THE ORDINARY COMPONENT OF ℓ-ISOGENY GRAPH OF ELLIPTIC CURVES

by

Kübra Kaytancı

B.S., Mathematics, Boğaziçi 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

2017

ACKNOWLEDGEMENTS

I would like to express my gratitude to my thesis supervisor, Assoc. Prof. Ekin Özman for her help and guidance during my studies. She always motivated me patiently throughout this work and shaped my way of mathematical thinking.

I also would like to thank Assoc. Prof. Ayhan Günaydın and Assist. Prof. Ayberk Zeytin for participating in my thesis committee with their valuable comments.

I am deeply thankful to my family and friends. Without their support and encouragement, it would be much harder for me to write this thesis.

İlkiz Bildik and Fulya Taştan deserve special thanks for their sincere friendship, their willingness to help as well as colleagueship in the path of pursuing the degree.

ABSTRACT

THE ORDINARY COMPONENT OF ℓ-ISOGENY GRAPH OF ELLIPTIC CURVES

In this thesis, our aim is to understand ℓ-volcanoes which are ordinary components of ℓ-isogeny graphs of elliptic curves over finite fields under certain conditions. In 1996, the structure of isogeny graphs of elliptic curves described by David Kohel in his PhD thesis [1]. Later, in 2002 Mireille Fouquet and Francois Morain extended Kohel's work by defining isogeny volcanoes [2]. Firstly, we give some basic definitions and tools as used throughout this thesis. Then we study the Kohel's theorem and give a 3-volcano of depth 2 over $\mathbb{F}_{409}$ as an example.

ÖZET

ELİPTİK EĞRİLERİN ℓ-İZOJENİ ÇİZGELERİNİN SIRADAN BİLEŞENLERİ

Bu tezde, amacımız sonlu cisimler üzerinde tanımlı eliptik eğrilerin ℓ-izojeni çizgelerinin sıradan bileşenlerini anlamaktır. Bu yapıya ℓ-volkan denir. 1996 yılında eliptik eğrilerin izojeni çizge yapısı David Kohel tarafından doktora tezinde tanımlandı [1]. Daha sonra 2002 yılında Mireille Fouquet ve Francois Morain, Kohel'in çalışmalarını geliştirip izojeni volkan tanımı yaptılar [2]. İlk olarak, tez boyunca kullanacağımız bazı temel tanım ve kavramlardan bahsedeceğiz. Daha sonra Kohel'in teoremini anlayıp, $\mathbb{F}_{409}$ üzerinde iki derinlikli 3-volkan örneğini vereceğiz.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF SYMBOLS

$\mathfrak{a}$	An ideal of $\mathcal{O}$
$\bar{\mathfrak{a}}$	Conjugate of an ideal $\mathfrak{a}$
$[\mathfrak{a}]$	Ideal class of an ideal $\mathfrak{a}$
$\mathbb{A}^n(K)$	The set of K-rational points of affine n space $\mathbb{A}^n$
C/K	A curve C defined over a field K
$Cl(\mathcal{O})$	The ideal class group of $\mathcal{O}$
$deg\phi$	Degree of the map ϕ
$deg_i\phi$	Inseparable degree of the map ϕ
$deg_s\phi$	Separable degree of the map ϕ
$D_{\mathfrak{q}}$	The decomposition group of $\mathfrak{q}$ over $\mathfrak{p}$
$E(K)$	Group of K-rational points on the elliptic curve E over K
E_Λ	the elliptic curve isomorphic to $\mathbb{C}/\Lambda$
$Ell_{\mathcal{O}}(\mathbb{C})$	Isomorphism class of elliptic curves defined 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
$G_{2k}(\Lambda)$	The Eisenstein series of weight $2k$
$G_\ell(K)$	ℓ-isogeny graph over K
$H_D(X)$	The Hilbert class polynomial of discriminant D
$h(\mathcal{O})$	The class number of $\mathcal{O}$
$I_{\mathfrak{q}}$	The inertia group of $\mathfrak{q}$ over $\mathfrak{p}$
j	the j-invariant of an elliptic curve
$\overline{K}$	Algebraic closure of a field K
$K(V)$	Function field of V/K
$[m]$	Multiplication-by-m map
$N(\mathfrak{a})$	Norm of an ideal $\mathfrak{a}$
O	The identity element on an elliptic curve
$\mathbb{P}^n(K)$	The set of K-rational points of projective n space $\mathbb{P}^n$
$Tr(\mathfrak{a})$	Trace of an ideal $\mathfrak{a}$

π_E	p^{th} Frobenius map
$\sigma_{\mathfrak{p}}$	Frobenius element in $Gal(L/K)$
$\Phi_\ell(X)$	Modular polynomial of an order ℓ
Λ	Lattice
$\mathcal{O}$	An order in a quadratic field K
Δ	Discriminant of an order $\mathcal{O}$
ϕ^*	A map of function fields induced by rational map of curves
$\wp(z;\Lambda)$	The Weierstrass $\wp$-function
$\hat{\phi}$	The dual isogeny of ϕ
$\left(\frac{\cdot}{\cdot}\right)$	Legendre symbol

LIST OF ACRONYMS/ABBREVIATIONS

CM	Complex Multiplication

1. INTRODUCTION

Volcanoes are undirected graphs whose names come from the geological term. For prime ℓ, isogeny volcanoes are the ordinary components of ℓ-isogeny graphs of elliptic curves. The aim of this thesis is to understand the construction of isogeny volcanoes by using the article [3]. The thesis is organized as follow :

In Chapter 2, we will study on elliptic curves. Some basic definitions and tools will be given which are required to define an isogeny volcano. Most of them are cited from the book "The Arithmetic of Elliptic Curves" [4].

In Chapter 3, we will explain orders in a quadratic number field K, especially in an imaginary quadratic field. We will focus on ideals of an order in a quadratic field by giving definitions and relations between them.

In Chapter 4, our aim is to express elliptic curves over $\mathbb{C}$ as quotients $\mathbb{C}/\Lambda$ for some lattice $\Lambda \subset \mathbb{C}$. The given definitions and results are mostly referred to [4–6]. Moreover, by defining the CM action we will show that there is a one-to-one correspondence between the ideal class groups and the isomorphism classes of elliptic curves with complex multiplication by an order in an imaginary quadratic field. [7].

In Chapter 5, we want to show that every elliptic curve with CM by an order in an imaginary quadratic field K is defined over an algebraic extension of $\mathbb{Q}$ [5]. Moreover, there is an injective group homomorphism between $Gal(L/K)$ and $Cl(\mathcal{O})$ where L is the splitting field of the Hilbert Class Polynomial [8].

In Chapter 6, our aim is to show that the injective homomorphism between $Gal(L/K)$ and $Cl(\mathcal{O})$ is also surjective. So we need to define some notions from the algebraic number theory. Most of them are referred to [8–11].

In Chapter 7, we will define an isogeny volcano and state Kohel's Theorem [3]. Then we will give a proof of the theorem.

In the last chapter, we will give an explicit example of a 3-volcano of depth 2 over $\mathbb{F}_{409}$.

2. ELLIPTIC CURVES

2.1. Algebraic Varieties and Curves

In this section, some basic notions and facts about algebraic geometry will be given. They will be used to study elliptic curves. Our main reference for this chapter is "The Arithmetic of Elliptic Curves" [4].

Let K be a field and $\overline{K}$ be its algebraic closure.

Definition 2.1. *Affine n-space over* $\overline{K}$ *is the set of n-tuples*

$$\mathbb{A}^n(\overline{K}) = \mathbb{A}^n = \{P = (x_1, \ldots, x_n) : x_i \in \overline{K}\}.$$

The set of K*-rational points* $\mathbb{A}^n$ *is the set*

$$\mathbb{A}^n(K) = \{P = (x_0, \ldots, x_n) \in \mathbb{A}^n : x_i \in K\}.$$

Definition 2.2. *Let* $\overline{K}[X] = \overline{K}[X_1, \ldots, X_n]$ *be the polynomial ring in n-independent variables and let* $I \subset \overline{K}[X]$ *be an ideal. For each ideal* I*, we have*

$$V_I = \{P \in \mathbb{A}^n : f(P) = 0 \text{ for all } f \in I\}.$$

Any set of the form V_I *is called an affine algebraic set.*

Definition 2.3. *If* V *is an algebraic set, then the ideal of* V *is the set*

$$I(V) = \{f \in \overline{K}[X] : f(P) = 0 \text{ for all } P \in V\}.$$

When $I(V)$ *is a prime ideal in* $\overline{K}[X]$*, then the affine algebraic set* V *is called an affine variety.*

Definition 2.4. *Let V be an affine variety, $P \in V$ be a point and $f_1, \ldots, f_m \in \overline{K}[X]$ be a set of generators of $I(V)$. Then V is nonsingular (or smooth) at P if the $m \times n$ matrix*

$$\left(\frac{\partial f_i}{\partial X_j}(P) \right) \quad \textit{for } 1 \leq i \leq m \textit{ and } 1 \leq j \leq n$$

has rank $n - dim(V)$. Here $dim(V)$ is the transcendence degree of $\overline{K}(V)$ over $\overline{K}$. If V is nonsingular at every point, then V is called nonsingular (or smooth).

Definition 2.5. *The projective n-space over K, denoted by $\mathbb{P}^n(K)$*

$$\mathbb{P}^n(K) = (\mathbb{A}^{n+1}(K) \setminus (0, 0, \ldots, 0))/\sim$$

with the equivalence relation

$$(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n) \quad \Leftrightarrow \quad \exists \lambda \in K^* \textit{ such that } x_i = \lambda y_i \textit{ for all } i.$$

A polynomial $f \in \overline{K}[X] = \overline{K}[X_0, X_1, \ldots, X_n]$ is homogeneous of degree d if

$$f(\lambda X_0, \ldots, \lambda X_n) = \lambda^d f(X_0, \ldots, X_n) \text{ for all } \lambda \in \overline{K}. \tag{2.1}$$

An ideal $I \subset \overline{K}[X]$ is homogenous if it is generated by homogeneous polynomials. A projective algebraic set is any set of the form

$$V_I = \{P \in \mathbb{P}^n(K) : f(P) = 0 \text{ for all homogeneous } f \in I\} \tag{2.2}$$

for a homogeneous ideal I. If V is a projective algebraic set, the homogeneous ideal of V, denoted $I(V)$ is the ideal of $\overline{K}[X]$ generated by

$$\{f \in \overline{K}[X] : f \text{ is homogeneous and } f(P) = 0 \text{ for all } P \in V\}. \tag{2.3}$$

A projective algebraic set is called a projective variety if its homogeneous ideal $I(V)$ is a prime ideal in $\overline{K}[X]$.

Definition 2.6. *Let V_1, $V_2 \subset \mathbb{P}^n$ be projective varieties. A rational map from V_1 to V_2 is a map of the form*

$$\phi : V_1 \longrightarrow V_2, \quad \phi = [f_0, \ldots, f_n],$$

where functions $f_0, \ldots, f_n \in \overline{K}(V_1)$. Note that for all $i \in \{0, 1, \ldots, n\}$, f_i has the property that for every point $P \in V_1$ at which $f_0, \ldots, f_n$ are all defined,

$$\phi(P) = [f_0(P), \ldots, f_n(P)] \in V_2.$$

A rational map

$$\phi = [f_0, \ldots, f_n] : V_1 \longrightarrow V_2$$

is regular at $P \in V_1$ if there is a function $g \in \overline{K}(V_1)$ such that

(i) each gf_i is regular at P;
(ii) there exists i in $\{0, 1 \ldots, n\}$ such that $(gf_i)(P) \neq 0$.

A rational map which is regular at every point is called morphism.

Definition 2.7. *A (affine/ projective) curve is one dimensional (affine/projective) variety.*

2.1.1. Maps Between Curves

In this section, a curve means a projective curve.

Theorem 2.8. *[4, Theorem 2.3.] Let $\phi : C_1 \longrightarrow C_2$ be a morphism of a curves. Then ϕ is either constant or surjective.*

Definition 2.9. *Let $C_1 \longrightarrow C_2$ be a map of curves defined over K. If ϕ is constant, then we define the degree of ϕ to be 0. Otherwise, we say that ϕ is a finite map. Let $\phi^* : K(C_2) \longrightarrow K(C_1)$ be a map of function fields induced by rational map of curves satisfying $\phi^* f = f \circ \phi$. Then we define its degree to be*

$$deg\phi = [K(C_1) : \phi^* K(C_2)].$$

Moreover, ϕ is called separable, inseparable or purely inseparable if the field extension $K(C_1)/\phi^* K(C_2)$ has the corresponding property. The notation of the separable and inseparable degree of the extensions are $deg_s\phi$ and $deg_i\phi$, respectively.

2.1.2. Frobenius Map

Assume that $char(K) = p$ is prime and $q = p^r$ where $r \in \mathbb{Z}^+$. Let $f \in K[X]$ be an arbitrary polynomial. Then f^q is the polynomial obtained by raising each of the coefficients of f to the power q. Then for any curve C over K, we can define a new curve C^q over K such that its homogeneous ideal $I(C^q)$ is generated by $\{f^q : f \in I(C)\}$. The q^{th}- power Frobenius morphism is a natural map from C to C^q, given in [4], by

$$\phi : C \longrightarrow C^q, \qquad \phi([x_0, \ldots, x_n]) = [x_0^q, \ldots, x_n^q]. \tag{2.4}$$

Note that

$$\begin{aligned} f^q(\phi(P)) &= f^q(x_0^q, \ldots, x_n^q) \\ &= (f(x_0, \ldots, x_n))^q \qquad \text{since char}(K) = p \\ &= 0 \qquad\qquad\qquad\qquad\quad \text{since } f(P) = 0. \end{aligned}$$

So for each point $P = [x_0, \ldots, x_n] \in C$ the image $\phi(P)$ is a zero of each generator f^q of $I(C^q)$. Therefore ϕ maps to C to C^q.

Proposition 2.10. *[4, Proposition 2.11.] Let K be a field of characteristic $p > 0$ and let $q = p^r$. let C be a curve over K and $\phi : C \longrightarrow C^q$ the q^{th} power Frobenius morphism. Then*

(i) $\phi^* K(C^q) = K(C)^q = \{f^q : f \in K(C)\}$,
(ii) ϕ *is purely inseparable,*
(iii) $deg\phi = q$.

Corollary 2.11. *[4, Corollary 2.12.] Every map $\psi : C_1 \longrightarrow C_2$ of smooth curves over a field of characteristic p factors as*

$$C_1 \xrightarrow{\phi} C_1^q \xrightarrow{\lambda} C_2 \tag{2.5}$$

where $q = deg_i(\psi)$, the map ϕ is the q^{th}-power Frobenius map, and the map λ is separable.

2.2. Elliptic Curves

Definition 2.12. *An elliptic curve is a smooth projective curve with a base point. It has an equation of the form*

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \tag{2.6}$$

with coefficients $a_1, \ldots, a_6 \in \overline{K}$. The base point is the point at infinity $O = [0, 1, 0]$.

Consider the nonhomogeneous coordinates $x = X/Z$ and $y = Y/Z$, we can write Equation 2.6 for an elliptic curve E as

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{2.7}$$

This equation is called the Weierstrass equation of E.

As in [4] when the characteristic of a field $\overline{K}$ is not 2, by using the change of variables $(x, y) \longrightarrow (x, \frac{1}{2}(y - a_1x - a_3))$, we get

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6 \tag{2.8}$$

where

$$b_2 = a_1^2 + 4a_4, \qquad b_4 = 2a_4 + a_1a_3, \qquad b_6 = a_3^2 + 4a_6.$$

Moreover, when char$\overline{K} \neq 2, 3$ and by using the substitution $(x, y) \longrightarrow (\frac{x-3b_2}{36}, \frac{y}{108})$, we get

$$E : y^2 = x^3 - 27c_4x - 54c_6 \tag{2.9}$$

where

$$c_4 = b_2^2 - 24b_4, \qquad c_6 = -b_2^3 + 36b_2b_4 - 216b_6.$$

Define the quantities as :

$$\begin{aligned} b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2, \\ \Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6, \\ j &= c_4^3/\Delta. \end{aligned}$$

Definition 2.13. *The quantity Δ is called the discriminant of a Weirstrass equation, the quantity j is called the j-invariant of an elliptic curve.*

Remark 2.14. *Let E be an elliptic curve given by the Weierstrass equation*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{2.10}$$

Let $P = (x_0, y_0)$ be a point on E. Then the polynomial

$$f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 \tag{2.11}$$

satisfies $f(P) = 0$.

The point P is a singular point given by $f(x, y)$ if and only if $\frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0$. Otherwise, P is called a nonsingular point given by $f(x, y)$.

Taylor expansion of a function $f(x, y)$ at a point $P = (x_0, y_0)$ is

$$\begin{aligned} f(x,y) = f(x_0,y_0) &+ \frac{\partial f}{\partial x}(x_0,y_0)(x-x_0) + \frac{\partial f}{\partial y}(x_0,y_0)(y-y_0) \\ &+ \frac{1}{2!}\Big[\frac{\partial^2 f}{\partial x^2}(x_0,y_0)(x-x_0)^2 + 2\frac{\partial f}{\partial x}\frac{\partial f}{\partial y}(x_0,y_0)(x-x_0)(y-y_0) + \dots\Big] \\ &+ \dots . \end{aligned}$$

Consider that P is nonsingular, then we have

$$f(x, y) - f(x_0, y_0) = ((y - y_0) - \alpha(x - x_0))((y - y_0) - \beta(x - x_0)) - (x - x_0)^3 \tag{2.12}$$

for some $\alpha, \beta \in \overline{K}$.

Definition 2.15. *The singular point P is called a node if $\alpha \neq \beta$. The lines*

$$y - y_0 = \alpha(x - x_0) \quad \textit{and} \quad y - y_0 = \beta(x - x_0)$$

are tangent lines at P. If $\alpha = \beta$, then P is called a cusp. The tangent line at P

$$y - y_0 = \alpha(x - x_0).$$

Remark 2.16. *Any two Weierstrass equations for an elliptic curve E are related by a change of variables of the form*

$$x = u^2x' + r \quad \text{and} \quad y = u^3y' + su^2y' + t \tag{2.13}$$

where $u, r, s, t \in \overline{K}$ and $u \neq 0$.

After substituting change of variables to the Weierstrass equation, we have

$$u^{12}\Delta' = \Delta \quad \text{and} \quad j' = j. \tag{2.14}$$

Let $charK$ be different than 2 and 3. Let E be an elliptic curve given by the Weierstrass equation of the form

$$E : y^2 = x^3 + Ax + B. \tag{2.15}$$

Then the only change of variables preserving the Equation 2.15 is

$$x = u^2x' \quad \text{and} \quad y = u^3y' \quad \text{for some } u \in \overline{K}^*. \tag{2.16}$$

Proposition 2.17. *[4, Proposition 1.4.]*

(i) Two elliptic curves are isomorphic over $\overline{K}$ if and only if they both have the same j-invariant.

(ii) Let $j_0 \in \overline{K}$. There exists an elliptic curve defined over $K(j_0)$ whose j-invariant is equal to j_0.

Proof. (i) Assume that two elliptic curves E_1 and E_2 are isomorphic over $\overline{K}$. By Equation 2.15 , we have $j(E_1) = j(E_2)$. Conversely, let E_1 and E_2 be two elliptic

curves such that $j(E_1) = j(E_2)$. The corresponding Weierstrass equations are

$$E_1 : y^2 = x^3 + Ax + B,$$
$$E_2 : y'^2 = x'^3 + A'x' + B'.$$

By the formula of j-invariant, since $j(E_1) = j(E_2)$, we have

$$\frac{(4A)^3}{4A^3 + 27B^2} = \frac{(4A')^3}{4A'^3 + 27B'^2}. \tag{2.17}$$

So,

$$A^3B'^2 = A'^3B^2 \tag{2.18}$$

There are 3 cases :

Case 1. If $A = 0$, then we have $j = 0$. Then $B \neq 0$ since $\Delta \neq 0$. So $A' = 0$. We get an isomorphism by $u = (B/B')^{1/6} \in \overline{K}^*$.

Case 2. If $B = 0$, then we have $j = 1728$. Then $A \neq 0$, since $\Delta \neq 0$. It gives $B' = 0$. Taking $u = (A/A')^{1/4} \in \overline{K}^*$, we obtain an isomorphism.

Case 3. If $AB \neq 0$, then $j \neq 0, 1728$. Then $A'B' \neq 0$. Taking $u = (A/A')^{1/4} = (B/B')^{1/6} \in \overline{K}^*$ we have the isomorphism.

(ii) First, choose $j_0 \neq 0, 1728$. Then

$$E : y^2 + xy = x^3 - \frac{36}{j_0 - 1728}x - \frac{1}{j_0 - 1728} \tag{2.19}$$

is defined over $K(j_0)$. Calculating the discriminant and j-invariant, we get $\Delta \neq 0$ and $j = j_0$.

For the case $j_0 = 0$, we can take the elliptic curve as $E : y^2 + y = x^3$. It has discriminant $\Delta = -27$. For the case $j_0 = 1728$, consider $E' : y^2 = x^3 + x$ with $\Delta = -64$. Both E and E' are defined over K. Therefore we get the result.

□

2.2.1. The Group Law

Let E be an elliptic curve given by the Weierstrass equation

$$E : f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0. \tag{2.20}$$

The Composition Law : Let $P, Q \in E(\overline{K})$ be given and let L_{PQ} denote the line through P and Q. Then $P + Q$ can be found by these 2 steps :

(i) $L_{PQ} \cap E(\overline{K}) = \{P, Q, R\}$.
(ii) $L_{RO} \cap E(\overline{K}) = \{R, O, P + Q\}$.

Note that for any P, $Q \in E(\overline{K})$, L_{PQ} intersects $E(\overline{K})$ at three points by Bézout's Theorem. For the proof of the theorem, see [12, I.7.8. page 54].

Observe that $E(\overline{K})$ is an abelian group with an identity element O [4, Proposition 2.2.].

2.2.2. Isogenies

Definition 2.18. *Let E_1 and E_2 be two elliptic curves. An isogeny from E_1 to E_2 is a morphism*

$$\phi : E_1 \longrightarrow E_2 \quad \textit{satisfying} \quad \phi(O_{E_1}) = O_{E_2}.$$

Two elliptic curves E_1 and E_2 are isogenous if there exists an isogeny from E_1 to E_2 with $\phi(E_1) \neq \{O\}$.

Theorem 2.19. *[4, Theorem 3.6.] Let $\phi, \psi : E_1 \longrightarrow E_2$ be two morphisms of elliptic curves E_1 and E_2. Then $\phi + \psi$ is also a morphism of elliptic curves E_1 and E_2.*

Moreover, if $\phi, \psi_1, \psi_2 : E \longrightarrow E$ *are endomorphisms of an elliptic curve* E*, then* $\phi \circ (\psi_1 + \psi_2) = (\phi \circ \psi_1) + (\phi \circ \psi_2)$ *is also an endomorphism of* E*.*

Since $E(\overline{K})$ has an abelian group structure, then

$$Hom(E_1, E_2) = \{\text{isogenies from } E_1 \text{ to } E_2\} \tag{2.21}$$

is also group satisfying $(\phi + \psi)(P) = \phi(P) + \psi(P)$ where $\phi, \psi \in Hom(E_1, E_2)$ and $P \in E_1$. The addition $+$ on the right hand side of the equation is a group operation on E_2.

Thus $End(E) = Hom(E, E)$ is a ring with addition law given before and multiplication law as composition

$$(\phi\psi)(P) = \phi(\psi(P)). \tag{2.22}$$

The ring $End(E)$ is called the endomorphism ring of E.

Definition 2.20. *Let* $m \in \mathbb{Z}$*. Then there is a natural isogeny*

$$\begin{aligned} [m] : E &\longrightarrow E \\ P &\longmapsto [m]P \end{aligned}$$

which is called the multiplication-by-m map. If $m > 0$*, then* $[m](P) = \underbrace{P + \cdots + P}_{m-times}$*. If* $m < 0$*,* $[m](P) = \underbrace{-P - \cdots - P}_{m-times}$*. If* $m = 0$*, then* $[0]P = O$*.*

Definition 2.21. *Let* E *be an elliptic curve and* $m \in \mathbb{Z}$ *with* $m \geq 1$*. The* m*-torsion subgroup of* E *is the set of points of* E *of order* m *denoted as*

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

Note that $E[m]$ *is also the kernel of the multiplication-by-m map.*

We have an injection $\mathbb{Z} \longrightarrow End(E)$ taking $m \in \mathbb{Z}$ to $[m] \in End(E)$. So we always have $\mathbb{Z} \subseteq End(E)$. When $\mathbb{Z} \neq End(E)$, we say that E has complex multiplication(CM). [4, Remark 4.3.]

Theorem 2.22. *[4, Theorem 4.10.] Let $\phi : E_1 \longrightarrow E_2$ be a nonzero isogeny. Then :*

(i) For every $Q \in E_2$,

$$|\phi^{-1}(Q)| = deg_s\phi \tag{2.23}$$

where $deg_s\phi$ is the separable degree of the map ϕ.

(ii) Suppose that ϕ is separable. Then

$$|ker\phi| = deg\phi \tag{2.24}$$

and $\overline{K}(E_1)$ is a Galois extension of $\phi^*\overline{K}(E_2)$.

Proposition 2.23. *[4, Proposition 4.12.] Let E be an elliptic curve and Φ be a finite subgroup of E. There exist a unique elliptic curve E' and a separable isogeny*

$$\phi : E \longrightarrow E' \quad satisfying \quad ker\phi = \Phi. \tag{2.25}$$

Remark 2.24. *[4, Corollary 5.4.] Let E be an elliptic curve over K and $m \in \mathbb{Z}$. Assume that $m \neq 0$ in K. Then the multiplication-by-m map on E is a finite separable endomorphism.*

Theorem 2.25. *[4, Theorem 6.1.] Let $\phi : E_1 \longrightarrow E_2$ be a non-constant isogeny of degree m. There exist a unique isogeny*

$$\hat{\phi} : E_2 \longrightarrow E_1 \quad satisfying \quad \hat{\phi} \circ \phi = [m]. \tag{2.26}$$

Definition 2.26. *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 2.25. Observe that if $\phi = [0]$*, then we set* $\hat{\phi} = [0]$.

Fact 2.27. *[4, Theorem 6.2.] Let* $\phi : E_1 \longrightarrow E_2$ *be a non-constant isogeny.*

(i) Let $m = deg\phi$*. Then we have its dual* $\hat{\phi}$ *satisfying* $\hat{\phi} \circ \phi = [m]$ *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) $\hat{\hat{\phi}} = \phi$

Corollary 2.28. *[4, Corollary 6.4.] Let* E *be an elliptic curve and* $m \in \mathbb{Z}$ *with* $m \neq 0$.

(i) If $m \neq 0$ *in* K*, i.e. if either* $char(K) = 0$ *or* $p = char(K) > 0$, $p \nmid m$*, then*

$$E[m] = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}. \tag{2.27}$$

(ii) If $char(K) = p > 0$*, then one of the followings is true :*

(a) $E[p^e] = \{O\}$ *for all* $e = 1, 2, \ldots$.

(b) $E[p^e] = \mathbb{Z}/p^e\mathbb{Z}$ *for all* $e = 1, 2, \ldots$.

Proof. (i) For all $d|m$ and $d \neq 0$, we have $[d]$ is separable by Corollary 2.24. It implies that $|E[d]| = |ker[d]| = d^2$. Recall that $E[d]$ is subgroup of all elements of order d. We have an element of order d at maximal. By the fundamental theorem of finitely generated abelian groups, we have

$$E[m] = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}. \tag{2.28}$$

(ii) Let ϕ be the p^{th} Frobenius map

$$\begin{aligned} |E[p^e]| &= deg_s[p^e] && \text{by Theorem 2.22} \\ &= (deg_s(\hat{\phi} \circ \phi)^e && \text{since } \hat{\phi} \circ \phi = [p] \\ &= (deg_s\hat{\phi})^e && \text{by Theorem 2.10} \end{aligned}$$

and also $deg\phi = p = deg\hat{\phi}$. So,

(a) If $deg_s\hat{\phi} = 1$, i.e. $\hat{\phi}$ is inseparable, then we have $|E[p^e]| = 1$ for all e. Thus we have

$$E[p^e] = \{O\} \quad \text{for all } e = 1, 2, \ldots. \tag{2.29}$$

(b) If $deg_s\hat{\phi} = p$, i.e $\hat{\phi}$ is separable, then $|E[p^e]| = p^e$ for all e. By the fundamental theorem of finite abelian groups,

$$E[p^e] = \frac{\mathbb{Z}}{p^e\mathbb{Z}} \quad \text{for all } e = 1, 2, \ldots \tag{2.30}$$

□

Remark 2.29. *For any prime $\ell \neq charK$, we have $E[\ell] = \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$. So there are $(\ell + 1)$-many cyclic subgroups in $E[\ell]$ of order ℓ. Each of which is the kernel of a separable ℓ-isogeny by Propositon 2.23. Since there are $\ell^2 - 1(= (\ell - 1)(\ell + 1))$-many elements except identity and $\ell - 1$ is the number of non-identity elements in the subgroup of order ℓ, it gives us $\ell + 1$ cyclic subgroups of order ℓ. [3]*

Definition 2.30. *Let A be an abelian group. A function*

$$d : A \longrightarrow \mathbb{R}$$

is a quadratic form if it satisfies the following conditions:

(i) $d(\alpha) = d(-\alpha)$ *for all* $\alpha \in A$,

(ii) The pairing

$$\begin{aligned} A \times A &\longrightarrow \mathbb{R} \\ (\alpha, \beta) &\longmapsto d(\alpha + \beta) - d(\alpha) - d(\beta), \end{aligned}$$

is bilinear.

A quadratic form d *is positive definite if the followings are satisfied:*

(iii) $d(\alpha) \geq 0$ *for all* $\alpha \in A$,

(iv) $d(\alpha) = 0$ *if and only if* $\alpha = 0$.

Corollary 2.31. *[4, Corollary 6.3.] Let* E_1 *and* E_2 *be two elliptic curves. The degree map*

$$deg : Hom(E_1, E_2) \longrightarrow \mathbb{Z} \tag{2.31}$$

is a positive definite quadratic form.

Proof. $(i), (iii), (iv)$ are obviously satisfied. We will show that the pairing $Hom(E_1, E_2) \times Hom(E_1, E_2) \longrightarrow \mathbb{Z}$ satisfying $\langle \phi, \psi \rangle = deg(\phi + \psi) - deg(\phi) - deg(\psi)$ is bilinear for any ϕ, $\psi \in Hom(E_1, E_2)$. We have an injection $[\quad] : \mathbb{Z} \longrightarrow End(E)$.

$$\begin{aligned} [\langle \phi, \psi \rangle] &= [deg(\phi + \psi)] - [deg(\phi)] - [deg(\psi)] \\ &= \widehat{(\phi + \psi)} \circ (\phi + \psi) - \hat{\phi} \circ \phi - \hat{\psi} \circ \psi \\ &= (\hat{\phi} + \hat{\psi}) \circ (\phi + \psi) - \hat{\phi} \circ \phi - \hat{\psi} \circ \psi \\ &= \hat{\phi} \circ (\phi + \psi) + \hat{\psi} \circ (\phi + \psi) - \hat{\phi} \circ \phi - \hat{\psi} \circ \psi \\ &= (\hat{\phi} \circ \psi) + (\hat{\psi} \circ \phi). \end{aligned}$$

Then we have

$$\begin{aligned}[\langle\phi, \psi_1 + \psi_2\rangle] &= \hat{\phi} \circ (\psi_1 + \psi_2) + (\widehat{\psi_1 + \psi_2}) \circ \phi \\ &= \hat{\phi} \circ \psi_1 + \hat{\phi} \circ \psi_2 + \hat{\psi_2} \circ \phi + \hat{\psi_1} \circ \phi \\ &= \langle\phi, \psi_1\rangle + \langle\phi, \psi_2\rangle.\end{aligned}$$

Similarly, we can show that $[\langle(\phi_1 + \phi_2), \psi\rangle] = \langle\phi_1, \psi\rangle + \langle\phi_2, \psi\rangle$. So, it is bilinear. □

Lemma 2.32. *Let E be an elliptic curve over K. For any $\pi \in End(E)$, we have $\pi + \hat{\pi} = 1 + deg\pi - deg(id - \pi)$.*

Proof. Take $\pi \in End(E)$. Then we have

$$\begin{aligned}[deg(id - \pi)] = (\widehat{id - \pi}) \circ (id - \pi) = (\hat{id} - \hat{\pi}) \circ (id - \pi) = (id - \hat{\pi}) \circ id - (id - \hat{\pi}) \circ \pi \\ &= [1] - (\hat{\pi} + \pi) + \hat{\pi} \circ \pi \\ &= [1] - (\hat{\pi} + \pi) + [deg\pi].\end{aligned}$$

So we have $\hat{\pi} + \pi = [1 + deg\pi - deg(id - \pi)]$. The map $\hat{\pi} + \pi$ is multiplication-by-n map for some $n \in \mathbb{Z}$. □

Definition 2.33. *Let K be a $\mathbb{Q}$-algebra that is finitely generated over $\mathbb{Q}$. An order R of K is a subring of K that is a finitely generated $\mathbb{Z}$-module such that $R \otimes_{\mathbb{Z}} \mathbb{Q} = K$.*

Theorem 2.34. *[4, Theorem 9.3.] Let R be a ring of characteristic 0 having no zero divisors. Assume that R satisfies the following :*

(i) R has rank at most four as a $\mathbb{Z}$-module.

(ii) R has an anti-involution $\alpha \mapsto \hat{\alpha}$ satisfying

$$\widehat{\alpha + \beta} = \hat{\alpha} + \hat{\beta}, \quad \widehat{\alpha\beta} = \hat{\beta}\hat{\alpha}, \quad \hat{\hat{\alpha}}, \quad \hat{a} = a \text{ for some } a \in \mathbb{Z} \subset R \tag{2.32}$$

(iii) For $\alpha \in R$, the product $\alpha\hat{\alpha}$ is nonnegative, and $\alpha\hat{\alpha} = 0$ if and only if $\alpha = 0$.

Then R is one of the following:

a. $R \simeq \mathbb{Z}$,
b. *R is an order in an imaginary quadratic extension of $\mathbb{Q}$,*
c. *R is an order in a quaternion algebra over $\mathbb{Q}$.*

Corollary 2.35. *[4, Corollary 9.4.] The endomorphism ring of an elliptic curve E/K is either $\mathbb{Z}$ or an order in an imaginary quadratic field or an order in a quaternion algebra.*

Proof. Notice that

(i) $End(E)$ is a free $\mathbb{Z}$-module rank at most 4. For the proof see [4, III.7.5. page 91].
(ii) $End(E)$ has anti-involution $\phi \mapsto \hat{\phi}$ satisfying

$$\widehat{\phi+\psi} = \hat{\phi}+\hat{\psi}, \quad \widehat{\phi\psi} = \hat{\psi}\hat{\phi}, \quad \hat{\hat{\phi}} = \phi, \quad \hat{a} = a \text{ for some } a \in \mathbb{Z} \subset End(E) \quad (2.33)$$

by Fact 2.27.
(iii) For $\phi \in End(E)$, $\phi \circ \hat{\phi} = 0$ if and only if $\phi = 0$ by Corollary 2.31.

Then Theorem 2.34 implies the desired result. □

Definition 2.36. *The endomorphism algebra of E is $End^0(E) := End(E) \otimes_{\mathbb{Z}} \mathbb{Q}$.*

Theorem 2.37. *[4, Theorem 3.1.] Let K be a field of characteristic p and E/K an elliptic curve. For each integer $r \geq 1$, let*

$$\phi_r : E \longrightarrow E^{p^r} \text{ and } \hat{\phi} : E^{p^r} \longrightarrow E \quad (2.34)$$

be the p^r- power Frobenius map and its dual.

(i) The followings are equivalent:

(a) $E[p^r] = 0$ *for all* $r \geq 1$.

(b) $\hat{\phi}_r$ *is (purely) inseparable for all* $r \geq 1$.

(c) The map $[p] : E \longrightarrow E$ *is purely inseparable and* $j(E) \in \mathbb{F}_{p^2}$.

(d) $End(E)$ *is an order in a quaternion algebra.*

(ii) If the equivalent conditions in (i) do not hold , then

$$E[p^r] = \mathbb{Z}/p^r\mathbb{Z} \text{ for all } r \geq 1. \tag{2.35}$$

If further $j(E) \in \overline{\mathbb{F}}_p$, *then* $End(E)$ *is an order of a quadratic imaginary field.*

Proof. (i) $\underline{(a) \implies (b)}$: Assume that $E[p^r] = 0$ for all r$\geq$1. Since Frobenius map is purely inseparable, $deg_s[p^r] = deg_s(\phi_r \circ \hat{\phi}_r) = deg_s(\hat{\phi}_r)$

Also we have $deg_s[p^r] = (deg_s[p])^r = (deg_s(\hat{\phi}))^r$ where $\hat{\phi}$ is dual isogeny of p^{th}-power Frobenius map.

It gives us $ker[p^r] = E[p^r]$, since $E[p^r] = \{P \in E : [p^r]P = O\}$. We know that the order of the kernel of an isogeny is equal to its separable degree. So, $deg_s[p^r] = |ker[p^r]| = |E[p^r]| = 0$. Therefore we get $\hat{\phi}_r$ is purely inseparable for all $r \geq 1$.

$\underline{(b) \implies (c)}$: Assume that $\hat{\phi}_r$ is (purely) inseparable for all $r \geq 1$. Since $deg_s(\hat{\phi}_r) = deg_s[p^r] = (deg_s[p])^r$, we have $deg_s[p] = 1$.

By Corollary 2.11 , $\hat{\phi}$ factors as

$$E^p \xrightarrow{\pi} E^{p^2} \xrightarrow{\psi} E \tag{2.36}$$

where $p = deg_i(\phi)$, the map π is the p^{th}-power Frobenius map, and the map ψ has degree one. Since the map ψ is isomorphism, $j(E) = j(E^{p^2}) = (j(E))^2$. Therefore $j(E) \in \mathbb{F}_{p^2}$.

$\underline{(c) \implies (d)}$: Suppose that the map $[p] : E \longrightarrow E$ is purely inseparable and $j(E) \in \mathbb{F}_{p^2}$. We want to show that $End(E)$ is an order in a quaternion algebra. Assume, to the contrary, that $End(E)$ is a number field, i.e. $End(E) \otimes_{\mathbb{Z}} \mathbb{Q} \simeq \mathbb{Q}$

or $End(E) \otimes_{\mathbb{Z}} \mathbb{Q} \simeq \mathbb{Q}(\sqrt{d})$ where $d < 0$ and d is squarefree.

Let E' be an elliptic curve which is isogenous to E and $\psi : E \longrightarrow E'$ be an isogeny. Let $[p]_E$ denote multiplication-by-p map from E to E. Since $\psi \circ [p]_E = [p]_{E'} \circ \psi$, $deg_i[p]_E = deg_i[p]_{E'}$. Hence, $[p]_{E'}$ is purely inseparable and $|E'[p]| = 1$. By $(a \Rightarrow b \Rightarrow c)$, $j(E') \in \mathbb{F}_{p^2}$. This implies that there are finitely many elliptic curves which are isogenous to E (up to isomorphism).

Let $\ell \in \mathbb{Z}$ be a prime such that $\ell \neq p$ and ℓ remains prime in $End(E')$. So we have $E[\ell^n] = \mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^n\mathbb{Z}$. Therefore we can get a chain of subgroups of E such that

$$\Phi_1 \subset \Phi_2 \subset \cdots \subset E \quad \text{where} \quad \Phi_n = \mathbb{Z}/\ell^n\mathbb{Z}. \tag{2.37}$$

Since each Φ_n is a finite subgroup of E, there exists a unique elliptic curve $E_n = E/\Phi_n$ and a separable isogeny $\phi_n : E \longrightarrow E_n$ such that $ker\phi_n = \Phi_n$ by Proposition 2.23. There are finitely many E_n (up to isomorphism), so $i, j > 0$ can be chosen as $E_i \simeq E_{i+j}$. Then we get a natural projection $\pi : E_i \longrightarrow E_{i+j} \simeq E_i$ with kernel Φ_{i+j}/Φ_i which is cyclic of order ℓ^j.

Note that for the element π of the ring $End(E_m)$, $N(\pi) = \pi\bar{\pi} = deg\pi$ [1] . So π factors as $u \circ [\ell^{j/2}]$ for some $u \in Aut(E_i)$ and j must be even. But the kernel of $[\ell^{j/2}]$ is $\mathbb{Z}/\ell^{j/2}\mathbb{Z} \times \mathbb{Z}/\ell^{j/2}\mathbb{Z}$ which is not cyclic. So, we get a contradiction. Therefore $End(E)$ is an order in a quaternion algebra.

$\underline{(d) \implies (b)}$: For the proof, see in [4, Teorem 3.1.].

(ii) We already showed that if (a) does not hold, then we have

$$E[p^r] = \mathbb{Z}/p^r\mathbb{Z} \text{ for all } r \geq 1. \tag{2.38}$$

Assume that $j(E) \in \overline{\mathbb{F}}_p$ and the equivalent conditions in (i) are not satisfied. Let E' be an elliptic curve over $\overline{\mathbb{F}}_{p^r}$ which has the same j-invariant of E, i.e $E \simeq E'$. Let ϕ_r be p^r-power Frobenius endomorphism of E such that the isomorphic image of ϕ_r in $\mathbb{Z}$. When we consider the degree of ϕ_r, we get $\phi_r = [p^{r/2}]$. Since Frobenius

[1] See Remark 4.13

map is purely inseparable, $|kerE[p^{r/2}]| = |E[p^{r/2}]| = deg_s\phi_r = 1$ By part (i), we have a contradiction, then $End(E') \neq \mathbb{Z}$. Moreover, $End(E')$ is not an order in a quaternion algebra by assumption part (i). Therefore $End(E')$ is an order in an imaginary quadratic field by Corollary 2.35.

□

Definition 2.38. *Let E be an elliptic curve over a field K with $charK = p > 0$. If $E[p] = \mathbb{Z}/p\mathbb{Z}$, then E is called ordinary. If $E[p] = \{O\}$, then E is called supersingular.*

Theorem 2.39. *[13, Theorem 14.1.] Let $\phi : E_1 \longrightarrow E_2$ be an isogeny. Then E_1 is supersingular(ordinary) if and only if E_2 is supersingular(ordinary).*

Proof. Let $[p]_{E_1} \in End(E_1)$ and $[p]_{E_2} \in End(E_2)$ for some $p \in \mathbb{Z}$. Then we have

$$\begin{aligned}
[p]_{E_2} \circ \phi &= \phi \circ [p]_{E_1} \\
deg_i([p]_{E_2} \circ \phi) &= deg_i(\phi \circ [p]_{E_1}) \\
deg_i([p]_{E_2})deg_i(\phi) &= deg_i(\phi)deg_i([p]_{E_1}) \\
deg_i([p]_{E_2}) &= deg_i([p]_{E_1}).
\end{aligned}$$

This implies that $deg_i([p])_{E_1} = deg_i([p]_{E_2}) = 1$ if and only if $|E_1[p]|$ and $|E_2[p]|$ are both equal to the degree of multiplication-by-p map, i.e. E_1 and E_2 are both ordinary. The same proof works for supersingular case. □

3. ORDERS

In this chapter, we will study orders in a quadratic number field K, especially imaginary quadratic field and ideals of an order. These are mostly cited from the book "The primes of the form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication" [6], the book "Solving Pell Equation" [14], and lecture notes [7].

Definition 3.1. *An order $\mathcal{O}$ in a quadratic field K is a subset $\mathcal{O} \subset K$ such that*

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

Remark 3.2. *Let $\mathcal{O}$ be an order and K be its field of fraction. The ring of integers $\mathcal{O}_K$ is called a maximal order. Since $\mathcal{O}_K$ and $\mathcal{O}$ are free $\mathbb{Z}$-modules of rank 2, we have $[\mathcal{O}_K : \mathcal{O}] < \infty$. The index $[\mathcal{O}_K : \mathcal{O}]$ is called the conductor of $\mathcal{O}$.*

Definition 3.3. *Let $\alpha \mapsto \bar{\alpha}$ be the nontrivial automorphism of K. Suppose $\mathcal{O} = [\alpha, \beta]$ is any order of K. The discriminant $\Delta(\mathcal{O})$ of $\mathcal{O}$ is*

$$\Delta(\mathcal{O}) = \begin{vmatrix} \alpha & \beta \\ \bar{\alpha} & \bar{\beta} \end{vmatrix}^2 = (\alpha\bar{\beta} - \bar{\alpha}\beta)^2.$$

Lemma 3.4. *[6, Lemma 7.2.] Let $\mathcal{O}$ be an order in a quadratic field K of discriminant d_K. Then $\mathcal{O}$ has finite index in $\mathcal{O}_K$. If we set $f = [\mathcal{O}_K : \mathcal{O}]$, then*

$$\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K = [1, fw_K], \tag{3.1}$$

where $w_K = \frac{d_K + \sqrt{d_K}}{2}$.

Proof. Let $f = [\mathcal{O}_K : \mathcal{O}]$. Then we get $f\mathcal{O}_K \subset \mathcal{O}$. So $\mathbb{Z} + f\mathcal{O}_K \subset \mathcal{O}$. Observe that $\mathbb{Z} + f\mathcal{O}_K = [1, fw_K]$ and also it has index f in $\mathcal{O}_K$. Hence, the result follows. □

Observe that the discriminant of an order $\mathcal{O}$ does not depend on the integral basis α and β of $\mathcal{O}$. By Lemma 3.4, we can write $\mathcal{O} = [1, fw_K]$. Then we get $\Delta(\mathcal{O}) = f^2 d_K$. Since the discriminant d_K of quadratic number field K is congruent to 0 or 1 modulo 4, so is $\Delta(\mathcal{O})$.

Every nonzero ideal $\mathfrak{a}$ of $\mathcal{O}$ has finite index. The norm of a nonzero ideal $\mathfrak{a}$ of an order $\mathcal{O}$ is defined as $N(\mathfrak{a}) = |\mathcal{O}/\mathfrak{a}| < \infty$.

Definition 3.5. *An ideal $\mathfrak{a}$ of $\mathcal{O}$ is proper if*

$$\mathcal{O} = \{\beta \in K : \beta\mathfrak{a} \subset \mathfrak{a}\}.$$

Remark 3.6. *Principal ideals are always proper.*

Definition 3.7. *A fractional ideal of $\mathcal{O}$ is a subset of K which is of the form $\alpha\mathfrak{a}$, where $\alpha \in K^*$ and $\mathfrak{a}$ is an $\mathcal{O}$-ideal.*

A fractional $\mathcal{O}$- ideal $\mathfrak{b}$ is proper provided that

$$\mathcal{O} = \{\beta \in K : \beta\mathfrak{b} \subset \mathfrak{b}\}.$$

Definition 3.8. *Let $\mathcal{O}$ be an order in a quadratic field K and $\mathfrak{a}$,$\mathfrak{b}$ be two fractional $\mathcal{O}$-ideals. Then $\mathfrak{a}$ and $\mathfrak{b}$ are said to be equivalent if $\gamma\mathfrak{a} = \delta\mathfrak{b}$ for some γ, $\delta \in \mathcal{O}$. If $\mathfrak{a}$ is a fractional ideal $\mathcal{O}$-ideal, then $[\mathfrak{a}]$ denotes the set of all fractional $\mathcal{O}$-ideals that are equivalent to $\mathfrak{a}$. It is called the ideal class of an ideal $\mathfrak{a}$.*

Definition 3.9. *A fractional $\mathcal{O}$-ideal $\mathfrak{a}$ is invertible if there is another fractional $\mathcal{O}$-ideal $\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{b} = [\mathcal{O}]$.*

Lemma 3.10. *[6, Lemma 7.5.] Let $K = \mathbb{Q}(\tau)$ be a quadratic field, and $ax^2 + bx + c$ be the minimal polynomial of τ where a, b and c are relatively prime integers. Then $[1, \tau]$ is a proper fractional ideal for the order $[1, a\tau]$ of K.*

Proof. Observe that $a\tau \in K$ satisfies a polynomial $x^2+bx+ca$. It is an algebraic integer. So $\mathcal{O} := [1, a\tau]$ is order of K. Then we need to show that $[1, \tau]$ is a proper fractional ideal for the order $[1, a\tau]$ of K, it means that $[1, a\tau] = \{\alpha \in K : \alpha[1, \tau] \subset [1, \tau]\}$.

Clearly, $[1, a\tau] \subset \{\alpha \in K : \alpha[1, \tau] \subset [1, \tau]\}$. Let $\alpha \in K$ such that $\alpha[1, \tau] \subset [1, \tau]$. Then we get $\alpha \in [1, \tau]$ and $\alpha\tau \in [1, \tau]$. Since $\alpha \in [1, \tau]$, there exist $m, n \in \mathbb{Z}$ such that $\alpha = m + n\tau$. Since $ax^2 + bx + c$ is the minimal polynomial of τ, we get $\tau^2 = \frac{-c-b\tau}{a}$. Substitute τ^2 to $\alpha\tau = m\tau + n\tau^2$ and get

$$\alpha\tau = \frac{-cn}{a} + \left(\frac{-bn}{a} + m\right)\tau. \tag{3.2}$$

We know that $a\tau$ is an algebraic integer, it implies that n must be divisible by a since $(a, b, c) = 1$. Then α can be written as $m + k(a\tau)$ where $n = ak$ for some $k \in \mathbb{Z}$. Therefore $\alpha \in [1, a\tau]$ [6, Lemma 7.5.]. □

Proposition 3.11. *[6, Proposition 7.4.] Let $\mathcal{O}$ be an order in a quadratic field K and $\mathfrak{a}$ a fractional $\mathcal{O}$-ideal. Then $\mathfrak{a}$ is proper if and only if $\mathfrak{a}$ is invertible.*

Proof. Assume that $\mathfrak{a}$ is invertible. So there exists a fractional $\mathcal{O}$-ideal $\mathfrak{b}$ satisfying that $\mathfrak{ab} = \mathcal{O}$. We want to show that $\mathfrak{a}$ is proper. Obviously, $\mathcal{O} \subset \{\alpha \in K : \alpha\mathfrak{a} \subset \mathfrak{a}\}$.

Let $\alpha \in K$ and $\alpha\mathfrak{a} \subset \mathfrak{a}$, then

$$\alpha\mathcal{O} = \alpha(\mathfrak{ab}) = (\alpha\mathfrak{a})\mathfrak{b} \subset \mathfrak{ab} = \mathcal{O}. \tag{3.3}$$

So we get $\alpha \in \mathcal{O}$. It shows that $\{\alpha \in K : \alpha\mathfrak{a} \subset \mathfrak{a}\} \subset \mathcal{O}$. Therefore $\mathcal{O} = \{\alpha \in K : \alpha\mathfrak{a} \subset \mathfrak{a}\}$.

Conversely, assume that $\mathfrak{a}$ is a proper fractional $\mathcal{O}$-ideal. Note that $\mathfrak{a}$ is a $\mathbb{Z}$-module of rank 2. We can write it as $\mathfrak{a} = [\alpha, \beta]$ where $\alpha, \beta \in K$. Then $\mathfrak{a} = \alpha[1, \tau]$ such that $\tau = \beta/\alpha$. Let $ax^2 + bx + c$ be the minimal polynomial of τ. Then by Lemma 3.10 , $[1, \tau]$ is proper fractional ideal for $\mathcal{O} = [1, a\tau]$. Let $\alpha \mapsto \bar{\alpha}$ be the nontrivial

automorphism of K. Take another root of ax^2+bx+c as $\bar{\tau}$, we get $\bar{\mathfrak{a}} = \bar{\alpha}[1,\bar{\tau}]$ which is a proper fractional ideal for $\mathcal{O} = [1, a\bar{\tau}]$ by Lemma 3.10. Then

$$\begin{aligned} a\mathfrak{a}\mathfrak{a}' &= a\alpha\alpha'[1,\tau][1,\tau'] \\ &= N(\alpha)a[1,\tau,\tau',\tau\tau'] \quad \text{since } N(\alpha) = \alpha\alpha' \\ &= N(\alpha)[a, a\tau, -b, c] \quad \text{since } \tau+\tau' = -b/a \text{ and } \tau\tau' = c/a \\ &= N(\alpha)[1, a\tau] \quad \text{since } (a,b,c) = 1 \\ &= N(\alpha)\mathcal{O}. \end{aligned}$$

Choose $\mathfrak{b} = \frac{a\alpha'}{N(\alpha)}$ such that $\mathfrak{a}\mathfrak{b} = \mathcal{O}$. So $\mathfrak{a}$ is invertible.

Therefore $\mathfrak{a}$ is proper if and only if $\mathfrak{a}$ is invertible. □

Definition 3.12. *The ideal class group $Cl(\mathcal{O})$ is the multiplicative group of equivalence classes of proper fractional $\mathcal{O}$-ideals. The class number of $\mathcal{O}$ is the order of ideal class group $Cl(\mathcal{O})$. It is denoted by $h(\mathcal{O})$.*

$$Cl(\mathcal{O}) = \frac{\{\textit{non-zero proper fractional } \mathcal{O}\textit{-ideals}\}}{\{\textit{non-zero principal fractional } \mathcal{O}\textit{-ideals}\}}.$$

Theorem 3.13. *[6, Theorem 23.3.] Let E be an elliptic curve defined over k with CM by an order $\mathcal{O}_1$ in an imaginary quadratic field K. Suppose that there exist a prime degree ℓ-isogeny $\varphi : E \longrightarrow E'$. Then E' has CM by an order $\mathcal{O}_2$ in K, and one of the followings holds:*

(i) $\mathcal{O}_1 = \mathcal{O}_2$,
(ii) $[\mathcal{O}_1 : \mathcal{O}_2] = \ell$,
(iii) $[\mathcal{O}_2 : \mathcal{O}_1] = \ell$.

Proof. Let $\hat{\varphi} : E' \longrightarrow E$ be the dual isogeny of φ. For every $\tau \in End(E)$, we have an isogeny $\gamma = \varphi \circ \tau \circ \hat{\varphi} \in End(E')$. Since $End(E')$ is a ring, we can find the degree and

trace of γ. The degree of γ is

$$deg\gamma = deg(\varphi \circ \tau \circ \hat{\varphi}) = (deg\varphi)^2 deg\tau. \tag{3.4}$$

And the trace of γ is

$$Tr(\gamma) = \gamma + \hat{\gamma} = \varphi \circ \tau \circ \hat{\varphi} + \varphi \circ \hat{\tau} \circ \hat{\varphi} = \varphi \circ \tau \circ \hat{\varphi} + \hat{\varphi} \circ \hat{\tau} \circ \varphi = \hat{\varphi} \circ (\tau + \hat{\tau}) \circ \varphi = (deg\varphi) Tr(\tau). \tag{3.5}$$

We can conclude that γ and $(deg\varphi)\tau$ are the roots of the characteristic polynomial $x^2 - (Tr)x + deg$.[2] So $\mathbb{Q}(\gamma) \simeq \mathbb{Q}((deg\varphi)\tau) \simeq \mathbb{Q}(\tau)$ and $End^0(E) \subseteq End^0(E')$.

Similarly, take an arbitrary $\tau' \in End(E')$. There is $\gamma' = \hat{\varphi} \circ \tau' \circ \varphi \in End(E')$ with $deg\gamma' = (deg\varphi)^2 deg\tau'$ and $Tr(\gamma') = (deg\varphi) Tr(\tau')$. Hence, we have $\mathbb{Q}(\gamma') \simeq \mathbb{Q}(\tau')$ and $End^0(E') \subseteq End^0(E)$. Thus $End^0(E) = End^0(E') = K$. Then E' has CM by $\mathcal{O}_2$ in K.

Now, consider $\mathcal{O}_1 = [1, \tau]$ and $\mathcal{O}_2 = [1, \tau']$ for some $\tau, \tau' \in \mathbb{H}$. Then $\varphi \circ \tau \circ \hat{\varphi} = [\ell\tau] \in End(E')$ since $[\tau]$ is multiplication map and $\hat{\varphi} \circ \varphi = [\ell]$. Also $\ell\tau \in \mathcal{O}_2$ since $End(E') \simeq \mathcal{O}_2$. By the same way, we have $\hat{\varphi} \circ \tau' \circ \varphi = [\ell\tau']$ and $\ell\tau' \in \mathcal{O}_1$. This implies that $[1, \ell\tau] \subseteq \mathcal{O}_2 = [1, \tau']$ and $[1, \ell\tau'] \subseteq \mathcal{O}_1 = [1, \tau]$. Thus we have

$$[1, l^2\tau] \subseteq [1, \ell\tau'] \subseteq [1, \tau]. \tag{3.6}$$

Note that the index $[[1, \tau] : [1, \ell^2\tau]]$ is ℓ^2. So there are three cases for the index of $[1, \ell\tau']$ in $[1, \tau]$ which are 1, ℓ or ℓ^2. If the index is 1, then $[\mathcal{O}_2 : \mathcal{O}_1] = \ell$. If the index is ℓ, then $\mathcal{O}_1 = \mathcal{O}_2$. If the index is ℓ^2, then $[\mathcal{O}_1 : \mathcal{O}_2] = \ell$. □

Definition 3.14. *Let $\varphi : E \longrightarrow E'$ be a prime degree ℓ-isogeny of elliptic curves E and E' with CM by orders $\mathcal{O}_1$ and $\mathcal{O}_2$ in an imaginary quadratic field K, respectively. Then*

[2] See Remark 4.13

(i) we say that φ *is horizontal isogeny if* $\mathcal{O}_1 = \mathcal{O}_2$,

(ii) we say that φ *is vertical(descending) isogeny if* $[\mathcal{O}_1 : \mathcal{O}_2] = \ell$,

(iii) we say that φ *is vertical(ascending) isogeny if* $[\mathcal{O}_2 : \mathcal{O}_1] = \ell$.

4. COMPLEX MULTIPLICATION

In this chapter, our aim is to express an elliptic curve over $\mathbb{C}$ as a quotient $\mathbb{C}/\Lambda$ for some lattice $\Lambda \subset \mathbb{C}$. Given definitions and theorems are mostly from [4–6]. Moreover, we will show existence of a one-to-one correspondence between ideal class groups and isomorphism classes of elliptic curves by CM action given as in [7].

Definition 4.1. *A lattice $\Lambda \subset \mathbb{C}$ is an additive subgroup $\Lambda = \mathbb{Z}\lambda_1 + \mathbb{Z}\lambda_2$ of $\mathbb{C}$ generated by $\mathbb{R}$-linearly independent complex numbers λ_1 and λ_2. It is denoted by $\Lambda = [\lambda_1, \lambda_2]$.*

Definition 4.2. *If Λ_1 is a sublattice of Λ_2 such that the group Λ_2/Λ_1 is cyclic, then we say that Λ_1 is a cyclic sublattice of Λ_2.*

Lemma 4.3. *[8, Lemma 21.2.] Let $\Lambda = [1, \tau]$ be a lattice with $\tau \in \mathbb{H}$. The cyclic sublattices of Λ with a prime index ℓ are the lattice $[1, \ell\tau]$ and the lattices $[\ell, \tau + k]$ where $0 \leq k < \ell$.*

Definition 4.4. *Let $\Lambda \subset \mathbb{C}$ be a lattice. The Weierstrass $\wp$-function (relative to Λ)is defined by the series*

$$\wp(z;\Lambda) = \frac{1}{z^2} + \sum_{\substack{w\in\Lambda \\ w\neq 0}} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2} \right).$$

The Eisenstein's series of weight 2k (for Λ)is the series

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

Remark 4.5. *[4, Remark 3.5.1.] There is a relation between $\wp(z)$ and $\wp'(z)$ such that*

$$\wp'(z)^2 = 4\wp(z)^3 - 60G_4(\Lambda)\wp(z) - 140G_6(\Lambda) \quad \textit{for every } z \in \mathbb{C} - \Lambda. \tag{4.1}$$

We define g_2 and g_3 as

$$g_2 = g_2(\Lambda) = 60G_4(\Lambda) \qquad \textit{and} \qquad g_3 = g_3(\Lambda) = 140G_6(\Lambda). \tag{4.2}$$

Proposition 4.6. *[4, Proposition 3.6.] Let $g_2 = g_2(\Lambda)$ and $g_3 = g_3(\Lambda)$ be the quantities associated to lattice $\Lambda \subset \mathbb{C}$. The polynomial $f(x) = 4x^3 - g_2x - g_3$ has distinct roots, so its discriminant $\Delta(\Lambda) = g_2^3 - 27g_3^3$ is nonzero.*

Definition 4.7. *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 4.8. *Note that since $\Delta(\Lambda)$ is not equal to 0, j-invariant is always well-defined.*

Let Λ_1 and Λ_2 be lattices in $\mathbb{C}$. Assume that $\alpha \in \mathbb{C}$ such that $\alpha\Lambda_1 \subset \Lambda_2$. By multiplication- by-$\alpha$ map, we get an induced map

$$\phi_\alpha : \mathbb{C}/\Lambda_1 \longrightarrow \mathbb{C}/\Lambda_2, \qquad \phi_\alpha(z) = \alpha z (\text{mod } \Lambda_2). \tag{4.3}$$

Let $z_1, z_2 \in \Lambda_1$ such that $z_1 = z_2$. Then we get

$$\phi(z_1) = \alpha z_1 (\text{mod } \Lambda_2) = \alpha z_2 (\text{mod } \Lambda_2) = \phi(z_2). \tag{4.4}$$

So ϕ is well-defined. Let $z_1, z_2 \in \mathbb{C}/\Lambda_1$. Then

$$\phi(z_1+z_2) = \alpha(z_1+z_2)(\text{mod } \Lambda_2) = \alpha z_1(\text{mod } \Lambda_2) + \alpha z_2(\text{mod } \Lambda_2) = \phi(z_1)+\phi(z_2). \tag{4.5}$$

So induced map is a well-defined group homomorphism.

Theorem 4.9. *[4, Theorem 4.1.] With notation as above,*

a. *the association*

$$\{\alpha \in \mathbb{C} : \alpha\Lambda_1 \subset \Lambda_2\} \longrightarrow \left\{ \begin{array}{c} \textit{holomorphic maps} \\ \phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2 \\ \textit{with } \phi(0) = 0 \end{array} \right\} \tag{4.6}$$

$$\alpha \longmapsto \phi_\alpha \tag{4.7}$$

is a bijection.

b. *let E_1 and E_2 be elliptic curves corresponding to lattices Λ_1 and Λ_2, respectively. We have $E_1 : y^2 = 4x^3 - g_2(\Lambda_1)x - g_3(\Lambda_1)$ and $E_2 : y^2 = 4x^3 - g_2(\Lambda_2)x - g_3(\Lambda_2)$. Then the natural inclusion*

$$\{\textit{isogenies } \phi : E_1 \to E_2\} \longrightarrow \left\{ \begin{array}{c} \textit{holomorphic maps} \\ \phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2 \\ \textit{with } \phi(0) = 0 \end{array} \right\} \tag{4.8}$$

is bijection.

Theorem 4.10 (Uniformization Theorem)**.** *[4, Theorem 5.1.] For every elliptic curve $E/\mathbb{C}$, there exists a lattice $\Lambda \subset \mathbb{C}$ and an isomorphism*

$$f : \mathbb{C}/\Lambda \longrightarrow E(\mathbb{C}) \tag{4.9}$$

$$z \longmapsto [\wp(z;\Lambda), \wp'(z;\Lambda), 1]. \tag{4.10}$$

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

Corollary 4.11. *[4, Corollary 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. First, assume that Λ_1 and Λ_2 are homothetic lattices. There exist an $\alpha \in \mathbb{C}^*$ satisfying $\Lambda_2 = \alpha\Lambda_1$. Then

$$g_2(\Lambda_2) = g_2(\alpha\Lambda_1) = 60G_4(\alpha\Lambda_1) = 60 \sum_{\substack{w\in\alpha\Lambda_1 \\ w\neq 0}} w^{-4} = 60\alpha^{-4} \sum_{\substack{w\in\Lambda_1 \\ w\neq 0}} w^{-4} = \alpha^{-4} g_2(\Lambda_1) \quad (4.11)$$

and

$$g_3(\Lambda_2) = g_3(\alpha\Lambda_1) = 140G_6(\alpha\Lambda_1) = 140 \sum_{\substack{w\in\alpha\Lambda_1 \\ w\neq 0}} w^{-6} = 140\alpha^{-4} \sum_{\substack{w\in\Lambda_1 \\ w\neq 0}} w^{-6} = \alpha^{-6} g_2(\Lambda_1). \quad (4.12)$$

So

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

Since j-invariants are equal, we can deduce that elliptic curves E_1 and E_2 are isomorphic.

Conversely, assume that E_1 and E_2 are isomorphic, it means that they have the same j-invariants. So lattices Λ_1 and Λ_2 satisfy $j(\Lambda_1) = j(\Lambda_2)$. By using the definition of j-invariant, we can choose $\alpha \in \mathbb{C}^*$ such that

$$\alpha^4 = \frac{g_2(\Lambda_1)}{g_2(\Lambda_2)} \qquad \text{and} \qquad \alpha^6 = \frac{g_3(\Lambda_1)}{g_3(\Lambda_2)}. \quad (4.13)$$

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

Theorem 4.12. *[4, Theorem 5.5.] Let $E/\mathbb{C}$ be an elliptic curve. Let λ_1 and λ_2 be generators for the lattice Λ associated to E by the Uniformization Theorem. Then one of the following is true:*

(i) $End(E) = \mathbb{Z}$.

(ii) The field $\mathbb{Q}(\lambda_2/\lambda_1)$ is an imaginary quadratic extension of $\mathbb{Q}$ and $End(E)$ is isomorphic to an order in $\mathbb{Q}(\lambda_2/\lambda_1)$.

Proof. By the Uniformization Theorem, there exists a lattice $\Lambda = [\lambda_1, \lambda_2]$ where $\lambda_1, \lambda_2 \in \mathbb{C}$. Let $\tau = \frac{\lambda_2}{\lambda_1}$. Then we get

$$\Lambda = [\lambda_1, \lambda_2] = \lambda_1[1, \tau]. \tag{4.14}$$

Since $\lambda_1 \in \mathbb{C}^*$, Λ and $[1, \tau] = \mathbb{Z} + \tau\mathbb{Z}$ are homothetic. Therefore we may consider Λ as $[1, \tau]$ instead of $[\lambda_1, \lambda_2]$. Define

$$\mathcal{O} = \{\alpha \in \mathbb{C} : \alpha\Lambda \subset \Lambda\}, \tag{4.15}$$

By Theorem 4.9, $\mathcal{O} \simeq End(E)$. For all α in $\mathcal{O}$, the inclusion $\alpha[1, \tau] \subset [1, \tau]$ gives us

$$\alpha = a + b\tau \quad \text{and} \quad \alpha\tau = c + d\tau \quad \text{for some } a, b, c, d \in \mathbb{Z}. \tag{4.16}$$

When we write $\tau = \frac{c}{\alpha - d}$, we get $\alpha^2 - (a + d)\alpha + ad - bc = 0$. So $\mathcal{O}$ is an integral extension of $\mathbb{Z}$.

Assume that $\mathcal{O} \neq \mathbb{Z}$ and take an element α in $\mathcal{O} - \mathbb{Z}$. Since $\alpha = a + b\tau$, b can not be zero. So we can get rid of α in the above equations. Then the equation

$$b\tau^2 - (a - d)\tau - c = 0 \tag{4.17}$$

holds. Since $\tau \notin \mathbb{R}$, we have that $\mathbb{Q}(\tau)$ is an imaginary quadratic extension of $\mathbb{Q}$. Since every $\alpha \in \mathcal{O}$ is also an element of $\mathbb{Q}(\tau)$, we have the inclusion $\mathcal{O} \subset \mathbb{Q}(\tau)$ and also $\mathcal{O}$ is integral over $\mathbb{Z}$. Therefore $\mathcal{O}$ is an order in $\mathbb{Q}(\tau)$. □

Remark 4.13. *Let Λ be lattice in $\mathbb{C}$. Assume that $\alpha \in \mathbb{C}$ satisfying $\alpha\Lambda \subset \Lambda$. We have an induced map*

$$\phi_\alpha : \mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\Lambda, \qquad \phi_\alpha(z) = \alpha z (mod\ \Lambda). \tag{4.18}$$

where $\mathbb{C}/\Lambda \simeq E$ is the elliptic curve over $\mathbb{C}$ by the Uniformization Theorem.

Then ϕ_α gives an isogeny and also there exists its dual isogeny $\phi_{\hat{\alpha}} : \mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\Lambda$. Both ϕ_α and $\phi_{\hat{\alpha}}$ are in $End(\mathbb{C}/\Lambda)$. By Theorem 4.12, we have $End(\mathbb{C}/\Lambda) \simeq \mathcal{O}$ for some $\mathcal{O} = [1, \tau]$ in an imaginary quadratic field K where $\tau \in \mathbb{C}$. Then

$$\begin{aligned} \mathcal{O} &\xrightarrow{\sim} End(\mathbb{C}/\Lambda) \\ r = a + b\tau &\longmapsto \quad \psi \\ \bar{r} = a' - b'\tau &\longmapsto \quad \hat{\psi} \end{aligned}$$

where $a, b \in \mathbb{Z}$ and $\bar{r}$ be the conjugate of r. Therefore we can conclude that the conjugate element of ψ in the ring $End(\mathbb{C}/\Lambda)$ corresponds to the dual isogeny of ψ. So $N(\psi) = \psi\bar{\psi} = deg\psi$.

If $\mathbb{Z} \subset End(E) \simeq \mathcal{O}$ is satisfied Theorem 4.12, then we say that E has complex multiplication by the order $\mathcal{O}$ in the imaginary quadratic field $\mathbb{Q}(\tau)$.

The natural question is that how can we construct an elliptic curve which has CM by $\mathcal{O}$ if $\mathcal{O}$ is a given order in an imaginary quadratic field K. [7]

Let K be an imaginary quadratic field and $\mathcal{O}$ an order in K. If $\mathfrak{a}$ is a proper fractional ideal of $\mathcal{O}$, then $\mathfrak{a}$ can be seen as a lattice in $\mathbb{C}$. By the Uniformization Theorem, we get the corresponding elliptic curve $E_\mathfrak{a}$ whose endomorphism ring is

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

Definition 4.14. *Given an order $\mathcal{O}$ in an imaginary quadratic field K. Let $S_\mathcal{O}(k)$ be the set of all elliptic curves over k of which endomorphism rings are isomorphic to $\mathcal{O}$. Let E_1, $E_2 \in S_\mathcal{O}(k)$. We say E_1 is equivalent to E_2 (denoted $E_1 \sim E_2$) if E_1 and E_2 are isomorphic elliptic curves over k. Then $Ell_\mathcal{O}(k)$ denotes $S_\mathcal{O}(k)/\sim$.*

There is a one-to-one correspondence between homothetic lattices and isomorphism classes of elliptic curves which are obtained from these lattices, it means that Λ and $\alpha\Lambda$ for some $\alpha \in \mathbb{C}^*$ give the same elliptic curve in $Ell_{\mathcal{O}}(\mathbb{C})$. We will denote $\mathbb{C}$-isomorphism class of elliptic curves which are obtained by the lattice Λ by $\{E_\Lambda\}$.

Let $\mathcal{O}$ be an order in an imaginary quadratic field K. Take an arbitrary proper fractional $\mathcal{O}$-ideal $\mathfrak{a}$ with generators α and β, i.e. $\mathfrak{a} = [\alpha, \beta]$. Observe $\mathfrak{a} \subset \mathbb{C}$, so $\mathfrak{a}$ is a lattice.

Consider a lattice $\Lambda = [1, \tau]$ and an order $\mathcal{O} = [1, w]$ in an imaginary quadratic field K with $End(E_\Lambda) \simeq \mathcal{O}$. By Theorem 4.9, $End(E_\Lambda) \simeq \{\alpha \in \mathbb{C} : \alpha\Lambda \subset \Lambda\} = \mathcal{O}$. Since $w \in \mathcal{O}$, we have $w \in \Lambda$ such that $w = a + b\tau$ for some a, $b \in \mathbb{Z}$. Observe that

$$b\Lambda = [b, b\tau] = [b, w - a] = [b, w] \tag{4.19}$$

since $b(w-a)+ab = bw \in [b, w-a]$ and $b \in [b, w-a]$. So w must be in $[b, w-a]$. Observe that $[b, w]$ is an $\mathcal{O}$-ideal since $[b, w] \subset \mathcal{O}$ and $\mathcal{O}[b, w] \subset [b, w]$. Denote $\mathfrak{a} = [b, w]$. The equality gives us that Λ is homothetic to an $\mathcal{O}$-ideal $\mathfrak{a}$.
Therefore we can conclude that when $\mathfrak{a}$ and $\mathfrak{b}$ are proper fractional $\mathcal{O}$-ideals, $\mathfrak{a}$ and $\mathfrak{b}$ are equivalent in $Cl(\mathcal{O})$ if and only if they are homothetic as lattices in $\mathbb{C}$.

Proposition 4.15. *Let $\mathcal{O}$ be an order in an imaginary quadratic field K. Then there is a bijection*

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

.

Proof. Let $[\mathfrak{a}] = [\mathfrak{b}]$ in $Cl(\mathcal{O})$. Observe that $\mathfrak{a}$ and $\mathfrak{b}$ are equivalent proper fractional ideals of $\mathcal{O}$. Then they have the same j-invariant. Therefore $\{E_{\mathfrak{a}}\} = \{E_{\mathfrak{b}}\}$ and also the map is well-defined.

Consider $[\mathfrak{a}]$, $[\mathfrak{b}] \in Cl(\mathcal{O})$ with $\{E_{\mathfrak{a}}\} = \{E_{\mathfrak{b}}\}$. By Corollary 4.11, $\mathfrak{a}$ and $\mathfrak{b}$ are homothetic as lattices. So the map is injective.

Let $E \in Ell_{\mathcal{O}}(\mathbb{C})$. By the Uniformization Theorem there is a lattice Λ such that $E \simeq \mathbb{C}/\Lambda$. So for some proper fractional $\mathcal{O}$-ideal $\Lambda = \mathfrak{a}$ up to homothety. Then the map is also surjective. This implies a one-to-one relation between the ideal class group $Cl(\mathcal{O})$ and the isomorphism class of elliptic curves $Ell_{\mathcal{O}}(\mathbb{C})$. □

4.1. The CM action

Let E be an elliptic curve over $\mathbb{C}$ and $\mathcal{O}$ be an order in an imaginary quadratic field K such that $End(E) \simeq \mathcal{O}$. By the Uniformization Theorem and Remark 4, there is a proper fractional $\mathcal{O}$-ideal $\mathfrak{b}$ such that $E \simeq E_{\mathfrak{b}}$. There is a map

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

Take $([\mathfrak{a}], \{E_{\mathfrak{b}}\}) = ([\mathfrak{a}'], \{E_{\mathfrak{b}'}\})$ in $Cl(\mathcal{O}) \times Ell_{\mathcal{O}}(\mathbb{C})$. This gives us that $[\mathfrak{a}] = [\mathfrak{a}']$ and $\{E_{\mathfrak{b}}\} \simeq \{E_{\mathfrak{b}'}\}$. Then we have $\{E_{\mathfrak{a}^{-1}\mathfrak{b}}\} \simeq \{E_{\mathfrak{a}'^{-1}\mathfrak{b}'}\}$.

If $\mathfrak{a}$ is a principal fractional $\mathcal{O}$-ideal, whose class represents the identity element in $Cl(\mathcal{O})$, then for any $\{E_{\mathfrak{b}}\} \in Ell_{\mathcal{O}}(\mathbb{C})$, we have $[\mathfrak{a}] * \{E_{\mathfrak{b}}\} = \{E_{\mathfrak{a}^{-1}\mathfrak{b}}\} = \{E_{\mathfrak{b}}\}$ since $\mathfrak{b}$ and $\mathfrak{a}^{-1}\mathfrak{b}$ are homothetic.

Let $\mathfrak{a}$, $\mathfrak{b}$, and $\mathfrak{c}$ be arbitrary proper fractional $\mathcal{O}$-ideals. Then

$$[\mathfrak{a}] * ([\mathfrak{b}] * \{E_{\mathfrak{c}}\}) = [\mathfrak{a}] * \{E_{\mathfrak{b}^{-1}\mathfrak{c}}\} = \{E_{\mathfrak{a}^{-1}\mathfrak{b}^{-1}\mathfrak{c}}\} = \{E_{(\mathfrak{b}\mathfrak{a})^{-1}\mathfrak{c}}\} = \{E_{(\mathfrak{a}\mathfrak{b})^{-1}\mathfrak{c}}\} = [\mathfrak{a}\mathfrak{b}] * \{E_{\mathfrak{c}}\}. \tag{4.20}$$

Therefore we can conclude that there is a group action of $Cl(\mathcal{O})$ on $Ell_{\mathcal{O}}(\mathbb{C})$.

Theorem 4.16. *The action of $Cl(\mathcal{O})$ on $Ell_{\mathcal{O}}(\mathbb{C})$ is transitive and free.*

Proof. Let $\mathfrak{a}$ and $\mathfrak{b}$ be any proper fractional $\mathcal{O}$-ideals. Take a proper fractional $\mathcal{O}$-ideal $\mathfrak{c} = \mathfrak{b}\mathfrak{a}^{-1}$. Then

$$[\mathfrak{c}] * \{E_{\mathfrak{b}}\} = [\mathfrak{b}\mathfrak{a}^{-1}] * \{E_{\mathfrak{b}}\} = \{E_{\mathfrak{a}\mathfrak{b}^{-1}\mathfrak{b}}\} = \{E_{\mathfrak{a}}\}. \tag{4.21}$$

Thus the ideal class group $Cl(\mathcal{O})$ transitively acts on $Ell_{\mathcal{O}}(\mathbb{C})$. [7]

Moreover, take $\mathfrak{c} \in Cl(\mathcal{O})$ satisfying $[\mathfrak{c}] * \{E_{\mathfrak{b}}\} = \{E_{\mathfrak{b}}\}$ for any $\{E_{\mathfrak{b}}\} \in Ell_{\mathcal{O}}(\mathbb{C})$. Then $\{E_{\mathfrak{c}^{-1}\mathfrak{b}}\} = \{E_{\mathfrak{b}}\}$. This implies that $\mathfrak{c}^{-1}\mathfrak{b}$ and $\mathfrak{b}$ are homothetic. So $\mathfrak{c}$ is principal fractional $\mathcal{O}$-ideal. Therefore the action is also free. [7] □

Remark 4.17. *The ideal class group $Cl(\mathcal{O})$ is a finite group. (For the proof see in [9, Corollary 2.].) Since there is a bijection between $Cl(\mathcal{O})$ and $Ell_{\mathcal{O}}(\mathbb{C})$, we have $|Cl(\mathcal{O})| = |Ell_{\mathcal{O}}(\mathbb{C})|$.*

Let $\mathfrak{a}$ and $\mathfrak{b}$ invertible $\mathcal{O}$-ideals. Then we have an inclusion $\mathfrak{b} \subset \mathfrak{a}^{-1}\mathfrak{b}$ and an induced isogeny $\phi_{\mathfrak{a}} : E_{\mathfrak{b}} \longrightarrow E_{\mathfrak{a}^{-1}\mathfrak{b}} = [\mathfrak{a}] * E_{\mathfrak{b}}$.

Definition 4.18. *Let E be an elliptic curve over $\mathbb{C}$ satisfying $End(E) \simeq \mathcal{O}$ where $\mathcal{O}$ is an order in an imaginary quadratic field K. Take an arbitrary invertible $\mathcal{O}$-ideal $\mathfrak{a}$. We define*

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

It is called the group of $\mathfrak{a}$-torsion points of E.

Proposition 4.19. *[7, Theorem 18.11.] Let E be an elliptic curve over $\mathbb{C}$ with $End(E) \simeq \mathcal{O}$ where $\mathcal{O}$ is an order in an imaginary quadratic field K. For any arbitrary invertible $\mathcal{O}$-ideal $\mathfrak{a}$, we have a natural isogeny $\phi_{\mathfrak{a}} : E \longrightarrow [\mathfrak{a}] * E$ with the action $*$ of $Cl(\mathcal{O})$ on $Ell_{\mathcal{O}}(\mathbb{C})$. Then the followings hold :*

(i) $E[\mathfrak{a}]$ *is the kernel of the natural isogeny* $E \longrightarrow [\mathfrak{a}] * E$.

(ii) The natural isogeny $E \longrightarrow [\mathfrak{a}] * E$ *has degree* $N\mathfrak{a}$.

Proof. (i) Let $\mathfrak{b}$ be a proper fractional $\mathcal{O}$-ideal corresponding to E, i.e. $E = E_{\mathfrak{b}}$. There is an isomorphism $\mathbb{C}/\mathfrak{b} \longrightarrow E_{\mathfrak{b}}$. Then

$$\begin{aligned} E[\mathfrak{a}] &= \{z \in \mathbb{C}/\mathfrak{b} : [\alpha]z = O \text{ for all } \alpha \in \mathfrak{a}\} \\ &= \{z \in \mathbb{C} : \alpha z \in \mathfrak{b} \text{ for all } \alpha \in \mathfrak{a}\}/\mathfrak{b} \\ &= \{z \in \mathbb{C} : z\mathfrak{a} \subseteq \mathfrak{b}\}/\mathfrak{b} \\ &= \mathfrak{a}^{-1}\mathfrak{b}/\mathfrak{b} \quad \text{since } z\mathcal{O} \subseteq \mathfrak{a}^{-1}\mathfrak{b} \\ &= ker(\mathbb{C}/\mathfrak{b} \xrightarrow{z \longmapsto z} \mathbb{C}/\mathfrak{a}^{-1}\mathfrak{b}) \\ &= ker(E \longrightarrow [\mathfrak{a}] * E). \end{aligned}$$

(ii) First, observe that $deg(\phi_{\mathfrak{a}}) = |E[\mathfrak{a}]|$. We want to show that $[\mathfrak{a}^{-1}\mathfrak{b} : \mathfrak{b}] = [\mathfrak{b} : \mathfrak{a}\mathfrak{b}]$. Take any $x + \mathfrak{b}$ in $\mathfrak{a}^{-1}\mathfrak{b}/\mathfrak{b}$ where $x \in \mathfrak{a}^{-1}\mathfrak{b}$ and $x \notin \mathfrak{b}$. Then we have $x\mathfrak{a} \subset \mathfrak{b}$. For any $a \in \mathfrak{a}$, we have $ax \in \mathfrak{b}$. Since $x \notin \mathfrak{b}$, we also have $ax \notin \mathfrak{a}\mathfrak{b}$. So we get a nonzero element $ax + \mathfrak{a}\mathfrak{b} \in \mathfrak{b} + \mathfrak{a}\mathfrak{b}$.

Similarly, now take an arbitrary element $x + \mathfrak{a}\mathfrak{b}$ in $\mathfrak{b}/\mathfrak{a}\mathfrak{b}$ where $x \in \mathfrak{b}$ and $x \notin \mathfrak{a}\mathfrak{b}$. Then we have $x\mathfrak{a}^{-1} \subset \mathfrak{a}^{-1}\mathfrak{b}$. For any $a \in \mathfrak{a}^{-1}$, we have $ax \in \mathfrak{a}^{-1}\mathfrak{b}$. Since $x \notin \mathfrak{a}\mathfrak{b}$, we also have $ax \notin \mathfrak{b}$. So we get a nonzero element $ax + \mathfrak{b} \in \mathfrak{a}^{-1}\mathfrak{b}/\mathfrak{b}$. So

$$|E[\mathfrak{a}]| = |\mathfrak{a}^{-1}\mathfrak{b}/\mathfrak{b}| = [\mathfrak{a}^{-1}\mathfrak{b} : \mathfrak{b}] = [\mathfrak{b} : \mathfrak{a}\mathfrak{b}] = [\mathcal{O} : \mathfrak{a}\mathcal{O}] = N\mathfrak{a}. \tag{4.22}$$

□

4.2. Ordinary Elliptic Curves over Finite Fields

Let k be the finite field with q elements. Let E be an elliptic curve with CM by an order $\mathcal{O}$ in an imaginary quadratic field K. Denote q^{th}-Frobenius map as π_E [3].

Let $P = (X, Y) \in E(\mathbb{F}_q)$ with $\pi_E(P) = (X^q, Y^q) = (X, Y) = P$. So we have $\pi_E(P) - P = \mathcal{O}$. It gives $(\pi_E - id)(P) = O$. Conversely take an arbitrary element P in $ker[\pi_E - id]$. Then we have $\pi_E(P) - P = O$. So $P \in E(\mathbb{F}_q)$. Thus

$$\begin{aligned} |E(\mathbb{F}_q)| &= |ker(\pi_E - id)| \\ &= deg(\pi_E - id) && \text{since } (\pi_E - id) \text{ is separable} \\ &= (\widehat{\pi_E - id})(\pi_E - id) \\ &= \hat{\pi}_E\pi_E - (\hat{\pi}_E + \pi_E) + 1 \end{aligned}$$

where $\hat{\pi}_E\pi_E = N(\pi_E) = q$ and $(\hat{\pi}_E + \pi_E) = t := Tr(\pi_E)$.

Then π_E satisfies the characteristic polynomial $\pi_E^2 - t\pi_E + q = 0$. Since $End(E)$ is isomorphic to $\mathcal{O}$, there is an algebraic integer with trace t and norm q which corresponds to π_E. So

$$4q = t^2 - v^2 D_K \quad \text{where } v = [\mathcal{O}_K : \mathbb{Z}[\pi_E]] \quad \text{and} \quad disc(\mathcal{O}_K) = D_K. \tag{4.23}$$

5. THE HILBERT CLASS FIELD

Our aim is to show that every elliptic curve with CM can be defined over an algebraic extension of $\mathbb{Q}$ [5]. Let $\mathcal{O}$ be an order in an imaginary quadratic field K with discriminant D. We will define the Hilbert Class Polynomial $H_D(X)$ and the splitting field L of $H_D(X)$ over K. Then we will observe that both $Cl(\mathcal{O})$ and $Gal(L/K)$ act on the roots of $H_D(X)$. Moreover, there is an injective group homomorphism between $Gal(L/K)$ and $Cl(\mathcal{O})$ [8].

Proposition 5.1. *[5, Proposition 2.1.]*

(i) Let E be an elliptic curve over $\mathbb{C}$. Let and $\sigma : \mathbb{C} \longrightarrow \mathbb{C}$ be any field automorphism of $\mathbb{C}$. Then

$$End(E) \simeq End(E^\sigma). \tag{5.1}$$

(ii) Let E be an elliptic curve over $\mathbb{C}$ with CM by an order $\mathcal{O}$ in an imaginary quadratic field K. Then $j(E) \in \overline{\mathbb{Q}}$.

(iii)

$$Ell_{\mathcal{O}}(\mathbb{C}) \simeq Ell_{\mathcal{O}}(\overline{\mathbb{Q}}). \tag{5.2}$$

Proof. (i) Let $\phi : E \longrightarrow E$ be an endomorphism and $\sigma \in Aut(\mathbb{C})$. Then σ acts on the Weierstrass coefficients of elliptic curves such that $E^\sigma : y^2 = x^3 + \sigma(A) + \sigma(B)$. Taking arbitrary ϕ, $\psi \in End(E)$, we have $\phi^\sigma : E^\sigma \longrightarrow E^\sigma$ with the following properties $(\phi + \psi)^\sigma = \phi^\sigma + \psi^\sigma$ and $(\phi \circ \psi)^\sigma = \phi^\sigma \circ \psi^\sigma$. Thus we have an induced map $\sigma : End(E) \longrightarrow End(E^\sigma)$ which is a ring homomorphism. Hence, σ has an inverse $\sigma^{-1} : End(E^\sigma) \longrightarrow End(E)$ implying that $End(E) \simeq End(E^\sigma)$.

(ii) By part (i), we can say that E^σ has also CM by $\mathcal{O}$. We have $j(E) = j(E^\sigma) = j(E)^\sigma$. The first equality holds by Proposition 2.17 and the second equality holds since the j-invariant is a rational combination of coefficients of a Weierstrass

equation. Since $j(E^\sigma) \in Ell_{\mathcal{O}}(\mathbb{C})$ and there are finitely many $j(E) \in Ell_{\mathcal{O}}(\mathbb{C})$, every $\sigma \in Aut(\mathbb{C})$ permutes elements of the isomorphism class of an elliptic curve. Therefore $[\mathbb{Q}(j(E)) : \mathbb{Q}] \leq h(\mathcal{O}) < \infty$. Hence, $j(E)$ is an algebraic number.

(iii) We have $\overline{\mathbb{Q}} \subset \mathbb{C}$. We want to show that there is a bijection between $Ell_{\mathcal{O}}(\overline{\mathbb{Q}})$ and $Ell_{\mathcal{O}}(\mathbb{C})$. Define a natural inclusion map as

$$\gamma : Ell_{\mathcal{O}}(\overline{\mathbb{Q}}) \longrightarrow Ell_{\mathcal{O}}(\mathbb{C}). \tag{5.3}$$

Let E_1 and E_2 be representatives of two isomorphism classes in $Ell_{\mathcal{O}}(\overline{\mathbb{Q}})$ such that $\gamma(E_1) = \gamma(E_2)$. This equality gives us $j(E_1) = j(E_2)$. By Proposition 2.17 , we get $E_1 \simeq E_2$ over $\overline{\mathbb{Q}}$. So the map is injective.

Take an arbitrary element $E \in Ell_{\mathcal{O}}(\mathbb{C})$. By part (ii), j-invariant of E is in $\overline{\mathbb{Q}}$. By Proposition 2.17 part (ii), there exists an elliptic curve E' defined over $\mathbb{Q}(j(E))$ such that $j(E') = j(E)$. By Proposition 2.17 part(i), $E \simeq E'$ over $\mathbb{C}$. So $\gamma(E') = E$, the map is surjective. Therefore the map is bijective.

□

Fact 5.2. *[8] Let $\mathcal{O}$ be an order with discriminant D in an imaginary quadratic field K. The elements of $Ell_{\mathcal{O}}(\mathbb{C})$ are algebraic integers. The all elements have the same minimal polynomial over K such that*

$$H_D(X) = \prod_{j(E) \in Ell_{\mathcal{O}}(\mathbb{C})} (X - j(E)) \in \mathbb{Z}[X]. \tag{5.4}$$

It is known as the Hilbert class polynomial of discriminant D. This implies that every elliptic curve E over $\mathbb{C}$ with CM by $\mathcal{O}$ is defined over a number field $K(j(E))$ where $j(E)$ is an algebraic integer.

Theorem 5.3. *[8, Theorem 21.3. page 2] For all j_1, $j_2 \in \mathbb{C}$, we have the modular polynomial $\Phi_N(j_1, j_2) = 0$ if and only if j_1 and j_2 are the j-invariants of elliptic curves over $\mathbb{C}$ that are related by a cyclic isogeny of degree N.*

Let $\mathcal{O}$ be an order in an imaginary quadratic field K with discriminant D and E_1 be an elliptic curve with CM by $\mathcal{O}$. Then $Gal(\overline{K}/\ K)$ acts on $Ell_{\mathcal{O}}(\overline{\mathbb{Q}})$ via the action described in Proposition 5.1. Take an arbitrary $\sigma \in Gal(\overline{K}/K)$. Then we already showed that E_1^{σ} has CM by $\mathcal{O}$. There exists a proper fractional $\mathcal{O}$- ideal $\mathfrak{a}$ satisfying $E_1^{\sigma} = [\mathfrak{a}] * E_1$ since the action is transitive by Theorem 4.16. From Section 4.1, we know that there is a $Cl(\mathcal{O})$-action on $Ell_{\mathcal{O}}(\overline{\mathbb{Q}})$. For some proper fractional $\mathcal{O}$-ideal $\mathfrak{b}$, we have $E_2 = [\mathfrak{b}] * E_1$ which is an elliptic curve with CM by $\mathcal{O}$. Observe that

$$\begin{aligned}
E_2^{\sigma} &= ([\mathfrak{b}] * E_1)^{\sigma} \\
&= [\mathfrak{b}^{\sigma}] * E_1^{\sigma} && \text{II.2.5. in [5]} \\
&= [\mathfrak{b}] * E_1^{\sigma} && \text{since } \mathfrak{b} \subset K \\
&= [\mathfrak{b}] * ([\mathfrak{a}] * E_1) \\
&= [\mathfrak{a}] * ([\mathfrak{b}] * E_1) \\
&= [\mathfrak{a}] * E_2.
\end{aligned}$$

Then there is a group homomorphism

$$\begin{array}{ccc} Gal(L/K) & \longrightarrow & Cl(\mathcal{O}) \\ \sigma & \longmapsto & [\mathfrak{a}] \end{array}$$

where $E^{\sigma} = [\mathfrak{a}] * E$ and L is the splitting field of $H_D(X)$. The identity automorphism in $Gal(L/K)$ is the only automorphism acting on $Ell_{\mathcal{O}}(\overline{\mathbb{Q}})$ trivially. Moreover, we know that $Cl(\mathcal{O})$-action on $Ell_{\mathcal{O}}(\overline{\mathbb{Q}})$ is a free action by Theorem 4.16. So we have an injective group homomorphism.

6. ALGEBRAIC NUMBER THEORY

In the previous chapter, we showed that there is an injective group homomorphism between $Gal(L/K)$ and $Cl(\mathcal{O})$ where $\mathcal{O}$ is an order in an imaginary quadratic field K and L is the splitting field of $H_D(X)$. The purpose of this chapter is to show that the homomorphism is also surjective. First, we need to define some notions from the algebraic number theory. Most of them can be found in [8–11, 15].

A number ring is a subring of a number field. Number rings are not always unique factorization domains. Number rings have three special properties which will be stated in the Definition 6.1, and that any integral domain with these properties also has the unique factorization of ideals.

Definition 6.1. *A Dedekind domain is an integral domain R such that*

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

Theorem 6.2. *[9, Theorem 14.] Every number ring is a Dedekind domain.*

Let K be an imaginary quadratic number field and L a finite extension of K. Moreover, let $\mathcal{O}_K$ and $\mathcal{O}_L$ be the ring of integers of K and L, respectively.

Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$. Since $\mathcal{O}_L$ is a Dedekind domain, the ideal in $\mathfrak{p}\mathcal{O}_L$ factorizes uniquely. Then the factorization of a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ in $\mathcal{O}_L$ is given by

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1^{e_1}\mathfrak{q}_2^{e_2}\dots\mathfrak{q}_r^{e_r} \tag{6.1}$$

in which $\mathfrak{q}_i$'s are distinct primes of $\mathcal{O}_L$ containing $\mathfrak{p}$. The integer e_i is the ramification index of $\mathfrak{q}_i$ over $\mathfrak{p}$. We have also a residue field extension $\mathcal{O}_L/\mathfrak{q}_i$ of $\mathcal{O}_K/\mathfrak{p}$ and the inertia

degree of $\mathfrak{q}_i$ over $\mathfrak{p}$ is $f_i = [\mathcal{O}_L/\mathfrak{q}_i : \mathcal{O}_K/\mathfrak{p}]$, see [6, page 100].

Fact 6.3. *When L is a Galois extension of K with Galois group $Gal(L/K)$, then the ramification index of $\mathfrak{q}_i$ over $\mathfrak{p}$ are all equal to e for all i and the inertia degree of $\mathfrak{q}_i$ over $\mathfrak{p}$ are all equal to f for all i. In this case, we say the ramification index of $\mathfrak{p}$ is e. Similarly the inertia degree of $\mathfrak{p}$ is f. Moreover, $Gal(L/K)$ acts on the primes lying over $\mathfrak{p}$ transitively. If there are r-many primes lying over $\mathfrak{p}$, then $[L : K] = n = efr$. [10, Theorem 3.34]*

Definition 6.4. *Let L be a Galois extension of K. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ and $\mathfrak{q}$ be a prime ideal of $\mathcal{O}_L$ containing $\mathfrak{p}$.*

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

$$\begin{aligned} D_{\mathfrak{q}} &= \{\sigma \in Gal(L/K) : \sigma(\mathfrak{q}) = \mathfrak{q}\} \\ &= \{\sigma \in Gal(L/K) : \sigma(\alpha) \equiv 0 (mod\ \mathfrak{q}) \leftrightarrow \alpha \equiv 0 (mod\ \mathfrak{q}) \forall \alpha \in \mathcal{O}_L\} \end{aligned}$$

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

$$I_{\mathfrak{q}} = \{\sigma \in Gal(L/K) : \sigma(\alpha) \equiv \alpha (mod\ \mathfrak{q}) \text{ for all } \alpha \in \mathcal{O}_L\}.$$

Observe that $\sigma(\alpha) \equiv 0 \pmod{\mathfrak{q}}$ if and only if $\alpha \equiv 0 \pmod{\mathfrak{q}}$. Hence we have $I_{\mathfrak{q}} \leq D_{\mathfrak{q}} \leq Gal(L/K)$. Since $\sigma(\mathfrak{q}) = \mathfrak{q}$ and $\sigma(\mathcal{O}_L) = \mathcal{O}_L$, σ induces $\tilde{\sigma} : \mathcal{O}_L/\mathfrak{q} \longrightarrow \mathcal{O}_L/\mathfrak{q}$ is an automorphism which fixes $\mathcal{O}_K/\mathfrak{p}$. Therefore $\tilde{\sigma} \in Gal(\mathcal{O}_L/\mathfrak{q}\Big/\mathcal{O}_K/\mathfrak{p})$.

Consider the map

$$\begin{aligned} f : D_{\mathfrak{q}} &\longrightarrow Gal(\mathcal{O}_L/\mathfrak{q}\Big/\mathcal{O}_K/\mathfrak{p}) \\ \sigma &\longmapsto \quad \tilde{\sigma}. \end{aligned}$$

The map f is group homomorphism whose kernel is $I_{\mathfrak{q}}$. Any element σ of $I_{\mathfrak{q}}$ satisfies $\sigma(x) - x \in \mathfrak{q}$ for all $x \in \mathcal{O}_L$ [6, page 101-102].

6.1. The Frobenius Automorphism

Let L be a Galois extension of K with Galois group $Gal(L/K)$. Let $\mathfrak{p}$ be an unramified prime in L, i.e. $e = 1$. Then $I_{\mathfrak{q}} = \{1\}$ and we have an isomorphism

$$D_{\mathfrak{q}} \longrightarrow Gal(\mathcal{O}_L/\mathfrak{q}\Big/\mathcal{O}_K/\mathfrak{p}). \tag{6.2}$$

So $Gal(\mathcal{O}_L/\mathfrak{q}\Big/\mathcal{O}_K/\mathfrak{p})$ is generated by the special automorphism $\tilde{\sigma}$ such that

$$\tilde{\sigma}(x) = x^{\|\mathfrak{p}\|} \quad \text{for all } x \in \mathcal{O}_L/\mathfrak{q} \tag{6.3}$$

where $\| \mathfrak{p} \|$ denotes the index $N\mathfrak{p}$. The corresponding automorphism $\sigma_{\mathfrak{q}} \in D_{\mathfrak{q}}$ satisfies

$$\sigma_{\mathfrak{q}}(\alpha) \equiv \alpha^{\|\mathfrak{p}\|} (\text{mod } \mathfrak{q}) \quad \text{for all } \alpha \in \mathcal{O}_L. \tag{6.4}$$

It is called the Frobenius automorphism of $\mathfrak{q}$ over $\mathfrak{p}$. We denote $\sigma_{\mathfrak{q}}$ by $\left[\frac{L/K}{\mathfrak{q}}\right]$ [9].

Remark 6.5. *If $\mathfrak{q}'$ is another prime lying over $\mathfrak{p}$ in $\mathcal{O}_L$, then there exists $\sigma \in Gal(L/K)$ such that $\sigma(\mathfrak{q}) = \mathfrak{q}'$. Let $\tau \in D_{\mathfrak{q}'}$. We have*

$$\sigma(\mathfrak{q}) = \mathfrak{q}' = \tau(\mathfrak{q}') = \tau(\sigma(\mathfrak{q})). \tag{6.5}$$

This implies that $\mathfrak{q} = \sigma^{-1}\tau\sigma(\mathfrak{q})$ and $\sigma^{-1}\tau\sigma \in D_{\mathfrak{q}}$. Thus $\tau \in \sigma D_{\mathfrak{q}}\sigma^{-1}$.

Let $\tau \in \sigma D_{\mathfrak{q}}\sigma^{-1}$, then $\sigma^{-1}\tau\sigma \in D_{\mathfrak{q}}$. It implies that $\sigma^{-1}\tau\sigma(\mathfrak{q}) = \mathfrak{q}$. Then

$$\mathfrak{q}' = \sigma(\mathfrak{q}) = \tau\sigma(\mathfrak{q}) = \tau(\mathfrak{q}'), \tag{6.6}$$

hence $\tau \in D_{\mathfrak{q}'}$ and $\sigma D_{\mathfrak{q}}\sigma^{-1} = D_{\mathfrak{q}'}$.

Similarly, we have $I_{\mathfrak{q}'} = \sigma I_{\mathfrak{q}} \sigma^{-1}$.

Let σ *be the Frobenius automorphism of* $\mathfrak{q}$ *over* $\mathfrak{p}$. *Let* $\sigma_{\mathfrak{q}'}$ *be the Frobenius automorphism of* $\mathfrak{q}'$ *over* $\mathfrak{p}$ *where* $\tau(\mathfrak{q}) = \mathfrak{q}'$ *for some* $\tau \in Gal(L/K)$. *Then*

$$\begin{aligned} \tau\sigma_{\mathfrak{q}}(\alpha) &\equiv \tau(\alpha^{\|\mathfrak{p}\|})(mod\ \tau\mathfrak{q}) \\ &\equiv \tau(\alpha^{\|\mathfrak{p}\|})(mod\ \mathfrak{q}'). \end{aligned}$$

Since every element in $\mathcal{O}_L$ *can be expressed in terms of* $\tau^{-1}(\alpha)$, *we have*

$$\begin{aligned} \tau\sigma_{\mathfrak{q}}\tau^{-1}(\alpha) &\equiv \tau(\tau^{-1}\alpha)^{\|\mathfrak{p}\|})(\ mod\ \mathfrak{q}') \\ \sigma_{\mathfrak{q}'}(\alpha) &\equiv \alpha^{\|\mathfrak{p}\|}(\ mod\ \mathfrak{q}') \quad \text{for all } \alpha \in \mathcal{O}_L. \end{aligned}$$

This shows that Frobenius automorphisms are conjugate to each other in $Gal(L/K)$. *[16, Proposition 8.2.2.]*

Definition 6.6. *When* L *is an unramified abelian extension of* K, *conjugates of the Frobenius automorphisms are all equal to* $\sigma_{\mathfrak{q}}$. *A unique Frobenius automorphism* $\sigma_{\mathfrak{p}}$ *is determined by an unramified prime* $\mathfrak{p}$ *of* K. *The map*

$$\mathfrak{p} \longrightarrow \sigma_{\mathfrak{p}}$$

sends unramified primes $\mathfrak{p}$ *to the* $\sigma_{\mathfrak{p}}$ *where* $\sigma_{\mathfrak{p}}(\alpha) \equiv \alpha^{\|\mathfrak{p}\|}(\ mod\ \mathfrak{q})$ *for all* $\alpha \in \mathcal{O}_L$. *It is called the Artin map.*

We will use the Artin map to prove that $\Psi : Gal(L/K) \longrightarrow Cl(\mathcal{O})$ is surjective, hence an isomorphism [8].

Theorem 6.7. *[11, Theorem 22.1.] Let* $\mathcal{O}$ *be an imaginary quadratic order of discriminant* D *and let* L *be the splitting field of* $H_D(X)$ *over* $K = \mathbb{Q}(\sqrt{D})$. *The map*

$$\Psi : Gal(L/K) \longrightarrow Cl(\mathcal{O})$$

which sends $\sigma \in Gal(L/K)$ to the unique $\alpha \in Cl(\mathcal{O})$ for which $j(E)^\sigma = j([\alpha] * E)$ holds for all $j(E) \in Ell_{\mathcal{O}}(L)$ is a group isomorphism that commutes with the actions of $Gal(L/K)$ and $Cl(\mathcal{O})$ on $Ell_{\mathcal{O}}(L)$.

Theorem 6.8. *[11, Theorem 22.3.] Let $\mathcal{O}$ be an order in an imaginary quadratic field $K = \mathbb{Q}(\sqrt{D})$ with discriminant D and L the splitting field of $H_D(X)$ over K. Let p be a prime not dividing D. The followings statements are equivalent:*

(i) p is the norm of a principal $\mathcal{O}$-ideal,
(ii) $\left(\frac{D}{p}\right) = 1$ and $H_D(X)$ splits completely in $\mathbb{F}_p[X]$,
(iii) p splits completely in L,
(iv) $4p = t^2 - v^2 D$ for some integers t and v with $t \not\equiv 0 (mod\ p)$.

Proof. Let $K = \mathbb{Q}(\sqrt{D})$ and $\mathcal{O}_K = [1, w_K]$ be its ring of integers where $w_K = \frac{D_K + \sqrt{D_K}}{2}$ and $D_K = \Delta(\mathcal{O}_K)$. Let $\mathcal{O} = [1, f w_K]$ be an order in $\mathcal{O}_K$ where $f = [\mathcal{O}_K : \mathcal{O}]$. Then the discriminant of $\mathcal{O}$ is $D = f^2 D_K$.

$\underline{(i) \implies (iv)}$: Assume that p is the norm of a principal $\mathcal{O}$-ideal (λ). Then we have $(\lambda) \subset [1, \lambda]$. Observe that $[1, \lambda]$ is a suborder of $\mathcal{O}$ with the index $v = [\mathcal{O} : [1, \lambda]]$ for some $v \in \mathbb{Z}$. Since $|\mathcal{O}/(\lambda)| > |\mathcal{O}/[1, \lambda]|$ we have $v < p$. By Lemma 3.4 the discriminant of $[1, \lambda]$ equals to $v^2 D$. Then let $t := \lambda + \bar{\lambda}$, we have a minimal polynomial of λ such that $x^2 - tx + p$. The discriminant of the polynomial is $t^2 - 4p = v^2 D$. So we get $4p = t^2 - v^2 D$ for some integers t and v with $t \not\equiv 0(\text{mod p})$.

$\underline{(iv) \implies (i)}$: Let $4p = t^2 - v^2 D$ for some integers t and v with $t \not\equiv 0(\text{mod p})$. Take $a = \frac{t - v f D_K}{2}$ and $b = v$. Then set $\lambda := a + b f w_K = \frac{t + v f \sqrt{D_K}}{2}$. If D is odd, then $t \equiv v(\text{mod } 2)$. If D is even, then $t \equiv f D_K(\text{mod } 2)$. In both cases, we have $\lambda \in \mathcal{O}$. Moreover, it has norm p.

$\underline{(i) \implies (ii)}$: By $(i) \implies (iv)$, we assume that $4p = t^2 - v^2 D$ for some integers t and v with $t \not\equiv 0(\text{mod p})$. Then $4p = t^2 - v^2 D \equiv 0(\text{mod p})$ implies that $D \equiv \square(\text{mod p})$, i.e. $\left(\frac{D}{p}\right) = 1$. If $\mathfrak{p}$ is a principal $\mathcal{O}$-ideal of norm p, then $\mathfrak{p}\mathcal{O}_K$ is unramified in L since

L is a maximal unramified abelian Galois extension of K. Then $[\mathfrak{p}]$ acts trivially on $Ell_{\mathcal{O}}(L)$. By Theorem 6.7 $\sigma_{\mathfrak{p}}$ acts trivially on the roots of $H_D(X)$. Since $N\mathfrak{p} = \mathfrak{p}\bar{\mathfrak{p}} = p$, the roots of $H_D(X)$ is in $\mathcal{O}_K/\mathfrak{p} = \mathbb{F}_p$. Hence, $H_D(X)$ splits completely in $\mathbb{F}_p[X]$.

$\underline{(ii) \implies (iii)}$: Let $\left(\frac{D}{p}\right) = 1$. Then $D \equiv \square(\text{mod p})$ has solution, i.e p splits into distinct primes of norm p in $\mathcal{O}_K$ as $p = \mathfrak{p}\bar{\mathfrak{p}}$. So $\mathcal{O}_K/\mathfrak{p} \simeq \mathbb{F}_p$. Now assume $H_D(X)$ splits completely in $\mathbb{F}_p[X]$. Then $H_D(X)$ splits completely in $\mathcal{O}_K/\mathfrak{p}$. Moreover, the roots of $H_D(X)$ are all fixed by $\sigma_{\mathfrak{p}}$. It implies $[\mathcal{O}_L/\mathfrak{q} : \mathcal{O}_K/\mathfrak{p}] = 1$ since norm of ideals $\mathfrak{q}$ equal to p for every prime $\mathfrak{q}$ lying above $\mathfrak{p}$. So, p splits completely in L.

$\underline{(iii) \implies (i)}$: Let p split completely in L, i.e. $p\mathcal{O}_L = \mathfrak{q}_1\mathfrak{q}_2 \dots \mathfrak{q}_n$ where $\mathfrak{q}_i$ distinct primes of norm p in $\mathcal{O}_L$. Take $\mathfrak{p}$ be any prime in $\mathcal{O}_K$ lying over p, then $\mathfrak{p}\mathcal{O}_L$ divides $p\mathcal{O}_L$. It implies that there exist a prime $\mathfrak{q}$ in $\mathcal{O}_L$ lying over p dividing $\mathfrak{p}\mathcal{O}_L$. So we get $\mathbb{F}_p \subseteq \mathcal{O}_K/\mathfrak{p} \subseteq \mathcal{O}_L/\mathfrak{q}$. Then $\mathbb{F}_p = \mathcal{O}_K/\mathfrak{p}$ and $\mathfrak{p}$ has norm p. Therefore the Frobenius automorphism in $Gal(L/K)$ is trivial, i.e $\sigma_{\mathfrak{p}} = id$. By Theorem 6.7, the corresponding ideal class $[\mathfrak{p} \cap \mathcal{O}] \in Cl(\mathcal{O})$ is a principal $\mathcal{O}$-ideal. [11, Theorem 22.3.] □

Lemma 6.9. *[17, Lemma 23.5.] Let E be an elliptic curve over k with CM by an order $\mathcal{O}$ of discriminant D in an imaginary quadratic field K. Let ℓ be prime different than chark. If ℓ divides $[\mathcal{O}_K : \mathcal{O}]$, then there are no horizontal ℓ-isogenies from E, and otherwise the number of horizontal ℓ-isogenies is $1 + \left(\frac{D}{\ell}\right) \in \{0, 1, 2\}$.*

Proof. Let $\mathcal{O}_K = [1, \tau]$ and $\mathcal{O} = [1, f\tau]$ where f is the conductor of $\mathcal{O}$. Assume $\ell | [\mathcal{O}_K : \mathcal{O}]$. Then there exist $n > 0$ satisfying $f = n\ell$. So $\mathcal{O} = [1, \ell n\tau]$. Consider cyclic sublattices of $\mathcal{O}$ with index ℓ. They are of the form $\mathcal{O}_1 = [1, \ell^2 n\tau]$ and $\mathcal{O}_2 = [\ell, \ell n\tau + k]$ for $0 \leq k \leq \ell$ by Lemma 4.3. Since $\ell n\tau \notin \mathcal{O}_1$, $\mathcal{O}_1$ is not an ideal of $\mathcal{O}$. Suppose that $\mathcal{O}_2$ is an ideal of $\mathcal{O}$. Then $\ell^2 n\tau$ must be in $\mathcal{O}_2$. Hence, $\ell(\ell n\tau + k) - \ell^2 n\tau = \ell k \in \mathcal{O}_2$. So $k, \ell n\tau \in \mathcal{O}_2$. We get $\mathcal{O}_2 = [\ell, \ell n\tau] = \ell[1, n\tau]$, but $n\tau \notin \mathcal{O}$. It gives us that $\mathcal{O}_2$ can not be a proper $\mathcal{O}$-ideal. Therefore there are no horizontal ℓ-isogenies from E.

Suppose $\ell \nmid [\mathcal{O}_K : \mathcal{O}] = f$, i.e. $(\ell, f) = 1$. Take $\mathfrak{a}$ as an $\mathcal{O}_K$-ideal with norm ℓ. Then it gives an $\mathcal{O}$-ideal $\mathfrak{a} \cap \mathcal{O}$ with norm ℓ since f and ℓ are prime to each other.

Moreover, the inverse of $\mathfrak{a}\cap\mathcal{O}$ is $\frac{1}{\ell}(\bar{\mathfrak{a}}\cap\mathcal{O})$ since $(\mathfrak{a}\cap\mathcal{O})\frac{1}{\ell}(\bar{\mathfrak{a}}\cap\mathcal{O}) = \frac{1}{\ell}(\ell\mathcal{O}_K\cap\mathcal{O}) = \mathcal{O}$. The last equality holds because ℓ is prime to $[\mathcal{O}_K : \mathcal{O}]$. So $\mathfrak{a}\cap\mathcal{O}$ is a proper $\mathcal{O}$-ideal. To the contrary, assume that $\mathfrak{a}$ is a proper $\mathcal{O}$-ideal of norm ℓ. So $\mathfrak{a}\mathcal{O}_K + f\mathcal{O}_K = (\mathfrak{a}+f\mathcal{O})\mathcal{O}_K = \mathcal{O}\mathcal{O}_K = \mathcal{O}_K$. Since $|\mathcal{O}/\mathfrak{a}|$ is prime to f, we have the second equality. So $\mathfrak{a}\mathcal{O}_K$ is an $\mathcal{O}_K$-ideal of norm ℓ. Therefore the number of proper $\mathcal{O}$-ideals of norm ℓ is the number of $\mathcal{O}_K$-ideals of norm ℓ, which is $1 + \left(\frac{D}{\ell}\right)$ [17, Lemma 23.5.]. □

Remark 6.10. *Every horizontal ℓ-isogeny corresponds to the CM action of a proper fractional $\mathcal{O}$-ideal $\mathfrak{l}$ of norm ℓ. In the split case, we have $\left(\frac{D}{\ell}\right) = 1$. So $(l) = \mathfrak{l}\bar{\mathfrak{l}}$. Then $\mathfrak{l}$-orbits of $Ell_{\mathcal{O}}(\mathbb{C})$ corresponds to the cosets of $\langle[\mathfrak{l}]\rangle$ in $Cl(\mathcal{O})$. For more details see [17, page 3].*

7. ISOGENY VOLCANO

In this chapter, we will define an isogeny volcano and state Kohel's Theorem. Given definitions and theorems are mostly from [3, 17]

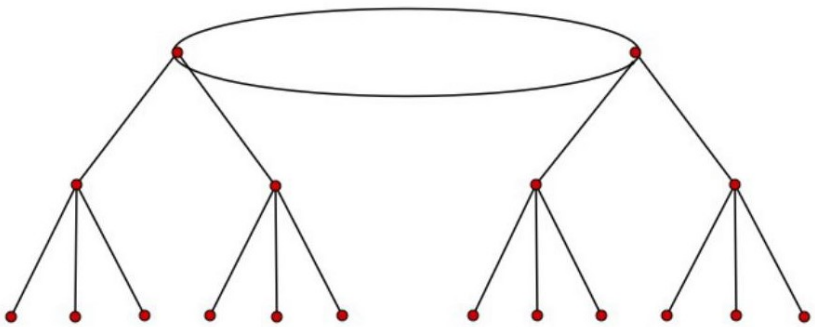

Figure 7.1. A volcano.

Definition 7.1. *An ℓ-volcano V is a connected undirected graph whose vertices are partitioned into one or more levels $V_0, \ldots, V_d$ such that the following hold :*

(i) The subgraph on V_0 (the surface) is a regular graph of degree at most 2.

(ii) For $i > 0$, each vertex in V_i has exactly one neighbor in level V_{i-1}, and this accounts for every edge not on the surface.

(iii) For $i < d$, each vertex in V_i has degree $\ell + 1$.

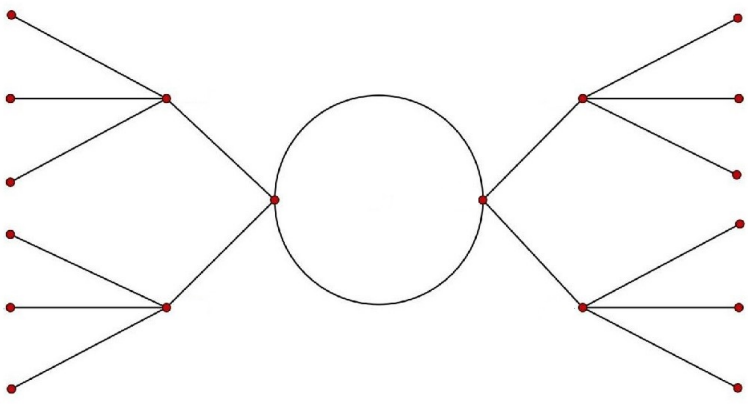

Figure 7.2. A 3-volcano of depth 2 .

An ℓ-volcano allows self-loops, which is an edge whose vertices are the same, and multi-edges, which are two or more edges with the same two vertices. The depth of a volcano is notated as d. As you see in the Figure 7.2, we have a 3-volcano of depth 2. The degree of the subgraph of level surface V_0 is the number of edges of a vertex in V_0. Also depth d equals to 2. For all $i < 2$ each vertex in V_i has degree 4 which is the number of edges of a vertex in V_i.

Definition 7.2. *The ℓ-isogeny graph $G_\ell(k)$ is the graph whose vertices are the isomorphism classes of elliptic curves over k and whose edges are ℓ-isogenies between the curves corresponding to the vertices.*

Observe that when $chark$ is prime p, depending on the p-torsion subgroup $E[p]$, we have either an ordinary or a supersingular elliptic curve. If E is supersingular (ordinary), then any elliptic curve isogenous to E is also supersingular(ordinary) by Theorem 2.39. That is the reason $G_\ell(k)$ involves ordinary and supersingular components. Our aim is to show that ordinary component of $G_\ell(\mathbb{F}_p)$ gives an ℓ-volcano. The vertices of $G_\ell(\mathbb{F}_p)$ are j-invariants an ordinary elliptic curves and its edges are ℓ-isogenies.

Theorem 7.3 (Kohel)**.** *[3, Theorem 7.] Let V be an ordinary component of $G_\ell(\mathbb{F}_q)$ that does not contain 0 and 1728. Then V is an ℓ-volcano for which the following hold:*

(i) The vertices in level V_i all have the same endomorphism ring $\mathcal{O}_i$.
(ii) The subgraph on V_0 has degree $1 + \left(\frac{D_0}{\ell}\right)$, where $D_0 = disc(\mathcal{O}_0)$.
(iii) If $\left(\frac{D_0}{\ell}\right) \geq 0$, then $|V_0|$ is the order of $[\mathfrak{l}]$ in $Cl(\mathcal{O}_0)$; otherwise $|V_0| = 1$.
(iv) The depth of V is $d = \nu_\ell((t^2 - 4q)/D_0)/2$, where $t^2 = (Tr(\pi_E))^2$ for $j(E) \in V$.
(v) $\ell \nmid [\mathcal{O}_K : \mathcal{O}_0]$ and $[\mathcal{O}_i : \mathcal{O}_{i+1}] = \ell$ for $0 \leq i < d$.

Proof. Let V be an ordinary component of $G_\ell(\mathbb{F}_q)$. Every vertex of V determines an ordinary elliptic curve and every edge of V is an ℓ-isogenies. In each level V_i of V, the orders $\mathcal{O}_i$ differ by powers of ℓ by Theorem 3.13, i.e $[\mathcal{O}_i : \mathcal{O}_{i+1}] = \ell$. Assume that ℓ^d is the largest power. Then we have $V_0, V_1, \ldots, V_d$ as a partition of V and in each

V_i we have orders $\mathcal{O}_0, \mathcal{O}_1, \ldots, \mathcal{O}_d$ satisfying $\ell \nmid [\mathcal{O}_K : \mathcal{O}_0]$ and $[\mathcal{O}_j : \mathcal{O}_i] = \ell^{i-j}$ where $d \geq i \geq j \geq 0$ by Lemma 6.9. So part (i) and (iv) are done. By Lemma 6.9 we also have (ii). Consider $Cl(\mathcal{O}_0)$-action on $Ell_{\mathcal{O}_0}(\mathbb{F}_q)$. Let E be an elliptic curve with CM by $\mathcal{O}_0$ and $\left(\frac{D_0}{\ell}\right) \geq 0$.The CM action of $[\mathfrak{l}]$ on $Ell_{\mathcal{O}_0}(\mathbb{F}_q)$ gives $[\mathfrak{l}] * E = E'$. Then E' is an elliptic curve with CM by $\mathcal{O}_0$ and horizontal ℓ-isogenous to E. So the order of $[\mathfrak{l}]$ gives $|V_0|$. When $\left(\frac{D_0}{\ell}\right) = 0$, then $|V_0| = 1$ by Remark 6.10.

By Theorem 6.8, if $4q = t^2 - v^2 D_0$, where π_E is q^{th} Frobenius map for an elliptic curve E with CM by $\mathcal{O}_i$ and $t^2 = (Tr(\pi_E))^2$, then $H_{D_0}(X)$ splits completely in $\mathbb{F}_q[X]$. So $Ell_{\mathcal{O}_i}(\mathbb{F}_q) \neq \emptyset$ but $Ell_{\mathcal{O}_{d+1}}(\mathbb{F}_q) = \emptyset$ since v is related to the index $[\mathcal{O} : \mathcal{O}_i]$ by Lemma 3.4, i.e. $\ell^d \nmid v$. Finally, by Theorem 5.3 the degree of modular polynomial for level ℓ gives us each vertex in V_i has degree $\ell + 1$. Therefore V is an ℓ-volcano [17, Theorem 23.2. page 8]. $\square$

8. EXAMPLE

In this chapter, our aim is to construct a 3-volcano with depth 2 over $\mathbb{F}_{409}$. We start with a field $K = \mathbb{Q}(\sqrt{-5})$. The 3-volcano with depth 2 contains levels V_0, V_1, and V_2. Each vertex in each level of the volcano has same endomorphism ring which is isomorphic to an order in an imaginary quadratic field. We will construct that the surface V_0 contains vertices which are elliptic curves with endomorphism ring isomorphic to the ring of integers $\mathcal{O}_K$ of K. Then we want to find a prime p which splits in the ring of integers $\mathcal{O}_K$ of K and satisfies the condition in the Kohel's Theorem. After we will determine elliptic curves defined over $\mathbb{F}_p$ in each levels V_0, V_1, and V_2.

Observe that the maximal order of K is $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ with the discriminant $D_0 = -20$. Then calculate the class number of the maximal order which is the number of elliptic curves with CM by $\mathcal{O}_K$. In our example, there are 2 elliptic curves with CM by $\mathcal{O}_K$.

$H_{D_0}(X)$ represents the Hilbert Class Polynomial for discriminant -20 which is

$$H_{D_0}(X) = x^2 - 1264000x - 681472000. \tag{8.1}$$

We want to find a prime which splits in the splitting field of $H_{D_0}(X)$. Since we want to find a 3-volcano with depth 2, we can choose the prime p as 409. Observe that 409 can be written as

$$4.409 = 4^2 + 3^{(2.2)}.20. \tag{8.2}$$

So by Theorem 6.8, $p = 409$ splits in $\mathcal{O}_K$ and also $H_{D_0}(X)$ splits completely in $\mathbb{F}_{409}$. Then the roots of H_{D_0} mod 409 gives us the j-invariants of the elliptic curves with CM

by $\mathcal{O}_K$. The j-invariants and corresponding elliptic curves are :

$$j_1 = 209 \qquad E_1 : y^2 + xy = x^3 + 27x + 40$$
$$j_2 = 390 \qquad E_2 : y^2 + xy = x^3 + 100x + 90.$$

Note that E_1 and E_2 are both ordinary elliptic curves and 3-isogenous over $\mathbb{F}_{409}$.

Here are Magma codes that gives us the computation.

```
K:= QuadraticField(−5);
O:=MaximalOrder(K);
ClassNumber(O);
h < x >:=HilbertClassPolynomial(−20);
IsSplit(409, O);
S < x >:=PolynomialRing(GF(409));
h := S!h;
Roots(h);
Factorization(h);
E1:=EllipticCurveFromjInvariant(GF(409)!209);
E2:=EllipticCurveFromjInvariant(GF(409)!390);
IsOrdinary(E1);
IsOrdinary(E2);
```

Figure 8.1. Algorithm for detecting 3-isogenous elliptic curves defined over $\mathbb{F}_{409}$ with the endomorphism ring $\mathbb{Z}[\sqrt{-5}]$.

After that our aim is to show that roots of modular polynomial for level 3 over $\mathbb{F}_{409}$ gives us j-invariants of 3-isogenous elliptic curves over $\overline{\mathbb{F}}_{409}$ by Theorem 5.3. We already found E_1 and E_2 which are on the surface since they have the same endomorphism ring $\mathcal{O}_K$. Let's see how we can decide elliptic curves in level V_1 and V_2. Elliptic curves in level V_1 and V_2 have the same endomorphism rings isomorphic to $\mathcal{O}_1$ and $\mathcal{O}_2$, respectively. The index $[\mathcal{O}_K : \mathcal{O}_i]$ is 3^i for each $i = 1, 2$.

Here is the calculation using Magma :

```
f < x, y >:=ClassicalModularPolynomial(3);
R < x, y >:=PolynomialRing(GF(409), 2);
f := R!f;
for i in GF(409) do
for j in GF(409) do
r:=Evaluate (f, [i, j]);
if r eq 0 then print i,j;
end if;
end for;
end for;
```

Figure 8.2. Algorithm for detecting j-invariants of 3-isogenous elliptic curves defined over $\mathbb{F}_{409}$.

Observe that E_1 with $j = 209$ is 3-isogenous to elliptic curves with j-invariants 125, 196, 390. Moreover, E_2 with $j = 390$ is 3-isogenous to elliptic curves with j-invariants 209, 315, 326. So we can deduce that elliptic curves E_3, E_4, E_5 and E_6 with $j = 125$, 196, 315 and 326 have same endomorphism ring which is isomorphic to an order $\mathcal{O}_1$ satisfying $[\mathcal{O}_K : \mathcal{O}_1] = 3$. Similarly there are elliptic curves E_7, E_8, E_9 with j-invariants are 22, 222 and 388 which are 3-isogenous to E_3. Moreover, we can find 9 more j-invariants of an elliptic curves, each three of them, respectively, 3-isogenous to E_4, E_5 and E_6. Also all E_i for $7 \leq i \leq 18$ have same endomorphism ring that is isomorphic to $\mathcal{O}_2$ satisfying $[\mathcal{O}_K : \mathcal{O}_2] = 9$. Therefore it gives us a 3-volcano of depth 2 over $\mathbb{F}_{409}$.

Our example can be visualized by the figure below. It is originated from the Figure 7.2. The numbers of each vertices represent the j-invariants of elliptic curves E_i for $1 \leq i \leq 18$.

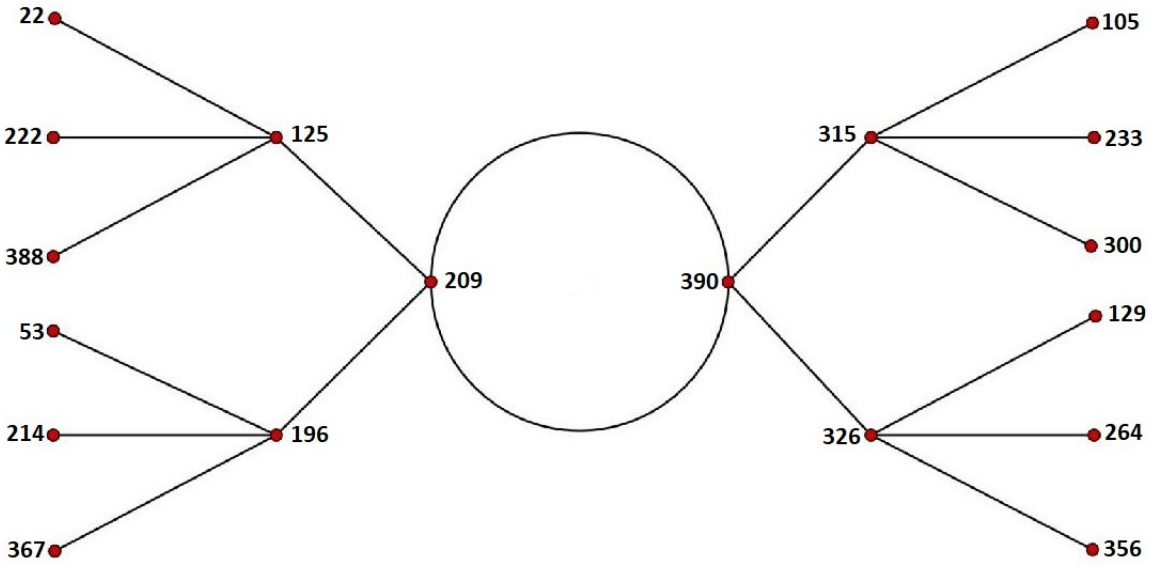

Figure 8.3. A 3-volcano of depth 2 over $\mathbb{F}_{409}$.

9. CONCLUSION

Volcanoes are graph-theoretic terms. Isogeny volcanoes are the ordinary components of ℓ-isogeny graphs of elliptic curves. In this thesis, we firstly gave some basic notions about elliptic curves and orders in an imaginary quadratic field, then we showed that there is a one-to-one correspondence between the ideal class group and the isomorphism classes of elliptic curves with CM by an order in an imaginary quadratic field. In a further step, we showed that every elliptic curve with CM by an order in an imaginary quadratic field is defined over an algebraic extension of $\mathbb{Q}$. Afterwards, we defined the Hilbert class polynomial of discriminant D as $H_D(X)$ which is the minimal polynomial of the j-invariants of the elliptic curves with CM by an order in an imaginary quadratic field with discriminant D. By Theorem 6.8, we saw that if $k = \mathbb{F}_p$ with $4p = t^2 - v^2D$ and $t \not\equiv 0(\mathrm{mod}p)$ then $H_D(X)$ splits into distinct linear factors in $\mathbb{F}_p[X]$ and its roots are the reductions of j-invariants of elliptic curves defined over the splitting field of $H_D(X)$. Lastly, we stated the main Theorem 7.3, which is that, except for the components of 0 or 1728, the ordinary components of ℓ-isogeny graphs of elliptic curves over finite fields are ℓ-volcanoes. Also, we gave an explicit example of 3-volcano of depth 2 over $\mathbb{F}_{409}$.

REFERENCES

1. Kohel, D., *Endomorphism rings of elliptic curves over finite fields*, Ph.D. Thesis, Univeristy of California at Berkeley, 1996.

2. Fouquet, M. and F. Morain, "Isogeny Volcanoes and the SEA algorithm, Algorithmic Number Theory and Sympo", *ANTS 2002: Algorithmic Number Theory Symposium- ANTS V*, pp. 276–291, 2002.

3. Shutherland, A. V., "Isogeny Volcanoes", *ANTS X: Proceedings of the Tenth Algorithmic Number Theory Symposium, 2012, 507-530*, 2013.

4. Silverman, J. H., *The Arithmetic of Elliptic Curves*, Vol. 2, Springer, 2009.

5. Silverman, J. H., *Advances Topics in the Arithmetic of Elliptic Curves*, Springer, 1994.

6. Cox, D. A., *Primes of the Form x^2+ny^2 : Fermat, Class Field Theory and Complex Multiplication*, John Wiley & Sons, Inc, 1989.

7. Shutherland, A. V., *The CM action*, 2015, `https://ocw.mit.edu/courses/mathematics/18-783-elliptic-curves-spring-2015/lecture-notes/MIT18_783S15_lec18.pdf`, accessed at July 2017.

8. Shutherland, A. V., *The Hilbert class polynomial*, 2015, `https://ocw.mit.edu/courses/mathematics/18-783-elliptic-curves-spring-2015/lecture-notes/MIT18_783S15_lec21.pdf`, accessed at July 2017.

9. Marcus, D. A., *Number Fields*, Springer, 1977.

10. Milne, J. S., *Algebraic Number (v3.07)*, 2017, `http://www.jmilne.org/math/CourseNotes/ANT.pdf`, accessed at July 2017.

11. Shutherland, A. V., *Ring class fields and the CM method*, 2015, https://ocw.mit.edu/courses/mathematics/18-783-elliptic-curves-spring-2015/lecture-notes/MIT18_783S15_lec22.pdf, accessed at July 2017.

12. Hartshorne, R., *Algebraic Geometry*, Springer, 1977.

13. Shutherland, A. V., *Ordinary and supersingular elliptic curves*, 2015, https://ocw.mit.edu/courses/mathematics/18-783-elliptic-curves-spring-2015/lecture-notes/MIT18_783S15_lec14.pdf, accessed at July 2017.

14. Jacobson, M. J. and J. H. C. Williams, *Solving the Pell Equation*, Springer, 2009.

15. Neukirch, J., *Algebraic Number Theory*, Springer, 1999.

16. Ash, R. B., *Factoring of Prime Ideal in Galois Extensions*, http://www.math.uiuc.edu/∼r-ash/Ant/AntChapter8.pdf, accessed at July 2017.

17. Shutherland, A. V., *Isogeny volcanoes*, 2015, https://ocw.mit.edu/courses/mathematics/18-783-elliptic-curves-spring-2015/lecture-notes/MIT18_783S15_lec23.pdf, accessed at July 2017.