ELLIPTIC CURVES AND USE OF THEIR ENDOMORPHISM RINGS IN CRYPTOGRAPHY

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF APPLIED MATHEMATICS
OF
MIDDLE EAST TECHNICAL UNIVERSITY

BY

ALİ MERT SÜLÇE

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF MASTER OF SCIENCE
IN
CRYPTOGRAPHY

SEPTEMBER 2019

Approval of the thesis:

ELLIPTIC CURVES AND USE OF THEIR ENDOMORPHISM RINGS IN CRYPTOGRAPHY

submitted by **ALİ MERT SÜLÇE** in partial fulfillment of the requirements for the degree of **Master of Science in Cryptography Department, Middle East Technical University** by,

Prof. Dr. Ömür Uğur
Director, Graduate School of **Applied Mathematics** ______________

Prof. Dr. Ferruh Özbudak
Head of Department, **Cryptography** ______________

Prof. Dr. Ersan Akyıldız
Supervisor, **Cryptography, METU** ______________

Examining Committee Members:

Assoc. Prof. Dr. Murat Cenk
Institute of Applied Mathematics, METU ______________

Prof. Dr. Ersan Akyıldız
Institute of Applied Mathematics, METU ______________

Assoc. Prof. Dr. Oğuz Yayla
Department of Mathematics, Hacettepe University ______________

Date: ______________

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name: ALİ MERT SÜLÇE

Signature :

ABSTRACT

ELLIPTIC CURVES AND USE OF THEIR ENDOMORPHISM RINGS IN CRYPTOGRAPHY

Sülçe, Ali Mert
M.S., Department of Cryptography
Supervisor : Prof. Dr. Ersan Akyıldız

September 2019, 68 pages

Although elliptic curves have been studied for hundreds of years, the inception of elliptic curve cryptography is 1985 by Koblitz's and Miller's independent proposals that is based on the discrete logarithm problem on an elliptic curve defined over a finite field. After that date, there are a lot of advances and studies in elliptic curve cryptography(ECC) which provide high security with relatively small block sizes and high speed compared to the other public key cryptosystems. For instance, 160-bit elliptic curve key provides the same level of security as a 1024-bit RSA key. Meantime, quantum computers, which provide efficient and very fast parallel computation, are developed. In the near feature, widely used public key cryptosystems, including ECC, are vulnerable to quantum algorithms which means not only ECC but also almost all public key cryptosystems will be dead or seriously wounded in the near future. Therefore, efficient public key systems should be designed for post-quantum world. In this world, elliptic curves with some properties do not lose their popularity. In this work, we shall study the mathematical backgrounds of elliptic curves and isogenies on elliptic curves which are the essential concept in post-quantum cryptography(PQC).

Keywords: Elliptic curves, isogeny, endomorphism, endomorphism rings of elliptic curves

ÖZ

ELİPTİK EĞRİLER VE ONLARIN ENDOMORFİZMA HALKALARININ KRİPTOGRAFİDE KULLANIMI

Sülçe, Ali Mert
Yüksek Lisans, Kriptografi Bölümü
Tez Yöneticisi : Prof. Dr. Ersan Akyıldız

Eylül 2019, 68 sayfa

Eliptik eğriler yüzlerce yıldır çalışılıyor olmasına rağmen eliptik eğri şifrelemesinin(ECC) doğuşu Koblitz'in ve Miller'ın sonlu cisimler üzerinde tanımladıkları eliptik eğrilerde ayrık probleme dayanan çalışmasıyla 1985 de gerçekleşmiştir. Bu tarihten sonra, diğer açık anahtarlı kripto sistemlere göre daha güvenilir bir sistemi daha hızlı ve daha küçük boyutlu anahtarlarla bize sunan ECC ile ilgili birçok çalışma ve ilerleme yaşanmıştır. Örneğin, 160-bit eliptik eğri anahtarıyla sağlanan güvenlik ancak 1024-bit RSA anahtarıyla sağlanabilmektedir. Bu süre zarfında, daha etkili ve çok daha hızlı hesaplamalar yapabilen kuantum bilgisayarları geliştirilmiştir. Eliptik eğri kriptosistemleri dahil yaygın olarak kullanılan açık anahtarlı kriptosistemler kuantum bilgisayarlar ile savunmasız hale gelmişlerdir ve bu da açık anahtarlı kriptosistemlerin yakın gelecekte kırılmasına ya da ciddi bir şekilde zarar görmesi anlamına gelmektedir. Bu nedenle kuantum sonrası dünya için kuantum algoritmalarına dayanıklı açık anahtarlı sistemler tasarlanmalıdır. Bu dünyada bazı özellikleri ile birlikte eliptik eğriler popülerliğini kaybetmezler. Bu çalışmada, biz eliptik eğrilerin matematiksel temellerini ve PQC için temel kavram olan eliptik eğrilerdeki izojenileri çalışacağız.

Anahtar Kelimeler: Eliptik eğriler, izojeni, endomorfizma, eliptik eğrilerin endomorfizma halkaları

To my family...

ACKNOWLEDGMENTS

First and foremost, I owe my gratitude to my supervisor Prof. Dr. Ersan Akyıldız for his guidance and stimulating suggestions.

Also, I would like to thank my committee members, Assoc. Prof. Dr. Murat Cenk and Assoc. Prof. Dr. Oğuz Yayla for their brilliant comments and advices. I also would like to express my gratitude to all people at Department of Mathematics and Institute of Applied Mathematics at METU. Assoc. Prof. Dr. Ali Doğanaksoy and Dr. Muhiddin Uğuz, who introduce me to cryptography, deserve my special gratitude.

This study would not be possible without the support of my friends and colleagues whose comments are very valuable for this thesis.

I deliver my utmost thanks and appreciation to Çağla. Her love and continuous support are fundamental source of motivation for me.

Last but not least, my deepest heartfelt gratitude and respect belongs to my dear mother and father for their endless love, encouragement and help not only during the time spent on this thesis but also throughout all my life. I thank to my sister for always being with me and making my life more enjoyable.

TABLE OF CONTENTS

LIST OF TABLES

TABLES

LIST OF FIGURES

FIGURES

CHAPTER 1

INTRODUCTION

Cryptography, which began around 2000 B.C. in Egypt where hieroglyphics were used, is one of the oldest fields of technical study which goes back at least 4000 years. The only purpose of the primary cryptography, derived from ancient Greek kryptos meaning hidden and graphein which means writing, is the study of message secrecy. However, in modern world, cryptography that is considered a branch of mathematics and computer science is used in many areas from the top secret government communication to get a cash from an ATM.

The information that one part(say A) wants to send the other part(say B) is called plaintext. A who has the plaintext encrypts it by using the key and gets the resulting ciphertext. Over the channel such as internet, A sends the ciphertext to B. The channel is always assumed as insecure. Although one can see the ciphertext in the insecure channel, she cannot find out the plaintext. However, B, who has the key, can decrypt the ciphertext and obtain the message from A.

There are four main goals for information security and cryptography. They are confidentiality, authentication, data integrity and non-repudiation. Algorithms, protocols and systems which is used to satisfy these main aims of cryptography is called cryptosystems. However, the security of the cryptosystems should be based on the key, not on the obscurity of the cryptosystems which is known as Kerckhoffs's principle. Today, there are two major types of cryptosystems: the symmetric(private) key and the asymmetric(public) key.

In the symmetric key cryptosystems, the encryption or the decryption keys are known by both A and B. Keys are generally same or they are derived from each other easily. An important advantage of this systems is that they are usually fast, but the difficulty of key exchange between between A and B is a major disadvantage. Symmetric key cryptosystems are divided into two parts: block and stream ciphers.In block ciphers, the message in fixed length strings called block is encrypted at a time such as DES, IDEA, AES. On the other hand, it is operated on a single bit of the message at a time in stream ciphers such as RC4, A5.

In the asymmetric key cryptosystems [7], there are two different keys, namely, private and public key, used for encryption and decryption for each user. It is computationally difficult to obtain one key from another. Also in public key systems, one-way function is used. When we use those functions, we can easily compute the output for a given input, but it is hard to find the inverse of given output. Behind the one-way functions, there are several difficult mathematical problems such as integer factorization problem(IFP) and discrete logarithm problem(DLP). Rivest–Shamir–Adleman(RSA) algorithm, the Digital Signature Algorithm(DSA), Elliptic Curve Digital Signature Algorithm(ECDSA) are well-known and commonly used examples of asymmetric key cryptosystems [11].

Four decades ago asymmetric key cryptosystems made a revolutionary breakthrough in cryptography. However, Peter Shor showed that quantum computers could break asymmetric key cryptosystem based on IFP and DLP [2]. Nowadays, quantum computing and post-quantum cryptosystems are two of the most trending topics of cryptography.

Elliptic curves have been studied as a pure mathematical concepts for hundreds of years. Today, it plays an important role in crytography, especially in asymmetric key cryptosystems and post-quantum cryptosystems [4] and [6]. In this thesis, we give an overview of the properties of elliptic curves. In Chapter 2, we introduce some mathematical backgrounds of elliptic curves such as varieties, morphisms and divisors [17], [15]. Then we study Riemann-Roch's theorem [16] and define the genus 1 curves. In Chapter 3, we study isomorphism on elliptic curves and classificate the elliptic curves according to the characteristics of field where curve is defined over. At the beginning of Chapter 4, we define the group structure on elliptic curves and we get the point addition and point doubling formulas [13] and [14]. Then we concentrate on the isogenies between elliptic curves. Lastly, we research the endomorphism rings of elliptic curves [1]. In Chapter 5, we give the conclusion of the thesis.

CHAPTER 2

PRELIMINARY TO THE ELLIPTIC CURVES

In Chapter 2, we are going to give mathematical basics which are essential to understand elliptic curves. In this respect, some facts about fields, affine and projective varieties, maps between them and divisors have been given. Lastly, we study Riemann-Roch theorem and define the elliptic curves.

2.1 Fields

We define a **field** K as a set with two binary operations $+$ and $\cdot$, called addition and multiplication satisfying

$$\begin{aligned} + : K * K &\to K \\ (a, b) &\to a + b \end{aligned}$$

$$\begin{aligned} \cdot : K * K &\to K \\ (a, b) &\to a \cdot b \end{aligned}$$

- K is an abelian group under addition(with identity element 0_K),
- $K \setminus \{0_K\}$ is abelian group under multiplication,
- The multiplication is distributive on to addition at the right and the left, that is, $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$ where $\forall a, b, c \in K$.

Ex 2.1.1. $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ are infinite fields. $\mathbb{Z} \setminus p\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, ...\overline{p-1}\}$ is finite field with p elements with a prime p.

For a field F, K which is a subset of F is called a **subfield** of F if K is also a field under the binary operations of K. F itself is naturally a subfield of F. A subfield K is named **proper** if $K \subsetneqq F$.

Let F be a field and K be a subfield of F. Then we say that F a **field extension** of K. If $K \subsetneqq F$, the extension is called proper.

A **prime field** P is a field which does not have any proper subfield. For instance, $\mathbb{Q}$ and $\mathbb{Z} \setminus p\mathbb{Z}$ are prime fields.

The smallest positive integer n satisfying $n1_F = 1_F + ... + 1_F = 0_F$ is **characteristic** of F. If there is no positive such n then we say that F has characteristic zero. If there is a positive integer k such that $k1_F = 1_F + ... + 1_F = 0_F$ then we say F has nonzero characteristic.

Ex 2.1.2. char($\mathbb{C}$)=char($\mathbb{Q}$)=char($\mathbb{R}$)=0 and char($\mathbb{Z} \setminus p\mathbb{Z}) = p$ for any prime p.

Let F be a field. The smallest(w.r.t. inclusion) subfield P of F (which is the intersection of all subfield of F) is called the prime field of the field F.

$$P \cong \begin{cases} \mathbb{Q}, & \text{if} \quad \text{char}(F) = 0 \\ \mathbb{Z}/p\mathbb{Z}, & \text{if} \quad \text{char}(F) = p \end{cases}$$

Let F be a field, K be a subfield of F and S be a subset of F. The smallest (in the sense of inclusion) subfield of F containing K and the subset S is denoted by $K(S)$ and called the **extension of K** by adjoining the elements of S. In fact, $K(S)$ is the intersection of all subfields of F containing K and S. If $S = \{\alpha\}$ then we can denote $K(S)$ as $K(\alpha)$. $K(\alpha)$ is called **simple extension** of K and α is a **defining element** for $K(\alpha)$.

Ex 2.1.3. $\mathbb{Q}\sqrt{2} = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ is a simple extension of $\mathbb{Q}$.

The **degree of field extension** F over K is the dimension of F as vector space over K. The degree of F/K is $[F : K] = \dim_K F$. If $[F : K] < \infty$, then F/K is called **finite extension**. Otherwise, F/K is called an **infinite extension**.

Ex 2.1.4. $\mathbb{R}/\mathbb{Q}$ is an infinite extension. $\mathbb{C}/\mathbb{R}$ is a finite extension. In fact, $[\mathbb{C} : \mathbb{R}] = 2$ because $\{1, i\}$ is a basis for $\mathbb{C}$ as a vector space over $\mathbb{R}$. $\mathbb{C} = \{a + ib \mid a, b \in \mathbb{R}\}$.

Let F be a field, K be a subfield of F and $\alpha \in F$. Then α is said to be **algebraic** over K if $a_n\alpha^n + \cdots + a_1\alpha + a_0 = 0$ for some $a_i \in K$ not all zero for $i = 0, \ldots, n$ with $n > 0$ integer. In other words, α is algebraic over K if and only if $\exists f \in K[x]$, $f \neq 0$ and $f(\alpha) = 0_F$. Let F be a field, K be a subfield of F and $\alpha \in F$. Then α is said to be **transcendental** over K if and only if there is no $a_0, a_1, \ldots, a_n \in K$ not all zero such that $a_n\alpha^n + \cdots + a_1\alpha + a_0 = 0_F$.

Ex 2.1.5. $\sqrt{2}$ is algebraic over $\mathbb{Q}$. e, π are transcendental over $\mathbb{Q}$.

Let F be an extension of K. We say F is an **algebraic extension** of K when each element of F is algebraic over K.

Theorem 1. *If L is an algebraic extension of F and F is an algebraic extension of K, then L is an algebraic extension of K.*

Proof. see [9] page 213. □

Let F be a field, $\alpha \in F$ and $K < F$ be a subfield of F. If α is algebraic over K, then there is a unique irreducible monic polynomial $g \in K[x]$ such that $g(\alpha) = 0_F$. The polynomial g is the **minimal polynomial** of α over K. We can define the degree of α over K to be $\deg_K(\alpha) = \deg(g)$.

An irreducible polynomial $g \in K[x]$ is **separable** if it has no multiple roots in any extension of F. Otherwise, it is said to be **inseparable**.

Let $K < F$. An algebraic element $\alpha \in F$ is separable if its minimal polynomial is **separable**. Otherwise, it is **inseparable**.

When every element $\alpha \in F$ is separable over K, an algebraic extension $K < F$ is **separable**. Otherwise, it is **inseparable**.

Let F be an algebraic extension of a field K and let $\sigma : K \to L$ be an embedding of F in L that is an algebraically closed field. The cardinality of the set $\hom_\sigma(E, L)$ is the **separable degree** of F over K and it is denoted by $[F : K]_S$.

Theorem 2. *If $K < F < E$ is algebraic then $[E : K]_S = [E : F]_S.[F : K]_S$.*

Proof. see [12] page76. □

If $(x - \alpha)^n$ is the form of the minimal polynomial of F for some $n \geq 1$, then an element α is **purely inseparable** over F. When every element is purely inseparable over F, an algebraic extension E of F is **purely inseparable**.

If $F < E$ is finite we know $[E : F]_s \mid [E : F]$. Therefore we can write $[E : F] = [E : F]_s.[E : F]_i$ where $[E : F]_i$ is called **inseparable degree** of E over F.

Remark: Let $F < E$ and $[E : F] = [E : F]_s \cdot [E : F]_i$. Then

- If $[E : F]_i = 1$, then $[E : F] = [E : F]_s$ and E is separable over F.
- If $[E : F]_i > 1$, then E is inseparable over F.
- If $[E : F]_s = 1$, then E is purely inseparable over F.

Theorem 3. *Let E be an algebraic extension of F. Let E' be the composition of all subfield K of E such that $F \subset K$ and K is separable over F. Then E' is separable over F and E is purely inseparable over E'. That is $F \subset E'$ separable extension, $E' \subset E$ purely inseparable extension: $F \subset E' \subset E$.*

2.2 Basic Algebraic Geometry

For notation, if we denote a field by K, then $\bar{K}$ is a fixed algebraic closure of K.

2.2.1 Affine Varieties:

Given K and positive integer n, n-dimensional **affine space** over K is the set

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

Also, K-rational points points of $\mathbb{A}^n$ is

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

Let $\bar{K}[X] = \bar{K}[X_1, ..., X_n]$ be a polynomial ring and I be an ideal such that $I \in \bar{K}[X]$. Then we set $V \subset K^n$ such that

$$V = V(I) = \{P = (x_1, ..., x_n) \in K^n : f(P) = 0 \quad \forall f \in I\}.$$

V is called **affine algebraic set** defined by I. If the ideal I defining $V = V(I)$ has a generator whose coefficients in K, then we say V is defined over K. In this case, the set of K-rational points of V is the set

$$V(K) = V \cap \mathbb{A}(K).$$

When the polynomials $f_1, f_2, \cdots, f_s$ are the set of generators of I, denoted by $I = \langle f_1, f_2, \cdots, f_s \rangle$, $V = V(I) = V(f_1, f_2, \cdots, f_s)$ is the set of all points such that $f_1(P) = f_2(P) = \cdots = f_s(P) = 0$.

Examples:

In the plane $\mathbb{R}^2$ with the algebraic set $V(x^2 + y^2 - 1)$ is the circle centered at the origin with radius=1 .

The algebraic set $V(XZ, YZ)$ over $\bar{\mathbb{K}}^3$ is the union of the plane $Z = 0$ with the line of equation $X = 0$ and $Y = 0$.

The algebraic set $V(X^n + Y^n = 1)$ over $\mathbb{Q}$ for $n \geq 3$ is

$$V \cong \begin{cases} (1,0), (0,1), & \text{if} \quad n \quad \text{is odd,} \\ (\pm 1, 0), (0, \pm 1), & \text{if} \quad n \quad \text{is even.} \end{cases}$$

For an algebraic set V, we can define ideal of V

$$I(V) = \{f \in \bar{K}[X] : f(P) = 0, \quad \forall P \in V\}.$$

We can say $V(I(V)) = V$; but $I(V) = \sqrt{I} = \{f \in K : \exists n \mid f^n \in I\}$= radius of I.

Remark: Let $f_1, f_2, \cdots, f_s \in \bar{K}[X]$. Then $\langle f_1, f_2, \cdots, f_s \rangle \subset I(V(f_1, \cdots, f_s))$. However, the equality may not occur. For example, $\langle f_1, f_2 \rangle = \langle x^2, y^2 \rangle \subset I(V(x^2, y^2))$ but $\langle x^2, y^2 \rangle \neq I(V(x^2, y^2))$. Since $x^2 = y^2 = 0$, $V\{x^2, y^2\} = \{(0,0)\}$, but ideal of $\{(0,0)\}$ is $\langle x, y \rangle$. It is clear that $x \in \langle x, y \rangle$ but $x \notin \langle x^2, y^2 \rangle$ so $\langle x^2, y^2 \rangle \neq I(V(x^2, y^2))$.

An affine algebraic set $V \subset K^n$ is **irreducible** if it is not a non-trivial union of two algebraic set. In other words, V is irreducible whenever V is written in the form $V = V_1 \cup V_2$ where V_1 and V_2 affine varieties then either $V = V_1$ or $V = V_2$.

Ex 2.2.1. The affine algebraic set $V(XZ, YZ) \in K^3$ is not irreducible. The affine algebraic set $V(X_1 - x_1, ..., X_n - x_n)$ is irreducible.

Remark: An affine algebraic set V is irreducible if and only if $I(V)$ is a prime ideal.

An affine algebraic set V is called an **affine variety** if $I(V)$ is a prime ideal in $\bar{K}[X]$.

Let V be affine variety. Its coordinate ring is the quotient ring defined by $K[V] = K[X]/I(V)$. If V is a variety. then $K[V]$ is an integral domain. Its fraction ring(quotient fild) is denoted by $K(V)$ and called **function field** of V.

The **dimension** of an affine variety is the transcendence degree of $\bar{K}(V)$ over $\bar{K}$ and denoted by dim(V).

Ex 2.2.2.

- dim$K^n = n$.
- If $V \subset K^n$ is given by a single nonconstant polynomial equation $f(X_1, ..., X_n) = 0$, then dim$(V(f)) = n - 1$.

Let V be an affine variety, $P \in V$ and $f_1, ..., f_m \in \bar{K}[X]$ be a set of generators for $I(V)$. V is **non-singular** at P if the $m \times n$ matrix $(\frac{\partial f_i}{\partial X_j}(P))_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$ has rank $n -$ dim(V). V is **smooth** if it is non-singular at every point.

Ex 2.2.3. $V(y^2 - x^3 - x)$ is smooth. $V(y^2 - x^3 - x^2)$ is not smooth.

2.2.2 Projective Varieties:

The **projective n-space** over a field denoted by P^n or $P^n(\bar{K})$ is the set of lines through the origin or, equivalently, is the set of all $(n+1)$ tuples $(x_0, ..., x_n)$ where each $x_i \in \bar{K}$ such that at least one x_i is non-zero.

$$P^n(\bar{K}) = (K^{n-1} - 0 \backslash \sim)$$

where $(x_0, ..., x_n) \sim (y_0, ..., y_n)$ if there exist a $\lambda \in \bar{K}^*$ such that $x_i = \lambda y_i$ for all i. An equivalence class $\{(\lambda x_0, ..., \lambda x_n) : \lambda \in \bar{K}^*\}$ is denoted by $[x_0 : ... : x_n]$ and called **homogeneous coordinate**.

The set of K-rational points in $P^n(K)$ is the set

$$P^n(K) = \{[x_0 : ... : x_n] \in P^n : \forall x_i \in K\}.$$

For $0 \leq i \leq n$, the affine chart $U_i \subset P^n$ is the set $\{[x_0 : ... : x_n] : x_i \neq 0\}$. The affine chart U_i is one-to-one correspondence with the affine n-space via the map $\{[x_0 : ... : x_n] \to (\frac{x_0}{x_i}, ..., \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, ..., \frac{x_n}{x_i})$ Then the set $\{[x_0 : ... : x_n] : x_i = 0\}$ is isomorphic to P^{n-1} and is the hyperplane at infinity in U_i.

A polynomial $f \in K[X]$ is called **homogeneous** of degree d if for all $\lambda \in K$, $f(\lambda x_0, ..., \lambda x_n) = \lambda^d f(x_0, ..., x_n)$. It means also all of the monomials of f have total degree d. An ideal $I \subset K[X]$ is homogeneous if it is generated by homogeneous polynomials.

Let $f \in K[X] = K[X_1, ..., X_n]$ be a polynomial of total degree d. Then

$$f^h = x_0^d f(\frac{x_1}{x_0}, ..., \frac{x_n}{x_0})$$

is a degree d homogeneous polynomial in $K[X_1, ..., X_n]$ and it is called **homogenization** of f.

Conversely, for a homogeneous polynomial $g \in K[X_0, ..., X_n]$,

$$g^* = g(1, x_1, ..., x_n) \in K[X_1, ..., X_n]$$

is **dehomogenization** with respect to X_1 of g.

Ex 2.2.4. $f(x, y) = y^2 - x^3 - x^2 - 1$ is a polynomial of total degree $d = 3$. Then $f^h = Z^3 f(\frac{X}{Z}, \frac{Y}{Z}) = ZY^2 - X^3 - ZX^2 - Z^3$ is homogeneous polynomial. Conversely, $f^h(X, Y, 1) = y^2 - x^3 - x^2 - 1 = f(x, y)$ is dehomogenization with respect to Z.

For each homogeneous ideal $I \in K[X]$, we can write $V = \{P \in \mathbb{P}^n : f(P) = 0$ for all homogeneous $f \in I\}$ which is a subset of $\mathbb{P}^n$. A **projective algebraic set** is any set of the form above $V \in \mathbb{P}^n(\bar{K})$ for a homogeneous ideal I. If $f_1, ..., f_s \in K[X_1, ..., X_n]$ are a set of homogeneous generator of I, then V is the set of points P such that $f_1(P) = \cdots = f_s(P) = 0$.

For a projective algebraic set V, the **homogeneous ideal** of V which is represented by $I(V)$ is generated by

$$\{f \in K[X] : f \quad \text{is homogeneous and} \quad f(P) = 0, \forall P \in V\}.$$

A projective algebraic set is called a **projective variety** if its homogeneous ideal $I(V)$ is a prime ideal.

Ex 2.2.5. Given a projective variety $V(y^2 = x^3 + x + 7)$, the homogeneous equation is $Y^2Z = X^3 + XZ^2 + 7Z^3$ where $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$.
To find the point at infinity, we put $Z = 0$ then $\infty = [0 : 1 : 0]$. Thus,

$$V(Q) = \{(x, y) \in A^2(\mathbb{Q}) : y^2 = x^3 + x + 7\} \cup \{\infty\}.$$

Some significant properties of a projective variety $\mathbb{P}^n$ can be defined in terms of affine subvariety $\mathbb{P}^n \cap \mathbb{A}^n$. For the following definition, let $\mathbb{P}^n$ be projective variety, $\mathbb{A}^n \subset \mathbb{P}^n$ be affine variety, $\mathbb{P}^n \cap \mathbb{A}^n$ be affine subvariety and a point $P \in \mathbb{P}^n \cap \mathbb{A}^n$. The **dimension** of $\mathbb{P}^n$ is the dimension of $\mathbb{P}^n \cap \mathbb{A}^n$. $\mathbb{P}^n$ is **nonsingular** or **smooth** at P if $\mathbb{P}^n \cap \mathbb{A}^n$ is nonsingular at P. The **function field of** $\mathbb{P}^n$ denoted by $K(\mathbb{P}^n)$, is the function field of $\mathbb{P}^n \cap \mathbb{A}^n$. The function field of $\mathbb{P}^n$, $\bar{K}(X_0, ..., X_n) = K(\mathbb{P}^n)$ consists of rational functions $F(X) = \frac{f(x)}{g(x)}$ for which f and g are homogeneous polynomials of the same degree. In other words, the function field of a projective variety $\mathbb{P}^n$ is the field of rational functions $F(X) = f(x)/g(x)$ such that

- f and g are homogeneous of the same degree,
- $g \notin I(V)$,
- two functions f_1/g_1 and f_2/g_2 are equal if $f_1g_2 - f_2g_1 \in I(V)$.

2.2.3 Maps Between Varieties

2.2.3.1 Affine Morphism

Let $X \subseteq A^m$ and $Y \subseteq A^n$ be affine varieties. A **morphism** $f : X \to Y$ is a map defined by polynomials $f_1, \cdots, f_n \in K[X_1, \cdots, X_m]$ such that $f(P) := (f_1(P), \cdots, f_n(P))$ where $f(P) \in Y$ for all points $P \in X$.

If $f : X \to Y$ and $g : Y \to Z$ are morphisms of varieties X, Y, Z where $X \subseteq A^m$, $Y \subseteq A^n$ and $Z \subseteq A^r$, then $(g \circ f) : X \to Z$ such that

$$(g \circ f)(P) := g(f(P)) = (g_1(f_1(P), \cdots, f_n(P)), \cdots, g_r(f_1(P), \cdots, f_n(P))).$$

Ex 2.2.6. $f : A^2 \to A^2$ is a morphism defined by $f(x_1, x_2) = (x_1, x_1x_2)$.

Theorem 4. *Every morphism $f : X \to Y$ of affine varieties is continuous. That is, the inverse map $f^{-1}(Z)$ for any algebraic subset $Z \subseteq Y$ is an algebraic subset of X.*

We say that two affine varieties X and Y are **isomorphic** if there exists $f : X \to Y$ and $g : Y \to X$ such that both $f \circ g$ and $g \circ f$ are the identity morphism on X and Y, respectively. It is denoted by $X \simeq Y$.

2.2.3.2 Rational Maps and Morphism of Projective Varieties

Let $X \subseteq P^m$ and $Y \subseteq P^n$ be projective varieties. A **rational map** $f : X \to Y$ is a map of the form $f = [f_0 : \cdots : f_n]$ where $f_0, \cdots, f_n \in \bar{K}[X]$ not all zero and for any point $P \in X$ at which $f_0, \cdots, f_n$ are all defined: $f(P) = [f_0(P) : \cdots : f_n(P)] \in Y$. Alternatively, we can define the rational map $f : X \to Y$ as a tuple of homogeneous polynomials in $\bar{K}[X_0, \cdots, X_m]$ that all have the same degree and not all of which lie in $I(X)$. If there is $\lambda \in \bar{K}^*$ such that $\lambda f_0, \cdots, \lambda f_n \in \bar{K}[X]$ then $[f_0 : \cdots : f_n]$ and $[\lambda f_0 : \cdots : \lambda f_n]$ give the same map on points.

A rational map $f = [f_0 : \cdots : f_n] : X \to Y$ is **regular** at $P \in X$ if there is homogeneous polynomials $g_0, \cdots, g_n \in \bar{K}[X]$ such that $g_0, \cdots, g_n$ have same degree and at least one g_i is non-zero and also $f_i g_j = f_j g_i \ (modI\ (X))$ for all $0 \leq i, j \leq n$.

A **morphism** is a rational map that is regular at every point.

We define the **isomorphism** between projective varieties same as affine varieties. In other words, let X and Y be projective varieties. We can say X and Y are **isomorphic**, $X \simeq Y$, if there area morphism $f : X \to Y$ and $g : Y \to X$ such that both $f \circ g$ and $g \circ f$ are the identity maps on X and Y, respectively.

2.3 Curves and Divisors

In this part, we introduce curves and divisors. Divisors are essential part to understand the group structure of elliptic curves.

2.3.1 Curves

By a curve C defined over a field $\bar{K}$, we mean one dimensional non-singular projective variety $C = V(f_1, ..., f_m)$ in $\mathbb{P}^n$ where $f_i(x_0, ..., x_n)$ are homogeneous polynomials defined over $\bar{K}$ for each $i = 1, ..., m$.

Notation: A curve over a field K is denoted by $C(K)$. If the curve defined over $\bar{K}$ then it is denoted by $C(\bar{K}) = C$. We know that $C(K) \subset C$.

Curves of degree 1,2,3,4 are called lines, planes, cubics and quadratics, respectively.

Examples:
$C = V(f)$ where $f(x, y, z) = ax + bz - y$ over $\bar{K}$. Then

$$C = \{[x : y : 1] : (x, y) \in K^2 \quad \text{such that} \quad ax - y = -b\} \cup \{[1 : a : 0]\}.$$

$C = V(g)$ where $g(x, y, z) = ax^2 + by^2 + cxy + dxz + eyz + fz^2$ over $\mathbb{Q}$. Then

$C(\mathbb{Q}) = \{[x : y : 1] : (x, y) \in \mathbb{Q}^2 \quad \text{st} \quad ax^2 + by^2 + cxy + dx + ey + f = 0\} \cup \{\infty_1, \infty_2\}.$

$C = V(h)$ where $h(x, y, z) = x^3 + axz^2 + bz^3 - y^2z$ over $\bar{K}$. When we put $z = 0$ we have $x^3 = 0$. So $\infty = [0 : 1 : 0]$. Then

$$C = \{[x : y : 1] : (x, y) \in \bar{K}^2 \quad \text{st} \quad y^2 = x^3 + ax + b\} \cup \{\infty\}.$$

Every rational map $\phi : C \to V$ from a smooth projective curve C to a projective variety V is a **morphism**.

Field of rational function on C is all morphisms from C to $\mathbb{P}^1$,

$$\bar{K}(C) = \{f : C \to \mathbb{P}^1\} = Mor(C, \mathbb{P}^1)$$

which is a field of transcendental degree 1.

Remark: The projective curve $C \subset P^n$ may be singular but there is always a non-singular model $\tilde{C}$ in $K(\tilde{C}) = K(C)$.

Let $\phi : C_1 \to C_2$ be a non-constant rational map. Then there is a map (called pull-back map which will be discussed in next section) $\phi^* : K(C_2) \to K(C_1)$. The **degree of morphism of curves** $\phi : C_1 \to C_2$ is the degree of the corresponding extension of function fields $\deg \phi = [K(C_1) : \phi^* K(C_2)]$. If ϕ is constant, then we define the degree of ϕ to be 0.

Remark: Let C_1 and C_2 be nonsingular projective curves and $\phi : C_1 \to C_2$ be a morphism. Up to isomorphism, there is a unique curve C_3 and $\phi : C_1 \to C_2$ can be factorized via a separable map $\phi_2 : C_3 \to C_2$.

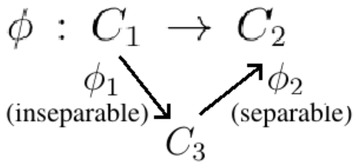

Figure 2.1

2.3.2 Divisors

Let $P \in C$. The local ring at the point P is the subring of the function field of C defined by

$$K[C]_P = \{(\frac{f}{g}) \in K(C) : g(P) \neq 0\}.$$

There is a unique maximal ideal

$$M_P = \{\psi \in K[C]_P : \psi(P) = 0\}.$$

If C is a curve and $P \in C$ is nonsingular point, then $K[C]_P$ is a discrete valuation ring with $M_P = \langle t_p \rangle$, generated with t_p. t_p is called **uniformizing parameter** such that $t_p(P) = 0$.

Each function $f \in K[C]_P$ can be written in the form of $f = t_p^r.g$ where $r \in \mathbb{Z}$ and $g(P) \neq 0$, $g(P) \neq \infty$. The integer r is the **order of** f at P and symbolized by $\text{ord}_P(f) = r$. Given any $f, g \in \bar{K}[C]_P$, we can define the order of f/g as

$$\text{ord}(f/g) = \text{ord}(f) - \text{ord}(g).$$

Let $f : C \to \mathbb{P}^1$ be a nonzero morphism then for any y in $\mathbb{P}^1$ $f^{-1}(y) = \{x \in C : f(x) = y\}$ is a finite set because C is irreducible projective curve. In particular,

$f^{-1}(0) = \{p \in C : f(p) = 0\}$ is called **zeros of** f in C, $f^{-1}(\infty) = \{q \in C : f(q) = \infty\}$ is called **poles of** f in C are finite sets. Therefore, $\text{ord}_P(f) = 0$ except for finitely many $P \in C$. When P is a pole, $\text{ord}_P(f) < 0$ and when P is a zero, $\text{ord}_P(f) > 0$.

Ex 2.3.1. On $y^2 = x^3 - x$, $f(x, y) = x$. Then $t_p = y$ is uniformizer at point $P = (0, 0)$ because $x = y^2 \frac{1}{x^2-1}$. Note that $g(x, y) = \frac{1}{x^2-1}$ is nonzero and finite at P. Thus, $\text{ord}_P(f) = 2$

Let C be a curve over K with $K = \bar{K}$. A **divisor** of C is a sum

$$D = \sum_{P \in C} n_P(P)$$

for all but finitely many integer $n_P = 0$. The set of points P for which $n_p \neq 0$ is called the **support** of D.

The **degree of divisors** is defined by

$$\deg(D) = \sum_{P \in C} n_P.$$

The divisors of curve C defined over $\bar{K}$ form a free abelian group under addition. It is called **divisor group** of a curve C and denoted by $\text{Div}(C)$.

Remark: The divisor of degree 0

$$\text{Div}^0(C) = \{D \in \text{Div}(C) : \deg D = 0\} \subset \text{Div}(C)$$

is a subgroup of $\text{Div}(C)$.

Let f be a non-zero rational function in $\bar{K}(C)^*$. Then the divisor of f is given by

$$\text{div}(f) = \sum_{P \in C} \text{ord}_P(f)(P)$$

is called **principal divisor**. In other words, if $D = \text{div}(f)$ for some $f \in \bar{K}(C)^*$ then divisor $D \in \text{Div}(C)$ is principal .

For any principal divisor $\text{div}(f) = \sum_{P \in C} \text{ord}_P(f)(P)$, we can define

$$\text{div}_0(f) = \sum_{\text{ord}_{P(f)>0}} \text{ord}_P(f)(P)$$

which is called **divisor of zeros**, and

$$\text{div}_\infty(f) = \sum_{\text{ord}_{P(f)<0}} -\text{ord}_P(f)(P)$$

and call **divisor of poles**.

Property: Let C be a smoth curve and $f \in \bar{K}(C)^*$, then

i. $\text{div}(f) = 0$ if and only if $f \in \bar{K}^*$,

ii. $\deg(\text{div}(f)) = 0$.

Two divisors are linearly equivalent, $D_1 \sim D_2$, if $D_1 - D_2$ is principal. It means $D_1 - D_2 = \text{div} f$ for $f \in \bar{K}(C)$. **The Picard group** or divisor class group of C which is denoted by $\text{Pic}(C)$ is the quotient of $\text{Div}(C)$ by its subgroup principal divisors:

$$\text{Pic}(C) = \text{Div}(C) \backslash \sim .$$

Because of the above property, the principal divisors form a subgroup of $\text{Div}^0(C)$. We can define the Picard group of C to be the quotient of of $\text{Div}^0(C)$ by the subgroup principal divisors:

$$\text{Pic}^0(C) = \text{Div}^0(C) \backslash \sim .$$

Let $\phi : C_1 \to C_2$ be a morphism and $\phi^* : \bar{K}(C_2) \to \bar{K}(C_1)$ be the corresponding morphism of function fields. **The ramification degree** or **the ramification index** of ϕ at P, denoted by $e_\phi(P)$, is

$$e_\phi(P) = \text{ord}_P(\phi^* t_{\phi(P)})$$

where $t_{\phi(P)} \in K(C_2)$ is uniformizer at $\phi(P)$.

Remark: $e_\phi(P) \geq 1$. If $e_\phi(P) = 1$, then ϕ is **unramified** at P.

Proposition 1. *Let $\phi : C_1 \to C_2$ be a nonconstant map of smooth curves. For every $Q \in C_2$,*

$$\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \deg(\phi).$$

Ex 2.3.2. Let $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ be a map where $\phi([X, Y]) = [X^3(X - Y)^2, Y^5]$. Then ϕ is ramified at the points $[0, 1]$ and $[1, 1]$: $e_\phi([0, 1]) = 3$ and $e_\phi([1, 1]) = 2$. Therefore,

$$\sum_{P \in \phi^{-1}([0,1])} e_\phi(P) = e_\phi([0, 1]) + e_\phi([1, 1]) = 5 = \deg(\phi).$$

Let $\phi : C_1 \to C_2$ be a morphism defined over $\bar{K}$.
The **pullback map** ϕ^* on divisors is the homomorphism

$$\phi^* : \mathrm{Div} C_2 \to \mathrm{Div} C_1$$
$$\phi^*((Q)) = \sum_{P \in \phi^{-1}(Q)} e_\phi(P)(P)$$

where (Q) denotes the divisor in DivC_2 with support Q and $n_Q = 1$.
The **pushforward map** ϕ_* on divisors is the homomorphism

$$\phi_* : \mathrm{Div} C_1 \to \mathrm{Div} C_2$$
$$\phi_*((P)) = (\phi P)$$

Properties: Let $\phi : C_1 \to C_2$ be a nonconstant map of smooth curves.

i. $\deg(\phi^*(D_2)) = \deg(D_2) \deg \phi$ for all $D_2 \in \mathrm{Div}(C_2)$,

ii. $\deg(\phi_*(D_1)) = \deg(D_1)$ for all $D_1 \in \mathrm{Div}(C_1)$,

iii. $\phi^*(\mathrm{div}(f)) = \mathrm{div}(\phi^*(f))$ for all $f \in \bar{K}(C_2)$,

iv. $\phi_*(\mathrm{div}(f)) = \mathrm{div}(\phi_*(f))$ for all $f \in \bar{K}(C_1)$,

v. $\phi_* \circ \phi^*(D_2) = (\deg(\phi))D_2$ for all $D_2 \in \mathrm{Div}(C_2)$,

vi. If $\psi : C_2 \to C_3$ is another such map, then $(\psi \circ \phi)^* = \phi^* \circ \psi^*$ and $(\psi \circ \phi)_* = \phi_* \circ \psi_*$,

vii. Both ϕ^* and ϕ_* are group homomorphisms.

In particular, ϕ^* takes $\mathrm{Div}^0(C_2)$ to $\mathrm{Div}^0(C_1)$ and it maps principal divisors to principal divisors, similar to ϕ_*. Thus, they induce maps

$$\phi^* : \mathrm{Pic}^0(C_2) \to \mathrm{Pic}^0(C_1),$$
$$\phi_* : \mathrm{Pic}^0(C_1) \to \mathrm{Pic}^0(C_2).$$

2.4 Riemann-Roch Theorem

Let $D = \sum n_P(P)$ be a divisor on C and $\text{ord}_P(D) = n_P$. If $n_p \geq 0$ for every $P \in C$ then $D \geq 0$ and we say that D is **effective**(**positive**). Moreover, we say $D_1 \geq D_2$ where $D_1 = \sum n_P(P)$ and $D_2 = \sum m_P(P)$ are two divisors in $\text{Div}(C)$ if and only if $n_p \geq m_p$ for all P. For a $f \in \bar{K}(C)^*$, when we assume f is regular at everywhere except one point $P \in C$ and has a pole of order at most n at P, we can say that

$$\text{div}(f) \geq -n(P).$$

Let $D \in \text{Div}(C)$, we define

$$L(D) = \{f \in \bar{K}(C)^* : \text{div}(f) \geq -D\} \cup \{0\}.$$

L(D) is a finite-dimentional vector space over $\bar{K}$ because

- $\text{div}\lambda f = \text{div}f + \text{div}\lambda = \text{div}f$ for all $\lambda \in K^*$,
- $\text{ord}_P(f+g) \geq min(\text{ord}_P(f), \text{ord}_P(g))$.

We define its dimention by $l(D) = \dim_{\bar{K}} L(D)$.

Ex 2.4.1. Let $D = 3[P] - 2[Q]$. Then $L(D)$ is the set of function in $\bar{K}(C)^*$ such that functions have at most triple pole at P and at least double zero at Q.

Proposition 2. *Let C be a curve over $\bar{K}$ and D_1, D_2 be divisors on C.*

i. *If* $\deg D < 0$, *then* $L(D) = 0$.

ii. *If* $D_1 \sim D_2$, *then* $L(D_1) \simeq L(D_2)$.

iii. $L(0) = \bar{K}$.

iv. $l(D) < \infty$.

v. *If* $\deg(D) = 0$ *then* $l(D) = 0$ *or* $l(D) = 1$.

The following theorem is adapted from Rieman-Roch's theorem.

Theorem 5. *There exists a positive integer $g \in \mathbb{N}$ such that*

1. $l(D) \geq \deg(D) - g + 1$,
2. $l(D) = \deg(D) - g + 1$ *if* $\deg(D) > 2g - 1$

for all divisors $D \in Div(C)$. *The integer* g *is called* ***genus*** *of* C.

Lemma 1. *If* C *is isomorphic to* $\mathbb{P}^1$ *then* $l(D) = \deg D + 1$ *for all* $d \geq 0$.

Theorem 6. *Let* C *be a curve defined over* K. *Then*

1. *C has genus zero if and only if it is isomorphic to* $\mathbb{P}^1$.
2. *C has genus one if and only if it is isomorphic to a plane cubic of the form*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad (*)$$

   with $a_1, a_2, a_3, a_4, a_6 \in K$.

Proof. 1. Let C be a curve such that $C \simeq \mathbb{P}^1$. Then C has genus 0 from above Lemma1 and Riemann-Roch Theorem5.

Now assume C has genus 0 curve and P is a rational point. Since $\deg D = 1 > 2g - 2 = -2$ holds, $l(D) = \deg D - g + 1 = 1 - 0 + 1 = 2$. Then we have a non-constant function $f \in L(D)$. This function f has a pole only at P and there is no pole at anywhere else. Therefore, $\text{div}_\infty = \deg P = 1$ and so f gives a morphism from C to $\mathbb{P}^1$ whose degree is one. Since isomorphism is a degree-one morphism and $f \in K(C)$, C is isomorphic to $\mathbb{P}^1$.

2. Assume C is a curve with $g = 1$ and P is a rational point on C. For any $n \in \mathbb{Z}^+$, we have $\deg(nP) = n \geq 2g - 2 = 0$. By Theorem 5,

$$l(nP) = \deg D - g + 1 = n + 1 - 1 = n.$$

Now, let $n = 2$. Then $\dim(L(2P)) = 2$. For some $x \in (K(C) - K)$, $L(2P)$ has a basis of the form $\{1, x\}$ since $K \in L(2P)$ and $0 \geq -2P$. For $n = 3$, $L(3P)$ which contains $L(2P)$ has dimension 3 and for some $y \in K(C)^*$, $\{1, x, y\}$ is the form of basis for $L(3P)$. The functions $1, x, y, x^2$ contained by $L(4P)$ are linearly independent because poles of functions have distinct orders which are 0,2,3,4 at P, respectively. For this reason, we can say that $L(4P)$ has a basis of the form $\{1, x, y, x^2\}$. Similarly, we can say that $L(5P)$ has a basis of the form $(1, x, y, x^2, xy)$. However, all of $1, x, y, x^2, x^3, y^2, xy$ are in $L(6P)$. Although the dimension of space is 6, there are 7 elements in K-vector space. Therefore, they must be linearly dependent. A linear equation which is satisfied by these elements must contain terms ax^3 and by^2 with $a, b \neq 0$. If we change x by ax/y and y by by/a, after multiplying through by b^3/a^4 and homogenizing we obtain an equation in the form $(*)$.

Conversely, we assume a curve C over K is defined of the form $(*)$. When we homogenize this equation, we get

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

$P = (0 : Y : 0) = (0 : 1 : 0)$ is the only rational point with $Z = 0$.

As a curve, C is an irreducible algebraic set, so equation of $(*)$ is also irreducible. Moreover, $K(C) = K(x, y)$ and the minimal equation of y over $K(x)$ has degree 2. Therefore, the function x is a morphism $(X : Z)$ from C to $\mathbb{P}^1$ of degree 2. Therefore, $\text{div}_0 x = 2$ Since any nonzero function on a curve has the same number of zeros and poles, we have $\text{div}_\infty x = 2$. The function x only has pole at points with $Z = 0$ which means that function x has double pole at P. Because of the same reason, the function y has a pole of order 3 at P. $\{x^i y^j\}$ denotes the set of functions whose poles of order $n = 2i + 3j$ at P for $n = 0$ and all $n \geq 2$. None of these functions has any other poles. Thus we can construct a set of n linearly independent functions with poles of order $0, 2, 3, ..., n$, all of which lie $L(nP)$. When we applying Theorem 5 with n

$$n \leq l(nP) = \deg(nP) - g + 1 = n - g + 1$$

so the genus of C is at most 1.

Now we need to show $g \neq 0$. Let τ be the rational map such that $\tau : (X : -Y - a_1X - a_3Z : Z)$. On the RHS of the equation $(*)$, the map τ changes nothing. On the LHS, we have

$$\begin{aligned}\tau(Y(Y + a_1X + a_3Z)) &= (-Y - a_1X - a_3Z)(-Y - a_1X - a_3Z + a_1X + a_3Z) \\ &= (Y(Y + a_1X + a_3Z))\end{aligned}$$

so the map τ also changes nothing on the LHS. Therefore, τ is a morphism from C to C. Since she morphism τ is invertible and its inverse is also τ, τ is an automorphism. Clearly $\tau(0:1:0) = (0:1:0)$ is fixed. To find points with $Z \neq 0$ which are fixed, $Y = -(Y + a_1X + a_3Z)$. Suppose char$(K) \neq 2$, this is equivalent to $Y = -(a_1X + a_3Z)/2$. There are then three possibilities for X, corresponding to the roots of cubic

$$X^3 + a_2X^2 + a_4X + a_6Z + (a_1X + a_3Z)^2/4.$$

These roots are distinct because a repeated root would corresponds to a singularity on the smooth curve C. Thus τ fixes exactly 4 points in $\bar{K}(C)$. If $g = 0$, then C is isomorphic to $\mathbb{P}^1$ and the only automorphism of $\mathbb{P}^1$ that fixes four points in $\mathbb{P}^1$ is the identity map. But τ is not the identity map on $\bar{K}(C)$. Thus, $g \neq 0$.

With different argument, we can show $g \neq 0$ if char$(K) = 2$.

Hence, $g = 1$.

□

Equation in the above form $(*)$ is called **Weierstrass equation**. A Weierstrass equation with $a_1 \cdot a_2 \cdot a_3 = 0$ is called **short Weierstrass equation**.

An **elliptic curve E** over finite field K is a genus one curve.

Remark: Let E be elliptic curve defined over K.

1. If the characteristic of K is different than 2 and 3, E can be defined by the following short Weierstrass equation

$$y^2 = x^3 + a_4x + a_6$$

   using change of coordinates.

2. If char$(K) = 2$, then E can be written in the following forms

$$y^2 + xy = x^3 + a_2x^2 + a_6$$

   or

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

3. If $\mathrm{char}(K) = 3$, then E is

$$y^2 = x^3 + a_2x^2 + a_6$$

or

$$y^2 = x^3 + a_4x + a_6.$$

CHAPTER 3

CLASSIFICATION OF ELLIPTIC CURVES

As we have seen in previous chapter, genus one curves are called elliptic curves and they correspond plane cubic curves in $\mathbb{P}^2$ given by Weierstrass equation. Our aim in this chapter is to classify theese equations up to isomorphism. If you want to see the proofs of some theorems in this chapter, you can look [3], [8] and [10].

Let K be a field and $E(K)$ be an elliptic curve over K given by

$$E(K) : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

where $a_1, a_2, a_3, a_4, a_6 \in K$.

The **discriminant** of elliptic curve E which is denoted by Δ is $\Delta = -d_2^2d_8 - 8d_4^3 - 27d_6^2 + 9d_2d_4d_6$ where

$$\begin{aligned}
d_2 &= a_1^2 + 4a_2, \\
d_4 &= 2a_4 + a_1a_3, \\
d_6 &= a_3^2 + 4a_6, \\
d_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2.
\end{aligned}$$

Remark: When $\Delta \neq 0$, we can say the elliptic curve is smooth.

Let E_1 and E_2 be two elliptic curves over K which are given by Weierstrass equations as follows

$$E_1 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$
$$E_2 : y^2 + \bar{a}_1xy + \bar{a}_3y = x^3 + \bar{a}_2x^2 + \bar{a}_4x + \bar{a}_6$$

where all $a_i, \bar{a}_i \in K$.

It can be checked that E_1 is isomorphic to E_2 over F if and only if there exist $u, r, s, t \in F$ such that the change of variables

$$(x, y) \longrightarrow (u^2x + r, u^3y + u^2sx + t)$$

transforms equation E_1 into the equation E_2. We note that the isomorphism is defined over F where $K \subseteq F \subseteq \bar{K}$.

There is an important parameter for elliptic curve which is **j-invariant**. j-invariant of elliptic curve E is $j(E) = \frac{c_4^3}{\Delta}$ where $c_4 = d_2^2 - 24d_4$. Isomorphisms over $\bar{K}$ can be checked by means of j-invariants. In fact, there is an isomorphism form E_1 to E_2 over $\bar{K}$ if and only if $j(E_1) = j(E_2)$.

The admissible change of variables can be simplify the Weierstrass equation. We study separately each case where the underlying field K has characteristic 2 or 3 or different from 2 and 3. In the following table, we can see the short elliptic curve equations after the transformations.

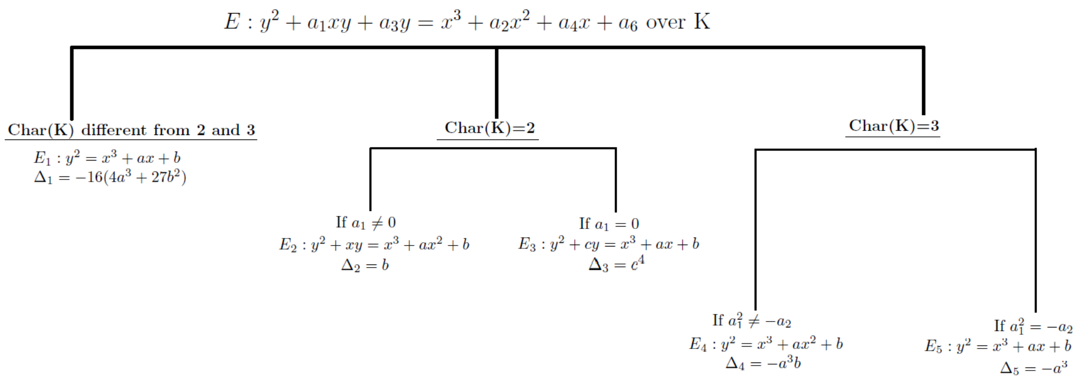

Figure 3.1

3.1 Isomorphism Classes of Elliptic Curve over Fields K with $\text{char}(K) \neq 2, 3$

Let $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ be elliptic curve defined over K where $\text{char}(K) \neq 2, 3$. This Weierstrass equation can be simplified by applying admissible change of variables

$$(x,y) \to (\frac{x-3a_1^2-12a_2}{36}, \frac{y-3a_1x}{216} - \frac{a_1^3+4a_1a_2-12a_3}{24})$$

transform E to $E_1 : y^2 = x^3 + ax + b$ where $a, b \in K$.

Since $\Delta = -d_2^2 d_8 - 8d_4^3 - 27d_6^2 + 9d_2d_4d_6$ and $d_2 = 0, d_4 = 2a, d_6 = 4b, d_8 = -a^2$ for E_1, the discriminant of E_1 is $\Delta = 0 - 64a^3 - 27 \cdot 4 \cdot 4b^2 + 0$ which is equal to $\Delta = -16(4a^3 + 27b^2)$.

Since $j(E) = \dfrac{c_4^3}{\Delta}$ where $c_4 = d_2^2 - 24d_4$, we get

$$j(E_1) = \frac{(-48a)^3}{-16(4a^3+27b^2)} = 1728\frac{4a^3}{(4a^3+27b^2)}.$$

Ex 3.1.1. Let $E_1 : y^2 = x^3+x+1$, $E_2 : y^2 = x^3+16x+64$ and $E_3 : y^2 = x^3+4x+8$ be elliptic curves defined over $\mathbb{Q}$. Then
$j(E_1) = 1728\dfrac{4}{31}$,
$j(E_2) = 1728\dfrac{4(16)^3}{(4.16^3+27.64^2)} = 1728\dfrac{4}{31}$,
$j(E_3) = 1728\dfrac{4(4)^3}{(4.4^3+27.8^2)} = 1728\dfrac{4}{31}$,
so $j(E_1) = j(E_2) = j(E_3)$. Thus, we can say E_1,E_2 and E_3 are isomorphic to each other in $\bar{\mathbb{Q}}$.
In fact,

$$\begin{aligned}\phi_1 :& E_1(Q) \to E_2(Q)\\ &(x,y) \to (2^2x, 2^3y)\end{aligned}$$

is a group homomorphism and clearly $2 \in \mathbb{Q}$. Therefore, E_1 is isomorphic to E_2 over $\mathbb{Q}$.

$$\begin{aligned}\phi_2 :& E_1(Q) \to E_3(Q)\\ &(x,y) \to (\sqrt{2}^2x, \sqrt{2}^3y)\end{aligned}$$

Therefore, E_1 is isomorphic to E_3 over $\mathbb{Q}(\sqrt{2})$, but not over $\mathbb{Q}$.

Two elliptic curves E_1, E_2 over K (with any characteristics) are said to be **twist of** each other if they are isomorphic over $\bar{K}$. They are called **quadratic/cubic/quartic twists** if they are isomorphic over a quadratic/cubic/quartic extension of K.

Ex 3.1.2. E_1 and E_3 in the previous example are twist elliptic curves.

Basically, we have 3 different cases for $E : y^2 = x^3 + ax + b$.

Case 1: $j(E) = 0$

Since $j(E) = 1728\frac{4a^3}{(4a^3 + 27b^2)}$, $j(E) = 0$ implies that $a = 0$ and $b \neq 0$.

If $E_1(K) : y^2 = x^3 + b$ and $E_2(K) : y^2 = x^3 + u^6 b$ for some $u \in K^*$, then $E_1 \simeq E_2$. There exists $\xi \in K^*$ such that $\xi = u^6$ for $u \in K^*$. $K^*/(K^*)^6 = \{g^6 : g \in K^*\}$ The number of $K^*/(K^*)^6$ is also the number of non-isomorphic class of E. Therefore, there are 6 non-isomorphic class of $j = 0$ curves and they are

$$
\begin{aligned}
y^2 &= x^3 + 1 \simeq y^2 = x^3 + u^6, \\
y^2 &= x^3 + \xi \simeq y^2 = x^3 + \xi u^6, \\
y^2 &= x^3 + \xi^2 \simeq y^2 = x^3 + \xi^2 u^6, \\
y^2 &= x^3 + \xi^3 \simeq y^2 = x^3 + \xi^3 u^6, \\
y^2 &= x^3 + \xi^4 \simeq y^2 = x^3 + \xi^4 u^6, \\
y^2 &= x^3 + \xi^5 \simeq y^2 = x^3 + \xi^5 u^6,
\end{aligned}
$$

where $\forall u \in K^*$.

Case 2: $j(E) = 1728$

$j(E) = 1728$ implies that $a \neq 0$ and $b = 0$.

If $E_1(K) : y^2 = x^3 + ax$ and $E_2(K) : y^2 = x^3 + u^4 ax$ for some $u \in K^*$, then $E_1 \simeq E_2$.

There exists $\xi \in K^*$ such that $\xi = u^4$ for $u \in K^*$. $K^*/(K^*)^4 = \{g^4 : g \in K^*\}) = \langle \xi^4 \rangle = \{1, \xi, \xi^2, \xi^3\}$ The number of $K^*/(K^*)^4$ is also the number of non-isomorphic class of $E(K) : y^2 = x^3 + ax$. Therefore, there are 4 non-isomorphic class of

$j = 1728$ curves and they are

$$y^2 = x^3 + x,$$
$$y^2 = x^3 + \xi x,$$
$$y^2 = x^3 + \xi^2 x,$$
$$y^2 = x^3 + \xi^3 x$$

where $\forall u \in K^*$.

Case 3: $j \neq 0, 1728$

Assume that j$\neq$ 0,1728 and $E_1 : y^2 = x^3 + ax + b$ and $E_2 : y^2 = x^3 + \bar{a}x + \bar{b}$.

If $j(E_1) = j(E_2) = j$, then $\frac{j}{j-1728} = -\frac{4a^3}{27b^2} = -\frac{4\bar{a}^3}{27\bar{b}^2}$. This implies that $(\frac{a}{\bar{a}})^3 = (\frac{b}{\bar{b}})^2$. Therefore, we can say that $E_1 \simeq E_2$ if and only if $(\frac{a}{\bar{a}})^3 = (\frac{b}{\bar{b}})^2$. Let u be a solution of $u^2 = (\frac{a}{\bar{a}}) \cdot (\frac{\bar{b}}{b})$ where $u \in K^*$.Then,

$u^4 = (\frac{a}{\bar{a}})^2 \cdot (\frac{\bar{b}}{b})^2 = (\frac{a}{\bar{a}})^2 \cdot (\frac{\bar{a}}{a})^3 = \frac{\bar{a}}{a}$, so $\bar{a} = u^4 \cdot a$

$u^6 = (\frac{a}{\bar{a}})^3 \cdot (\frac{\bar{b}}{b})^3 = (\frac{b}{\bar{b}})^2 \cdot (\frac{\bar{b}}{b})^3 = \frac{\bar{b}}{b}$, so $\bar{b} = u^6 \cdot b$.

$E_1 \simeq E_2$ if and only if $\frac{\bar{a}}{a} \cdot \frac{b}{\bar{b}} = u^2 = \xi \in K^*$ is a square if and only if $\xi \in (K^*)^2$.

Therefore, there are 2 non-isomorphic elliptic curves over K with the same j-invariant. They are:

$$y^2 = x^3 + ax + b,$$
$$y^2 = x^3 + ax + \xi b.$$

Ex 3.1.3. Let $E_1 : y^2 = x^3 - 3x + b$ and $b \neq \pm 2$ (because $j(E_1) = 1728\frac{4a^3}{(4a^3 + 27b^2)}$ and $4^3 + 27b^2 = 4(-3)^3 + 27(b^2) \neq 0 \leftrightarrow b \neq \pm 2$) over $\mathbb{F}_q$. Then

$$j(E_1) = 1728\frac{4(-3)^3}{(4(-3)^3 + 27b^2)} = -1728\frac{4}{b^2 - 4}.$$

Let $E_2 : y^2 = x^3 - 3x + b\alpha$. If $\alpha \notin (K^*)^2$, then j-invariants are different.

So we can choose $\frac{q-1}{2}$ distinct(non-isomorphic) elliptic curves over $\mathbb{F}_q$.

3.2 Isomorphism Classes of Elliptic Curves over Fields K with $\mathrm{char}(\mathrm{K}) = 2$

Let $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ be elliptic curve defined over K where char$(K) = 2$. This Weierstrass equation can be simplified by applying admissible change of variables.

According to the coefficient a_1, there are two different cases.

Firstly, let us suppose that $a_1 \neq 0$, then the admissible change of variables

$$(x, y) \to (a_1^2x + \frac{a_3}{a_1}, a_1^3y + \frac{a_1^2a_4 + a_3^2}{a_1^3})$$

transform E to $E_1 : y^2 + xy = x^3 + ax^2 + b$ where $a, b \in K$.

This curve is non-singular iff $b \neq 0$. Equation has discriminant $\Delta = b$ and the j-invariant is $j(E_1) = \frac{1}{b}$.

When $E : y^2 + xy = x^3 + ax^2 + b$, we have two isomorphism classes over K. For given $b^{-1} \in K^*$, they are

$$E_1 : y^2 + xy = x^3 + 0x + b,$$
$$E_2 : y^2 + xy = x^3 + \gamma x + b$$

where $Tr(\gamma) = 1$.

Secondly, if $a_1 = 0$, then the admissible change of variables

$$(x, y) \to (x + a_2, y)$$

transform E to $E_1 : y^2 + cy = x^3 + ax + b$ where $a, b, c \in K$.

This equation is non-singular if and only if $c \neq 0$. Such curve has discriminant $\Delta = c^4$ and the j-invariant is $j(E_1) = 0$.

When $E : y^2 + cy = x^3 + ax + b$ over $K = \mathbb{F}_q = \mathbb{F}_{2^m}$, we have 2 different cases.

For odd m, there are 3 isomorphism classes of elliptic curves over $\mathbb{F}_{2^m}$. A representative form of each class is

$$
\begin{aligned}
E_1 &: y^2 + y = x^3, \\
E_2 &: y^2 + y = x^3 + x, \\
E_3 &: y^2 + y = x^3 + x + 1.
\end{aligned}
$$

For even m, there are 7 isomorphism classes of elliptic curves over $\mathbb{F}_{2^m}$. Let γ be a non-cube in $\mathbb{F}_{2^m}$ and let $\alpha, \beta, \delta, \omega \in F_{2^m}$ be such that $Tr(\gamma^{-2}\alpha) = 1$,$Tr(\gamma^{-4}\beta) = 1$, $Tr(\delta) \neq 0$, $Tr(\omega) = 1$. Then a representative from each class is

$$
\begin{aligned}
E_1 &: y^2 + \gamma y = x^3 && (Type1), \\
E_2 &: y^2 + \gamma y = x^3 + \alpha && (Type1), \\
E_3 &: y^2 + \gamma^2 y = x^3 && (Type1), \\
E_4 &: y^2 + \gamma^2 y = x^3 + \beta && (Type2), \\
E_5 &: y^2 + y = x^3 + \delta x && (Type3), \\
E_6 &: y^2 + y = x^3 && (Type3), \\
E_7 &: y^2 + y = x^3 + \omega && (Type3).
\end{aligned}
$$

3.3 Isomorphism Classes of Elliptic Curves over Fields K with $\mathrm{char}(\mathrm{K}) = 3$

Let $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ be elliptic curve defined over K where char$(K) = 3$. This Weierstrass equation can be simplified by applying admissible change of variables and then E is given by a medium Weierstrass equation

$$E' : y^2 = x^3 + a_2x^2 + a_4x + a_6$$

with $a_2, a_4, a_6 \in K$.

In fact, we can separate two cases for simplicity.

If $a_1^2 \neq -a_2$, then the admissible change of variables

$$(x, y) \to (x + \frac{d_4}{d_2}, y + a_1x + a_1\frac{d_4}{d_2} + a_3)$$

where $d_2 = a_1^2 + a_3$ and $d_4 = a_4 - a_1a_3$, transforms E to the curve

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

where $a, b \in K$.This curve has discriminant $\Delta = -a^3b$.

Let $E_1 : y^2 = x^3 + ax^2 + b$ and $E_2 : y^2 = x^3 + \bar{a}x^2 + \bar{b}$ be elliptic curves over $\mathbb{F}_q = \mathbb{F}_{3^n}$ and $E_1 \simeq E_2$. Then we have an isomorphism such that

$$\begin{aligned} \phi_1 :& E_1(\mathbb{F}_q) \to E_2(\mathbb{F}_q) \\ & (x, y) \to (u^2x, u^3y) \end{aligned}$$

where $u \in \mathbb{F}_q$. When $u = 1$, then ϕ gives an automorphism. Since we have $(q-1)$ distinct values for u, simple calculation shows that $(q-1)^2/((q-1)/2) = 2(q-1)$ isomorphism classes exist. Thus, the number of isomorphism classes of $E : y^2 = x^3 + ax^2 + b$ over $\mathbb{F}_q = \mathbb{F}_{3^n}$ is $2(q-1)$.

If $a_1^2 = -a_2$, then the admissible change of variables

$$(x, y) \to (x, y + a_1x + a_1x + a_3)$$

transforms E to the curve

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

where $a, b \in K$.Such curve has discriminant $\Delta = -a^3$.

To find the number of isomorphism classes of $E : y^2 = x^3 + ax + b$ over $\mathbb{F}_q$, we study 2 different cases.

Firstly, we suppose that E is defined over $\mathbb{F}_q = \mathbb{F}_{3^n}$ where n is odd. In this case, there are exactly 4 distinct isomorphism classes of elliptic curves over F_q. Let $\alpha, \beta, \gamma \in F_q$ with $Tr(\alpha) = 0$, $Tr(\beta) = 1$ and $Tr(\gamma) = -1$. The representation of these isomorphism classes is

$$\begin{aligned} E_1 :& y^2 = x^3 + x + 1, \\ E_2 :& y^2 = x^3 - x + \alpha, \\ E_3 :& y^2 = x^3 - x + \beta, \\ E_4 :& y^2 = x^3 - x + \gamma. \end{aligned}$$

Moreover, the isomorphism class of E_1 contains exactly $\frac{(q-1)\cdot q}{2}$ curves and each of the isomorphism class of E_2,E_3 and E_4 contains exactly $\frac{(q-1)\cdot q}{6}$ curves.

Secondly, we suppose that E is defined over $\mathbb{F}_q = \mathbb{F}_{3^n}$ where n is even. In this case, there are exactly 6 distinct isomorphism classes of elliptic curves over F_q. Let ξ be a primitive 4th root of unity in F_q and $\alpha, \beta \in F_q$ such that Tr($\xi\alpha$) $\neq 0$ and Tr($\frac{\xi\beta}{w^3}$) $\neq 0$.A complete list of representation of these isomorphism classes consists is

$$\begin{aligned}
E_1 :& y^2 = x^3 + x, \\
E_2 :& y^2 = x^3 + wx, \\
E_3 :& y^2 = x^3 + w^2x, \\
E_4 :& y^2 = x^3 + w^3x, \\
E_5 :& y^2 = x^3 + x + \alpha, \\
E_6 :& y^2 = x^3 + w^2x + \beta.
\end{aligned}$$

Moreover, each of the isomorphism class of E_1 and E_3 contains exactly $\frac{(q-1)\cdot q}{12}$ curves, each of the isomorphism class of E_2 and E_4 contains exactly $\frac{(q-1)\cdot q}{4}$ curves and each of the isomorphism class of E_5 and E_6 contains exactly $\frac{(q-1)\cdot q}{6}$ curves.

CHAPTER 4

GROUP STRUCTURE AND ISOGENY

4.1 Group Structure

We recall that for an elliptic curve E defined over a field K, Pic$^0(E) = $ Div$^0 E/\sim$ where $D_1 \sim D_2$ iff $D_1 - D_2 = $ div(f) for some $f \in \overline{K}(E)^*$. Moreover, Pic$^0_F(E) =$ Div$^0_F E/\sim$ for any field $K \subseteq F \subset \overline{K}$ if $D_i = \sum a_j(P)$ for $P \in E(F)$.Clearly, Picard group has an additive Abelian group structure and Pic^0_F is a subgroup of Pic$^0(E)$. We note that for E given by Weierstrass equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ where $a_i \in K$, and $\infty = [0 : 1 : 0]$ is an element in $E(K)$.

Theorem 7 (Canonical Form of $D \in$ Pic$_F(E)$)**.** *Let F be a field such that $K \subseteq F \subset \overline{K}$. Then for any $D \in$ Pic$^0_F(E)$, there exists a unique $P \in E(F)$ such that $D \simeq [P] - [\infty]$. [18]*

Proof. Let $D = D_1 - D_2$ and $D_1 = \sum_{i=1}^{r} m_i[P_i]$ and $D_2 = \sum_{j=1}^{s} k_j[Q_j]$ and $\sum_{i=1} m_i = \sum_{j=1} k_j = n.$

Firstly, we want to find D_1. Let $D_1 = [P_1] + [P_2] + [P_3] + \cdots$.

Say $l_1 = \overline{P_1P_2}$ is a line joining P_1 and P_2 in $F(E)$. This line cuts E at a unique point $R_1 \in E$ so we have $l_1 \cap E = \{P_1, P_2, R_1\}$. Then div$(l_1) = [R_1] + [P_1] + [P_2] - 3[\infty]$.

So we can rewrite D_1 such that

$$D_1 = (\text{div}(l_1) - [R_1] + 3[\infty]) + [P_3] + \cdots - n[\infty]$$

Now say $l_2 = \overline{R_1\infty}$ is a line joining R_1 and the point at infinity. $l_2 \cap E = \{R_1, R_2, \infty\}$.

Therefore, $\text{div}(l_2) = [R_1] + [R_2] + [\infty] - 3[\infty]$. So

$$D_1 = \text{div}(l_1) - (\text{div}(l_2) - R_2 - [\infty]) + P_3 + \cdots - n[\infty]$$
$$D_1 = [R_2] + [P_3] + \cdots + (n-1)[\infty] + \text{div}(\frac{l_1}{l_2})$$

When continuing this procedure by applying similar steps,we get

$$D_1 = [P] - [\infty] + \text{div}(l_i)$$

And similarly, we can get

$$D_2 = [Q] - [\infty] + \text{div}(l_j)$$

Therefore; $D = D_1 - D_2 = [P] - [Q] + \text{div}(\frac{l_i}{l_j})$.

Now say $S = [P] - [Q]$, we can rewrite S.

Let $l_3 = \overline{Q\infty}$ be a line joining Q and ∞, so

$$\text{div}(l_3) = [Q] + [\overline{Q}] - 2[\infty]$$

$$S = [P] + [\overline{Q}] - 2[\infty] - \text{div}(l_3)$$

Let $l_4 = \overline{P\overline{Q}}$ be a line joining P and $\overline{Q}$, so

$$\text{div}(l_4) = [P] + [\overline{Q}] + [R_3] - 3[\infty]$$
$$S = -[R_3] + [\infty] + \text{div}(\frac{l_4}{l_3})$$

Let $l_5 = \overline{R_3\infty}$ be a line joining R_3 and ∞, so

$$\text{div}(l_5) = [R_3] + [\overline{R_3}] - 2[\infty]$$
$$S = -[\overline{R_3}] - [\infty] + \text{div}(\frac{l_4}{l_3 l_5})$$

When we put S in the D, we get

$$D = [R] - [\infty] + \text{div}(g)$$

□

Remark: The algorithm given in the proof actually computes $f \in F(E)$ such that $D = [P] - [\infty] + \text{div}(f)$.

Let us do this in the following example.

Ex 4.1.1. Let E be an elliptic curve over $\mathbb{F}_{11}$ given by

$$y^2 = x^3 + 4x$$

and $P = (0, 0), Q = (2, 4), R = (4, 5)$ and $S = (6, 3)$ be points on E.Then $D = [P] + [Q] + [R] + [S] - 4[\infty]$.

The line joining P and Q is $l_1 : y - 2x = 0$. It is tangent to E at Q.

$$\text{div}(l_1) = [P] + 2[Q] - 3[\infty].$$

The line joining Q and ∞, that is vertical line through Q is $l_2 : x - 2 = 0$ and $E \cap l_2 = \{(2, 4), (2, -4), \infty\}$.

$$\text{div}(l_2) = [(2, 4)] + [(2, -4)] + [\infty] - 3[\infty].$$

Therefore, $D = [(2, -4)] + \text{div}(\frac{l_1}{l_2}) + [R] + [S] - 3[\infty]$.

Similarly, we have

$$[R] + [S] = [(2, 4)] + [\infty] + \text{div}(\frac{y + x + 2}{x - 2}).$$

Therefore, $D = [(2, -4)] + [(2, 4)] - 2[\infty] + \text{div}(\frac{y+x+2}{x-2}) + \text{div}(\frac{l_1}{l_2})$ which is

$$D = \text{div}(l_2) + \text{div}(\frac{y + x + 2}{x_2}) + \text{div}(\frac{l_1}{l_2})$$
$$D = \text{div}(\frac{(y - 2x)(y + x + 2)}{x - 2}) = \text{div}(g)$$

When the function g is simplified, we have $D = \text{div}(x^2 - y)$.

Fact: Let C be a smooth curve. If there exists a morphism $f : C \longrightarrow \mathbb{P}^1$ such that $\text{div}(f) = [P] - [Q]$, then f is an isomorphism, namely, $C \cong \mathbb{P}^1$.

The Canonical Form Theorem allows us to introduce an abelian group structure on $E(F)$ as follows:

$$\phi : E(F) \longrightarrow \text{Pic}^0_F(E)$$
$$P \longmapsto [P] - [\infty]$$

ϕ is one-to-one and onto map: Let $P, Q \in E(F)$ and $\phi(P) = \phi(Q)$ then $[P] - [\infty] \sim [Q] - [\infty]$. Therefore, $\text{div}(f) = [P] - [Q]$. So there exists f such that

$$f : E \longrightarrow \mathbb{P}^1$$

$$P \longmapsto 0$$

$$Q \longmapsto \infty$$

By the fact, f is an isomorphism so $E \cong \mathbb{P}^1$. Since E is genus 1 curve and $\mathbb{P}^1$ has genus 0, this is a contradiction. Thus ϕ map is 1-1 map.

Also, ϕ is onto map because of canonical form theorem. That is for all $D \in \text{Pic}_F(E)$, there exists a $P \in E$ such that $D \sim [P] - [Q]$.

1-1 and onto map $\phi : E(F) \longrightarrow \text{Pic}_F^0(E)$ introduces a unique group structure on $E(F)$. In this group, identity element corresponds to $\infty = [0 : 1 : 0]$ and the inverse of $P = (x_1, y_1)$ is unique $\overline{P} = (x_2, y_2) \in E(F)$.

1) Inverse: Given $P \in E(F)$, finding inverse of P, i.e., $\overline{P} \in E(F)$.

Let $P = [x : y : 1] \in E$ and E is given by the equation

$$E : Y^2Z + a_1XYZ + a_2YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

Assume that $l = \overline{P\infty}$ is a line joining P and ∞ such that $l : AX + BY + CZ = 0$. Since $P = [x_1 : y_1 : 1]$ and $\infty = [0 : 1 : 0]$ both on E and l, we can find $A = 1, B = 0$ and $C = x_1$. Therefore $l : X - x_1Z = 0$ and $\{P, \infty\} \in E \cap l$. Say $E \cap l = \{P, \overline{P}, \infty\}$. Then

$$\text{div}(l) = [P] + [\overline{P}] + [\infty] - 3[\infty]$$

$$\text{div}(l) - ([P] - [\infty]) = [\overline{P}] - [\infty]$$

Thus, $-([P] - [\infty]) \sim [\overline{P}] - [\infty]$ which means that inverse of P is $\overline{P}$. Now, we will calculate $\overline{P} = [x_2 : y_2 : 1]$.

Since $\overline{P} \in l$, we get $x_2 - x_1 = 0$. Thus $x_2 = x_1$.

Since $\overline{P} \in E : Y^2Z + a_1XYZ + a_2YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$ and $Z = 1$ and $X = x_1 = x_2, Y^2 + a_1x_1Y + a_3Y = x_1^3 + a_2x_1^2 + a_4x_1 + a_6 = c$ where c is a constant. Therefore, we get a polynomial of degree 2.

$$Y^2 + (a_1x_1 + a_3)Y + c = 0$$

Since the roots of polynomial are y_1 and y_2 we can conclude

$$y_1 + y_2 = -(a_1x_1 + a_3)$$

Thus , if $P = (x_1, y_1)$ then $\overline{P} = (x_2, y_2) = (x_1, -(a_1x_1 + a_3 + y_1))$.

Remark: We recall that the short Weierstrass equation of elliptic curves changes according to the characteristics of fields K where the curve is defined. Therefore;

i. If char$(K) \neq 2, 3$, then $E_1 : y^2 = x^3 + a_4x + a_6$. Let $P = (x, y) \in E_1$, then inverse of P is $\overline{P} = (x, -y)$ because $a_1 = a_3 = 0$.

ii. If char$(K) = 2$ then either $E_2 : y^2 + xy = x^3 + a_2x^2 + a_6$ or $E_3 : y^2 + a_3y = x^3 + a_4x + a_6$. For E_2, where $a_1 = 1$ and $a_3 = 0$, given any point $P = (x, y) \in E_2, \overline{P} = (x, -x - y) = (x, x + y)$ since char$(K) = 2$. For E_3, where $a_1 = 0$, given any $P = (x, y) \in E_3$, inverse is $\overline{P} = (x, -y - a_3) = (x, y + a_3)$.

iii. If char$(K) = 3$ then either $E_4 : y^2 = x^3+a_2x^2+a_6$ or $E_5 : y^2 = x^3+a_4x+a_6$. In both case, $a_1 = a_3 = 0$. Therefore, for any $P = (x, y) \in E_4$ or $P = (x, y) \in E_5$ we have $\overline{P} = (x, -y)$.

2) Point Addition: Given $P_1, P_2 \in E(F)$,finding $P_3 \in E(F)$ such that $P_3 = P_1 + P_2$.

Let $E : Y^2Z+a_1XYZ+a_3YZ^2 = X^3+a_2X^2Z+a_4XZ^2+a_6Z^3$ be an elliptic curve and $P_1 = [x_1 : y_1 : 1], P_2 = [x_2 : y_2 : 1] \in E$. We want to find $P_3 = [x_3 : y_3 : 1]$ such that $P_1 + P_2 = P_3$.

Assume l is a line joining P_1 and P_2. Then there is another point $R \in E \cap l$ such that $E \cap l = \{P_1, P_2, R\}$.

$$\text{div}(l) = [P_1] + [P_2] + [R] - 3[\infty]$$
$$\text{div}(l) - ([R] - [\infty]) = [P_1] + [P_2] - 2[\infty]$$

Thus, $[P_1] + [P_2] - 2[\infty] \sim -([R] - [\infty])$. It means $P_1 + P_2 = -R$. Now, let us to calculate $P_3 = -R$.

Since $P_1 = [x_1 : y_1 : 1]$ and $P_2 = [x_2 : y_2 : 1]$

$$\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} x_1 \\ y_1 \\ z_1 \end{bmatrix} + t \begin{bmatrix} x_1 - x_2 \\ y_1 - y_2 \\ 0 \end{bmatrix}$$

$$t = \frac{x - x_1}{x_1 - x_2} = \frac{y - y_1}{y_1 - y_2}.$$

Therefore, $l : \overline{P_1P_2} : (X - x_1)(y_1 - y_2) - (Y - y_1)(x_1 - x_2) = 0$

$$l : X(y_1 - y_2) + Y(x_2 - x_1) + x_1y_2 - x_2y_1$$

When we say $\lambda = \frac{(y_1-y_2)}{(x_1-x_2)}$ we get

$$Y = X\lambda + \frac{x_1y_2 - x_2y_1}{(x_1 - x_2)} = X\lambda + c$$

Since both $R \in l$ and $R \in E$ we can put y in the elliptic curve equation:

$$(X\lambda + c)^2 + a_1X(X\lambda + c) + a_3(X\lambda + c) = X^3 + a_2X^2 + a_4X + a_6$$
$$0 = -X^3 + (\lambda^2 + a_1\lambda - a_2)X^2 + (2\lambda c + a_1c + a_3c - a_4)X + (c^2 + a_3c - a_6)$$

Sum of roots of above equation is

$$x_1 + x_2 + x_3 = (\lambda^2 + a_1\lambda - a_2).$$

Therefore, $x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$.

Since $R = [x_3 : y_3 : 1] \in l$, R satisfies the equation

$$l : \overline{P_1P_2} : (x_3 - x_1)(y_1 - y_2) - (y_3 - y_1)(x_1 - x_2) = 0$$

$$(x_3 - x_1)(y_1 - y_2) = (y_3 - y_1)(x_1 - x_2)$$
$$y_3 = \frac{(x_3 - x_1)(y_1 - y_2)}{(x_1 - x_2)} + y_1$$

Therefore, $y_3 = \lambda(x_3 - x_1) + y_1$.

Remark: We can adopt $P_1 + P_2 = P_3 = -R$ according to the short Weierstrass equations:

i. If char$(K) \neq 2, 3$, $E_1 = y^2 = x^3 + a_4x + a_6$. For $P_1 = (x_1, y_1), P_2 = (x_2, y_2), P_1 + P_2 = P_3 = (x_3^{'}, y_3^{'})$ where $x_3^{'} = \lambda^2 - x_1 - x_2$ and $y_3^{'} = \lambda(x_1 - x_3^{'}) - y_1$

ii. If char$(K) = 2$ then either $E_2 : y^2 + xy = x^3 + a_2x^2 + a_6$ or $E_3 : y^2 + a_3y = x^3 + a_4x + a_6$. For $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$ on E_2 where $a_1 = 1, P_1 + P_2 =$

$P_3 = (x_3^{'}, y_3^{'})$ where $x_3^{'} = \lambda^2 + \lambda - a_2 - x_1 - x_2 = \lambda^2 + \lambda + x_1 + x_2 + a_2$ and $y_3^{'} = \lambda(x_1 + x_3^{'}) + y_1 + x_3$. On the other hand, for $P_1, P_2 \in E_3$, $P_1 + P_2 = P_3 = (x_3^{'}, y_3^{'})$ where $a_1 = a_2 = 0$ $x_3^{'} = \lambda^2 + x_1 + x_2$ and $y_3^{'} = (\lambda)(x_1 + x_3^{'}) + y_1 + a_3$.

iii. If char$(K) = 3$, then either $E_4 : y^2 = x^3 + a_2x^2 + a_6$ or $E_5 : y^2 = x^3 + a_4x + a_6$. For $P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in E_4$ where $a_1 = 0, P_1 + P_2 = P_3 = (x_3^{'}, y_3^{'}$ where $x_3^{'} = \lambda^2 - x_1 - x_2 - a_2$ and $y_3^{'} = \lambda(x_1 - x_3^{'}) - y_1$. On the other hand, on $E_5, x_3^{'} = \lambda^2 - x_1 - x_2$ for any given $P_1(x_1, y_1) + P_2(x_2, y_2) = P_3(x_3, y_3)$ where $P_1, P_2, P_3 \in E_5$ since $a_1 = a_2 = 0$ and $y_3^{'} = \lambda(x_1 - x_3^{'}) - y_1$.

3) Point Doubling: Given any $P_1 \in E(K)$ finding $2P_1 = P_2 \in E(K)$.

Let $E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ + a_6Z^3$ be an elliptic curve and $P_1 = [x_1 : y_1 : 1] \in E$. We want to find $P_2 = [x_2 : y_2 : 1]$ such that $2P_1 = P_2$.

Assume l is a tangent line to E on P_1. Then there is another point $R \in E \cap l$ such that $E \cap l = \{P_1, R\}$.

$$\text{div}(l) = [P_1] + [P_1] + [R] - 3[\infty]$$
$$\text{div}(l) - ([R] - [\infty]) = 2[P_1] - 2[\infty]$$

Thus, $2[P_1] - 2[\infty] \sim -([R] - [\infty])$ which implies $2P_1 = -R$. Now let us to calculate $P_2 = -R$.

Tangent line to E at P:

$$l : (a_1y_1 - 3x_1^2 - 2a_2x_1 - a_4)(X - x_1) + (2y_1 + a_1x_1 + a_3)(Y - y_1) = 0$$
$$l : Y = \frac{(3x_1^2 + 2a_2x_1 + a_4 - a_1y_1)(X - x_1)}{2y_1 + a_1x_1 + a_3} + y_1$$

When saying $\mu = \dfrac{(3x_1^2 + 2a_2x_1 + a_4 - a_1y_1)}{2y_1 + a_1x_1 + a_3}, l : Y = \mu(X - x_1) + y_1$.

For easy computation, firstly we compute Y^2:

$$Y^2 = \mu^2(X^2 - 2x_1X + x_1^2) + 2\mu y_1X - 2\mu x_1y_1 + y_1^2$$

Since $R \in E$, we put Y and $Z = 1$ into the E equation:

$E : \mu^2x^2 + (2\mu y_1 - 2\mu^2x_1)X + \mu^2x_1^2 - 2\mu x_1y_1 + y_1^2 + a_1(\mu(X - x_1) + y_1)X + a_3(\mu(X - x_1) + y_1) - X^3 - a_2X^2 - a_4X - a_6 = 0$
$-X^3 + (\mu^2 + a_1\mu - a_2)X^2 + (2\mu y_1 - 2\mu^2x_1 - a_1x_1 + y_1 + a_3\mu - a_4)X + c = 0$

Sum of roots of above equations

$$2x_1 + x_2 = \mu^2 + a_1\mu - a_2.$$

Therefore; $x_2 = \mu^2 - a_1\mu - a_2 - 2x_1$.That is

$$x_2 = (\frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3})^2 + a_1(\frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}) - a_2 - 2x_1.$$

Since $R \in l$, R satisfies the equation

$$l : y_2 = \mu(x_2 - x_1) + y_1.$$

Remark: We can adopt $2P_1 = -R = P_2(x_2', y_2')$ according to the short Weierstrass equations:

i. For char$(K) \neq 2, 3$, $E_1 = y_1^2 = x^3 + a_4x + a_6$. For $P_1 = (x_1, y_1) \in E_1, 2P_1 = P_2 = (x_2', y_2')$ on E where $a_1 = a_2 = a_3 = 0, x_2' = (\frac{3x_1^2+a_4}{2y_1})^2 - 2x_1$ and $y_2' = (\frac{3x_1^2+a_4}{2y_1}) - (x_1 - x_2') - y_1$.

ii. If char$(K) = 2$ then either $E_2 : y^2 + xy = x^3 + a_2x^2 + a_6$ or $E_3 : y^2 + a_3y = x^3 + a_4x + a_6$. For $P_1 = (x_1, y_1)$ on E_2 where $a_1 = 1, a_4 = a_3 = 0, 2P_1 = P_2(x_2', y_2')$ where $x_2' = (\frac{3x_1^2+2a_2x_1-y_1}{2y_1+x_1})^2 + (\frac{3x_1^2+2a_2x_1-y_1}{2y_1+x_1}) - a_2 - 2x_1$. Since char$(K) = 2$ we can rewrite x_2' such as $x_2' = (\frac{x_1^2+y_1}{x_1})^2 + (\frac{x_1^2+y_1}{x_1}) + a_2$ and $y_2' = (x_1 + \frac{y_1}{x_1})(x_1 + x_2) + y_1 + x_2 = x_1^2 + x_1x_2' + \frac{y_1}{x_1}x_2' + x_2'$. If $P_1 \in E_3$ where $a_1 = a_2 = 0$, then $x_3' = (\frac{3x_1^2+a_4}{2y_1+a_3})^2 - 2x_1$. Since char$(K) = 2$, $x_2' = (\frac{x_1^2+a_4}{a_3})^2$. and $y_2' = (\frac{x_1^2+a_4}{a_3})(x_1 + x_2') + y_1 + a_3$.

iii. If char$(K) = 3$ then either $E_4 : y^2 = x^3 + a_2x^2 + a_6$ or $E_5 : y^2 = x^3 + a_4x + a_6$. If $P_1(x_1, y_1) \in E_4$ where $a_1 = a_3 = a_4 = 0$ then $x_2' = (\frac{3x_1^2+2a_1x_1}{2y_1})^2 - a_2 - 2x_1$. Since char$(K) = 3$, $x_2' = (\frac{a_2x_1}{y_1})^2 + x_1 + a_2$ and $y_2' = (\frac{a_2x_1}{y_1})(x_1 - x_2') - y_1$. If $P_1 \in E_5$ where $a_1 = a_3 = a_2 = 0$, then $x_2' = (\frac{3x_1^2+a_4}{2y_1})^2 - 2x_1$. Since char$(K) = 3$, $x_2' = (\frac{a_4}{2y_1})^2 + x_1$ and $y_2' = (\frac{a_4}{2y_1})(x_1 - x_2') - y_1$.

To sum up, we can see all inverse, addition and doubling formulas according to character of K.

E:	$y^2 = x^3 + a_4x + a_6$	$y^2 + xy = x^3 + a_2x^2 + a_6$	$y^2 + a_3y = x^3 + a_4x + a_6$	$y^2 = x^3 + a_2x^2 + a_6$
P. Inverse	$(x, -y)$	$(x, x + y)$	$(x, y + a_3)$	$(x, -y)$
P. Addition	$x = \lambda^2 - x_1 - x_2$ $y = \lambda(x_1 - x) - y_1$	$x = \lambda^2 + \lambda + a_2 + x_1 + x_2$ $y = \lambda(x_1 + x) + y_1 + x$	$x = \lambda^2 + x_1 + x_2$ $y = \lambda(x_1 + x) + y_1 + a_3$	$x = \lambda^2 - x_1 - x_2 - a_2$ $y = \lambda(x_1 - x) - y_1$
P. Doubling	$x = (\frac{3x_1^2+a_4}{2y_1})^2 - 2x_1$ $y = (\frac{3x_1^2+a_4}{2y_1}) - (x_1 - x) - y_1$	$x = (\frac{x_1^2+y_1}{x_1})^2 + (\frac{x_1^2+y_1}{x_1}) + a_2$ $y = x_1^2 + x_1x + \frac{y_1}{x_1}x + x$	$x = (\frac{x_1^2+a_4}{a_3})^2$ $y = (\frac{x_1^2+a_4}{a_3})(x_1 + x) + y_1 + a_3$	$x = (\frac{a_2x_1}{y_1})^2 + x_1 + a_2$ $y = (\frac{a_2x_1}{y_1})(x_1 - x) - y_1$

Table 4.1: Point inverse, addition and doubling formulas

The map

$$\phi : E(F) \longrightarrow \text{Pic}_F^0(E)$$

is introduced a group structure on $E(F)$. Note that once we have an abelian group structure on $E(F)$ defined on above, then we can define the sum map:

$$\text{sum} : \text{Div}_F(E) \longrightarrow E(F)$$

as sum$(\sum a_i[P]) = \sum a_p P$, which is well-defined and group homomorphism.

This induces a group homomorphism

$$\text{sum} : \text{Div}_F^0(E) \longrightarrow E(F)$$

To able induce a group homomorphism on $\text{Pic}_F^0(E)$, we have to show that $\text{sum}(\text{div}(f)) = \infty$ for any $f \in F(E)^*$.

Proof. This is indeed the case as one can show by using arguments discussed above. Let D_1 and D_2 be two elements in $\text{Pic}_F^0(E)$. Therefore, $D_1 - D_2 = \text{div}(f)$ for some $f \in F(E)^*$.

From the proof of the canonical form of D, we see that

$$D_i = [P_i] - [\infty] + \text{div}(\prod_{i=1} l_i^{\pm 1})$$

where l means line. Then

$$D_1 - D_2 = [P_1] - [P_2] + \text{div}(\prod_j l_j^{\pm 1})$$

Since $E \ncong \mathbb{P}^1$, we know $P_1 = P_2$. Therefore,

$$\text{div}(f) = D_1 - D_2 = \text{div}(\prod_j l_j^{\pm 1}) = \text{div} \sum_j (\pm \text{div} l_j).$$

Due to the group structure on $E(F)$ we know that sum(div(l_j)) $= 0$. Thus,

$$\begin{aligned} \text{sum}(\text{div}(f)) &= \text{sum}(\sum_j \pm(\text{div} l_j)) \\ &= \sum \pm \text{sum}(\text{div} l_j) \\ &= \infty \end{aligned}$$

$\square$

Therefore, the inverse of $\phi : E(F) \longrightarrow \text{Pic}_F^0(E)$ is nothing but the

$$\text{sum} : \text{Pic}_F^0(E) \longrightarrow E(F)$$

$$\text{sum}(\sum a_i[P_i]) \longmapsto \sum a_i P$$

$$[P] - [\infty] \longmapsto P - \infty = P$$

4.2 Isogeny Between Elliptic Curves

We recall that for two varieties $V \subset \mathbb{P}^n(\bar{K})$ and $V' \subset \mathbb{P}^m(\bar{K})$, a rational map $\phi : V \to V'$ is $\phi = [f_0 : \ldots : f_m]$ such that for any $P \in V$, $\phi(P) = [f_0(P) : \ldots : f_m(P)]$ where all $f_i \in \bar{K}(V)^{m+1} \setminus \{0, \ldots, 0\}$ are defined and do not all vanish.

Let ϕ^* be a pull-back map $\phi^* : \bar{K}(E_2) \to \bar{K}(E_1)$ for two elliptic curves E_1 and E_2. Then the **degree of morphism** between elliptic curves, $\deg \phi$, is the degree of corresponding field extension $[K(E_1) : \phi^*(K(E_2))]$. We say $\deg \phi = 0$ if ϕ is constant. The map ϕ is separable if the corresponding field extension $K(E_1) \setminus \phi^*(K(E_2))$ is separable which means the minimal polynomial of any element has no multiple roots in algebraic closure.

Remark: If ϕ is a morphism with $\deg \phi = 1$, then ϕ is called isomorphism.

Let E be an elliptic curve and $P \in E$.

$$\begin{aligned} [-] :& E \to E \\ & P \to -P \end{aligned}$$

is an isomorphism.

Translation-by-Q map

$$\begin{aligned} t_Q : & E \to E \\ & P \to P + Q \end{aligned}$$

is an isomorphism for all $Q \in E$.

Multiplication-by-m map

$$\begin{aligned} [m] : & E \to E \\ & P \to P + \cdots + P \end{aligned}$$

is an morphism for all $m \in \mathbb{N}^*$.

Remark: A rational map between elliptic curves induces a group homomorphism if and only if it preserves the identity element.

Let $\phi : E_1 \to E_2$ be a morphism with $\phi(\infty) = \infty$. We know that there are maps $\psi_1 : E_1 \to \text{Pic}^0(E_1)$, push-forward map $\phi_* : \text{Pic}^0(E_1) \to \text{Pic}^0(E_2)$ and the sum map $\text{sum}_2 : \text{Pic}^0(E_2) \to E_2$. Since ψ_1, sum_2 and ϕ_* are all group homomorphisms, then

$$\phi : \text{sum}_2 \circ \phi_* \circ \psi_1$$

is also group homomorphism.

$$\begin{array}{rccc} \phi : & E_1 & \longrightarrow & E_2 \\ & \psi_1 \downarrow & & \uparrow sum_2 \\ \phi_* : & Pic^0(E_1) & \to & Pic^0(E_2) \end{array}$$

Figure 4.1

If $\phi : E_1 \to E_2$ is a morphism with $\phi(\infty) = \infty$, then ϕ is called **isogeny**. Two elliptic curves are called **isogenous** if there exists a non-constant isogeny between them.

Any morphism between elliptic curves $\psi : E_1 \to E_2$ can be written as $\psi : t_{\psi(\infty)} \circ \phi$ where $t_{\psi(\infty)}$ is translation map defined above and ϕ is an isogeny. In other word, $\phi : t_{-\psi(\infty)} \circ \psi$ is an isogeny for a morphism ψ.

We denote the set of isogenies from E_1 to E_2 by

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

If $E_1(K)$ and $E_2(K)$ are defined over a field K, then we have isogenies defined over K. We denote this case with $Hom_K(E_1, E_2)$.

Let $\phi : E_1 \to E_2$ be a nonconstant isogeny. We know that there are maps $\psi_2 : E_2 \to \text{Pic}^0(E_2)$, push-back map $\phi^* : \text{Pic}^0(E_2) \to \text{Pic}^0(E_1)$ and the sum map $\text{sum}_1 : \text{Pic}^0(E_1) \to E_1$.Since ψ_2, sum_1 and ϕ^* are all group homomorphisms, then

$$\hat{\phi} : \text{sum}_1 \circ \phi^* \circ \psi_2$$

is also group homomorphism. There is a basic fact that $\hat{\phi}$ is given by a rational map so we can say that $\hat{\phi} : E_2 \to E_1$ is an isogeny. The isogeny $\hat{\phi} : E_2 \to E_1$ satisfying

$$\begin{array}{cccc} \hat{\phi}: & E_2 & \longrightarrow & E_1 \\ & \psi_2 \downarrow & & \uparrow sum_1 \\ \phi^*: & Pic^0(E_2) & \rightarrow & Pic^0(E_1) \end{array}$$

Figure 4.2

$\hat{\phi} \circ \phi = [\deg \phi] = [m]$ is called **dual isogeny**.

Properties: Let $\phi : E_1 \to E_2$ be a nonconstant isogeny.

i. Dual isogeny $\hat{\phi} : E_2 \to E_1$ with the property $\hat{\phi} \circ \phi = [\deg \phi] = [m]$ is unique.

ii. Let $\lambda : E_2 \to E_3$ be another isogeny. Then

$$\widehat{\lambda \circ \phi} = \hat{\phi} \circ \hat{\lambda}$$

iii. Let $\psi : E_1 \to E_2$ be another isogeny. Then

$$\widehat{\phi + \psi} = \hat{\phi} + \hat{\psi}$$

iv. For all $m \in \mathbb{Z}$,

$$[\hat{m}] = [m]$$

and

$$\deg[\hat{m}] = \deg[m] = m^2$$

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

vi. $\hat{\hat{\phi}} = \phi$

Proof. i. Suppose that $\hat{\phi}$ and $\hat{\phi}'$ are two dual isogenies. Then

$$(\hat{\phi} - \hat{\phi}') \circ \phi = (\hat{\phi} \circ \phi) - (\hat{\phi}' \circ \phi) = [m] - [m] = [0]$$

Since ϕ is non-constant,$(\hat{\phi} - \hat{\phi}')$ must be constant. Thus, $\hat{\phi} = \hat{\phi}'$

ii. Let $n = \deg \lambda$. Then

$$(\hat{\phi} \circ \hat{\lambda}) \circ (\lambda \circ \phi) = \hat{\phi} \circ [n] \circ \phi = \hat{\phi} \circ \phi \circ [n] = [mn]$$

For the uniqueness statement

$$\hat{\phi} \circ \hat{\lambda} = \widehat{\lambda \circ \phi}$$

iii. See [15] page 83.

iv. This proof can be shown by induction.
By definition, we know that this is true for $m = 0$ and the situation is clear for $m = 1$. Now we assume this is true for $m - 1$, that is, $[m - 1] = \widehat{[m - 1]}$. Then using property (iii), we can write

$$[m] = [m - 1] + [1] = \widehat{[m - 1]} + \widehat{[1]} = \widehat{[m]}$$

Thus, $[m] = \widehat{[m]}$
Now let $\deg[m] = d$. Consider the multiplication-by-d map.

$$[d] = \widehat{[m]} \circ [m] = [m^2]$$

Since $Hom(E_1, E_2)$ is a torsion free Z-module, it follows that $d = m^2 = \deg[m]$

v. Let $m = \deg \phi$ then by property (iv) $m^2 = \deg[m] = \deg(\phi \circ \hat{\phi})$.So

$$m^2 = \deg(\phi \circ \hat{\phi}) = \deg(\phi) \circ \deg(\hat{\phi}) = m \deg(\hat{\phi})$$

Hence, $m = \deg(\hat{\phi})$ and $\deg(\phi) = \deg(\hat{\phi})$

vi. By definition and properties (i), (ii) and (iv)

$$\hat{\phi} \circ \phi = [m] = \widehat{[m]} = \widehat{\hat{\phi} \circ \phi} = \hat{\phi} \circ \hat{\hat{\phi}}$$

Thus, $\phi = \hat{\hat{\phi}}$.

□

Ex 4.2.1. Let char$(K) \neq 2$ and $a, b \in K$ with $b \neq 0$ and $r = a^2 - 4b \neq 0$. Consider E_1 and E_2 two elliptic curves

$$E_1 : y^2 = x^3 + ax^2 + bx,$$
$$E_2 : \bar{y}^2 = \bar{x}^3 - 2a\bar{x}^2 + r\bar{x}$$

let ϕ and $\hat{\phi}$ be two isogenies between E_1 and E_2

$$\phi : E_1 \to E_2$$
$$(x, y) \to (\frac{y^2}{x^2}, \frac{y(b - x^2)}{x^2})$$
$$\hat{\phi} : E_2 \to E_1$$
$$(\bar{x}, \bar{y}) \to (\frac{\bar{y}^2}{4\bar{x}^2}, \frac{\bar{y}(r - \bar{x}^2)}{8\bar{x}^2})$$

We can compute $\hat{\phi} \circ \phi = [2]$ on E_1 and $\phi \circ \hat{\phi} = [2]$ on E_2. Therefore, $\hat{\phi}$ and ϕ are examples of dual isogeny.

Let E be an elliptic curve and let $m \in \mathbb{N}^*$. The **m-torsion subgroup of E** which is denoted by $E[m]$ is the set of points of order m.

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

In other words, the set of m-torsion points of E is

$$E[m] = ker[m]$$

The **torsion subgroup of E** is the set of points of finite order.

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

If E is defined over K, then $E_{tors}(K)$ denotes the points of finite order in $E(K)$.

Remark: If m and n are coprime, then $E[mn] \simeq E[m] \times E[n]$

Theorem 8. *Let E be an elliptic curve over K and $m \in K^*$ so either char $(K) = 0$ or $p = char(K) > 0$ and $p \nmid m$. Then*

$$E[m] = \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}}$$

Let $E : y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6$ be an elliptic curve with $a_1, a_2, a_3, a_4, a_6 \in \bar{K}$ and $\sigma : a \to a^p$ be the Frobenius morphism. The **Frobenius morphism between elliptic curves** is

$$\begin{aligned}\Phi_p : & E \to E^\sigma \\ & (x, y) \to (x^p, y^p)\end{aligned}$$

where $E^\sigma : y^2 + a_1^p xy + a_3^p y = x^3 + a_2^p x^2 + a_4^p x + a_6^p$ is an elliptic curve over K. It is clear that $\Delta(E^\sigma) = \sigma(\Delta(E)) = \Delta(E)^p$ and $j(E^\sigma) = \sigma(j(E)) = j(E)^p$. Therefore, E^σ is nonsingular.

If $q = p^n$, then $\Phi_q = \Phi_p \circ \cdots \circ \Phi_p$

$$\begin{aligned}\Phi_q : & E \to E^{(\sigma)^n} \\ & (x, y) \to (x^q, y^q)\end{aligned}$$

Of course, the Frobenius map is a rational map and $\Phi(\infty) = \infty$. Therefore, the Frobenius map is an important isogeny.

If $K = \mathbb{F}_q$ where $q = p^n$, then $E^{(\sigma)^n} = E$ and Δ_q is the identity map on $E(\mathbb{F}_q)$ but it is not identity on E. In fact, $\Delta_q(P) = P$ iff P is $\mathbb{F}_q$-rational.

For a nonzero isogeny $\phi : E_1 \to E_2$, $ker\phi = \phi^{-1}(\infty)$.

Theorem 9. *Let $\phi : E_1 \to E_2$ be a nonzero isogeny. For every $Q \in E_2$*

$$\textit{number of} \quad \phi^{-1}(Q) = | \phi^{-1}(Q) | = \deg_s \phi.$$

Moreover, for every $P \in E_1$

$$e_\phi(P) = \deg_i \phi.$$

Proof. See [15] page 72. □

Corollary 1. *Let $\phi : E_1 \to E_2$ be a separable isogeny. Then ϕ is unramified. Moreover,* $\mid \phi^{-1}(\infty) \mid = \mid ker\phi \mid = \deg \phi$.

Remark: Frobenius morphism $\Phi_p : E \to E^\sigma$ is purely inseparable isogeny of degree p.

As Φ is injective map, $\mid ker\Phi \mid = 1$ and the ramification index $e_\Phi(Q) = p$ for every $Q \in E$. Although Φ is bijective, it is not an isomorphism because $\deg \Phi \neq 1$.

We recall that for any morphism between curves $\phi : C_1 \to C_2$, we have a unique factorization $\phi = \psi \circ \lambda$ where ψ is separable and λ is inseparable.

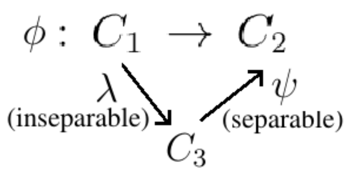

Figure 4.3

Also, we know $\deg(\phi) = \deg_s(\phi).\deg_i(\phi)$ where $\deg(\psi) = \deg_s(\phi)$ and $\deg(\lambda) = \deg_i(\phi)$ so $\deg(\phi) = \deg(\psi).\deg(\lambda)$.

Remark(*): For isogeny between elliptic curves $\phi : E_1 \to E_2$, this factorization is nothing but the following map $\phi = \psi \circ \Phi_q$ where $\Phi_q : E_1 \to E_1^{(\sigma)^n}$ and $\psi : E_1^{(\sigma)^n} \to E_2$.

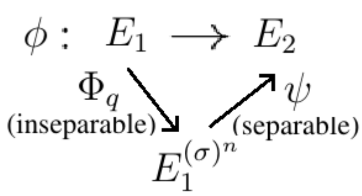

Figure 4.4

Note that when char$(K) = 0$, all maps are separable, so non-separable case occurs when char$(K) = p > 0$.

Let $\Phi_p : E \to E^\sigma$ be p-Frobenius isogeny. Then

$$V_p : E^\sigma \to E$$

is the dual of the Frobenius isogeny.

By definition of dual isogeny, we know $\hat{\phi} \circ \phi = [\deg \phi] = [m]$. Therefore, $V_p \circ \Phi_p = [\deg \Phi_p] = [p]$. Since $\deg[p] = p^2$, we conclude that $\deg V_p = p$ by multiplicativity of degree.

We have two different cases about V_p.

1. V_p is separable.
   This case is ordinary case. The elliptic curves such that such that V_p is separable where $V_p : E^\sigma \to E$ is called **ordinary elliptic curves**.

2. V_p is not separable.
   Then there exists an isogeny ψ such that $V_p = \psi \circ \Phi_p$ like remark(*)4.2. When we look the degree of ψ, we see $\deg \psi = 1$ so ψ is an isomorphism. Therefore, V_p is injective and so $[p] = V_p \circ \Phi_p = \psi \circ \Phi_p \circ \Phi_p$ is also injective. Thus, $ker[p] = \{\infty\}$. The elliptic curves such that V_p is not separable is called **supersingular elliptic curves**.

Corollary 2. *Let E be an elliptic curve over K with char$(K) = p > 0$, then either $E[p] = \{\infty\}$ or $E[p] \simeq \mathbb{Z}_p$.*

Proof. Let Φ_p be the p-Frobenius morphism. We know

$$E[p] = \{Q \in E : pQ = \infty\} \quad and \quad \mid \phi^{-1}(Q) \mid = \deg_s \phi$$

Therefore, $\mid E[p] \mid = \deg_s[p]$.

By definition, $\deg_s[p] = \deg_s(\Phi_p \circ V_p)$. Since Φ_p is purely inseparable, $\deg_s(\Phi_p \circ V_p) = \deg_s(V_p)$.

1. If V_p is separable, we know $\deg_s(V_p) = p$. It means $\mid E[p] \mid = p$. Thus, $E[p] \simeq \mathbb{Z}_p$.

2. If V_p is not separable, then $\deg_s(V_p) = 1$.Therefore, $\mid E[p] \mid = 1$. Thus, $E[p] = \{\infty\}$.

□

We can categorize the elliptic curves according to the $E[p]$. If $E[p] \simeq \mathbb{Z}_p$, then we call ordinary elliptic curves. If $E[p] = \{\infty\}$, then E is called supersingular elliptic curves.

Remark: If Φ_q is q-Frobenius map where $q = p^n$, then $E[q = p^n] = \{\infty\}$ for supersingular elliptic curves and $E[q] \simeq \mathbb{Z}_q$ for ordinary elliptic curves.

4.3 Endomorphism Ring of Elliptic Curves and Hasse's Theorem

Let E be an elliptic curve over a field K. A homomorphism $\alpha : E \to E$ given by rational function is called **endomorphism**. In other words, if α is an endomorphism then

- $\alpha(\infty) = \infty$
- $\alpha(P + Q) = \alpha(P) + \alpha(Q)$ for $P, Q \in E$
- There are rational functions $R_1(x, y)$ and $R_2(x, y)$ with coefficients in $\bar{K}$ such that
  $\forall P(x, y) \in E$, $\alpha(x, y) = (R_1(x, y), R_2(x, y))$

In the last section, we denoted the set of isogenies from E_1 to E_2 by $Hom(E_1, E_2)$. If $E = E_1 = E_2$, then

$$Hom(E, E) = End(E)$$

$End(E)$ denotes the set of all endomorphism of E. $End(E)$ is the ring under the following addition and multiplication laws which is composition. For all $\phi, \psi \in End(E)$, define

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

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

for all $P \in E$.

$End(E)$ is called **endomorphism ring** of E.

If we study the endomorphisms of $E(K)$, we restrict our attention to endomorphisms defined over K which are denoted by $End_K(E)$.

Ex 4.3.1. Let $P = (x, y) \in E$ and E be given by $E : y^2 + y = x^3 + x + 1$ over K where char$(K) = 2$.

$$\begin{aligned} \alpha :& E \to E \\ & P \to 2P \end{aligned}$$

$\alpha(P) = [2] = (R_1(P), R_2(P))$ where

$$\begin{aligned} R_1(x, y) &= (x^2 + 1)^2 \\ R_2(x, y) &= (x^2 + 1)(x + R_1(x, y)) + y + 1 \end{aligned}$$

Of course $\alpha(\infty) = \infty$ and $\alpha(P + Q) = \alpha(P) + \alpha(Q)$ for all $P, Q \in E$. Also, α is given by rational functions $R_1(x, y)$ and $R_2(x, y)$. Thus, we can conclude that α is an endomorphism . Moreover, by definition $\deg(\alpha) = \deg([2]) = 4$.

Remark: The map

$$\begin{aligned} \mathbb{Z} &\to End(E) \\ m &\to [m] \end{aligned}$$

is an injective ring homomorphism. This implies that End (E) is characteristic zero ring. If $\alpha\beta = 0$ for any $\alpha, \beta \in End(E)$, then either $\alpha = 0$ or $\beta = 0$. Indeed, $\deg(\alpha\beta) = \deg(\alpha)\deg(\beta)$ and $\alpha = 0$ iff $\deg(\alpha)$=0.

Similar to isogenies, we have the following properties for $\phi, \psi \in End(E)$

(i) $\deg(\phi\psi) = \deg(\phi)\deg(\psi)$,

(ii) $\deg_s(\phi\psi) = \deg_s(\phi)\deg_s(\psi)$,

(iii) $\deg_i(\phi\psi) = \deg_i(\phi)\deg_i(\psi)$.

Let $P, Q \in E$ and $\phi \in End(E)$. Then $\mid \phi^{-1}(Q) \mid = \mid ker(\phi) \mid$ and if ϕ is separable $\mid ker(\phi) \mid = \deg\phi$. Otherwise, $\mid ker(\phi) \mid = \deg_s\phi < \deg\phi$.

In particular, $\phi\psi$ is separable if and only if both ϕ and ψ are separable.

Let V be a vector space over a field $\mathbb{F}$. A **bilinear form** B on V is a function of two variables $V \times V \to \mathbb{F}$ which satisfies

- $B(v_1 + v_2, w) = B(v_1, w) + B(v_2, w)$,
- $B(v, w_1 + w_2) = B(v, w_1) + B(v, w_2)$,
- $B(av, w) = aB(v, w) \quad \forall a \in \mathbb{F}$,
- $B(v, aw) = aB(v, w) \quad \forall a \in \mathbb{F}$.

Let A be an abelian group. A function

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

is **quadratic form**, if it satisfies

- $d(\alpha) = d(-\alpha), \quad \forall \alpha \in A$,
- $A \times A \to \mathbb{R}$
  $(\alpha, \beta) \to d(\alpha + \beta) - d(\alpha) - d(\beta)$
  is bilinear.

A quadratic form d is **positive definite** if it satisfies

- $d(\alpha) \geq 0 \quad \alpha \in A$,
- $d(\alpha) = 0$ iff $\alpha = 0$.

Theorem 10. *Let E be elliptic curve. The degree map*

$$\deg : End(E) \to \mathbb{R}$$

is positive definite quadratic form.

Proof. $\deg(-\alpha) = \deg([-1] \circ \alpha) = \deg([-1]) \deg(\alpha) = \deg(\alpha)$ Also, we know that $\deg(\alpha) = 0$ iff $\alpha = 0$ and $\deg(\alpha) \geq 0$ for all $\alpha \in End(E)$. Therefore, the only thing to prove is

$$\langle \phi, \psi \rangle = \deg(\phi + \psi) - \deg(\phi) - \deg(\psi)$$

is bilinear.

Both sides are integer so we can look at their action E [] : $\mathbb{Z} \to End(E)$ and compute

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

Therefore,

$$\begin{aligned}
[\langle (\phi_1 + \phi_2), \psi \rangle] &= (\hat{\psi} \circ (\phi_1 + \phi_2)) + ((\widehat{\phi_1 + \phi_2}) \circ \psi) \\
&= (\hat{\psi} \circ \phi_1) + (\hat{\psi} \circ \phi_2) + (\hat{\phi}_2 \circ \psi) + (\hat{\phi}_1 \circ \psi) \\
&= (\hat{\psi} \circ \phi_1) + (\hat{\phi}_1 \circ \psi) + (\hat{\psi} \circ \phi_2) + (\hat{\phi}_2 \circ \psi) \\
&= [\langle \phi_1, \psi \rangle] + [\langle \phi_2, \psi \rangle]
\end{aligned}$$

Similarly, we can show $[\langle \phi, (\psi_1 + \psi_2) \rangle] = [\langle \phi, \psi_1 \rangle] + [\langle \phi, \psi_2 \rangle]$ and $[\langle m\phi, n\psi \rangle] = mn[\langle \phi, \psi \rangle]$ for all $m, n \in \mathbb{Z}$ and $\phi, \psi \in End(E)$.

Thus, degree map is positive definite quadratic form. □

Corollary 3. *(Parallelogram Identity) Let* $\alpha, \beta \in End(E)$. *Then we have*

$$\deg(\alpha + \beta) + \deg(\alpha - \beta) = 2\deg(\alpha) + 2\deg(\beta)$$

Proof. We know $\langle \alpha, \beta \rangle = \deg(\alpha + \beta) - \deg(\alpha) - \deg(\beta)$ is bilinear. Therefore, the equality $\langle \alpha, -\beta \rangle = -\langle \alpha, \beta \rangle$ holds and this equality is nothing but the parallellogram identity.

$$\begin{gathered}
\langle \alpha, -\beta \rangle = -\langle \alpha, \beta \rangle \\
\deg(\alpha - \beta) - \deg(\alpha) - \deg(-\beta) = -(\deg(\alpha + \beta) - \deg(\alpha) - \deg(\beta)) \\
\deg(\alpha + \beta) + \deg(\alpha - \beta) = 2\deg(\alpha) + 2\deg(\beta)
\end{gathered}$$

□

We know the degree of the multiplication by m map is $\deg([m]) = m^2$ as a property and we proved it in Section 4.2. Now we can prove this property in a easier way:

Proof. We can prove this property by induction. Clearly, this is true for $m = 0, \pm 1, \pm 2$. That is one can show easily $\deg([0]) = 0$,$\deg([\pm 1]) = 1$ and $\deg([2]) = 4$ using point addition formulas in Chapter 3.

Now assume $\deg([n]) = n^2$ is true for all $1 \leq n \leq m$.

Since $\deg([n+1]) + \deg([n-1]) = 2\deg([n]) + 2\deg([1])$ by Corollary3 and $\deg([n+1]) + (n-1)^2 = 2(n)^2 + 2.1^2$ by induction step, we get $\deg([n+1]) = 2(n)^2 + 2 - (n-1)^2 = (n+1)^2$.

Hence, we can conclude that $\deg([m]) = m^2$ for any $m \in \mathbb{Z}$. □

Let $\alpha, \beta \in End(E)$. We define

$$(\alpha, \beta) : End(E) \times End(E) \to \mathbb{Q}$$
$$(\alpha, \beta) = \frac{1}{2}\langle \alpha, \beta \rangle = \frac{1}{2}(\deg(\alpha + \beta) - \deg(\alpha) - \deg(\beta))$$

Proposition 3. *(α, β) is a positive definite symmetric bilinear form.*

Proof. $(\alpha, \beta) = (\beta, \alpha)$ symmetric bilinear form because $\langle \alpha, \beta \rangle$ is bilinear. Moreover,

$$\begin{aligned}(\alpha, \alpha) &= \frac{1}{2}\deg(\alpha + \alpha) - \deg(\alpha) - \deg(\alpha) \\ &= \frac{1}{2}(\deg[2]\deg(\alpha) - 2\deg(\alpha)) \\ &= \frac{1}{2}(4\deg(\alpha) - 2\deg(\alpha)) \\ &= \deg(\alpha)\end{aligned}$$

Hence, $(\alpha, \alpha) = \deg(\alpha) \geq 0$ □

Proposition 4. *Let $\alpha, \beta \in End(E)$. Then $\forall m, n \in \mathbb{Z}$*

$$\deg(m\alpha + n\beta) = m^2\deg(\alpha) + 2mn(\alpha, \beta) + n^2\deg(\beta)$$

Proof.

$$\begin{aligned}\deg(m\alpha + n\beta) &= (m\alpha + n\beta, m\alpha + n\beta) \\ &= (m\alpha, m\alpha + n\beta) + (n\beta, m\alpha + n\beta) \\ &= (m\alpha, m\alpha) + (m\alpha, n\beta) + (n\beta, m\alpha) + (n\beta, n\beta) \\ &= m^2 \deg(\alpha) + 2mn(\alpha, \beta) + n^2 \deg(\beta)\end{aligned}$$

□

Corollary 4. *(Cauchy-Schwartz) Let* $\alpha, \beta \in End(E)$*, then* $(\alpha, \beta)^2 \leq \deg(\alpha)\deg(\beta)$

Proof. If $\alpha = 0$ or $\beta = 0$, both sides of inequality are zero and there is nothing to prove. Otherwise, consider the map

$$\begin{aligned}&\mathbb{Z} \times \mathbb{Z} \to \mathbb{Q} \\ &(m, n) \to \deg(m\alpha + n\beta)\end{aligned}$$

We know $\deg(m\alpha+n\beta) = m^2 \deg(\alpha)+2mn(\alpha, \beta)+n^2 \deg(\beta)$ is symmetric bilinear form given by the matrix

$$M := \begin{bmatrix} \deg(\alpha) & (\alpha, \beta) \\ (\alpha, \beta) & \deg(\beta) \end{bmatrix}$$

This is positive definite if and only if the form

$$\begin{aligned}&\mathbb{Q} \times \mathbb{Q} \to \mathbb{Q} \\ &(x, y) \to (x, y).M(x, y)^T\end{aligned}$$

is positive definite.

Thus, its discriminant $\deg(\alpha)\deg(\beta) - (\alpha, \beta)^2$ must be positive

$$\begin{aligned}\deg(\alpha)\deg(\beta) - (\alpha, \beta)^2 > 0 \\ \deg(\alpha)\deg(\beta) > (\alpha, \beta)^2\end{aligned}$$

□

Let $\alpha \in End(E)$. **Trace of** α is denoted by $tr(\alpha) \in \mathbb{Z}$ and given by $tr(\alpha) = 1 + \deg\alpha - \deg([1] - \alpha)$.

Note that by parallelogram identity

$$tr(\alpha) = 1 + \deg\alpha - \deg([1] - \alpha) = \deg(\alpha + 1) - \deg\alpha - 1$$

Hence, we can write $tr(\alpha) = 2(\alpha, 1) = \deg(\alpha + 1) - \deg\alpha - 1$

Theorem 11. *Let $\alpha \in End(E)$. Then α satisfies the following relation*

$$\alpha \circ \alpha - [tr(\alpha)] \circ \alpha + [\deg(\alpha)] = 0$$

We will use the short form of this relation $\alpha^2 - tr(\alpha)\alpha + \deg(\alpha) = 0$, or $\alpha^2 - t\alpha + d = 0$.

The polynomial $X^2 - tX + d$ is called the **characteristic polynomial of** α.

Proof. To show $\alpha^2 - t\alpha + d = 0$, it is enough to prove $\deg(\alpha^2 - t\alpha + d) = 0$.

$$\begin{aligned}
&\deg(\alpha^2 - t\alpha + d) = (\alpha^2 - t\alpha + d, \alpha^2 - t\alpha + d)\\
&= (\alpha^2, \alpha^2 - t\alpha + d) - (t\alpha, \alpha^2 - t\alpha + d) + (d, \alpha^2 - t\alpha + d)\\
&= (\alpha^2, \alpha^2) - (\alpha^2, t\alpha) + (\alpha^2, d) - (t\alpha, \alpha^2) + (t\alpha, t\alpha) - (t\alpha, d) + (d, \alpha^2) - (d, t\alpha) + (d, d)\\
&= (\alpha^2, \alpha^2) - 2(\alpha^2, t\alpha) + 2(\alpha^2, d) + (t\alpha, t\alpha) - 2(t\alpha, d) + (d, d)\\
&= (\alpha^2, \alpha^2) + t^2(\alpha, \alpha) + d^2 - 2t(\alpha^2, \alpha) + 2d(\alpha^2, 1) - 2td(\alpha, 1)\\
&= \deg(\alpha^2) + t^2\deg(\alpha) + d^2 - 2t(\alpha^2, \alpha) + 2d(\alpha^2, 1) - 2td(\alpha, 1)\\
&= d^2 + t^2\deg(\alpha) + d^2 - 2t(\alpha^2, \alpha) + 2d(\alpha^2, 1) - 2td(\alpha, 1)\\
&= 2d^2 + t^2 d - 2t(\alpha^2, \alpha) + 2d(\alpha^2, 1) - t^2 d\\
&= 2d^2 - 2t(\alpha^2, \alpha) + 2d(\alpha^2, 1)
\end{aligned}$$

Firstly, we will compute (α^2, α)

$$\begin{aligned}
(\alpha^2, \alpha) &= \frac{1}{2}(\deg(\alpha^2 + \alpha) - \deg(\alpha^2) - \deg(\alpha))\\
&= \frac{1}{2}(\deg(\alpha)\deg(\alpha + 1) - \deg(\alpha^2) - \deg(\alpha))\\
&= \frac{1}{2}\deg(\alpha)(\deg(\alpha + 1) - \deg(\alpha) - 1)\\
&= \deg(\alpha)(\alpha, 1)
\end{aligned}$$

So, $(\alpha^2, \alpha) = 2\deg(\alpha)(\alpha, 1) = td$.

Secondly, we will compute $2d(\alpha^2, 1) = -2d(\alpha^2, -1)$

$$\begin{aligned} 2(\alpha^2, -1) &= \deg(\alpha^2 - 1) - \deg(\alpha^2) - \deg(-1) \\ &= \deg(\alpha - 1)\deg(\alpha + 1) - \deg(\alpha)^2 - 1 \\ &= (\deg(\alpha) + 2(\alpha, 1) + 1)(\deg(\alpha) - 2(\alpha, 1) + 1) - d^2 - 1 \\ &= (d + t + 1)(d - t + 1) - d^2 - 1 \\ &= d^2 - td + d + td - t^2 + t + d - t + 1 - d^2 - 1 \\ &= 2d - t^2 \end{aligned}$$

When we replace back, we get

$$\begin{aligned} \deg(\alpha^2 - t\alpha + d) &= 2d^2 - 2t(\alpha^2, \alpha) - 2d(\alpha^2, -1) \\ &= 2d^2 - t(td) - d(2d - t^2) \\ &= 2d^2 - t^2 d - 2d^2 + dt^2 \\ &= 0 \end{aligned}$$

□

Remark: Let E be an elliptic curve defined over $\mathbb{F}_q$. We know Frobenius endomorphism Φ_q is purely inseparable map. For $m, n \in \mathbb{Z}$, $[m] + [n] \circ \Phi_q : E \to E$ is separable if and only if $p \nmid m$.

Corollary 5. *Let E be elliptic curve over $\mathbb{F}_q$. Then $E(\mathbb{F}_q) = ker(\Phi_q - 1)$ and $\mid E(\mathbb{F}_q) \mid = \deg(\Phi_q - 1)$*

Proof. Let $P = (x, y) \in E(\mathbb{F})$. Then

$$\begin{aligned} (x^q, y^q) = (x, y) &\longleftrightarrow \Phi_q(P) = P \\ &\longleftrightarrow (\Phi_q - 1)(P) = 0 \\ &\longleftrightarrow P \in ker(\Phi_q - 1) \end{aligned}$$

Therefore, $E(\mathbb{F}_q) = ker(\Phi_q - 1)$. By the above remark we know that $(\Phi_q - 1)$ is separable. Thus,

$$\mid E(\mathbb{F}_q) \mid = \mid ker(\Phi_q - 1) \mid = \deg_s(\Phi_q - 1) = \deg(\Phi_q - 1)$$

□

Let E be an elliptic curve. It is very important to know the number of points of E for cryptographic applications.

Theorem 12 (Hasse's Inequality). *Let $\mathbb{F}_q$ be the finite field with $q = p^n$ elements for a prime p and E be the elliptic curve over $\mathbb{F}_q$. Then we have*

$$-2\sqrt{q} \leq \mid E(\mathbb{F}_q) \mid -(q+1) \leq 2\sqrt{q}$$

Proof. Let Φ_q be Frobenius endomorphism

$$\Phi_q : E \to E$$
$$(x, y) \to (x^q, y^q)$$

where $\deg(\Phi_q) = q$
By Corollary 5, $\mid E(\mathbb{F}_q) \mid = \deg(\Phi_q - 1)$.
By Proposition 4.3, $\deg(\Phi_q - 1) = \deg(\Phi_q) - 2(\Phi_q, 1) + 1 = q + 1 + 2(\Phi_q, 1)$
So $\mid E(\mathbb{F}_q) \mid = q + 1 + 2(\Phi_q, 1)$.
By Ccorollary 4, $(\Phi_q, 1)^2 \leq \deg \Phi_q \cdot \deg 1 = q$.
Therefore, $\mid (\Phi_q, 1) \mid \leq \sqrt{q}$
Since $\mid E(\mathbb{F}_q) \mid = q + 1 + 2(\Phi_q, 1)$, we get $\mid\mid E(\mathbb{F}_q) \mid -(q+1) \mid \leq 2\sqrt{q}$. □

Thus, for an elliptic curve over $\mathbb{F}_q$, Hasse's theorem gives a bound for the number of rational points on E

$$q + 1 - 2\sqrt{q} \leq \mid E(\mathbb{F}_q) \mid \leq q + 1 + 2\sqrt{q}$$

Ex 4.3.2. Let E be an elliptic curve over $\mathbb{F}_{11}$. Then the Hasse's inequality implies that

$$11 + 1 - 2\sqrt{11} \leq \mid E \mid \leq 11 + 1 + 2\sqrt{11}$$
$$4 < \mid E \mid < 20$$

We see $\Delta_\alpha(X) = X^2 - tr(\alpha)X + d$ is the characteristic polynomial of endomorphism α. When $\alpha = \Phi_q \in End(E)$, then $\Delta(X) = X^2 - tr(\Phi_q)X + q$ is the characteristic polynomial of Frobenius map of E defined over $\mathbb{F}_q$.

Corollary 6. *For a elliptic curve $E(\mathbb{F}_q)$ and Frobenius map Φ_q of $E(\mathbb{F}_q)$,*

$$tr(\Phi_q) = q + 1 - \mid E(\mathbb{F}_q) \mid$$

and

$$-2\sqrt{q} \le tr(\Phi_q) \le 2\sqrt{q}\sqrt{q}$$

Proof. From the proof of Hasse's inequality, we know that

$$\mid E(\mathbb{F}_q) \mid = \deg(\Phi_q - 1) = q + 1 - 2(\Phi_q, 1)$$

Thus, $tr(\Phi_q) = 2(\Phi_q, 1) = q + 1 - \mid E(\mathbb{F}_q) \mid$

By Hasse's inequality, we know

$$q + 1 - 2\sqrt{q} \le \mid E(\mathbb{F}_q) \mid \le q + 1 + 2\sqrt{q}$$

Hence, $-2\sqrt{q} \le tr(\Phi_q) \le 2\sqrt{q}\sqrt{q}$ □

Proposition 5. *Let $\alpha \in End(E)$. For an integer $k \ge 1$,*

$$tr(\alpha^{k+2}) = tr(\alpha)tr(\alpha^{k+1}) - \deg(\alpha)tr(\alpha^k)$$

where $\alpha^m \in End(E)$ and $\alpha^m = \alpha \circ \cdots \circ \alpha$ (m times).

Proof. We know that $\Delta_\alpha(X) = X^2 - tr(\alpha)X + \deg(\alpha)$. Then $\Delta_{\alpha^m}(X) = X^2 - tr(\alpha^m)X + \deg(\alpha^m)$. For any prime $l \neq p$, we have α_l and α_{l^m} linear maps on $\mathbb{Z}_l^2$.

If $M \in M_2(K)$ elementary computation enough to show

$$tr(M^{k+2}) = tr(M)tr(M^{k+1}) - det(M)tr(M^k)$$

with $tr(M^0) = 2$ and $M^0 = Id$.

Since $tr(\alpha^m) \mod l = tr(\alpha_l^m)$ and $det(\alpha^m) \mod l = det(\alpha_l^m)$ for infinitely many primes l, we get the result

$$tr(\alpha^{k+2}) = tr(\alpha)tr(\alpha^{k+1}) - \deg(\alpha)tr(\alpha^k)$$

for every $k = 1, 2, \cdots$ with $tr(\alpha) = 2(\alpha, 1)$ and $tr(\alpha^0) = 2$ □

Corollary 7. *Let $\Phi_q \in End(E)$ and t_k be the trace of $\Phi_{q^k} = (\Phi_q)^k$. Then*

$$t_k = tr(\Phi_q)^k = (\Phi_{q^k}) = q^k + 1 - \mid E(\mathbb{F}_{q^k}) \mid$$

and

$$t_k = t \cdot t_{k-1} - q \cdot t_{k-2}$$

Proof. It is easy result of the Proposition 4.3. □

This corollary allows to compute $\mid E(\mathbb{F}_{q^k}) \mid = q^k + 1 - t_k$ very efficiently as soon as $E(\mathbb{F}_{q^k})$ is known.

Corollary 8. *The elliptic curve E over $\mathbb{F}_q$ is supersingular if and only if $p \mid tr(\Phi_q)$*

Proof. Assume E is supersingular. Then $V_q = \hat{\Phi}_q = (isomorphism) \circ \Phi_q$ and $[q] = V_q \circ \Phi_q = (isomorphism) \circ \Phi_q \circ \Phi_q$ so $\Phi_q^2 = \psi \circ [q]$ where ψ is an isomorphism Characteristic polynomial is $\Phi_q^2 - tr(\Phi_q)\Phi_q + q = 0$. So

$$\begin{aligned} \Phi_q^2 + q &= tr(\Phi_q)\Phi_q \\ \psi \circ [q] + [q] &= tr(\Phi_q)\Phi_q \\ (\psi + 1)q &= tr(\Phi_q)\Phi_q \end{aligned}$$

When we look the degrees both sides

$$\begin{aligned} mq^2 &= [tr(\Phi_q)].q \\ mq^2 &= (tr(\Phi_q))^2.q \\ mq &= (tr(\Phi_q)) \end{aligned}$$

So $q \mid tr(\Phi_q)^2$ and thus $p \mid tr(\Phi_q)$.

Conversely, if $p \mid tr(\Phi_q)$, then $tr(\Phi_q) = k.p$ for some $k \in \mathbb{Z}$. Characteristic polynomial is

$$\begin{aligned} \Phi_q^2 - [k][p]\Phi_q + [q] &= 0 \\ \Phi_q^2 &= [k][p]\Phi_q - q \end{aligned}$$

We know $\Phi_q^2(P) = \infty$ for $P \in E$. But Φ_q is bijective. Therefore, $P = \infty$. So $E[p] = \{\infty\}$. Hence, E is supersingular curve. □

Corollary 9. *E is supersingular elliptic curve over $\mathbb{F}_p$ with $p \geq 5$ if and only if $tr(\Phi_p) = 0$. Then $\mid E(\mathbb{F}_p) \mid = p + 1$.*

Proof. E is supersingular elliptic curve over $\mathbb{F}_p$ if and only if $p \mid tr(\Phi_q)$ by Corollary 8.If $p \geq 5$ and $tr(\Phi_p) \neq 0$, then $\mid tr(\Phi_p) \mid \geq p$ but $\mid tr(\Phi_p) \mid \leq 2\sqrt{p}$ by Hasse's inequality. Therefore, $p \leq 2\sqrt{p}$ so $p \leq 4$. This contradict to $p \geq 5$ so $tr(\Phi_p) = 0$. By Corollary 6, $tr(\Phi_q) = q + 1- \mid E(\mathbb{F}_q) \mid$. Thus, $\mid E(\mathbb{F}_p) \mid= p + 1$. □

Remark: As we see in Theorem11, every $\alpha \in End(E)$ is at worst quadratic over $\mathbb{Z}$: It satisfies the quadratic equation $X^2 - tX + d$.
The above remark forces $End(E) = R$ where $\mathbb{Z} \subseteq End(E) = R \subseteq \bar{K}$.
If char$(K) = 0$, R is either rank 1 or R is of rank 2. Namely,

$$End(E) = \begin{cases} \mathbb{Z}, \\ \mathbb{Z} \times \mathbb{Z} = \mathbb{Z}[\alpha]. \end{cases}$$

Note that R is torsion free; that is,

$$\begin{aligned} \alpha^m = 0 \leftrightarrow \deg(\alpha^m) = 0 \leftrightarrow \deg(\alpha) = 0 \leftrightarrow \alpha = 0 \\ \leftrightarrow m\alpha = 0 \leftrightarrow \deg(m\alpha) = 0 \leftrightarrow \deg[m]\deg(\alpha) = 0 \\ \leftrightarrow m^2 \deg(\alpha) = 0 \leftrightarrow m = 0 \text{ or } \alpha = 0 \end{aligned}$$

If rank$(R) = 2$, then $R = \mathbb{Z}[\alpha]$ so endomorphism ring is an order in an imaginary quadratic filed. This case is CM-case(Complex Multiplication Case).

Thus, endomorphism ring of elliptic curves over K where char$(K) = 0$ is isomorphic to either $\mathbb{Z}$ or an order in an imaginary quadratic filed $R = \mathbb{Z}[\alpha] \subset \mathbb{Q}\sqrt{-D}$ where $D > 0$ is an integer and α satisfies the monic polynomial with integer coefficient(eg. $\mathbb{Z}[i], \mathbb{Z}[\sqrt{-5}]$).

Ex 4.3.3. Let $E(K) : y^2 = x^3 + x$ over $K = \mathbb{Q}(\sqrt{i})$ where $i^2 = 1$ and $\alpha(x, y) = (-x, iy)$. Then α is an endomorphism with $\alpha^2 = 1$ since

$$\alpha^2(x, y) = \alpha(-x, iy) = (x, -y).$$

In this case, $End(E) = \mathbb{Z}[i] = \mathbb{Z}[\alpha]$.

The **Hamiltonian quaternions** [18] is

$$H = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{Q}\}$$

where $i^2 = j^2 = k^2 = -1$ and $ij = k = -ji$. This is a non-commutative ring where every nonzero element has multiplicative inverse.

In general, a **definite quaternion algebra** is a ring of the form

$$\Theta = \{a + b\alpha + c\beta + d\alpha\beta \mid a, b, c, d \in \mathbb{Q}\}$$

where

$$\alpha^2, \beta^2 \in \mathbb{Q}, \quad \alpha^2 < 0, \beta^2 < 0, \quad \beta\alpha = -\alpha\beta.$$

To be a definite, $\alpha^2 < 0$ and $\beta^2 < 0$ are the requirements. In such a ring, every non-zero element has a multiplicative inverse. If again non-zero element has a multiplicative inverse when p-adic coefficients for some $p \leq \infty$, then the quaternion algebra is ramified at p. Otherwise, it is split at p.

If char$(K) = p \geq 2$, $End(E) = R$ where $\mathbb{Z} \subset R \subset \bar{K}$ is torsion free and $\mathbb{Z} \neq \mathbb{Z} \times \mathbb{Z} \simeq \mathbb{Z}[\sigma] \subseteq R$. Then R is either rank 2 or rank 4.

Ex 4.3.4. Let E be a Koblitz curve such that $E : y^2 + xy = x^3 + 1$ over $\mathbb{F}_2$. $\mid E(\mathbb{F}_2) \mid = 4 = 2 + 1 - t$ then $t = -1 = 2(\sigma, 1)$ (trace of σ). The characteristic polynomial of σ is $X^2 - tX + d = X^2 + X + 2 = 0$. So, $End(E(\mathbb{F}_2)) \simeq \mathbb{Z}[\sigma] = \mathbb{Z}[X]/\langle X^2 + X + 2\rangle$.

The following theorem summarize situation for characteristic p. For the proof of this theorem, see [5].

Theorem 13. *Let E be an elliptic curve over a finite field of characteristic p.*

1. *If E is ordinary, then $End(E)$ is an order in an imaginary quadratic field.*
2. *If E is supersingular, then $End(E)$ is a maximal order in a definite quaternion algebra that is ramified at p and ∞ and split at the other primes.*

Thus, we have 2 cases for $End(E) = R$ where char$(K) = p \geq 2$.

1. Usual case: End(E) has rank 2 is called ordinary case as the Example4.3.4 of Koblitz curve.
2. Unusual case: $End(E)$ has rank 4. In this case E is called supersingular and $End(E) = R$ is non-commutative and isomorphic to an order in a quaternion algebra.

CHAPTER 5

CONCLUSION

Elliptic curves are important and widely used in many areas in both asymmetric key cryptosystems and post-quantum cryptosystems. After we gave mathematical backgrounds of elliptic curves in Chapter 2, we classified the this curves according to characteristic of field K in Chapter 3. We got 4 different short Weierstrass equation and we counted non-isomorphic classes for each case. Namely,
if char$(K) \neq 2, 3$,

$$y^2 = x^3 + a_4x + a_6;$$

if char$(K) = 2$,

$$y^2 + xy = x^3 + a_2x^2 + a_6$$

or

$$y^2 + a_3y = x^3 + a_4x + a_6;$$

and if char$(K) = 3$,

$$y^2 = x^3 + a_2x^2 + a_6$$

or

$$y^2 = x^3 + a_4x + a_6.$$

In Chapter 4, we introduced the abelian group structure on elliptic curves with canonical form theorem. Then we studied isogeny on elliptic curves, dual isogeny and Frobenius morphism. Lastly, we focused on the endomorphism rings of elliptic curves. Moreover, we categorized the elliptic curves into two part: ordinary and supersingular.

REFERENCES

[1] S. Anni, Ma426: Elliptic curves, 2015.

[2] D. J. Bernstein, Introduction to post-quantum cryptography, in *Post-quantum cryptography*, pp. 1–14, Springer, 2009.

[3] M. Cenk and F. Özbudak, Isomorphism classes of ordinary elliptic curves over fields of characteristic 3, in *Mathematical Methods in Engineering*, pp. 151–158, Springer, 2007.

[4] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, and F. Vercauteren, *Handbook of elliptic and hyperelliptic curve cryptography*, Chapman and Hall/CRC, 2005.

[5] M. Deuring, Die typen der multiplikatorenringe elliptischer funktionenkörper, in *Abhandlungen aus dem mathematischen Seminar der Universität Hamburg*, volume 14, pp. 197–272, Springer, 1941.

[6] A. Enge, *Elliptic curves and their applications to cryptography: an introduction*, Springer Science & Business Media, 2012.

[7] S. D. Galbraith, *Mathematics of public key cryptography*, Cambridge University Press, 2012.

[8] D. Hankerson, A. J. Menezes, and S. Vanstone, *Guide to elliptic curve cryptography*, volume 46, Springer Science, 2004.

[9] I. N. Herstein, *Topics in algebra*, John Wiley & Sons, 2006.

[10] E. Jeong, Isomorphism classes of elliptic curves over finite fields with characteristic 3, J. Chungcheong Math. Soc, 22, pp. 207–213, 2009.

[11] A. J. Menezes, *Elliptic curve public key cryptosystems*, volume 234, Springer Science & Business Media, 2012.

[12] S. Roman, *Field theory*, volume 158, Springer Science & Business Media, 2005.

[13] S. Rubinstein-Salzedo, Elliptic curves, in *Cryptography*, pp. 141–155, Springer, 2018.

[14] S. Schmitt and H. G. Zimmer, *Elliptic Curves: A computational approach*, volume 31, Walter de Gruyter, 2008.

[15] J. H. Silverman, *The arithmetic of elliptic curves*, volume 106, Springer Science & Business Media, 2009.

[16] A. Sutherland, 18.782 introduction to arithmetic geometry, Fall 2013.

[17] V. Vitse, *Advanced Cryptography - Master SCCI*, 2015-2016.

[18] L. C. Washington, *Elliptic curves: number theory and cryptography*, Chapman and Hall/CRC, 2008.