2)^3 - 27g_3(\Lambda_2)^2} = 1728\frac{\alpha^{-12}g_2(\Lambda_1)^3}{\alpha^{-12}g_2(\Lambda_1)^3 - \alpha^{-12}27g_3(\Lambda_1)^2} = j(\Lambda_1).$$

Since j-invariants of the lattices Λ_1 and Λ_2 are the same, the elliptic curves E_1 and E_2 are isomorphic over $\mathbb{C}$ by Theorem 5.7.

Conversely, let us suppose that E_1 and E_2 are isomorphic. This implies that E_1 and E_2 have the same j-invariants by Proposition 5.7. Thus, lattices Λ_1 and Λ_2 satisfy the equality $j(\Lambda_1) = j(\Lambda_2)$. By using the definition of j-invariant, we can choose $\alpha \in \mathbb{C}^*$ satisfying the following condition

$$\alpha^4 = \frac{g_2(\Lambda_1)}{g_2(\Lambda_2)} \qquad \text{and} \qquad \alpha^6 = \frac{g_3(\Lambda_1)}{g_3(\Lambda_2)}. \tag{5.4}$$

This means that $\Lambda_2 = \alpha\Lambda_1$. Thus Λ_1 and Λ_2 are homothetic lattices. □

Theorem 5.43. [5, THEOREM 6.5.1.] *(Uniformization Theorem) Let $E/\mathbb{C}$ be an elliptic curve. Then, there exists a lattice $\Lambda \subset \mathbb{C}$ (unique up to homothety) and a complex analytic isomorphism such that*

$$f : \mathbb{C}/\Lambda \longrightarrow E(\mathbb{C}) \tag{5.5}$$

$$z \longmapsto [\wp(z;\Lambda), \wp'(z;\Lambda), 1]. \tag{5.6}$$

The elliptic curve is given by $E_\Lambda : y^2 = x^3 - Ax - B$ where $A = g_2(\Lambda) = 60G_4(\Lambda)$, $B = g_3(\Lambda) = 140G_6(\Lambda)$.

5.1.6. n-Torsion Points

Theorem 5.44. [5, COROLLARY 6.5.4.] *Let E be an elliptic curve over $\mathbb{C}$. The group of n-torsion points $E[n]$ is isomorphic to the direct sum of two cyclic groups of order n,*

$$E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

Proof. According to Uniformizaton Theorem (Theorem 5.43), the elliptic curve $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$ for some $\Lambda \subset \mathbb{C}$. Thus,

$$E[n] \cong \Big(\frac{\mathbb{C}}{\Lambda}\Big)[n] \cong \frac{\frac{1}{n}\Lambda}{\Lambda} \cong \Big(\frac{\mathbb{Z}}{n\mathbb{Z}}\Big)^2.$$

□

Fact 5.45. The last Theorem 5.44 shows that $E[n]$ is generated by two points P_1,$P_2 \in E[n]$. For any point P in $E[n]$, there exist $a_1, a_2 \in \mathbb{Z}/n\mathbb{Z}$ such that $P = a_1P_1 + a_2P_2$. In other words, P_1 and P_2 are the images of some generators of $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

5.2. Construction of $\mathbb{GL}_2(\mathbb{F}_p)$

In this section, we will examine how elliptic curves are related to Galois groups of Galois extensions. The main purpose is to construct these Galois extensions step by step by using elliptic curves.

Let K be a number field, i.e., K is a finite extension of $\mathbb{Q}$ such that $[K:\mathbb{Q}] = n$ for some positive integer n. Firstly, we know that there exists an element $\alpha \in K$ satisfying $K = \mathbb{Q}(\alpha)$ by Theorem 2.5. In other words, if $m_\alpha(x)$ is the minimal polynomial of α over $\mathbb{Q}$, then we obtain $\mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/\langle m_\alpha(x)\rangle$. Thus, we can find exactly n distinct field homomorphisms $\sigma_i : K \longrightarrow \mathbb{C}$ mapping α to a root α_i of the minimal polynomial $m_\alpha(x)$. Since $x_i's$ are all distinct, these maps are also distinct. Indeed, if $m_\alpha(x)$ had a multiple root x_i, then the derivative $m'_\alpha(x_i) = 0$ and x_i would be a zero of a polynomial having smaller degree than $m_\alpha(x)$. This gives a contradiction with the fact that $m_\alpha(x)$ is also minimal polynomial of x_i over $\mathbb{Q}$, since it is monic and irreducible polynomial. Then, we conclude that $m_\alpha(x)$ has no multiple root. Furthermore, we have $\mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/\langle m_\alpha(x)\rangle$ which is given by the first isomorphism theorem mapping a polynomial $f(x) \in \mathbb{Q}[x]$ to $f(\alpha)$. Thus, every element in $\mathbb{Q}(\alpha)$ can be written as $a_0 + a_1\alpha + ... + a_{d-1}\alpha^{d-1}$ where $d = deg(m_\alpha(x))$ and $a_0, ..., a_{d-1} \in \mathbb{Q}$. By using the fact $m_\alpha(\alpha_i) = 0$, we get the field isomorphism mapping α to α_i. Therefore, we have isomorphisms as follows

$$\mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/\langle m_\alpha(x)\rangle \cong \mathbb{Q}(\alpha_i) \subseteq \mathbb{C}$$

for each root α_i of the polynomial $m_\alpha(x)$.

5.2.1. Automorphisms of the Points of an Elliptic Curve

Let $K/\mathbb{Q}$ be an algebraic extension and let E be an elliptic curve. Let $\sigma : K \longrightarrow \mathbb{C}$ be a field homomorphism. Let us define a map on $E(K)$ such that

$$\begin{aligned} &E(K) \longrightarrow E(\bar{K}) \\ &P = (x, y) \mapsto \sigma(P) = (\sigma(x), \sigma(y)) \end{aligned} \quad .$$

If we consider homogeneous coordinates of points, this map sends a point $[x_0, x_1, x_2] \in E(K)$ to $\sigma([x_0, x_1, x_2]) = [\sigma(x_0), \sigma(x_1), \sigma(x_2)]$. It is easy to see that this map is well-defined and $\sigma(O) = O$. Some features of this map will be verified in the following proposition.

Proposition 5.46. [15, Proposition 6.3] *Let $K/\mathbb{Q}$ be a finite algebraic extension and let E be an elliptic curve defined by Weierstrass equation $y^2 = x^3 + ax^2 + bx + c$ where $a, b, c \in \mathbb{Q}$.*

(i) Let $\sigma : K \longrightarrow \mathbb{C}$ be a field homomorphism and let $P \in E(K)$. Let us define

$$\sigma(P) = \begin{cases} (\sigma(x), \sigma(y)) \text{ if } P = (x, y) \\ O \quad if \quad P = O. \end{cases}$$

Then, $\sigma(P) \in E(\bar{K})$.

(ii) Let $\sigma : K \longrightarrow \mathbb{C}$ be a field homomorphism and let P, Q be two points in $E(K)$. Then,

$$\sigma(P + Q) = \sigma(P) + \sigma(Q) \quad and \quad \sigma(-P) = -\sigma(P).$$

In particular, $\sigma(nP) = n(\sigma(P))$ for all integers n.

(iii) If $K/\mathbb{Q}$ is a Galois extension, then $\sigma(P) \in E(K)$ for all $P \in E(K)$ and for all $\sigma \in Gal(K/\mathbb{Q})$. Furthermore, we obtain $(\sigma\tau)(P) = \sigma(\tau(P))$ for all $\sigma, \tau \in Gal(K/\mathbb{Q})$.

(iv) Let $K/\mathbb{Q}$ be a Galois extension. Let $P \in E(K)$ be a point of order n and let σ be an element in $Gal(K/\mathbb{Q})$. Then $\sigma(P)$ is also point of order n.

Proof.

(i) Using homogeneous coordinates, it is easy to see that $\sigma(O) = O$. Let us now consider a point $P = (x, y) \in E(K)$. It is known that $y^2 - x^3 - ax^2 - bx - c = 0$ by definition of the elliptic curve E. Applying σ to both sides of the equality, we obtain:

$$\begin{aligned}
&\sigma(y^2 - x^3 - ax^2 - bx - c) = 0 \\
&\sigma(y)^2 = \sigma(x)^3 + \sigma(a)\sigma(x)^2 + \sigma(b)\sigma(x) + \sigma(c) \quad \text{since } \sigma \text{ is a field homomorphism,} \\
&\sigma(y)^2 = \sigma(x)^3 + a\sigma(x)^2 + b\sigma(x) + c \qquad\qquad \text{since } \sigma \text{ fixes } a, b, c \in \mathbb{Q}.
\end{aligned}$$

This means that $\sigma(P) = (\sigma(x), \sigma(y)) \in E(\bar{K})$.

(ii) Let us recall that if P, Q are K-rational points, the line passing through P and Q is also K-rational. Hence, $P + Q$ is also K-rational. We will again use the fact that σ is identity on $\mathbb{Q}$ here. For instance, if $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ where $x_1 \neq x_2$ and $y_1 \neq y_2$, we can use formulas given in Example 5.12. Since P and Q are K-rational points, the slope of the line passing through P and Q is $r = \frac{y_1 - y_2}{x_1 - x_2} \in K$. Thus, $\sigma(r)$ is well-defined, and we can compute the point $P + Q$. Since σ is $\mathbb{Q}$-homomorphism, we get:

$$\begin{aligned}
\sigma(x_3) &= \left(\frac{\sigma(y_1) - \sigma(y_2)}{\sigma(x_1) - \sigma(x_2)}\right)^2 - a - \sigma(x_1) - \sigma(x_2) \\
\text{and} \quad \sigma(y_3) &= \left(\frac{\sigma(y_1) - \sigma(y_2)}{\sigma(x_1) - \sigma(x_2)}\right)(\sigma(x_1) - \sigma(x_3)) - \sigma(y_1).
\end{aligned}$$

Thus,

$$\begin{aligned}
\sigma(P + Q) = (\sigma(x_3), \sigma(y_3)) &= (\sigma(x_1), \sigma(y_1)) + (\sigma(x_2), \sigma(y_2)) \\
&= \sigma(P) + \sigma(Q).
\end{aligned}$$

In a similar way, the fact $\sigma(-P) = -\sigma(P)$ can be proved easily. If $P = (x, y)$,

$$\sigma(-P) = (\sigma(x), \sigma(-y)) = (\sigma(x), -\sigma(y)) = \sigma(-P).$$

(iii) Let us assume that $K/\mathbb{Q}$ is a Galois extension. Thus, every field homomorphism $\sigma : K \longrightarrow \mathbb{C}$ is an automorphism. Thus, $\sigma(x), \sigma(y) \in K$. This concludes that $\sigma(P) \in E(K)$. The composition $(\sigma\tau)(P) = \sigma(\tau(P))$ can be seen easily in the same way.

(iv) Let $P \in E(K)$ have order n, and let m be the order of $\sigma(P)$. By using (ii), we get

$$n(\sigma(P)) = \sigma(nP) = \sigma(O) = O.$$

This means m divides n. Conversely, it is known that $O = m\sigma(P) = \sigma(mP)$ and apply σ^{-1} to both sides, we obtain

$$O = \sigma^{-1}(O) = \sigma^{-1}(\sigma(mP)) = (\sigma^{-1}\sigma)(mP) = mP.$$

So, n divides m. It is concluded that $m = n$.

□

5.2.2. Division Polynomials

In this subsection, we will define division polynomials in order to examine torsion subgroups of an elliptic curve. As we have seen in Example 5.18, multiplication by n-map is actually an isogeny, and it is given by rational functions. Division polynomials give formulas for these rational functions, they are used to compute points of order dividing n for an integer n.

Definition 5.47. *Let E be an elliptic curve defined over a field K with $char(K) \neq 2, 3$ and let $y^2 = x^3 + Ax + B$ be the Weierstrass equation of the elliptic curve E. The division polynomial $\psi_n \in \mathbb{Z}[x, y, A, B]$ is defined recursively as*

$\psi_0 = 0$

$\psi_1 = 1$

$\psi_2 = 2y$

$\psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2$

$\psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3)$

$\psi_{2n+1} = \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3 \quad for \quad n \geq 2$

$\psi_{2n} = (2y)^{-1}(\psi_n)(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2) \quad for \quad n \geq 2.$

Let us define the following polynomials by using division polynomials ψ_n's as follows:

$\phi_n = x\psi_n^2 - \psi_{n+1}\psi_{n-1}$

$\varphi_n = (4y)^{-1}(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2)$

Theorem 5.48. [16, Theorem 3.9] *Let E be an elliptic curve given by $y^2 = x^3 + Ax + B$ over a field K with $char(K) \neq 2$. Let $P = (x, y)$ be a point on the elliptic curve E and let n be a positive integer. Thus, the point nP is given by*

$$nP = \left(\frac{\phi_n(x)}{\psi_n^2(x)}, \frac{\varphi_n(x, y)}{\psi_n^3(x, y)} \right).$$

Fact 5.49. One can prove that $\psi(x,y)$ is a polynomial in x only for odd integers n. Since our aim is to calculate the x-coordinates of n-torsion points, we will restrict calculations to the polynomial $\psi(x)$.
The degree of the division polynomial can be found for an integer n, these are

$$deg(\psi_{2n}y) = \frac{n^2}{2} + 1, \quad deg(\psi_{2n+1}) = \frac{n^2-1}{2}.$$

The computations of the coordinates of n-torsion points for a large integer n are very complicated without using an computer algebra software. For instance, the implementation of the division polynomials exists in PARI/GP.

Example 5.50. Let E be an elliptic curve defined over $\mathbb{Q}$ given by $y^2 = x^3 + Ax + B$. Now, we will find 3-torsion points of the elliptic curve by using division polynomials. This example will be used later in order to construct $\mathbb{GL}_2(\mathbb{Z}/3\mathbb{Z})$.
Let $S = (x_S, y_S)$ be a point on the elliptic curve E. Firstly, we should compute the point $S + S = [2]S$. Since group operation is given by formulas, we need to find the tangent line of the curve at the point S. The tangent line equation is given in Definition 5.2, then we obtain the straight line as follows:

$$(3x_S^2 + A)(x - x_S) + 2y_S(y - y_S) = 0 \rightarrow y = -\frac{(A + 3x_S^2)x}{2y_S} + \frac{Ax_S + 3x_S^2 + 2y_S^2}{2y_S}.$$

If $y_S = 0$, then S is a 2-torsion point. For this reason, we assume $y_S \neq 0$. Let $\lambda_1 = -\frac{3x_S^2+A}{2y_S}$ be the slope and we find the coordinates of $[2]S$ as in Example 5.12.

$$x_{2S} = \lambda_1^2 - 2x_S \quad and \quad y_{2S} = \lambda_1(x_S - x_{2S}) - y_S.$$

Now, we will calculate the coordinates of $S + S + S = 3[S]$. Since x_S and x_{2S} are not equal, the slope λ_2 of the line passing through x_S and x_{2S} is given by

$$\lambda_2 = \frac{y_S - y_{2S}}{x_S - x_{2S}} = \frac{2y_S - \lambda_1(x_S - x_{2S})}{x_S - x_{2S}}.$$

The x-coordinate of $[3]S$ is obtained by $x_{3S} = \lambda_2^2 - x_S - x_{2S}$. The point S is 3-torsion point if and only if this coordinate is not finite. Thus, S is 3-torsion point if and only if λ_2 is not finite. This means that the denominator of λ_2 is zero. Thus, the necessary condition of the point S being 3-torsion is that $x_S - x_{2S} = 0$ as follows

$\leftrightarrow x_S - x_{2S} = 0$

$\leftrightarrow 3x_S - \lambda_1^2 = 0$

$\leftrightarrow 12x_S y_S^2 - (3x_S^2 + A)^2/4y_S^2 = 0$

$\leftrightarrow 12x_S(x_S^3 + Ax_S + B) - 9x_S^4 - 6Ax_S^2 - A^2 = 0$

$\leftrightarrow 3x_S^4 + 6Ax_S^2 + 12Bx_S - A^2 = 0.$

This is exactly the same condition given by division polynomials, namely $\psi_3(x_S) = 0$.

5.2.3. Galois Extension $\mathbb{Q}(E[n])/\mathbb{Q}$

Let E be an elliptic curve and $n \geq 1$. The subgroup $E[n]$ is used in order to construct Galois extension over $\mathbb{Q}$.

Proposition 5.51. [15, Theorem 6.5.] *Let E be an elliptic curve defined over $\mathbb{Q}$ and given by the Weierstrass equation $y^2 = x^3 + ax^2 + bx + c$ where $a, b, c \in \mathbb{Q}$. Then,*

(i) Let n be a positive integer and let $P = (x, y)$ be a point of order of dividing n on the elliptic curve E. The coordinates x and y of the point P are algebraic over $\mathbb{Q}$, i.e., x and y are roots of polynomials with rational coefficients.

(ii) Let $E[n] = \{O, (x_1, y_1), ..., (x_m, y_m)\}$ be the complete set of points of $E(\mathbb{C})$ of order dividing n, where $m = n^2 - 1$. Let K be the field extension of $\mathbb{Q}$ adjoining all the coordinates x_i, y_i where $1 \leq i \leq m$

$$K = \mathbb{Q}(E[n]) = \mathbb{Q}(x_1, y_1, ..., x_m, y_m).$$

Then, $K/\mathbb{Q}$ is a finite Galois extension over $\mathbb{Q}$.

Proof. (i) We will give a sketch of a computational proof. Let $P = (a, b)$ be a point of order dividing n on the elliptic curve E. The point $nP = (a_n, b_n)$ can be computed by using division polynomials where a_n and b_n denote the coordinates of the point nP for every integer n. According to Theorem 5.48, the coordinate a_n is given by

$$x\text{-coordinates of } nP = \left(\frac{\phi_n(x)}{\psi_n^2(x)}\right).$$

where $\phi_n(x)$ and $\psi_n^2(x)$ are relatively prime polynomials in $\mathbb{Q}[x]$. Let us write $A(x, y) = \frac{\phi_n(x,y)}{\psi_n^2(x,y)}$. Let $P_1 = (x_1, y_1)$ be any point of order dividing n, i.e. $[n]P_1 = O$. This implies that the rational function $A(x, y) = \frac{\phi_n(x,y)}{\psi_n^2(x,y)}$ is not defined. Then, the point $P_1 = (x_1, y_1)$ has order dividing n if and only if $\psi_n^2(x_1) = 0$. This proves that the x-coordinate of a point of order n is algebraic, since it is a root of the polynomial $\psi_n^2(x)$. Then the y-coordinate y_1 is also algebraic, since it is on the elliptic curve $y^2 = x^3 + ax^2 + bx + c$.

(ii) It is clear that the degree of the extension $K/\mathbb{Q}$ is finite. In fact, the coordinates x_i and y_i are algebraic over $\mathbb{Q}$ by the part (i). Since $E[n]$ is finite according to Theorem 5.44, we adjoin only a finite number of elements to $\mathbb{Q}$, and each of these elements has finite degree over $\mathbb{Q}$. Thus, K is a finite algebraic extension of $\mathbb{Q}$. Let us consider $\mathbb{Q}$-homomorphism $\sigma : K \longrightarrow \mathbb{C}$. In order to prove that K is a Galois extension over $\mathbb{Q}$, we have to prove that $\sigma(K) = K$. The map σ is completely determined by where it sends the coordinates x_i's and y_i's. Each point $P_i = (x_i, y_i)$ is a point of order dividing n. According to part (iv) of Proposition 5.46, we obtain $[n]\sigma(P_i) = \sigma([n]P_i) = \sigma(O) = O$ for any point $P_i = (x_i, y_i)$ of order dividing n. Thus, $\sigma(P_i)$ is also in $E[n]$. This means that $\sigma(P_i)$ is equal to one of the P_j's, where $1 \leq i \leq m$ with $i = j$ being allowed. This implies that $\sigma(K) \subset K$. Therefore, $K/\mathbb{Q}$ is a Galois extension.

□

5.2.4. Galois Representation

Let n be a positive integer. Let $P_i = (x_i, y_i)$ be points of order dividing n where $1 \leq i \leq m$. The field extension of $\mathbb{Q}$ generated by the coordinates of all points of order dividing n except O is $\mathbb{Q}(E[n]) = \mathbb{Q}(x_1, y_1, ..., x_m, y_m)$. It has been obtained that $\mathbb{Q}(E[n])$ is a Galois extension over rational numbers $\mathbb{Q}$ in Proposition 5.51. We will study the structure of the Galois group $Gal(\mathbb{Q}(E[n])/\mathbb{Q})$ of the Galois extension $\mathbb{Q}(E[n])/\mathbb{Q}$ in this subsection.

Theorem 5.52. *Let n be a fixed integer with $n \geq 2$. Let E be an elliptic curve given by the Weierstrass equation $y^2 = x^3 + ax^2 + bx + c$, where $a, b, c \in \mathbb{Q}$. Let $E[n]$ be the set of points of order dividing n and let P_1 and P_2 be the generators of the group $E[n]$. Then, there is a one-to-one group homomorphism*

$$\begin{aligned} \rho_n : & Gal(\mathbb{Q}(E[n])/\mathbb{Q}) \longrightarrow \mathbb{GL}_2(\mathbb{Z}/n\mathbb{Z}) \\ & \sigma \mapsto \varphi \circ \psi_\sigma \end{aligned}$$

Proof. The group homomorphism ρ_n will be constructed explicitly step by step in this proof. Let $P \in E[n]$ be a point of order dividing n. We know that $\sigma(P) \in E[n]$ for all $\sigma \in Gal(\mathbb{Q}(E[n])/\mathbb{Q})$ from Proposition 5.46. Thus each $\sigma \in Gal(\mathbb{Q}(E[n])/\mathbb{Q})$ induces a permutation of the set $E[n]$. This permutation is determined by

$$\sigma(P + Q) = \sigma(P) + \sigma(Q) \quad \sigma(-P) = -\sigma(P) \quad \sigma(O) = O.$$

Since $E[n]$ is an abelian group, every $\sigma \in Gal(\mathbb{Q}(E[n])/\mathbb{Q})$ result in a group homomorphism ψ_σ from $E[n]$ to itself,

$$\begin{aligned} \psi_\sigma : \quad & E[n] \longrightarrow E[n] \\ & P \mapsto \sigma(P) \end{aligned}$$

In fact, we have $[n]\psi_\sigma(P) = \psi_\sigma([n]P) = O$, and also the composition is preserved $\psi_{\sigma\tau}(P) = \psi_\sigma\psi_\tau(P)$ for any $\sigma, \tau \in Gal(\mathbb{Q}(E[n]/\mathbb{Q})$.
Furthermore, the homomorphism ψ_σ has an inverse $\psi_{\sigma^{-1}}$, namely the homomorphism corresponding to σ^{-1}. Then ψ_σ is automorphism such that $\psi_{\sigma^{-1}} = \psi_\sigma^{-1}$.

The set of automorphism of $E[n]$ forms a group, denoted by $Aut(E[n])$. Thus, the map

$$\begin{aligned} \psi :& Gal(\mathbb{Q}(E[n]/\mathbb{Q}) \longrightarrow Aut(E[n]) \\ & \sigma \mapsto \psi_\sigma \end{aligned}$$

is a group homomorphism.

Moreover, the group $E[n]$ can be generated by two points, namely P_1 and P_2. This means that any point $P \in E[n]$ can be written as $P = aP_1 + bP_2$ for some $a, b \in \mathbb{Z}/n\mathbb{Z}$. Thus, any homomorphism $g : E[n] \longrightarrow E[n]$ is determined by the images of the points P_1 and P_2. Also, we have obtained that $g(P_1)$ and $g(P_2)$ are in $E[n]$. So that one can find $\alpha, \beta, \gamma, \delta \in \mathbb{Z}/n\mathbb{Z}$ satisfying

$$g(P_1) = \alpha P_1 + \gamma P_2 \quad and \quad g(P_2) = \beta P_1 + \delta P_2.$$

Furthermore, for any $\alpha, \beta, \gamma, \delta \in \mathbb{Z}/n\mathbb{Z}$ the map g above is a group homomorphism of $E[n]$. Therefore, g can be represented by a matrix under the following map:

$$\begin{aligned} \varphi : Aut(E[n]) &\longrightarrow \mathbb{GL}_2(\mathbb{Z}/n\mathbb{Z}) \\ g \mapsto \varphi(g) &= \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \end{aligned}$$

where $\alpha, \beta, \gamma, \delta \in \mathbb{Z}/n\mathbb{Z}$ given by the definition of $g(P_1)$ and $g(P_2)$. It will be proved that φ is a group isomorphism.

Let us assume that $g, h \in Aut(E[n])$, we should show the following equality

$$\varphi(g \circ h) = \begin{bmatrix} \alpha_{g\circ h} & \beta_{g\circ h} \\ \gamma_{g\circ h} & \delta_{g\circ h} \end{bmatrix} = \begin{bmatrix} \alpha_g & \beta_g \\ \gamma_g & \delta_g \end{bmatrix} \begin{bmatrix} \alpha_h & \beta_h \\ \gamma_h & \delta_h \end{bmatrix} = \varphi(g)\varphi(h). \tag{5.7}$$

Let us check the first column of the matrix equality (5.8).

$$\begin{aligned} \alpha_{g\circ h}P_1 + \gamma_{g\circ h}P_2 &= (g \circ h)(P_1) && \text{by definition} \\ &= g(\alpha_h P_1 + \gamma_h P_2) \\ &= \alpha_h g(P_1) + \gamma_h g(P_2) \\ &= \alpha_h(\alpha_g P_1 + \gamma_g P_2) + \gamma_h(\beta_g P_1 + \delta_g P_2) \\ &= \alpha_g\alpha_h P_1 + \gamma_g\alpha_h P_2 + \beta_g\gamma_h P_1 + \delta_g\gamma_h P_2 \\ &= (\alpha_g\alpha_h + \beta_g\gamma_h)P_1 + (\gamma_g\alpha_h + \delta_g\gamma_h)P_2. \end{aligned}$$

By equating coefficients of P_1 and P_2 on both sides, we obtain

$$\alpha_{g\circ h} = \alpha_g\alpha_h + \beta_g\gamma_h \quad \textit{and} \quad \gamma_{g\circ h} = \gamma_g\alpha_h + \delta_g\gamma_h.$$

Thus, the first column of the matrix equality in (5.7) holds. We can proceed similarly for the second column equality by using P_2. These imply that φ is a group homomorphism. Notice that g is invertible since $g \in Aut(E[n])$. By using the facts that g is invertible and φ is a group homomorphism, we obtain:

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \varphi(gg^{-1}) = \begin{bmatrix} \alpha_g & \beta_g \\ \gamma_g & \delta_g \end{bmatrix} \begin{bmatrix} \alpha_{g^{-1}} & \beta_{g^{-1}} \\ \gamma_{g^{-1}} & \delta_{g^{-1}} \end{bmatrix} = \varphi(g)\varphi(g^{-1}).$$

Thus, $\varphi(g)$ is invertible and $\varphi(Aut(E[n])) \subseteq \mathbb{GL}_2(\mathbb{Z}/n\mathbb{Z})$. Finally, we can verify that φ is an isomorphism. Assume that $\varphi(g) = Id$, then it is easy to see that $g = Id$.

Furthermore, for any matrix

$$A = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \in \mathbb{GL}_2(\mathbb{Z}/n\mathbb{Z}),$$

one may consider the homomorphism defined by $g(P_1) = \alpha P_1 + \gamma P_2$ and $g(P_2) = \beta P_1 + \delta P_2$. We have already seen that this kind of application defines a homomorphism. Indeed, it is an isomorphism having inverse defined by A^{-1}. It is given by $g^{-1}(P_1) = \frac{\delta}{\triangle} P_1 - \frac{\gamma}{\triangle} P_2$ and $g^{-1}(P_2) = \frac{\beta}{\triangle} P_1 - \frac{\alpha}{\triangle}$ where $\triangle$ is the determinant of the matrix A.

Eventually, the group homomorphism is constructed by composing the two homomorphisms defined above:

$$\begin{aligned} \rho_n : & Gal(\mathbb{Q}(E[n])/\mathbb{Q}) \longrightarrow \mathbb{GL}_2(\mathbb{Z}/n\mathbb{Z}) \\ & \sigma \mapsto \varphi \circ \psi_\sigma \end{aligned}$$

There is left to show that the map ρ_n is injective. Let us assume that $\sigma \in Gal(\mathbb{Q}(E[n])/\mathbb{Q})$ is in the kernel of the map ρ_n, which means $\rho_n(\sigma) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

Then, $\sigma(P_1) = P_1$ and $\sigma(P_2) = P_2$, it follows that $\sigma(P) = P$ for every $P \in E[n]$. By definition $\sigma(P) = (x, y) = (\sigma(x), \sigma(y))$, this implies that σ fixes the x-coordinates and y-coordinates of every point in $E[n]$. Since the field $\mathbb{Q}(E[n])$ is generated by x and y coordinates of the points in $E[n]$ over $\mathbb{Q}$, σ fixes the generators of $\mathbb{Q}(E[n])$, then it fixes the whole field $\mathbb{Q}(E[n])$. So, σ is the identity element of $Gal(\mathbb{Q}(E[n]))$, and there is only the identity element in the kernel of the map ρ_n. Then ρ_n is bijective.

□

Definition 5.53. *(Galois Representation) The map*

$$\rho_n : Gal(\mathbb{Q}(E[n])/\mathbb{Q}) \longrightarrow \mathbb{GL}_2(\mathbb{Z}/n\mathbb{Z})$$

defined in the previous theorem is said to be Galois representation.

Remark 5.54. The map ρ_n is not always surjective. We will give two examples of elliptic curves E_1 and E_2 such that E_2 has a surjective Galois representation ρ_n and E_2 does not admit a surjective Galois representation ρ_n.

Let E be an elliptic curve determined by $y^2 = x^3 + ax^2 + bx + c$, where $a, b, c \in \mathbb{Q}$. Let $n = 2$ be fixed, we are going to consider 2-torsion points. Let $P = (x, y)$ be a point on the elliptic curve E. The coordinates of the point $P + P = 2P$ can be computed easily. The point P of the elliptic curve E satisfies $2P = O$ if and only if $P = -P$ if and only if $(x, y) = P = -P = (x, -y)$. Thus, y-coordinates of 2-torsion points must be 0, and x-coordinates can be found by plugging $y = 0$ in $y^2 = x^3 + ax^2 + bx + c$. Furthermore, we know that $E[2]$ has 4 elements since $E[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

(i) Let E_1 be an elliptic curve given by $y^2 = (x-1)(x-2)(x-3)$. Then, 2-torsion points of the elliptic curve E_1 is $E_1[2] = \{O, (1,0), (2,0), (3,0)\}$. Thus, we obtain $\mathbb{Q}(E_1[2]) = \mathbb{Q}$ and $Gal(\mathbb{Q}(E_1[2])/\mathbb{Q}) = Id$. The Galois representation ρ_2 is clearly not surjective in this case.

(ii) Let E_2 be an elliptic curve given by $y^2 = x^3 - 3$. Then, 2-torsion points of the elliptic curve E_2 is $E_2[2] = \{O, (\sqrt[3]{-3}, 0), (\sqrt[3]{-3}e^{2\pi i/3}, 0), (\sqrt[3]{-3}e^{4\pi i/3}, 0)\}$. Thus, we obtain $\mathbb{Q}(E_2[2]) = \mathbb{Q}(\sqrt[3]{-3}, e^{2\pi i/3})$, which is the splitting field of the polynomial $x^3 - 3 \in \mathbb{Q}[x]$. Moreover, we also know that $Gal(\mathbb{Q}(\sqrt[3]{-3}, e^{2\pi i/3}))/\mathbb{Q}$ has order 6. This means that ρ_2 is surjective, and we have $Gal(\mathbb{Q}(E_2[2])/\mathbb{Q} \cong \mathbb{GL}_2(\mathbb{Z}/2\mathbb{Z})$.

Actually, the representations ρ_n are "almost" onto for most elliptic curves, meaning that most of the elliptic curves have surjective images.

5.2.5. Construction of $\mathbb{GL}_2(\mathbb{Z}/3\mathbb{Z})$

In this subsection, we will use a particular elliptic curve E in order to construct $\mathbb{GL}_2(\mathbb{Z}/3\mathbb{Z})$ as a Galois group of a Galois extension over $\mathbb{Q}$. As we have seen in the previous subsection, $E[3]$ will have a special role to construct $\mathbb{GL}_2(\mathbb{Z}/3\mathbb{Z})$ as a Galois group. Therefore, we will present a general method to construct $\mathbb{GL}_2(\mathbb{Z}/n\mathbb{Z})$ as a Galois group for any positive integer n.

Let E be the elliptic curve given by the following Weierstrass equation

$$E: \quad y^2 = x^3 - x + 1/4.$$

Using the division polynomials and conditions given in Example 5.50, one has that the x-coordinates of points of order 3 in the elliptic curve E are roots of the following polynomial

$$3x^4 - 6x^2 + 3x - 1.$$

Since the points of order 3 are points on the elliptic curve E, the y-coordinates of points of order 3 in E are found by using the equation $y^2 = x_i^3 - x_i + 1/4$ for any root x_i where $1 \leq i \leq 4$. Actually, we do not have to find these coordinates. If exact values are needed, Viete formula can be used to find the roots of the above quartic equation.

Now, we have all the necessary information obtained in the previous section:

(i) $\mathbb{Q}(E[3])/\mathbb{Q}$ is a Galois extension.
(ii) The Galois representation $\rho_3 : Gal(\mathbb{Q}(E[3])/\mathbb{Q}) \to \mathbb{GL}_2(\mathbb{Z}/3\mathbb{Z})$ is a one-to-one group homomorphism.

Since we have two finite groups, we obtain $[\mathbb{Q}(E[3])/\mathbb{Q}] \leq |\mathbb{GL}_2(\mathbb{Z}/3\mathbb{Z})|$ by using (ii). We will now use the equivalence that $A \in \mathbb{GL}_2(\mathbb{Z}/3\mathbb{Z})$ if and only if $det(A) \neq 0$ in order to calculate cardinality of $\mathbb{GL}_2(\mathbb{Z}/3\mathbb{Z})$.

This happens if the columns of the matrix A are linearly independent. Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, and the column $\begin{bmatrix} a \\ c \end{bmatrix}$ may be anything different from 0-vector. So, we have 8 possibilities. For the second column $\begin{bmatrix} b \\ d \end{bmatrix}$, we can choose any vector which is linearly independent from the first column $\begin{bmatrix} a \\ c \end{bmatrix}$. Hence, we have 6 possibilities and the cardinality of $\mathbb{GL}_2(\mathbb{Z}/3\mathbb{Z})$ is $8.6 = 48$. The next step is to show that $[\mathbb{Q}(E[n]) : \mathbb{Q}] \geq 48$. So that we can conclude that $|\mathbb{GL}_2(\mathbb{Z}/3\mathbb{Z})| = 48$.

In order to find the degree of the extension $\mathbb{Q}(E[3])/\mathbb{Q}$, we will construct the splitting field K of the polynomial $3x^4 - 6x^2 + 3x - 1$ by using PARI/GP. The field K is the smallest field extension of $\mathbb{Q}$ containing all the x-coordinates of the points of order 3 in E. Then, we get the field $K = \mathbb{Q}[t]/\langle f(t) \rangle$ where $f(t)$ is the following irreducible polynomial:

$$f(t) = t^{24} - 12t^{23} + 70t^{22} - 264t^{21} + 718t^{20} - 1482t^{19} + 2357t^{18} - 2802t^{17} + 2152t^{16} - 216t^{15} - 2288t^{14} + 4224t^{13} - 4915t^{12} + 4224t^{11} - 2288t^{10} - 216t^9 + 2152t^8 - 2802t^7 + 2357t^6 - 1482t^5 + 718t^4 - 264t^3 + 70t^2 - 12t + 1.$$

This shows that the extension $K/\mathbb{Q}$ has degree 24. It is enough to prove that $K \neq \mathbb{Q}(E[3])$ in order to verify that the degree of $\mathbb{Q}(E[3])$ over $\mathbb{Q}$ is 48. Indeed, let α be a root of the polynomial $3x^4 - 6x^2 + 3x + 1$ in K. It can be seen that the polynomial $y^2 - \alpha^3 + \alpha - 1/4$ is irreducible over K by using PARI/GP. This implies that y coordinates of the points having x-coordinate α do not belong to K. Thus, $K \neq \mathbb{Q}(E[3])$ and we conclude that $[\mathbb{Q}(E[3]) : \mathbb{Q}] = |Gal(\mathbb{Q}(E[3])/\mathbb{Q})| = 48$.

Therefore, we have the isomorphism

$$Gal(\mathbb{Q}(E[3])/\mathbb{Q}) \cong \mathbb{GL}_2(\mathbb{Z}/3\mathbb{Z}).$$

Proposition 5.55. *Let E be an elliptic curve defined over $\mathbb{Q}$ by the Weierstrass equation $y^2 = x^3 + ax + b$. Let $p \neq 2$ be a prime number and let us assume that the Galois representation $\rho_p : Gal(\mathbb{Q}(E[p])/\mathbb{Q}) \longrightarrow \mathbb{GL}_2(\mathbb{Z}/p\mathbb{Z})$ is surjective. Then,*

(i) The division polynomial ψ_p, whose roots are the x-coordinates of the nontrivial p-torsion points in E, is irreducible over $\mathbb{Q}$ and its Galois group over $\mathbb{Q}$ is $\mathbb{GL}_2(\mathbb{F}_p)/\{\pm 1\}$.

(ii) Let $P = (x, y) \in E[p] - \{O\}$. The characteristic polynomial of the multiplication by $x + y$ map in $K(x, y)$ is irreducible. Furthermore, its Galois group over K is $\mathbb{GL}_2(\mathbb{Z}/p\mathbb{Z})$.

Proof.

(i) It is omitted. For the proof, see Theorem 2.1 in the paper [6].

(ii) Let G denote the Galois group $Gal(\mathbb{Q}(E[p])/\mathbb{Q})$. The set of conjugates of x is

$$C(x) = \{\sigma(x) : \sigma \in G\}.$$

Similarly, the set of conjugates of $x + y$ is

$$C(x + y) = \{\sigma(x + y) : \sigma \in G\}.$$

Indeed, $\sigma \in G$ defines an automorphism of $E[p]$ as proved in Subsection 7.2.1. Thus, we have inclusions:

$$C(x) = \{\sigma(x) : \sigma \in G\} \subseteq \{x_i : (x_i, \pm y_i) \in E[p]\}$$
$$C(x + y) = \{\sigma(x + y) : \sigma \in G\} \subseteq \{x_i \pm y_i : (x_i, \pm y_i) \in E[p]\}.$$

Furthermore, let $\{P, Q\}$ be a basis of $E[p]$. Let $T = (x_i, y_i)$ for each $x_i \in C(x)$. Since p is a prime number, a basis exists for any point P of order p. Thus, any element may be taken as a generator. So, $aP + bQ = T$ for some $a, b \in \mathbb{Z}/p\mathbb{Z}$.

Since $a \neq 0$ or $b \neq 0$, there exist $c, d, c', d' \in \mathbb{Z}/p\mathbb{Z}$ such that $M = \begin{bmatrix} a & c \\ b & d \end{bmatrix}$ and $M' = \begin{bmatrix} -a & c' \\ -b & d' \end{bmatrix}$ belong to $\mathbb{GL}_2(\mathbb{Z}/p\mathbb{Z})$. Since the Galois representation ρ_p is surjective by assumption, there exist $\tau, \tau' \in G$ such that $\rho_p(\tau) = M$ and $\rho_p(\tau') = M'$. Then, we obtain

$$\tau(P) = aP + bQ = T \quad \text{and} \quad \tau'(P) = -T = (x_i, -y_i)$$

This proves the equalities for $C(x)$ and $C(x+y)$

$$\begin{aligned} & C(x) = \{\sigma(x) : \sigma \in G\} = \{x_i : (x_i, \pm y_i) \in E[p]\} \\ \text{and} \quad & C(x+y) = \{\sigma(x+y) : \sigma \in G\} = \{x_i \pm y_i : (x_i, \pm y_i) \in E[p]\}. \end{aligned}$$

Thus, we have

$$\mathbb{Q}(E[p]) = \mathbb{Q}(\{x_i \pm y_i : (x_i, \pm y_i) \in E[p]\}) = \mathbb{Q}(C(x+y)).$$

Let $\{\beta_i\}_{i=1}^s$ be the set of all distinct conjugates of $x+y$. Since $\mathbb{Q}(E[p])/\mathbb{Q}$ is a Galois extension and $x+y$ belongs to $\mathbb{Q}(E[p])$, the minimal polynomial of $x+y$ over $\mathbb{Q}$, namely $m_{x+y}(t)$, can be written as

$$m_{x+y}(t) = \prod_{i=1}^{s} (t - \beta_i).$$

This proves that the splitting field of $m_{x+y}(t)$ is $\mathbb{Q}(E[p])$.

Also we have that Ψ_p is irreducible and it has no multiple zero. This means that $x_i \neq x_j$ for all $i \neq j$. Let us now consider the automorphism σ of $E[p]$ mapping $P \in E[p]$ to $-P \in E[p]$. Since the Galois representation ρ_p is surjective, there is an element of G inducing the automorphism σ. We will denote this element by σ as well.

Also, σ fixes all the x_i's by definition of $-P$. Thus, we can verify that $x_i + y_i \neq x_j - y_j$ for $i \neq j$. If we assumed that $A = x_i + y_i = x_j - y_j = -B$, we would obtain $\sigma(A) = -A = B$, so $x_i = x_j$, which is not possible for every $i \neq j$ by previous observation. If we apply similar argument to $Id \in Aut(E[p])$, we have that $x_i + y_i \neq x_j + y_j$ for any $i \neq j$. Eventually, we obtain $x_i + y_i \neq x_i - y_i$. Indeed, if $P = x_i + y_i = x_i - y_i$, we would have $P = -P$ and thus $2P = O$ which is impossible because P is a point of order $p \neq 2$.
Thus, $C(x + y)$ has $p^2 - 1$ distinct points and $deg(m_{x+y}(t)) = p^2 - 1$. Moreover, we have:

$$\mathbb{Q}(x + y) \subseteq \mathbb{Q}(x, y) \subseteq \mathbb{Q}(E[p]).$$

Now, we will find the degree of $\mathbb{Q}(x, y)/\mathbb{Q}(x + y)$. The minimal polynomial $\psi_p(t)$ is irreducible over $\mathbb{Q}$ and we also know the degree of the minimal polynomial $deg(\psi_p(t)) = \frac{p^2-1}{2}$. Thus, we get $[\mathbb{Q}(x) : \mathbb{Q}] = \frac{p^2-1}{2}$.

Notice that if $y \in \mathbb{Q}(x)$, we would obtain $\mathbb{Q}(x, y) = \mathbb{Q}(x)$. But this is not possible since $\mathbb{Q}(x + y) \subseteq \mathbb{Q}(x, y)$ and $[\mathbb{Q}(x + y) : \mathbb{Q}] = p^2 - 1 \geq \frac{p^2-1}{2}$. Thus, $y \notin \mathbb{Q}(x)$ and the minimal polynomial of y over $\mathbb{Q}(x)$ is $y^2 - x^3 - ax - b$. Then, $[\mathbb{Q}(x, y) : \mathbb{Q}] = p^2 - 1$ and $\mathbb{Q}(x, y) = \mathbb{Q}(x + y)$. This implies that the minimal polynomial $m_{x+y}(t)$ of $x + y$ over $\mathbb{Q}$ is also the characteristic polynomial of the multiplication by $(x + y)$-map in $\mathbb{Q}(x, y)$ according to Proposition 4.16.
Since ρ_p is surjective by assumption, we obtain $Gal(\mathbb{Q}(E[p])/\mathbb{Q}) \cong \mathbb{GL}_2(\mathbb{Z}/p\mathbb{Z})$. It is concluded that the Galois group of the Galois extension related to the polynomial $m(t) \in \mathbb{Q}[t]$ is isomorphic to $\mathbb{GL}_2(\mathbb{Z}/p\mathbb{Z})$ since the splitting field of $m(t)$ is $\mathbb{Q}(E[p])$.

□

Theorem 5.56. [17] *Let E be an elliptic curve given by Weierstrass equation with rational coefficients. Let us assume that E does not have complex multiplication. There exists an integer $N_E \geq 1$ related to the elliptic curve E such that if n is an integer coprime to N_E, then the Galois representation*

$$\rho_n : Gal(\mathbb{Q}(E[n])/\mathbb{Q}) \longrightarrow \mathbb{GL}_2(\mathbb{Z}/n\mathbb{Z})$$

is an isomorphism.

The proof of this theorem needs more advanced theory of elliptic curves. It was proved in 1972 in [17]. By using this theorem, one can prove the group $\mathbb{GL}_2(\mathbb{F}_p)$ is Galois group for any prime p.

The image of the Galois representation ρ_p for small primes p was studied in the paper [6] written by Reverter and Vila.

Application of the Proposition 5.55: We will now apply Proposition 5.55 in order to find a polynomial having Galois group $\mathbb{GL}_2(\mathbb{Z}/p\mathbb{Z})$. Let $P = (x, y)$ be be a point of order 3 on the elliptic curve $E : y^2 = x^3 - x + 1/4$. The minimal polynomial of x over $\mathbb{Q}$ is $\psi_3(t) = 3t^4 - 6t^2 + 3t - 1$, which is irreducible according to the part (i) of the Proposition 5.55. Thus, $\{1, x, x^2, x^3\}$ is a basis of $\mathbb{Q}(x)$ over $\mathbb{Q}$. Furthermore, one can prove that $y^2 - x^3 + x - 1/4$ is irreducible over $\mathbb{Q}(x)$ by using PARI/GP. Thus, $\{1, y\}$ is a basis of $\mathbb{Q}(x, y)$ over $\mathbb{Q}(x)$. Therefore, we find the basis $\{1, x, x^2, x^3, y, xy, x^2y, x^3y\}$ for $\mathbb{Q}(x, y)$ over $\mathbb{Q}$, and consider the matrix associated to the map:

$$\begin{aligned} m_{x+y} : \mathbb{Q}(x, y) &\longrightarrow \mathbb{Q}(x, y) \\ a &\mapsto a(x + y). \end{aligned}$$

Then, we get the following matrix:

$$M = \begin{pmatrix} 0 & 0 & 0 & 1/3 & 1/4 & 1/3 & 0 & 1/3 \\ 1 & 0 & 0 & -1 & -1 & -3/4 & 1/3 & -1 \\ 0 & 1 & 0 & 2 & 0 & 1 & -3/4 & 7/3 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & -3/4 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1/3 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 2 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

The characteristic polynomial of this matrix is the following

$$c_{x+y}(t) = t^8 - 2t^6 - \frac{26}{3}t^5 + \frac{283}{24}t^4 - 9t^3 + \frac{35}{4}t^2 - \frac{343}{72}t + \frac{5831}{6912}.$$

Let K' denote the splitting field of c_{x+y} over $\mathbb{Q}$. Then, the Galois group of the extension $K'/\mathbb{Q}$ is $\mathbb{GL}_2(\mathbb{Z}/3\mathbb{Z})$ by using PARI/GP.

6. THE GROUP $\mathbb{PSL}_2(\mathbb{F}_p)$ AS A GALOIS GROUP

Let p be a prime number and let $\mathbb{PSL}_2(\mathbb{F}_p)$ be the projective special linear group with entries in the finite field $\mathbb{F}_p$. In this chapter, our aim is to realize $\mathbb{PSL}_2(\mathbb{F}_p)$ as a Galois group of a Galois extension over $\mathbb{Q}$. This chapter consists of two sections. In the first section, we will give some necessary tools which will be used in the following section, these are Galois cohomology, twists of curves, modular curves, orders, and complex multiplication. In the second section, we will use the paper "Galois Groups via Atkin Lehner Twists", written by Pete Clark [9]. We will explain the method of the paper explicitly in order to construct $\mathbb{PSL}_2(\mathbb{F}_p)$ as a Galois group of a Galois extension over $\mathbb{Q}$.

6.1. Further Topics in Elliptic Curves and Modularity

In this section, we will study the tools which we will use later in the second section. We will cover dual isogenies, automorphism group of an elliptic curve, Galois cohomology, twists of a curve, modular curves, orders, complex multiplication, and Atkin-Lehner involutions in this section. These tools will lead to prove the main theorem in the second section of this chapter. Proofs of the statements are omitted in general, but relevant references are given.

6.1.1. Dual Isogenies

Theorem 6.1. [5, THEOREM 6.1.] *Let $\phi : E_1 \longrightarrow E_2$ be a nonconstant isogeny of degree m. There exists a unique isogeny*

$$\hat{\phi} : E_2 \longrightarrow E_1 \quad \textit{satisfying} \quad \hat{\phi} \circ \phi = [m].$$

Definition 6.2. *Let $\phi : E_1 \longrightarrow E_2$ be an isogeny. The dual isogeny of ϕ is the isogeny $\hat{\phi} : E_2 \longrightarrow E_1$ given by Theorem 6.1. Note that if $\phi = [0]$, then we set $\hat{\phi} = [0]$.*

Theorem 6.3. [5, THEOREM 6.2.] *Let $\phi : E_1 \longrightarrow E_2$ be a nonconstant isogeny.*

(i) Let $m = deg(\phi)$. Then its dual $\hat{\phi}$ satisfies $\hat{\phi} \circ \phi = [m]$ on E_1. Also, $\phi \circ \hat{\phi} = [m]$ on E_2.

(ii) Let $\lambda : E_2 \longrightarrow E_3$ be another isogeny. Then $\widehat{\lambda \circ \phi} = \hat{\phi} \circ \hat{\lambda}$.

(iii) Let $\psi : E_1 \longrightarrow E_2$ be another isogeny. Then $\widehat{\phi + \psi} = \hat{\phi} + \hat{\psi}$.

(iv) For all $m \in \mathbb{Z}$, $\widehat{[m]} = [m]$ and $deg[m] = m^2$.

(v) $deg(\hat{\phi}) = deg(\phi)$.

(vi) $\hat{\hat{\phi}} = \phi$

6.1.2. Automorphism Group

Let E be a given elliptic curve. In general, determining the structure of the endomorphism group of E is not easy. On the other hand, determining the automorphism group of E is much simpler, the exact structure of the automorphism group of E is known.

Theorem 6.4. [5, THEOREM 3.10.1] *Let E/K be an elliptic curve defined over K. Then the automorphism group $Aut(E)$ is a finite group of order dividing 24. The order of $Aut(E)$ is given precisely by the following table.*

Table 6.1. Automorphism Group

$\#Aut(E)$	$j(E)$	$char(K)$
2	$j(E) \neq 0, 1728$	-
4	$j(E) = 1728$	$char(K) \neq 2, 3$
6	$j(E) = 0$	$char(K) \neq 2, 3$
12	$j(E) = 0 = 1728$	$char(K) = 3$
24	$j(E) = 0 = 1728$	$char(K) = 2$

Corollary 6.5. [5, COROLLARY 3.10.2] *Let E/K be an elliptic curve defined over the field K with $char(K) \neq 2, 3$. Let*

$$n = \begin{cases} 2 \text{ if } j(E) \neq 0, 1728 \\ 4 \text{ if } j(E) = 1728 \\ 6 \text{ if } j(E) = 0 \end{cases} .$$

Then, there exists a natural isomorphism of $Gal(\overline{K}/K)$-modules

$$Aut(E) \cong \mu_n$$

where μ_n is the group of n-th roots of unity.

6.1.3. Galois Cohomology

Let K be a perfect field, let $\overline{K}$ be an algebraic closure of K, and let $Gal(\overline{K}/K)$ be the Galois group of the extension $\overline{K}/K$. The Galois group $Gal(\overline{K}/K)$ is defined as the inverse limit of the Galois groups $Gal(L/K)$ where L runs over all finite Galois extensions. Then, $Gal(\overline{K}/K)$ is a profinite group, i.e., an inverse limit of finite groups.

Definition 6.6. *A $Gal(\overline{K}/K)$ module is an abelian group M on which $Gal(\overline{K}/K)$ acts such that the action $Gal(\overline{K}/K) \times M \to M$ is continuous with respect to profinite topology on $Gal(\overline{K}/K)$ and the discrete topology on M. This action will be denoted by $(\sigma, m) \mapsto m^\sigma$. In other words, the action of $Gal(\overline{K}/K)$ on M satisfies that the stabilizer of m for each $m \in M$*

$$\{\sigma \in Gal(\overline{K}/K) : m^\sigma = m\}$$

is a subgroup having finite index in $Gal(\overline{K}/K)$.

Definition 6.7. *The* 0*-th cohomology group of a* $Gal(\overline{K}/K)$*-module* M *is defined as the group of invariant elements of* M *under the action* $Gal(\overline{K}/K)$ *given by*

$$H^0(Gal(\overline{K}/K), M) = \{m \in M : m^\sigma = m \quad \text{for } \sigma \in Gal(\overline{K}/K)\}.$$

Definition 6.8. *Let* M *be a* $Gal(\overline{K}/K)$*-module and let* $\xi : Gal(\overline{K}/K) \to M$ *be a map. The map* ξ *is continuous if it is continuous with respect to profinite topology on* $Gal(\overline{K}/K)$ *and the discrete topology on* M*. Equivalently, the map* ξ *is continuous if* $\xi^{-1}(m)$ *contains a subgroup having finite index in* $Gal(\overline{K}/K)$*. Let* $C(Gal(\overline{K}/K))$ *denote the group of continuous maps* $\xi : Gal(\overline{K}/K) \to M$*. The group of continuous* 1*-cocycles from* $Gal(\overline{K}/K)$ *to* M *is defined by the following set:*

$$Z^1(Gal(\overline{K}/K), M) = \{\xi \in C(Gal(\overline{K}/K)) : \xi(\sigma\tau) = \xi(\sigma)^\tau + \xi(\tau) \\ \text{for all } \sigma\tau \in Gal(\overline{K}/K)\}.$$

The group of coboundaries is defined as the subgroup of $Z^1(Gal(\overline{K}/K))$ *as follows:*

$$B^1(Gal(\overline{K}/K), M) = \{\xi \in Z^1(Gal(\overline{K}/K), M) : \exists m \in M \text{ such that} \\ \xi(\sigma) = m^\sigma - m \text{ for all } \sigma \in Gal(\overline{K}/K)\}.$$

The group $B^1(Gal(\overline{K}/K), M)$ is actually a subgroup of $Z^1(Gal(\overline{K}/K), M)$. Indeed, the property

$$\xi(\sigma\tau) = m^{\sigma\tau} - m = m^{\sigma\tau} - m^\tau + m^\tau - m = \xi(\sigma)^\tau + \xi(\tau)$$

is satisfied and the map $\sigma \mapsto m^\sigma - m$ is continuous since M is endowed with the discrete topology.

Definition 6.9. *The 1-st cohomology group of a $Gal(\overline{K}/K)$-module M is defined as the group*

$$H^1(Gal(\overline{K}/K), M) = \frac{Z^1(Gal(\overline{K}/K), M)}{B^1(Gal(\overline{K}/K), M)}.$$

An element in $H^1(Gal(\overline{K}/K), M)$ is said to be a cohomology class and it is denoted by $[\xi]$ for some 1-cocycle ξ.

Proposition 6.10. [5, Proposition B.2.5.] *Let K be a field. Let μ_m be the group of m-th roots of unity. Then*

(i) $H^1(Gal(\overline{K}/K), \overline{K}^+) = 0$.

(ii) $H^1(Gal(\overline{K}/K), \overline{K}^*) = 0$. *This is called Hilbert's Theorem 90.*

(iii) Let us suppose that $char(K) = 0$ does not divide m or $char(K)$. Then

$$H^1(Gal(\overline{K}/K), \mu_m) \cong K^*/(K^*)^m.$$

6.1.4. Nonabelian Galois Cohomology

We have defined cohomology groups of abelian $Gal(\overline{K}/K)$-modules M. Here, we will define cohomology groups of nonabelian $Gal(\overline{K}/K)$- modules M. The group operation on M will be written as a multiplication to emphasize that M may not be an abelian group.

Definition 6.11. *Let K be a perfect field and let M be a $Gal(\overline{K}/K)$-module (not necessarily abelian). The 0-th cohomology group of M is defined by the set*

$$H^0(Gal(\overline{K}/K), M) = \{m \in M : m^\sigma = m \quad for\ \sigma \in Gal(\overline{K}/K)\}.$$

In other words, it is a subgroup of $Gal(\overline{K}/K)$-invariant elements in M.

The set of 1-cocyles of $Gal(\overline{K}/K)$ into M is defined as the set of maps $\xi : Gal(\overline{K}/K) \longrightarrow M$ in which the maps ξ's are continuous with respect to Krull topology on $Gal(\overline{K}/K)$ and the discrete topology on M and satisfy the relation

$$\xi(\sigma\tau) = \xi(\sigma)^{\tau}\xi(\tau).$$

Let $Z^1(Gal(\overline{K}/K), M)$ denote the set of 1-cocycles. Notice that the set $Z^1(Gal(\overline{K}/K), M)$ of 1-cocycles is not a group in general. Indeed, the product of two cocycles may not be a cocyle since M is a nonabelian group.

Two cocycles ξ_1 and ξ_2 are cohomologous if there exists an $m \in M$ such that

$$m^{\sigma}\xi_1(\sigma) = \xi_2(\sigma)m \quad \text{for all } \sigma \in Gal(\overline{K}/K).$$

It is clear that this is an equivalence relation on the set of 1-cocycles. The 1-st cohomology set of M is defined as the set of 1-cocycles modulo this equivalence relation.

6.1.5. Twists

Definition 6.12. *Let K be a field. Let C/K be a smooth projective curve defined over K. The isomorphism group of C is defined to be the group of $\overline{K}$-isomorphisms from C to itself, denoted by $Isom(C)$. The subgroup of $Isom(C)$ which consists of isomorphisms defined over K is denoted by $Isom_K(C)$.*

Remark 6.13. The group $Isom(C)$ is generally called automorphism group of C, and denoted by $Aut(C)$. Let E be an elliptic curve. We have already defined $Aut(E)$ as the group of isomorphisms from E to E taking the identity O to O. In this case, we obtain $Aut(E) \neq Isom(E)$ since the group $Isom(E)$ has translation maps at least.

Definition 6.14. *Let K be a field and let C, C' be smooth curves defined over K. The curve C is said to be a twist of the curve C' if there exists a $\overline{K}$-isomorphism between C and C'. Two twists of the curve C' are regarded as equivalent if they are isomorphic over K. The set of twists of C modulo K-isomorphism is denoted by $Twist(C/K)$.*

Theorem 6.15. [5, THEOREM 10.2.2.] *Let C/K be a smooth projective curve. Let $\phi : C' \longrightarrow C$ be a $\overline{K}$-isomorphism chosen for every twist C'/K of C/K and define a map ξ as*

$$\xi : Gal(\overline{K}/K) \longrightarrow Isom(C) \quad with \quad \xi(\sigma) = \phi^{\sigma}\phi^{-1} \in Isom(C).$$

(i) The map ξ is a 1-cocycle, i.e.,

$$\xi(\sigma\tau) = \xi(\sigma)^{\tau}\xi(\tau) \text{ for all } \sigma, \tau \in Gal(\overline{K}/K).$$

The corresponding cohomology class in $H^1(Gal(\overline{K}/K), Isom(C))$ is denoted by $\{\xi\}$.

(ii) The cohomology class $\{\xi\}$ is given by K-isomorphism class of C', and it is independent from the choice of ϕ. Then, there is a natural map

$$\varphi : Twist(C/K) \longrightarrow H^1(Gal(\overline{K}/K), Isom(C)).$$

(iii) The map φ is a bijection. This implies that the twists of C/K up to K-isomorphism correspond bijectively with the elements of the 1-st cohomology set $H^1(Gal(\overline{K}/K), Isom(C))$.

Example 6.16. Let E/K be an elliptic curve defined over K with $char(K) \neq 2$, let $K(\sqrt{d})$ be a quadratic extension of K, and let

$$\chi : Gal(\overline{K}/K) \longrightarrow \{\pm 1\} \text{ with } \chi(\sigma) = \sqrt{d}^{\sigma}/\sqrt{d}$$

be the quadratic character associated to $K(\sqrt{d})/K$.
We will define a 1-cocycle by using χ

$$\xi : Gal(\overline{K}/K) \longrightarrow Isom(E) \text{ with } \xi(\sigma) = [\chi(\sigma)]$$

Let E^d/K be the corresponding twist of the elliptic curve E/K. We are going to give an equation for E^d/K. Let $y^2 = f(x)$ be a Weierstrass equation of the elliptic curve E/K and let us write $\overline{K}(E) = \overline{K}(x, y)$ and $\overline{K}(E^d) = \overline{K}(x, y)_\xi$. Since $[-1](x, y) = (x, -y)$, the action of $\sigma \in Gal(\overline{K}/K)$ on $\overline{K}(x, y)_\xi$ is given by the following formulas

$$\sqrt{d}^{\sigma} = \chi(\sigma)\sqrt{d}, \quad x^{\sigma} = x, \quad y^{\sigma} = \chi(\sigma)y.$$

Notice that the functions $x' = x$ and $y' = y/\sqrt{d}$ in $\overline{K}(x, y)_\xi$ are fixed by $Gal(\overline{K}/K)$, and they satisfy the equation $dy'^2 = f(x')$, which is the equation of an elliptic curve defined over K. Moreover, the identification $(x', y') \mapsto (x', y'\sqrt{d})$ verifies that this curve is isomorphic to E over $K(\sqrt{d})$. Checking the associated cocycle is ξ is easy. Thus, we have found an equation for E^d/K. The curve E^d is said to be the quadratic twist of E, more precisely, it is the twist of E by the quadratic character χ.

6.1.6. Modularity

Definition 6.17. *The modular group is defined as the group of* 2*-by-*2 *matrices whose determinants are* 1 *with integer entries*

$$\mathbb{SL}_2(\mathbb{Z}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{Z}, ad - bc = 1 \right\}.$$

Notice that the modular group is generated by the following two matrices

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}. \tag{6.1}$$

Remark 6.18. Every element in the modular group can be seen as an automorphism of the Riemann sphere $\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$, namely the fractional linear transformation

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} (\tau) = \frac{a\tau + b}{c\tau + d} \quad where \quad \tau \in \hat{\mathbb{C}}.$$

This means that if $c \neq 0$, then $-d/c$ is mapped to ∞ and ∞ is mapped to a/c. If $c = 0$, then ∞ is mapped to ∞. Since the identity matrix I and its negative $-I$ give the identity transformation, every pair $\pm\gamma$ of matrices in $\mathbb{SL}_2(\mathbb{Z})$ shows the same transformation. The group of transformations defined by the modular group is generated by the following maps

$$\tau \mapsto \tau + 1 \quad \text{and} \quad \tau \mapsto -1/\tau$$

since these transformations correspond to two matrix generators of the modular group described as in 6.1.

Definition 6.19. *The upper half plane is defined as the set*

$$\mathcal{H} = \{\tau \in \mathbb{C} : Im(\tau) > 0\}.$$

The following formula

$$Im(\gamma(\tau)) = \frac{Im(\tau)}{|c\tau + d|^2}, \quad \gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathbb{SL}_2(\mathbb{Z}), \tau \in \mathcal{H}$$

verifies that if $\gamma \in \mathbb{SL}_2(\mathbb{Z})$ and $\tau \in \mathcal{H}$, then $\gamma(\tau) \in \mathcal{H}$. In other words, the modular group maps the upper half plane to itself. Indeed, the modular group acts on the upper half plane, i.e., $I(\tau) = \tau$ for the identity matrix I and $(\gamma_1\gamma_2)(\tau) = \gamma_1(\gamma_2(\tau))$ for all $\tau \in \mathcal{H}$ and $\gamma_1, \gamma_1 \in \mathbb{SL}_2(\mathbb{Z})$.

Let N be a positive integer. The principal congruence subgroup of level N is defined as

$$\Gamma(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathbb{SL}_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \pmod{\text{N}} \right\}.$$

Let us consider the following natural surjective homomorphism:

$$\mathbb{SL}_2(\mathbb{Z}) \longrightarrow \mathbb{SL}_2(\mathbb{Z}/N\mathbb{Z}).$$

The subgroup $\Gamma(N)$ is the kernel of the homomorphism, thus it is normal in $\mathbb{SL}_2(\mathbb{Z})$. Since the homomorphism is also surjective, it induces an isomorphism

$$\mathbb{SL}_2(\mathbb{Z})/\Gamma(N) \cong \mathbb{SL}_2(\mathbb{Z}/N\mathbb{Z}).$$

This implies that the index $[\mathbb{SL}_2(\mathbb{Z}) : \Gamma(N)]$ is finite for all N.

Definition 6.20. *A subgroup Γ of the modular group $\mathbb{SL}_2(\mathbb{Z})$ is said to be a congruence subgroup if $\Gamma(N) \subset \Gamma$ for some $N \in \mathbb{Z}^+$. In this case, Γ is said to be a congruence subgroup of level N.*

It can be seen easily that every congruence subgroup Γ has a finite index in $\mathbb{SL}_2(\mathbb{Z})$ since $[\mathbb{SL}_2(\mathbb{Z}) : \Gamma(N)]$ is finite for all N. Besides the principal congruence subgroups, the most important congruence subgroups are

$$\Gamma_0(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathbb{SL}_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} * & * \\ 0 & * \end{bmatrix} \pmod{\text{N}} \right\} \text{ and}$$

$$\Gamma_1(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathbb{SL}_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} \pmod{\text{N}} \right\}$$

where $*$ shows any element of $\mathbb{Z}$.

It is easy to see that $\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N) \subset \mathbb{SL}_2(\mathbb{Z})$. Furthermore, these subsets are normal subgroups of each other.

Recall that two complex elliptic curves $\mathbb{C}/\Lambda_1$ and $\mathbb{C}/\Lambda_2$ are holomorphically isomorphic if and only if $m\Lambda_1 = \Lambda_2$ for some $m \in \mathbb{C}$ by Corollary 5.42. By seeing such two curves as equivalent, we obtain a quotient set of equivalence classes of complex elliptic curves. In a similar way, two points τ_1 and τ_2 in the upper half plane $\mathcal{H}$ are seen as equivalent if and only if $\gamma(\tau_1) = \tau_2$ for some $\gamma \in \mathbb{SL}_2(\mathbb{Z})$. By viewing two points as equivalent, we get a quotient set again. In fact, we will show that there exists a bijective correspondence between first quotient set and second quotient set. In other words, the equivalence classes of the points in the upper half plane are given by the isomorphism classes of complex elliptic curves.

Definition 6.21. *Let Γ be any congruence subgroup acting on $\mathcal{H}$. The modular curve $Y(\Gamma)$ is the quotient space of orbits under the action of Γ,*

$$Y(\Gamma) = \Gamma \setminus \mathcal{H} = \{\Gamma\tau : \tau \in \mathcal{H}\}.$$

The modular curve for $\Gamma_0(N)$ is denoted by $Y_0(N) = \Gamma_0(N) \setminus \mathcal{H}$ and the modular curve for $\Gamma_1(N)$ is denoted by $Y_1(N) = \Gamma_1(N) \setminus \mathcal{H}$.

Definition 6.22. *The points in $\Gamma \setminus \mathbb{Q} \cup \{\infty\}$ are called cusps of $X(\Gamma)$ which are Γ-equivalent to ∞. In order to compactify $Y(\Gamma)$, we need to add cusps to $Y(\Gamma)$.*

If $\Gamma = \mathbb{SL}_2(\mathbb{Z})$, all the rational numbers are Γ-equivalent to ∞, then $\mathbb{SL}_2(\mathbb{Z})$ has only one cusp, which is denoted by ∞. But, if Γ is a proper subgroup of $\mathbb{SL}_2(\mathbb{Z})$ fewer points are Γ-equivalent, thus Γ contain other cusps, denoted by rational numbers $\mathbb{Q}$.

Fact 6.23. Modular curves are indeed Riemann surfaces and they can be compactified. For detailed explanations, we refer reader to Chapter 2 in [18]. Also, compact Riemann surfaces can be defined by polynomial equations, meaning that modular curves are algebraic curves. We refer reader to Chapter 7 in [18] for details. Therefore, modular curves have both complex analytic and algebraic characterizations similar to complex elliptic curves.

Definition 6.24. *The compactification of the modular curve $Y(\Gamma)$ is given by*

$$X(\Gamma) = \Gamma \setminus \mathcal{H}^*$$

where $\mathcal{H}^* = \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$. We simply denote the compact modular curves by $X(\Gamma(N)) = X(N)$, $X(\Gamma_0(N)) = X_0(N)$ and $X(\Gamma_1(N)) = X_1(N)$ for modular curves $Y(\Gamma)$, $Y_0(N)$, and $Y_0(N)$ respectively.

We will continue with defining relevant data for the congruence subgroup $\Gamma_0(N)$ as follows.

Definition 6.25. *Let N be a positive integer. An enhanced elliptic curve for $\Gamma_0(N)$ is defined as an ordered pair (E, C) where E is a complex elliptic curve and C is a cyclic subgroup of E having order N. Two such pair (E_1, C_1) and (E_2, C_2) are regarded as equivalent if there is an isomorphism $E_1 \longrightarrow E_2$ which sends C_1 to C_2, and it is denoted by $(E_1, C_1) \cong (E_2, C_2)$. The set of equivalence classes of enhanced elliptic curves with respect to equivalence relation of pairs defined above is denoted by*

$$S_0(N) = \{ \text{ enhanced elliptic curves for } \Gamma_0(N)\} / \sim .$$

An element in $S_0(N)$ is denoted by $[E, C]$.

Theorem 6.26. [18, Theorem 1.5.1] *Let N be a positive integer. The moduli space of $\Gamma_0(N)$ is*

$$S_0(N) = \{[E_\tau, \langle 1/N, \Lambda_\tau \rangle] : \tau \in \mathcal{H}\}$$

where $\Lambda_\tau = \mathbb{Z} \oplus \tau\mathbb{Z}$ and E_τ is the complex elliptic curve corresponding to the lattice Λ_τ. Two points $[E_{\tau_1}, \langle 1/N, \Lambda_{\tau_1} \rangle]$ and $[E_{\tau_2}, \langle 1/N, \Lambda_{\tau_2} \rangle]$ are the same if and only if $\Gamma_0(N)\tau_1 = \Gamma_0(N)\tau_2$ holds. Then, there exists a bijective map

$$\begin{aligned} \psi : \quad & S_0(N) \longrightarrow Y_0(N) \\ & [\mathbb{C}/\Lambda_\tau, \langle 1/N, \Lambda_\tau \rangle] \mapsto \Gamma_0(N)\tau. \end{aligned}$$

Theorem 6.26 shows that the quotient of the upper half plane by the congruence subgroup $\Gamma_0(N)$ is determined by the sets of equivalence classes of elliptic curves enhanced by corresponding torsion data.

6.1.7. Orders

Definition 6.27. *Let K be a quadratic field. An order $\mathcal{O}$ in a quadratic field K is defined as a subset $\mathcal{O} \subset K$ satisfying the following conditions:*

(i) $\mathcal{O}$ is a subring of K which contains 1.
(ii) $\mathcal{O}$ is a finitely generated $\mathbb{Z}$-module.
(iii) $\mathcal{O}$ contains a $\mathbb{Q}$- basis of the field K.

Notice that the conditions (i) and (ii) show that an order $\mathcal{O}$ is a free $\mathbb{Z}$-module of rank 2. Also, the condition (iii) is equivalent to say that K is the field of fractions of $\mathcal{O}$. Alternatively, one may define an order in a more general setting as follows.

Definition 6.28. *Let K be a number field. An order $\mathcal{R}$ in K is defined as a subring of K which is a finitely generated $\mathbb{Z}$-module and it satisfies $\mathcal{R} \otimes_{\mathbb{Z}} \mathbb{Q} = K$.*

Remark 6.29. The ring of integers $\mathcal{O}_K$ is always an order in K. In fact, any order $\mathcal{O}$ in K is contained in the ring of integers $\mathcal{O}_K$, i.e. $\mathcal{O} \subset \mathcal{O}_K$. For this reason, the ring of integers $\mathcal{O}_K$ is called the maximal order in K.

Fact 6.30. The maximal order $\mathcal{O}_K$ in quadratic field K may be written in the following form

$$\mathcal{O}_K = [1, w_K], \quad w_K = \frac{disc(K) + \sqrt{disc(K)}}{2} \tag{6.2}$$

where $disc(K)$ is the discriminant of the field K. By using this fact, we can give a simple form of any order $\mathcal{O}$ in quadratic field K.

Lemma 6.31. [8, Lemma 7.2.] *Let K be a quadratic field and let $disc(K)$ be the discriminant of K. Let $\mathcal{O}$ be an order in K. Then, the order $\mathcal{O}$ has finite index in $\mathcal{O}_K$. Furthermore, let $f = [\mathcal{O}_K : \mathcal{O}]$. Then, an order $\mathcal{O}$ in K is given as follows*

$$\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K = [1, fw_K]$$

where $w_K = \frac{disc(K)+\sqrt{disc(K)}}{2}$.

Example 6.32.

(i) For the field quadratic $\mathbb{Q}(\sqrt{5})$, we find an order $\mathbb{Z}[\sqrt{5}] \subset \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ since $5 \equiv 1$ (mod 4).

(ii) For the field quadratic $\mathbb{Q}(\sqrt{-5})$, we find an order $\mathbb{Z}[\sqrt{-5}] \subset \mathbb{Z}[\sqrt{-5}]$ since $-5 \equiv 3$ (mod 4).

6.1.8. Complex Multiplication

In this subsection, we will examine elliptic curves with complex multiplication from complex analytical viewpoint. Throughout this subsection, let $E/\mathbb{C}$ be an elliptic curve defined over $\mathbb{C}$.

Theorem 6.33. [5, Theorem 5.5.] *Let $E/\mathbb{C}$ be an elliptic curve and let Λ be a lattice associated to the elliptic curve E with generators ω_1 and ω_2. Then, one of the following statements is satisfied:*

(i) The endomorphism ring of E is equal to $\mathbb{Z}$, i.e., $End(E) = \mathbb{Z}$.

(ii) $\mathbb{Q}(\omega_2/\omega_1)$ is an imaginary quadratic extension of $\mathbb{Q}$, and the endomorphism ring $End(E)$ is isomorphic to an order in $\mathbb{Q}(\omega_2/\omega_1)$.

Definition 6.34. *Let $E/\mathbb{C}$ be an elliptic curve. If $End(E) \cong \mathcal{O} \subset \mathbb{C}$ and $K = R \otimes_{\mathbb{Z}} \mathbb{Q}$, then we say that E has complex multiplication by $\mathcal{O}$, or that E has complex multiplication by K.*

Let $\mathcal{O}_K$ be the ring of integers of K. The ring of integers $\mathcal{O}_K$ is the maximal order in K by definition. Complex multiplication theory is easier when the attention is restricted to elliptic curves with complex multiplication by $\mathcal{O}_K$.

The Uniformization Theorem of Elliptic Curves (Theorem 5.43) states that there exists a lattice $\Lambda \subset \mathbb{C}$ and an isomorphism for every elliptic curve $E/\mathbb{C}$ such that

$$\begin{aligned} &\mathbb{C}/\Lambda \longrightarrow E(\mathbb{C}) \\ &z \mapsto (\wp(z,\Lambda), \wp'(z,\Lambda)). \end{aligned}$$

As we have seen in Corollary 5.42 the elliptic curve associated to a lattice Λ is denoted by E_Λ, and the Weierstrass equation correspond to E_Λ is

$$E_\Lambda : y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda).$$

In general, it is beneficial to study the set of elliptic curves in order to understand particular elliptic curves. For this reason, we should examine the set of elliptic curves with the same endomorphism ring in order to study a particular elliptic curve with complex multiplication. Note that elliptic curves mean isomorphism classes of elliptic curves.

Thus, elliptic curves $E/\mathbb{C}$ with the same endomorphism ring $End(E) \cong \mathcal{O}$ modulo isomorphism over $\mathbb{C}$ can be identified with lattices with the same endomorphism ring $End(E_\Lambda) \cong \mathcal{O}$ modulo homothety.

$$Ell_{\mathbb{C}}(\mathcal{O}) = \frac{\{elliptic \quad curves \quad E/\mathbb{C} \quad with \quad End(E) \cong \mathcal{O}\}}{isomorphism \quad over \quad \mathbb{C}}$$

$$= \frac{\{lattices \quad \Lambda \quad with \quad End(E_\Lambda) \cong \mathcal{O}\}}{homothety}.$$

Let K be a quadratic imaginary field and let $\mathcal{O}_K$ be its ring of integers. The natural question is that how can we construct an elliptic curve with complex multiplication by $\mathcal{O}_K$?

Let $\mathfrak{a}$ be a nonzero fractional ideal in $\mathcal{O}_K$. Since $\mathfrak{a} \subset K \subset \mathbb{C}$, it can be seen that $\mathfrak{a}$ is a lattice in $\mathbb{C}$. Indeed, $\mathfrak{a}$ is a $\mathbb{Z}$-module of rank 2 that is not in $\mathbb{R}$ from the definition of a fractional ideal in a quadratic imaginary field. Thus, we can obtain an elliptic curve $E_{\mathfrak{a}}$ whose endomorphism ring is $\mathcal{O}_K$ as follows:

$$\begin{aligned} End(E_{\mathfrak{a}}) &\cong \{\alpha \in \mathbb{C} : \alpha\mathfrak{a} \subset \mathfrak{a}\} && \text{given by the Uniformization Theorem} \\ &= \{\alpha \in K : \alpha\mathfrak{a} \subset \mathfrak{a}\} && \text{since } \mathfrak{a} \subset K \\ &= \mathcal{O}_K && \text{since } \mathfrak{a} \text{ is a proper fractional } \mathcal{O}\text{-ideal.} \end{aligned}$$

This means that every nonzero fractional ideal $\mathfrak{a}$ in K gives an elliptic curve with complex multiplication by $\mathcal{O}_K$. Also, we know that a homothety between two lattices gives isomorphism between two elliptic curves over $\mathbb{C}$ by Theorem 5.41. Thus, $\mathfrak{a}$ and $c\mathfrak{a}$ for $c \in \mathbb{C}$ give the same elliptic curve in $Ell_{\mathbb{C}}(\mathcal{O})$. Thus, we need to determine fractional ideals modulo principal ideals, which gives one of the main objects in algebraic number theory, namely ideal class group:

$$\begin{aligned} Cl(\mathcal{O}_K) = &\quad \text{ideal class group of } \mathcal{O}_K \\ &= \frac{\{\text{nonzero fractional ideals of K}\}}{\{\text{nonzero principal ideals of K}\}}. \end{aligned}$$

Let $\mathfrak{a}$ be a fractional ideal in K. The ideal class of $\mathfrak{a}$ in $Cl(\mathcal{O}_K)$ is denoted by $[\mathfrak{a}]$. Thus, there exists a map

$$\begin{aligned} &Cl(\mathcal{O}_K) \longrightarrow Ell_{\mathbb{C}}(\mathcal{O}_K) \\ &[\mathfrak{a}] \mapsto E_{\mathfrak{a}}. \end{aligned}$$

Fact 6.35. Let Λ be a lattice correspond to the elliptic curve $E_\Lambda \in Ell_{\mathbb{C}}(\mathcal{O}_K)$ and let $\mathfrak{a}$ be a nonzero fractional ideal in K. Thus, we can product them as follows

$$\mathfrak{a}\Lambda = \{a_1\lambda_1 + ... + a_s\lambda_s : a_i \in \mathfrak{a}, \lambda_i \in \Lambda\}.$$

The next proposition is the basis of study in complex multiplication. This proposition states that the ideal group $Cl(\mathcal{O}_K)$ of the ring of integers has a simply transitive action on the set $Ell_{\mathbb{C}}(\mathcal{O}_K)$ of elliptic curves over $\mathbb{C}$ with the same endomorphism ring $\mathcal{O}_K$.

Proposition 6.36. [7, Proposition 2.1.2.] *Let Λ be a lattice correspond to E_Λ. Let $\mathfrak{a}$ and $\mathfrak{b}$ be nonzero fractional ideals in K and let $\mathcal{O}_K$ be the ring of integers of K. Then,*

(i) $\mathfrak{a}\lambda$ *is a lattice in* $\mathbb{C}$.

(ii) The elliptic curve $E_{\mathfrak{a}\lambda}$ *has the endomorphism ring* $End(E_{\mathfrak{a}\lambda}) \cong \mathcal{O}_K$.

(iii) $E_{\mathfrak{a}\lambda} \cong E_{\mathfrak{b}\lambda}$ *if and only if* $[\mathfrak{a}] = [\mathfrak{b}]$ *in* $Cl(\mathcal{O}_K)$.

Thus, there exists a well-defined action of $Cl(\mathcal{O}_K)$ *on* $Ell_{\mathbb{C}}(\mathcal{O}_K)$ *given by*

$$\begin{aligned} Cl(\mathcal{O}_K) \times Ell_{\mathbb{C}}(\mathcal{O}_K) &\longrightarrow \quad Ell_{\mathbb{C}}(\mathcal{O}_K) \\ ([\mathfrak{a}], E_\Lambda) \qquad &\longmapsto [\mathfrak{a}] * E_\Lambda = E_{\mathfrak{a}^{-1}\Lambda} \end{aligned} \quad .$$

(iv) The action described above is simply transitive. In particular, we have

$$\#Cl(\mathcal{O}_K) = \#Ell_{\mathbb{C}}(\mathcal{O}_K).$$

Definition 6.37. *Let K be a field and let $\mathcal{O}_K$ be its ring of integers. Let E be an elliptic curve with complex multiplication by K. If $\mathfrak{a}$ is an integral ideal of $\mathcal{O}_K$, the following set*

$$E[\mathfrak{a}] = \{P \in E : [a]P = O \text{ for all } a \in \mathfrak{a}\}$$

is called the group of $\mathfrak{a}$-torsion points of E. If $\mathfrak{a} = m\mathcal{O}_K$, the group $E[\mathfrak{a}]$ is $E[m]$.

Remark 6.38. Let $\mathfrak{a}$ be an integral ideal of $\mathcal{O}_K$. Notice that $\Lambda \subset \mathfrak{a}^{-1}\Lambda$. This leads to a natural homomorphism

$$\begin{aligned} &\mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\mathfrak{a}^{-1}\Lambda \\ &z \mapsto z \end{aligned}$$

which induces a natural isogeny as follows

$$E_\Lambda \longrightarrow [\mathfrak{a}] * E_\Lambda.$$

Proposition 6.39. [7, Proposition 2.1.4.] *Let E be an elliptic curve in $Ell_{\mathbb{C}}(\mathcal{O}_K)$ and let $\mathfrak{a}$ be an integral ideal in $\mathcal{O}_K$.*

(i) $E[\mathfrak{a}]$ is the kernel of the natural map $E \longrightarrow [\mathfrak{a}] * E$.
(ii) $E[\mathfrak{a}]$ is a free $\mathcal{O}_K/\mathfrak{a}$-module of rank 1.

Corollary 6.40. [7, Corollary 2.1.5.] *Let $E \in Ell_{\mathbb{C}}(\mathcal{O}_K)$ and let $\mathfrak{a} \subset \mathcal{O}_K$ be an integral ideal.*

(i) The natural map $E \longrightarrow [\mathfrak{a}]$ has degree $N(\mathfrak{a})$.
(ii) Let $\alpha \in \mathcal{O}$. The endomorphism $[\alpha] : E \longrightarrow E$ has degree $|Norm_{K/\mathbb{Q}}(\alpha|)$.

6.1.9. Atkin-Lehner Involutions

In this subsection, our aim is to introduce Atkin-Lehner involutions. For more explanations, we refer the reader to the paper [19].

Let e be a prime such that $e \mid N$ and let α be such that $e^\alpha \mid\mid N$ which means that e^α divides N but $e^{\alpha+1}$ does not divide N. Let us choose $a, b, c, d \in \mathbb{Z}$ such that $e^\alpha ad - (N/e^\alpha)bc = 1$.

We define a matrix W_e

$$W_e = \frac{1}{\sqrt{e^\alpha}} \begin{bmatrix} e^\alpha a & b \\ Nc & e^\alpha d \end{bmatrix}. \tag{6.3}$$

It is obtained $(e, bc) = 1$, but we may have $e \mid a$ and $e \mid d$. . Also, W_e^{-1} is of the same form as W_e.

Let n be a composite number such that $n \mid N$. Then, we define

$$W_n := \prod_{e|n} W_e.$$

If $gcd(n, N/n) = 1$, then W_n has the same form as W_e where e^α is replaced with n in Equation (6.3). The matrix W_n with composite integer n only depends on the prime numbers dividing n. In fact, there are a variety of choices of n giving the same W_n. In the case of $n = N$, we can find a canonical representative given by

$$W_N = \frac{1}{\sqrt{N}} \begin{bmatrix} 0 & -1 \\ N & 0 \end{bmatrix}. \tag{6.4}$$

The most important feature of the matrices W_n will be proved in the following.

Lemma 6.41. [19, Lemma 8.] *For any two choices W_n and $W_n^{'}$, we obtain*

$$W_n \Gamma_0(N) W_n^{'} = \Gamma_0(N).$$

Proof. The fact $W_n \Gamma_0(N) W_n^{'} \subseteq \Gamma_0(N)$ is an easy calculation.
For the equality, we use the fact that the matrix W_n^{-1} has also the same form as W_n. Let $\gamma' = W_n^{-1} \gamma W_n^{'-1} \in \Gamma_0(N)$ for any $\gamma \in \Gamma_0(N)$. Thus, $\gamma = W_n \gamma^{'} W_n^{'} \in \Gamma_0(N)$. □

Recall that there are many possible choices of W_n and we do not choose any one over the others, since they are all equivalent up to multiplication by an element of $\Gamma_0(N)$ by Lemma 6.41.

Let τ_1 and τ_2 be elements of upper half plane $\mathcal{H}$. Let us assume that τ_1 and τ_2 are in the same $\Gamma_0(N)$-orbit, i.e., there exists an element $\gamma \in \Gamma_0(N)$ such that $\gamma\tau_1 = \tau_2$. Thus, $W_n\gamma W_n^{'} = \gamma' \in \Gamma_0(N)$ and $W_n\tau_2 = W_n\gamma\tau_1 = \gamma' W_n\tau_1$. Thus, $W_n\tau_1$ and $W_n\tau_2$ lie in the same $\Gamma_0(N)$-orbit. This implies that there exists a well-defined action of the W_n on the classical modular curve $X_0(N)$. Also, $W_nW_n^{-1}$ acts on $X_0(N)$ as the identity. It follows that W_n gives an involution on the classical modular curve $X_0(N)$.

Fact 6.42. Let N be a squarefree positive integer and let $\Gamma_0(N)$ be the congruence subgroup. The set of all cusps of $\Gamma_0(N)$ is given by $\mathbb{Q}^* = \mathbb{Q} \cup \{\infty\}$. Every element of $\mathbb{Q}^*$ is uniquely determined by a reduced fraction with positive numerator and $\infty = 1/0$, with one exception $0 = 0/1$. Two cusps are regarded as equivalent relative to $\Gamma_0(N)$ if and only if the denominators of both cusps have the same greatest common divisor with N. Thus, every equivalence class of cusps corresponds bijectively with every ordered decomposition $N = M_1M_2$ of two positive divisors. We can say that a cusp $\lambda = \lambda_1/\lambda_2$ are in M_2-class if the greatest common divisor of λ_2 and N is M_2. For instance, ∞ belongs to N-class. For each decomposition $N = M_1M_2$ and any cusp $\lambda = \lambda_1/\lambda_2$ of M_2-class, we may take a typical matrix ω_λ which sends λ to ∞

$$\omega_\lambda = \begin{bmatrix} 1 & 0 \\ 0 & M_1 \end{bmatrix} \begin{bmatrix} M_1c_1 & c_2 \\ -\lambda_2 & \lambda_1 \end{bmatrix} \text{ where } \begin{bmatrix} M_1c_1 & c_2 \\ -\lambda_2 & \lambda_1 \end{bmatrix} \in \mathbb{SL}_2(\mathbb{Z}) \text{ and } c_i \in \mathbb{Z}.$$

Furthermore, for any divisor M of N, we define the matrix W_M , which exists uniquely up to right or left Γ -multiplication, given by

$$W_M = \begin{bmatrix} Ma & b \\ Nc & Md \end{bmatrix} \text{ with determinant } M \text{ and } a, b, c, d \in \mathbb{Z}.$$

The matrix W_M normalizes the group $\Gamma_0(N)$ and $M^{-1}W_M^2 \in \Gamma_0(N)$. Moreover, $W_M = W_{M'}W_{M'}$ if $M = M'M''$ divides N. Since ω_λ is one of this form, we conclude that each cusp can be mapped to another cusp by an element of the normalizer of $\Gamma_0(N)$.

6.2. Realization of $\mathbb{PSL}_2(\mathbb{F}_p)$

Let p be a prime number and let $\mathbb{PSL}_2(\mathbb{F}_p)$ be the projective special linear group with entries in the finite field $\mathbb{F}_p$. In this chapter, our aim is to realize $\mathbb{PSL}_2(\mathbb{F}_p)$ infinitely often as a Galois group of a Galois extension over $\mathbb{Q}$ by using the paper [9]. Before starting examine the paper in detail, we will give some observations.

(i) An isogeny $\phi : E \longrightarrow E^{'}$ is a surjective morphism that maps O to $O^{'}$. Every isogeny induces a homomorphism between K-rational points of E and $E^{'}$. Also, every isogeny has a finite kernel, conversely, for every finite subgroup H of $E(K)$, there is an isogeny ϕ defined over K such that $ker(\phi) = H$ by Proposition 5.23. Moreover, every isogeny $\phi : E \longrightarrow E^{'}$ has a dual isogeny, namely $\hat{\phi} : E^{'} \longrightarrow E$ by Theorem 6.1. To sum up these statements, we can identify isogenies with finite subgroups.

(ii) Let $X_0(N)$ be the classical modular curve. It is an algebraic curve, furthermore it is a moduli space by Theorem 6.26. The noncuspidal points of the classical modular curve $X_0(N)$ parametrize tuples (E, ϕ) where E is an elliptic curve over $\mathbb{C}$ and C is a distinguished order N cyclic subgroup of E. In other words, the classical modular curve $X_0(N)$ classifies elliptic curves with torsion subgroups. Alternatively, there is also equivalent but more useful viewpoint. The classical modular curve $X_0(N)$ parametrizes tuples (E, ϕ) where $\phi : E \longrightarrow E^{'}$ is a degree N isogeny.

By combining these two observations, it can be concluded that we need to study $X_0(N)(\mathbb{Q})$ in order to study $\mathbb{Q}$-rational torsion subgroups of the elliptic curve E.

Our main object will be the classical modular curve $X_0(N)$ in this section. The Atkin-Lehner involution w_N acts on affine part of $X_0(N)$ such that w_N sends $\phi : E \longrightarrow E'$ to its dual isogeny $\hat{\phi} : E' \longrightarrow E$. It is uniquely characterized by $\hat{\phi} \circ \phi = [N]$. The classical modular curve $X_0(N)$ has always $\mathbb{Q}$-rational points since cusps are rational. Thus, $X_0(N)(\mathbb{Q}) \neq \emptyset$ for all N.

Let $C(N, d)$ be a curve which is obtained by twisting the classical modular curve $X_0(N)$ using the Atkin-Lehner involution $w_N \in Aut(X_0(N))$ and the quadratic extension $\mathbb{Q}(\sqrt{d})$. Let $\langle \sigma_d \rangle = Gal(\mathbb{Q}(\sqrt{d})$ be the generator of the Galois group of $\mathbb{Q}(\sqrt{d})$. Twisted curve $C(N, d)$ becomes isomorphic to $X_0(N)$ over $\mathbb{Q}(\sqrt{d})$, but it has a twisted Galois action on its $\mathbb{Q}(\sqrt{d})$-rational points. For any point $P \in C(N, d)(\mathbb{Q}(\sqrt{d})$, we define the action of $Gal(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$ as $P^{\sigma_d} = w_N \circ \sigma_d(P)$. If we consider $\mathbb{Q}$-rational points of the twisted curve $C(N, d)$, they are not immediate like the classical modular curve $X_0(N)$. In fact, $\mathbb{Q}$-rational points $C(N, d)(\mathbb{Q})$ are given by the following set

$$C(N, d)(\mathbb{Q}) = \{P \in X_0(N)(\mathbb{Q}(\sqrt{d})) : w_N \circ \sigma_d(P) = P\}.$$

We know that Atkin-Lehner involution w_N permutes cusps of $X_0(N)$ by Fact 6.42. Thus, the cusps of $X_0(N)$ do not stay rational on $C(N, d)$ since they are fixed by σ_d but not fixed by w_N. In order to determine $\mathbb{Q}$-rational points of twisted curve $C(N, d)$, we need to find points $X_0(N)$ which are fixed by Atkin-Lehner involution w_N.

The following conjecture and theorem will be used in the main theorem.

Conjecture 6.43. [5, Conjecture C.16.1.] *(Birch and Swinnerton-Dyer) Let $E/\mathbb{Q}$ be an elliptic curve. The L-series $L_E(s)$ has a zero at $s = 1$ of order equal to the rank of $E(\mathbb{Q})$.*

Theorem 6.44. [5, Theorem C.16.3.] *Let $E/\mathbb{Q}$ be an elliptic curve. Then the function $\xi_E(s)$ has an analytic continuation to the entire complex plane and satisfies the functional equation $\xi_E(s) = w\xi_E(2 - s)$ for some $w = \pm 1$. The quantity w is called the sign of the functional equation. Its parity determines whether the order of vanishing of $L_{E/\mathbb{Q}}(s)$ at $s = 1$ is odd or even.*

In 1974, Shih proved that $\mathbb{PSL}_2(\mathbb{F}_p)$ occurs regularly over $\mathbb{Q}$ if the Kronecker symbol $\left(\frac{N}{p}\right) = -1$ for some $N \in \{2, 3, 7\}$. After, Malle showed that $\left(\frac{5}{p}\right) = -1$ is also sufficient condition for $\mathbb{PSL}_2(\mathbb{F}_p)$ to be realized regularly over $\mathbb{Q}$. These two results leave a density $\frac{1}{16}$ set of primes unaccounted for.

In 1988, Serre proposed a new method, which is an extension of Shih's Theorem, to realize new groups $\mathbb{PSL}_2(\mathbb{F}_p)$ over $\mathbb{Q}$. This method is published in his book Topics in Galois Theory [20]. Serre shows that this new method works to realize $\mathbb{PSL}_2(\mathbb{F}_{47})$ over $\mathbb{Q}$ by referring to a calculation of Elkies. Notice that the case $p = 47$ is constructed by Malle's result but not by Shih's. In a strange way, there is no additional examples of the given method in [20]. The paper [9] analyses Serre's method in detail. In fact, the new method of Serre gives rise to realizations of $\mathbb{PSL}_2(\mathbb{F}_p)$ over $\mathbb{Q}$ for many primes p which are not constructed by previous results.

Theorem 6.45. [21, THEOREM 8] *Let $N \in \mathbb{Z}^+$ be a squarefree integer such that $\left(\frac{N}{p}\right) = -1$ and let $p^* = (-1)^{\frac{p-1}{2}}p$. Let $C(N, p)$ be the curve obtained by twisting the classical modular curve $X_0(N)$ using the Atkin-Lehner involution $w_N \in Aut(X_0(N))$ and the quadratic extension $\mathbb{Q}(\sqrt{p^*})/\mathbb{Q}$. Then there exists a regular Galois covering $Y \longrightarrow C(N, p)$ defined over $\mathbb{Q}$ with Galois group $\mathbb{PSL}_2(\mathbb{F}_p)$.*

The classical modular curve $X_0(N)$ has genus 0 for the following squarefree integers $N > 1$

$$N = 2, 3, 5, 7, 10, 13.$$

Furthermore, $X_0(N)$ has genus one among the following squarefree integers $N > 1$, namely

$$N = 11, 14, 15, 17, 19, 21.$$

Our purpose is to determine that $C(N, p)(\mathbb{Q})$ is infinite for which primes p such that $\left(\frac{N}{p}\right) = -1$.

In the case of $C(N,p) = \mathbb{P}^1$, the group $\mathbb{PSL}_2(\mathbb{F}_p)$ occurs regularly over $\mathbb{Q}$. This happens for all primes p when $N \in 2, 3, 7$, and we recover the earlier result of Shih's Theorem. More generally, when $C(N,p)(\mathbb{Q}) = \infty$, there remains the possibility of finding an irreducible specialization. In fact, we have the following theorem.

Theorem 6.46. [20, Corollary 5.4.2] *(Serre) Let $N \in \mathbb{Z}^+$ be a squarefree integer such that $\left(\frac{N}{p}\right) = -1$ and let $p^* = (-1)^{\frac{p-1}{2}}p$. Let $C(N,p)$ be the curve obtained by twisting the classical modular curve $X_0(N)$ using the Atkin-Lehner involution $w_N \in Aut(X_0(N))$ and the quadratic extension $\mathbb{Q}(\sqrt{p^*})/\mathbb{Q}$. If $C(N,p)(\mathbb{Q})$ is infinite, then there are infinitely many linearly disjoint Galois extensions $L/\mathbb{Q}$ with Galois group $G \cong \mathbb{PSL}_2(\mathbb{F}_p)$.*

In a chronological order, Shih proved that $\mathbb{PSL}_2(\mathbb{F}_p)$ is realized as a Galois group over $\mathbb{Q}$ for $\frac{7}{8}$ of all primes. Then, Malle showed that $\mathbb{PSL}_2(\mathbb{F}_p)$ occurs as a Galois group for $\frac{1}{4}$ of all primes. Together with Shih's and Malle's results, $\frac{15}{16}$ of all primes are obtained. The paper of Clark [9] gives $\frac{3}{8}$ of all primes conditionally on the conjecture of Birch and Swinnerton-Dyer, and there remains $\frac{5}{128}$ of the primes unaccounted for. Due to Clark's result, at least new 614 primes are found for which $\mathbb{PSL}_2(\mathbb{F}_p)$ occurs as a Galois group over $\mathbb{Q}$, but not found by Shih's or Malle's results. These new prime include two primes $p \equiv 1 (\text{mod } 4)$ for which the curves have analytic rank 2.

Theorem 6.47. [9, Theorem 3.] *Let $N = 11$ or 19. The twisted curve $C(N,p)(\mathbb{Q}) \neq \emptyset$ for all primes p. So $C(N,p)$ can be given the structure of a rational elliptic curve. More precisely, $C(N,p)$ is the quadratic twist of the classical modular curve $X_0(N)$ by p^*. It follows that:*

(i) For primes $p \equiv 1$ (mod 4), $\left(\frac{N}{p}\right) = -1$ if and only if $C(N,p)$ has odd analytic rank.

(ii) For primes $p \equiv -1$ (mod 4), $\left(\frac{N}{p}\right) = -1$ if and only if $C(N,p)$ has even analytic rank.

Proof. Let σ be the nontrivial element of $Gal(\mathbb{Q}(\sqrt{p^*})/\mathbb{Q})$. The points $P \in X_0(N)$ which stay $\mathbb{Q}$-rational on twisted curve $C(N,p)$ and on $X_0(N)$ are the points satisfying the following equalities:

$$\sigma(P) = P, \quad w_N \circ \sigma(P) = P$$
$$\text{or equivalently} \qquad w_N(P) = \sigma(P) = P$$

In other words, $\mathbb{Q}$-rational w_N-fixed points of $X_0(N)$ will stay rational on all twists, i.e., $C(N,p)(\mathbb{Q})$ consists of those points $P \in C(N,p)(\mathbb{Q}(\sqrt{p^*}))$ such that $w_N(\sigma(P)) = P$. The Atkin-Lehner involution w_N for squarefree $N > 3$ always has fixed points on $X_0(N)$. Indeed, let us assume that $(E,\phi) \in X_0(N)$ be a fixed point of w_N where E is an elliptic curve and $\phi : E \longrightarrow E^{'}$ is a degree N isogeny. Then, we have

$$w_N(E, \phi : E \longrightarrow E') = (E', \hat{\phi} : E' \longrightarrow E)$$

It turns out that $\phi : E \longrightarrow E' \cong E$ is a degree N endomorphism of the elliptic curve E. Thus $\phi \in End(E)$. If the isogeny ϕ were a multiplication by an integer map, its degree would be m such that $m^2 = N$ by Theorem 6.1. But this gives a contraction since N is a squarefree integer. This implies that the endomorphism ring $End(E)$ is strictly larger than $\mathbb{Z}$, i.e. the elliptic curve E has a complex multiplication. Then there exists an element $\pi \in \mathcal{O}$ whose norm is N, $\pi\overline{\pi} = N$ by Corollary 6.40. Thus, E has a complex multiplication by an order $\mathcal{O}$ such that $\mathcal{O} \subset \mathbb{Z}[\sqrt{-N}]$

Let C_1 be the set of $\mathbb{C}$-isomorphism classes of elliptic curves with CM by the maximal order of $\mathbb{Q}(\sqrt{-N})$ and let C_2 be the set of $\mathbb{C}$-isomorphism classes of elliptic curves with CM by the maximal order of $\mathbb{Z}[\sqrt{-N}]$. It is not hard to see that each of C_1 and C_2 leads to a set of w_N-fixed points. There is one complete Galois orbit of points corresponding to the ideal classes in the order $Z[\sqrt{-N}]$, and there is one complete Galois orbit of points corresponding to the ideal classes in the maximal order of $\mathbb{Q}(\sqrt{-N})$. If $N \equiv 1 \pmod 4$, we have repeated the same thing two times and there is only one orbit.

If $-N \equiv 1 \pmod 4$, these maximal orders are distinct and we obtain two different Galois orbits. In each case, we get a Galois orbit having a single element if and only if $\mathbb{Q}(\sqrt{-N})$ has class number 1. Thus, $C_1 \cup C_2$ gives all the w_N-fixed points if $N > 3$. Since a conic with a rational point is the projective line $\mathbb{P}^1$, this gives the proof in the genus 0 case.

So there are $\mathbb{Q}$-rational w_N-fixed points exactly when $\mathbb{Q}(\sqrt{-N})$ has class number 1, which happens when $N = 11, 19$. In the genus 1 case, we have a $\mathbb{Q}$-rational point, thus we can think it as the distinguished point and we can give the structure of an elliptic curve to $C(N,p)$ for all p. Let O be the unique fixed point of w_N which parametrizes an elliptic curve with $\mathbb{Z}[\frac{1+\sqrt{-N}}{2}]$ for $N = 11$ or 19. Therefore, $(X_0(N), O)$ and $(C(N,p), O)$ are rational elliptic curves. The elliptic curve $X_0(11)$ is given by a Weierstrass equation $y^2 + y = x^3 - x^2 - 10x - 20$ and the elliptic curve $X_0(19)$ is given by a Weierstrass equation $y^2 + y = x^3 + x^2 - 9x - 15$ by Result 4.1 in [22]. Also, we find that $X_0(11)$ has j-invariant $-122023936/161051$ and $X_0(19)$ has j-invariant $-89915392/6859$ by using PARI/GP. Since the j-invariant of $X_0(N)$ for $N = 11, 19$ is neither 0 nor 1728, the group of automorphisms $Aut(X_0(N)) = \{\pm 1\}$ by Theorem 6.4. Since w_N is an involution, we conclude that $w_N = -1$. In other words, the twist $C(N,p)$ of $X_0(N)$ by Atkin-Lehner involution w_N and $\mathbb{Q}(\sqrt{p^*})/\mathbb{Q}$ is just the quadratic twist by p^*. Finally, the signs of the functional equation of both $X_0(11)$ and $X_0(19)$ are found $+1$ by computing in PARI/GP. Thus, the sign of the functional equation for $C(N,p)$ is $\chi_{p^*}(-N) = \left(\frac{-N}{p}\right) = -1$ by Theorem 6 in [23].

□

Corollary 6.48. *Let us assume that rational elliptic curves with odd analytic rank have positive Mordell-Weil rank by Conjecture 6.43. Then for every p with $p \equiv 1 \pmod 4$ and which is a quadratic nonresidue either modulo 11 or modulo 19, the projective special linear group $\mathbb{PSL}_2(\mathbb{F}_p)$ are realized infinitely often as a Galois group over $\mathbb{Q}$.*

Remark 6.49. Let $C(N,d)$ be the curve obtained by twisting the classical modular curve $X_0(N)$ using the Atkin-Lehner involution $w_N \in Aut(X_0(N))$ and the quadratic extension $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$. Let σ be the generator of the Galois group G of the quadratic extension $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$. The twisted curve $C(N,d)$ has also a natural and interesting moduli interpretation, it parametrizes some special elliptic curves, called quadratic $\mathbb{Q}$-curves.

Definition 6.50. *A quadratic $\mathbb{Q}$-curve of degree N is defined as an elliptic curve E defined over a quadratic field $\mathbb{Q}(\sqrt{d})$ such that E and its Galois conjugate E^σ are isogenous i.e., there exists an isogeny $\phi : E \longrightarrow E^\sigma$ and the kernel of the isogeny ϕ is $\mathbb{Z}/N\mathbb{Z}$.*

The twisted curve $C(N,d)$ is moduli space of quadratic $\mathbb{Q}$-curves of degree N.

7. A SHORT SURVEY ON INVERSE GALOIS PROBLEM

The Inverse Galois Problem is one of the open problems in number theory, and it still has many unsolved cases. Firstly, Hilbert studied this problem systematically in the late 1800's. After that, many mathematicians have solved Inverse Galois Problem over rational numbers $\mathbb{Q}$ for particular finite groups.

In early 1800's, Evariste Galois explored a connection between fields and groups which provides a way to reformulate some problems from field theory in terms of group theory. Galois' ideas developed into a theory what we call Galois theory today. According to Fundamental Theorem of Galois Theory, there exists a correspondence between a Galois extension and its Galois group. But, this correspondence is very complicated in general. The Inverse Galois Problem is concerned with this complexity. In fact, since it is hard to consider a separable polynomial of degree n for any integer n, the Inverse Galois Problem asks the question from opposite direction:

Is every finite group realizable as the Galois group of a Galois extension of $\mathbb{Q}$*?*

In this first section of this chapter, we will give an overview of many known results. In the second section of this chapter, we will present some methods which are frequently used to solve the problem. The proofs of statements are omitted in this chapter, for more details we refer the reader to relevant references.

7.1. Known Results

The different versions of the Inverse Galois Problem can be formulated as follows.

(i) Existence Problem: Let G be a finite group and let K be a field. Can we determine whether G occurs as a Galois group over K? In other words, determine whether there exists a Galois extension L/K such that the Galois group $Gal(L/K)$ is isomorphic to a given group G. Such a Galois extension L is called a G-extension over K.

(ii) Construction Problem: If a group G is realizable as a Galois group over K, can we construct an explicit polynomial over K whose Galois groups is G? More interestingly, can we construct a family of polynomials over K possessing G as a Galois group?

The classical Inverse Galois Problem is defined as the existence problem for the base field rational numbers $K = \mathbb{Q}$.

After asking this question, one can naturally ask for a description of all Galois extensions of K with Galois group G. It is also interesting question whether or not we can construct the family of polynomials which gives all G-extensions of K. This is done by using generic polynomials.

Definition 7.1. *Let K be a field and let G be a finite group. A separable polynomial $f(t_1, ..., t_m, X) \in K(t_1, ..., t_m)[X] = K(t)[X]$ with coefficients in the rational function field $K(t_1..., t_m) = K(t)$ is said to be generic for G over K if it satisfies the following conditions:*

(i) The Galois group of the polynomial $f(t, X)$ is G (as a polynomial in X).

(ii) If L is an infinite field containing K and M/L is a Galois field extension with Galois group $H \leqslant G$, then there exists $c_1, ..., c_m \in L$ such that M is the splitting field of $f(c_1, ..., c_m, X)$ over L.

For more details, we refer the reader to a good reference on generic polynomials [24]. One can ask the next natural problems as follows:

(iii) Construction of Generic Polynomials: Let K and G be given as above, can we determine whether a generic polynomial exists for G-extensions over K? If it exists, can we find it? This leads to a further question.

(iv) The Number of Parameters: What is the smallest possible number of parameters of a generic polynomial of G-extensions over K?

Although not every finite group can be realized as a Galois group over certain fields, the existence problem (i) has been solved for some specific base fields K as follows:

(i) Let $K = \mathbb{C}(t)$ where t is an indeterminate. Then, any finite group G occurs as a Galois group over K. This follows basically from the Riemann Existence Theorem in [25] and [26].

(ii) If $K = \mathbb{F}_q$ is a finite field, the Galois group of every polynomial over K is a cyclic group.

(iii) If K is a p-adic field, any polynomial over K is solvable.

(iv) Let K be a p-adic field and let $K(t)$ be a function field over K with indeterminate t. Then, any finite group G is realized as a Galois group over $K(t)$ by the Harbater Existence Theorem in [27].

The construction problem (ii) is about constructing explicit polynomials with a given Galois group. Unfortunately, there are quite a few results on this problem. Some polynomials over $\mathbb{Q}$ are found by Malle, Matzat and others, many of them are found by using computer. For more details, we refer the reader to [28], [29]. Later, Abhyankar has found infinite series of polynomials in positive characteristic with various classical groups as Galois groups in [Abh2] .

If we deal with the problem of construction of generic polynomials (iii), some results are known in higher generality.

(i) The polynomial $x^p - x - t$ is generic for cyclic extensions of degree p over finite field $\mathbb{F}_p$ for all primes p by Artin-Schreier theory. The polynomial $x^n - t$ is generic for cyclic extensions of degree n over fields containing the primitive n-th roots of unity for all $n \in \mathbb{N}$ by Kummer theory.

(ii) The polynomial $x^n + t_1 x^{n-1} + ... + t_n$ is generic for S_n-extensions for any field and for all $n \in \mathbb{N}$ where S_n is the symmetric group.

(iii) The existence of generic polynomials over K for two groups G and H (they may be the same group) shows the existence of a generic polynomial for the direct product $G \times H$.

When we consider the problem of number of parameters (iv), what is the minimal number of parameters by assuming the existence of generic polynomials for the finite group G over the field K? The answer is immediate in some cases. For instance, $x^2 - t$ is generic for quadratic extensions over any field of characteristic different from 2, and clearly one parameter is the absolute minimum. On the other hand, it is difficult to determine the minimum number of parameters. Nonetheless, it is possible to find some lower bounds in some cases. For example in one-parameter case, there is a result as follows.

Proposition 7.2. [24, Proposition 8.1.4.] *Let K be a field and let G be a nontrivial finite group. Then a necessary condition for the existence of a one-parameter generic polynomial for G over K is that $G \hookrightarrow \mathbb{PGL}_2(K)$.*

The Inverse Galois Problem is significant when the base field K is lowered to $\mathbb{Q}$ (or an algebraic number field), or a function field in several indeterminates over $\mathbb{Q}$ (or over an algebraic number field).

An interesting formulation of the Inverse Problem over $\mathbb{Q}$ concerns with regular extensions. Let $t = (t_1, t_2, ..., t_n)$ be indeterminates. A finite Galois extension $K/\mathbb{Q}(t)$ is said to be regular, if $\mathbb{Q}$ is relatively algebraically closed in K, i.e., if each element in $K \setminus \mathbb{Q}$ is transcendental over $\mathbb{Q}$. Then the general question is asked:

The Regular Inverse Galois Problem: Is every finite group realisable as a Galois group of a regular extension of $\mathbb{Q}(t)$?

In what follows, we will give a list of important results in Inverse Galois Problem.

Theorem 7.3. [8, THEOREM 2.8.8.] *Any finite abelian group G is realized as a Galois group over $\mathbb{Q}$. In fact, a finite group G occurs as the Galois group of a subfield of the cyclotomic field $\mathbb{Q}(\xi_n)$, where ξ_n is an n-th root of unity for some natural number n.*

Theorem 7.4. [30] *The symmetric group S_n and the alternating group A_n for any $n \geq 1$ is realized as Galois groups over $\mathbb{Q}$.*

In 1937, the following important existence result was proved by A. Scholz [31] and H. Reichardt [32].

Theorem 7.5. *Every finite p-group occurs as a Galois group over $\mathbb{Q}$ for an odd prime p.*

The next important step about solvable groups was taken by Shafarevich. Shafarevich's proof is not constructive, and it does not give a polynomial having a finite solvable group as a Galois group.

Theorem 7.6. [33] *Every solvable group occurs as a Galois group over $\mathbb{Q}$.*

If we consider finite simple groups, the projective groups $\mathbb{PSL}_2(\mathbb{F}_p)$ for some odd primes p were first groups to be realized as Galois groups. The existence was obtained by Shih in 1974, and then polynomials were constructed over $\mathbb{Q}(t)$ by Malle and Matzat.

Theorem 7.7. [21] *Let p be an odd prime such that either 2, 3 or 7 is a quadratic non-residue modulo p. Then $\mathbb{PSL}_2(\mathbb{F}_p)$ occurs as a Galois group over $\mathbb{Q}$.*

Among the 26 sporadic simple groups, some of the Mathieu groups have been shown to be realized as Galois groups over $\mathbb{Q}$. For example:

Theorem 7.8. [34] *Four of the Mathieu groups, namely M_{11}, M_{12}, M_{22} and M_{24}, are realized as Galois groups over $\mathbb{Q}$.*

Also, Matzat and his collaborators constructed families of polynomials over $\mathbb{Q}(t)$ whose Galois groups are isomorphic to some Mathieu groups.

The most interesting result is the realization of the Monster group, which is the largest sporadic simple group. Thompson proved the following existence theorem.

Theorem 7.9. [35] *The monster simple group, a simple group of size $2^{46}.3^{20}.5^{9}.7^{6}.11^{2}.13^{3}.17.19.23.29.31.41.47.59.71$, is a Galois group of an extension over $\mathbb{Q}$.*

7.2. Important Methods

Many researchers on the Inverse Galois problem has been influenced from two ideas, namely Hilbert Irreducibility Theorem and Noether Problem. We will give an overview on these ideas in this subsection. Furthermore, a famous method in Inverse Galois Problem, called Rigidity Method, will be described at the end of this subsection.

Definition 7.10. *Let K be a field, and let $f(t,x)$ be an irreducible polynomial $K(t)[x] = K(t_1,...,t_m)(x_1,...,x_n)$. A Hilbert f-set H_f/K is defined as the set of tuples $a = (a_1,...,a_m) \in K^m$ such that $f(a,x) \in K[x]$ is well-defined and irreducible polynomial. Moreover, a Hilbert set of K^m is defined as the intersection of finitely many Hilbert f-sets and finitely many subsets of K^m of the form $\{a|g(a) \neq 0\}$ for a nonzero $g(t) \in K[t]$.*
The field K is called Hilbertian, if the Hilbert sets of K^m are nonempty for all m. In this case, they must necessarily be infinite.

Let K be a field with $char(K) = 0$. Then the following conditions are equivalent:

(i) K is Hilbertian.

(ii) If $f(t, x) \in K[t, x]$ has no roots in $K(t)$ as a polynomial in x, there exists an $a \in K$ such that $f(a, x)$ has no roots in K.

Theorem 7.11. [36, THEOREM 1.13] *Let K be a Hilbertian field, and let $f(t, x) \in K[t, x]$ be a monic, irreducible and separable polynomial. Then, there exists a Hilbert set of K^m such that the specialisations $f(a, x) \in K[x]$ of $f(t, x)$ are well-defined, irreducible and*

$$Gal(f(a, x)/K) \cong Gal(f(t, x)/K).$$

Corollary 7.12. *Let K be a Hilbertian field. If a finite group G is realized as a Galois group over $K(t)$, then it is realized over K as well.*

Theorem 7.13. [36, THEOREM 1.23] *(Hilbert irreducibility Theorem) The rational number $\mathbb{Q}$ is Hilbertian.*

Hilbert irreducibility Theorem enabled Hilbert to prove that the alternating group A_n and the symmetric group S_n can be realized as Galois groups over $\mathbb{Q}$ for all positive integers n.

Emmy Noether asked the following question in 1916:

Noether Problem: Let $L = \mathbb{Q}(t_1..., t_n)$ be the field of rational functions with n indeterminates. The symmetric group S_n acts on L by permuting the indeterminates. Let G be a transitive subgroup of S_n and let $K = L^G$ be the fixed field of G-invariant rational functions of L. Is K a rational extension of $\mathbb{Q}$? In other words, is K isomorphic to a field of rational functions over $\mathbb{Q}$?

Theorem 7.14. [37] *If G is finite group and $\mathbb{Q}(x)^G/\mathbb{Q}$ is rational (purely transcendental), then there exists a Galois extension $K/\mathbb{Q}$ with Galois group G.*

If the Noether Problem has an affirmative answer, then a finite group G occurs as a Galois group over $\mathbb{Q}$. Indeed, a finite group G occurs as a Galois group over any Hilbertian field of characteristic 0, like an algebraic number field.

The Noether Problem is still open for the alternating groups A_n. For example, A_5 has an affirmative answer, and this was proved by Maeda [Mae] in 1989. However, the answer is unknown for A_n, $n \geq 6$. This implies that the Noether Problem does not always have a positive answer, and it leads to another question. For which groups G does Noether Problem fail to have an affirmative solution?

Stronger results were proved by H. Lenstra. For instance, he showed that the smallest group for which the Noether Problem fails is the cyclic group C_8. Moreover, Lenstra gave a complete classification of abelian groups for which the Noether Problem fails.

Theorem 7.15. [38] *Let G be a finite abelian group and $K = \mathbb{Q}$. Then generic polynomials exist for G and $\mathbb{Q}$ if and only if G has no elements of order 8.*

Now, we will examine Rigidity method:

Definition 7.16. *Let G be a finite group. Let C_1,...,C_s , $s \geq 3$, be a s-tuple of conjugacy classes of G. Let us define following sets:*

$$\overline{A} = \overline{A}(C_1, ..., C_s) = \{(g_1, ..., g_s) \in C_1 \times ... \times C_s : g_1...g_s = 1\}$$
$$A = A(C_1, ..., C_s) = \{(g_1, ..., g_s) \in \overline{A} : \langle g_1, ..., g_s \rangle = G\}$$
$$\mathbb{Q}_C = \mathbb{Q}_{C_1,...,C_s} = \mathbb{Q}_{x_1,...,x_s} = \mathbb{Q}(\{\chi(C_i) \mid \chi \in Irr(G), 1 \leq i \leq s\})$$

where $x_i \in C_i$, $1 \leq i \leq s$ and $Irr(G)$ denotes the set of irreducible character of G. It is clear that $A \subset \overline{A}$ and G acts on A and $\overline{A}$ by conjugacy.

The family $(C_1, ..., C_s)$ is called rigid if A is nonempty and G acts transitively on A. The family $(C_1, ..., C_s)$ is called strictly rigid if it is rigid and $\overline{A} = A$.

Note that a conjugacy class C of G is called rational over $\mathbb{Q}$ if any irreducible character of G is rational on C. Thus, A is called rationally rigid if it is rigid and C_i is rational for $1 \leq i \leq s$.

Theorem 7.17. [39, THEOREM 4.8] *Let G be a finite group with center $\{1\}$. Let $A = A(C_1, ..., C_s)$, and $K = \mathbb{Q}_C = \mathbb{Q}_{C_1,...,C_s}$ and let t be an indeterminate over K. Let us assume that A is rigid. Then, there exists a Galois extension N of $K(t)$ unramified outside S with $Gal(N/\mathbb{Q}_C(t)) \cong G$ for any arbitrary chosen set $P = \{p_1, ..., p_s\}$ of prime divisors of $\mathfrak{p}_i \in \mathbb{P}(\mathbb{Q}_C(t)/\mathbb{Q}_C)$ of degree one such that the inertia groups over the $\mathfrak{p}_i$'s are generated by elements $\sigma_i \in C_i$. If A is rationally rigid, then we obtain $\mathbb{Q}_C = \mathbb{Q}$.*

The interest on Inverse Galois Problem has arisen in the past half century. A number of books and conference proceedings published such as Galois Groups over $\mathbb{Q}$ [40] edited by Y. Ihara, K. Ribet and J.-P. Serre in 1987, Topics in Galois Theory [20] written by J.-P. Serre in 1992, Recent Developments in the Inverse Galois Problem [41] edited by M. D. Fried in 1993, Groups as Galois groups, An Introduction [36] written by H. Volklein in 1996, and and Inverse Galois Theory [39] written by G. Malle and B. H. Matzat in 1999.

8. CONCLUSION

Inverse Galois Problem is one of the famous open problems in number theory. Which finite groups can be realized as Galois group of an extension over the rational numbers? Precisely, given a finite group G, does there exist a Galois extension with Galois group G?

We firstly gave an introduction to the Inverse Galois Problem. Then, we presented some different approaches to construct an extension of $\mathbb{Q}$ that gives a desired Galois group. In particular, we realized some specific groups as Galois groups, these groups are finite abelian groups, symmetric groups S_n, the general linear group $\mathbb{GL}_2(\mathbb{F}_p)$, and the projective special linear group $\mathbb{PSL}_2(\mathbb{F}_p)$. Finally, we gave a short survey about known results on Inverse Galois Problem.

Inverse Galois Problem is an extensive, interesting, and rich subject with many examples and results, and it has still many open cases. Unfortunately, it was not possible to cover the whole subject of Inverse Galois Problem in this thesis. Also, there exist many other results using applications from algebraic geometry, topology and many other branches of mathematics which are not covered in this thesis.

REFERENCES

1. Hilbert, D., "Uber die Irreduzibilitat ganzer rationaler Funktionen mit ganzzahligen Koeffizienten", *Journal fur die reine und angewandte Mathematik, 1892, 104-129*, 1892.

2. Dummit, D. S. and R. M. Foote, *Abstract Algebra*, John Wiley & Sons, Inc., 2004.

3. Marcus, D. A., *Number Fields*, Springer, 1977.

4. Lorenzini, D., *An Invitation to Arithmetic Geometry*, American Mathematical Society, 1996.

5. Silverman, J. H., *The Arithmetic of Elliptic Curves*, Vol. 2, Springer, 2009.

6. Reverter, A. and N. Vila, "Images of mod p Galois Representations Associated to Elliptic Curves", *Canadian Mathematical Bulletin, 2001, 313–322*, 2001.

7. Silverman, J. H., *Advances Topics in the Arithmetic of Elliptic Curves*, Springer, 1994.

8. Cox, D. A., *Primes of the Form x^2+ny^2 : Fermat, Class Field Theory and Complex Multiplication*, John Wiley & Sons, Inc, 1989.

9. Clark, P. L., "Galois groups via Atkin-Lehner twists", *Proceedings of the American Mathematical Society, 2007, 617-624*, 2007.

10. Serre, J. P., *A Course in Arithmetic*, Undergraduate Texts in Mathematics, Springer-Verlag, 1973.

11. Selmer, E. E., "On The Irreducibility of Certain Trinomials", *Mathematica Scandinavica, 1956, 287-302*, 1956.

12. Neukirch, J., *Algebraic number theory*, Springer, 1999.

13. Osada, H., "The Galois Groups of the Polynomials $X^n + aX^1 + b$", *Journal of Number Theory, 1985, 230-238*, 1985.

14. Reverter, A. and N. Vila, "Polynomials of Galois representations attached to elliptic curves", *Revista de la Real Academia de Ciencias Exactas*, 2000.

15. Silverman, J. H. and J. T. Tate, *Rational Points on Elliptic Curves*, Vol. 2, Springer, 2015.

16. Washington, L. C., *Elliptic curves: Number theory and Cryptography*, Vol. 2, Chapman & Hall/CRC, 2008.

17. Serre, J.-P., "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques", *Inventiones Mathematicae, 1972, 259-331*, 1972.

18. Diamond, F. and J. Shurman, *A First Course in Modular Forms*, Springer, 2005.

19. A.O.L and J. Lehner, "Hecke Operators on $\Gamma_0(N)$", *Math. Ann., 185, 1970, p. 134-160*, 1970.

20. Serre, J. P., *Topics in Galois Theory*, Vol. 2, Research Notes in Mathematics, A K Peters, Ltd, 2008.

21. yen Shih, K., "On the construction of Galois extensions of function fields and number fields", *Math. Ann. 207, 99-120, 1974*, 1974.

22. Yang, Y., "Defining Equations of Modular Curves", *Advances in Mathematics, 204, 481-508, 2006*, 2006.

23. Li, W.-C. W., "Newforms and Functional Equations", *Math. Ann., 212, 285-315, 1975*, 1975.

24. Jensen, C. U., A. Ledet and N. Yui, *Generic Polynomials: Constructive Aspects of the Inverse Galois Problem*, 2002.

25. Harbater, D., "Fundamental groups and embedding problems in characteristic p", *Recent developments in the Inverse Galois problem, Contemp. Math., 186, 353–369, 1995*, 1987.

26. Pop, F., "Étale Galois Covers of Affine Smooth Curves : The geometric case of a conjecture of Shafarevich On Abhyankar's conjecture", *Invent. Math., 120, 555–578, 1995*, 1995.

27. Harbater, D., "Galois Coverings of the Arithmetic Line", *Lecture Notes in Mathematics, 1240, Springer-Verlag, 165–195, 1987*, 1987.

28. Matzat, B. H., *Konstruktive Galoistheorie*, Vol. 1284, Lecture Notes in Math., 1987 Heidelberg, Springer,, 1987.

29. Malle, G., "Polynome mit Galoisgruppen $PGL_2(p)$ und $PSL_2(p)$ uber $\mathbb{Q}(t)$.", *Comm. Algebra, 21, 511-526, 1993*, 1993.

30. Hilbert, D., "Ueber die Irreduzibilität ganzer rationaler Funktionen mit ganzzahligen Koeffizienten", *Journ. f. reine angew. Math. Bd. 110, 104–129, 1892*, 1892.

31. Scholz, A., "Konstruktion algebraischer Zahlkörper mit beliebiger Gruppe von Primzahlpotenzordnung I", *Math. Z. 42, 161-188, 1937*, 1937.

32. Reichardt, H., "Konstruktion von Zahlkörpern mit gegebener Galoisgruppe von Primzahlpotenzordnung", *J. reine angew. Math. 177, 1-5, 1937*, 1937.

33. Shafarevich, I., "Construction of fields of algebraic numbers with given solvable Galois group", *Izv. Akad. Nauk SSSR Ser. Mat., 525–578, 1954*, 1954.

34. Matzat, B. H. and A. Zeh-Marschke, "Realisierung der Mathieugruppen $M_1 1$ und $M_1 2$ als Galoisgruppen über $\mathbb{Q}$", *Journal of Number Theory, 23, 195-202, 1986.*,

1986.

35. Matzat, B. H. and A. Zeh-Marschke, "Some finite groups which appear as Gal(L/K), where $K \subseteq \mathbb{Q}(\mu_n)$", *Journal of Algebra, 89, 437-499, 1984.*, 1984.

36. Völklein, H., *Groups as Galois Groups, An Introduction*, Springer, 1993.

37. Noether, E., "Gleichungen mit Vorgeschriebener Gruppe", *Math. Ann. 78, 221-229, 1916*, 1916.

38. Lenstra, H. W., "Rational Functions Invariant under a Finite Abelian Group", *Invent. Math., 25, 299–325, 1974*, 1974.

39. Malle, G. and B. H. Matzat, *Inverse Galois Theory*, Springer Monographs in Mathematics, Springer Verlag, 1999.

40. Ribet, K., Y. Ihara and J.-P. Serre, *Galois groups over* $\mathbb{Q}$, Mathematical Sciences Research Institute Publications, Springer-Verlag, 1993.

41. Fried, M. D., *Recent Developments in the Inverse Galois Problem*, Contemporary Mathematics, American Mathematical Society, 1993.

APPENDIX A: PARI/GP CODES

(i) Checking the isomorphism between two Galois extensions of polynomials $f(x)$ and $g(x)$ at the end of Subsection 4.2:

$f = x^5 - x - 1$;

$g = x^5 - 5 * x + 3$;

$nfisisom(f, g) = 0$

$\rightarrow$ Given two Galois extensions are not isomorphic.

(ii) Computation of the splitting field of the polynomial $3x^4 - 6x^2 + 3x - 1$:

$f1 = x^4 - 6 * x^2 + 3 * x - 1$;

$f2 = nfsplitting(f1)$;

$\rightarrow$ The command $nfsplitting$ computes a polynomial defining the splitting field of the given input polynomial. But, the output polynomial of the command $nfsplitting$ may be large.

$polredbest(f2) = x^{24} - 12x^{23} + 70x^{22} - 264x^{21} + 718x^{20} - 1482x^{19} + 2357x^{18} - 2802x^{17} + 2152x^{16} - 216x^{15} - 2288x^{14} + 4224x^{13} - 4915x^{12} + 4224x^{11} - 2288x^{10} - 216x^9 + 2152x^8 - 2802x^7 + 2357x^6 - 1482x^5 + 718x^4 - 264x^3 + 70x^2 - 12x + 1$

$\rightarrow$ The command *polredbest* is used to compute a simpler polynomial defining the same splitting field.

(iii) Test of irreducibility of $y^2 = x^3 + x - 1/4$ is irreducible over $\mathbb{Q}(x)$ in Application of the Proposition 5.55:

Since x is more dominant than y in PARI/GP, we use variable t instead of x such that $y^2 = t^3 + t - 1/4$.

$f = y^2 - t^3 - t + 1/4$

$polisirreducible(f) = 1$

$\rightarrow$ The command *polisirreducible* checks the irreducibility of a polynomial.

(iv) Finding Galois group of the polynomial $c_{x+y}(t) = t^8 - 2t^6 - \frac{26}{3}t^5 + \frac{283}{24}t^4 - 9t^3 + \frac{35}{4}t^2 - \frac{343}{72}t + \frac{5831}{6912}$ in Application of the Proposition 5.55:

$f = x^8 - 2x^6 - \frac{26}{3}x^5 + \frac{283}{24}x^4 - 9x^3 + \frac{35}{4}x^2 - \frac{343}{72}x + \frac{5831}{6912}$;

$polgalois(f) = [48, -1, 23,'' 2S\_4(8) = GL(2,3)'']$

$\rightarrow$ The command *polgalois* compute the Galois group of input polynomial. The output says that the Galois group has order 48 and signature -1, and it is isomorphic to $\mathbb{GL}_2(\mathbb{Z}/3\mathbb{Z})$.

(v) Computation of the j-invariant of the elliptic curve $X_0(11)$ given by $y^2 + y = x^3 - x^2 - 10x - 20$ used in Theorem 6.47:

$E1 = ellinit([0, -1, 1, -10, -20])$;

$\rightarrow$ This command defines the elliptic curve $X_0(11) : y^2 + y = x^3 - x^2 - 10x - 20$.

$E1.j = -122023936/161051$;

$\rightarrow$ The command $E1.j$ command computes the j-invariant of the elliptic curve.

In the same way, we can compute the j-invariant of the elliptic curve $X_0(19)$ given by $y^2 + y = x^3 + x^2 - 9x - 15$ used in Theorem 6.47 as follows:

$E2 = ellinit([0, 1, 1, -9, -15])$;

$E2.j = -89915392/6859$

(vi) Determination of the sign of the functional equation for the elliptic curve $X_0(11)$ given by $y^2 + xy + y = x^3 - x^2 - x - 14$ used in Theorem 6.47:

$E1 = ellinit([0, -1, 1, -10, -20])$;

$ellrootno(E1) = +1$

$\rightarrow$ The command *ellrootno* gives the sign of the functional equation for an elliptic curve.

Similarly, we can calculate the sign of the functional equation for the elliptic curve $X_0(19)$ given by $y^2 + y = x^3 + x^2 - 9x - 15$ used in Theorem 6.47:

$E2 = ellinit([0, 1, 1, -9, -15])$;

$ellrootno(E2) = +1$