Elliptic Curve Isogenies and Their Embedding into Homomorphisms of p-adic Tate Modules

by

Atonu Roy Chowdhury
20216008

A thesis submitted to the Department of Mathematics and Natural Sciences
in partial fulfillment of the requirements for the degree of
Bachelor of Science in Mathematics.

Department of Mathematics and Natural Sciences
BRAC University
January 2025.

Declaration

It is hereby declared that

1. The thesis submitted is my/our own original work while completing degree at Brac University.
2. The thesis does not contain material previously published or written by a third party, except where this is appropriately cited through full and accurate referencing.
3. The thesis does not contain material which has been accepted, or submitted, for any other degree or diploma at a university or other institution.
4. We have acknowledged all main sources of help.

Student's Full Name and Signature:

_____

Student Name
Student ID

Approval

The thesis titled **"Elliptic Curve Isogenies and Their Embedding into Homomorphisms of p-adic Tate Modules"** submitted by

1. Atonu Roy Chowdhury (20216008)

of Summer 2024 has been accepted as satisfactory in partial fulfillment of the requirement for the degree of B.S. in Mathematics, on 18 January 2025.

Examining Committee:

Supervisor: _____

Dr. Syed Hasibul Hassan Chowdhury
Professor
Department of Mathematics and Natural Sciences
BRAC University.

Program Coordinator: _____

Dr. Syed Hasibul Hassan Chowdhury
Professor
Department of Mathematics and Natural Sciences
Coordinator of Mathematics Program,
BRAC University.

Head of Department: _____

Dr. Md. Firoze H. Haque
Chairperson
Department of Mathematics and Natural Sciences
BRAC University

Abstract

This thesis investigates the interplay between the morphism spaces of elliptic curves and their associated Tate modules. Specifically, we focus on proving the injectivity of the map

$$\mathrm{Hom}\left(E_1, E_2\right) \otimes \mathbb{Z}_p \to \mathrm{Hom}\left(T_p\left(E_1\right), T_p\left(E_2\right)\right),$$

where E_1 and E_2 are elliptic curves, and $T_p\left(E\right)$ denotes the p-adic Tate module associated with the elliptic curve E. The result connects the algebraic structure of morphisms over elliptic curves with the module-theoretic properties of their Tate modules. We employ tools from algebraic geometry and p-adic number theory, focusing on the role of endomorphism rings and Tate modules. This work contributes to understanding how information about elliptic curve morphisms is preserved and reflected in the realm of p-adic arithmetic.

Keywords: Elliptic curves, isogeny, Tate module, p-adic arithmetic, algebraic geometry.

Acknowledgement

First and foremost, I express my deepest gratitude to my parents, Chinu Ghosh Roy and Ashim Roy Chowdhury, whose unwavering love, support, and sacrifices have been the foundation of all my achievements. Their constant encouragement and belief in me have been my greatest strength. Words fall short in conveying how profoundly thankful I am to my sisters, Joya Roy Chowdhury and Urmy Roy Chowdhury, for their endless support and for always standing beside me through every challenge and success.

I am sincerely grateful to Prof. Mahbubul Alam Majumdar for fostering an environment at BRAC University that encourages curiosity, dialogue, and the free exchange of ideas. His vision has greatly influenced my academic journey. I owe special thanks to Prof. Tibra Ali and Prof. Syed Hasibul Hassan Chowdhury, whose profound impact on my academic and personal life is immeasurable. Their mentorship has deeply shaped my mathematical thinking and has been instrumental in nurturing my intellectual growth and maturity.

I would also like to express heartfelt appreciation to Rafsanjany Jim, Tushar Mitra, and Arnab Chakraborty for engaging in countless insightful mathematical discussions that have significantly broadened my perspective and sharpened my understanding. My sincere thanks go to Dr. Md. Shariful Islam, Adeeb Shahriar Zaman, Siddiqur Rahman Milon, and Sazid Akhter Turzo—their inspiring lectures have left a lasting impression on me and fueled my passion for learning mathematics.

I am deeply thankful to my seniors Ahmed Rakin Kamal, Syeda Tasnuva Jahan, Kabbya Kantam Patwary, Nazmoon Falgunee Moon, Ipshita Bonhi Upoma, Sirajush Salekin, Shovan Sourav Datta Pranta, Nilormy Gupta Trisha, Jhorna Akter, Rifat Hasan Rubel, Sakal Roy, Hasan Kibria, Emon Hossain Raihan, and many others whose encouragement and motivation have been invaluable throughout this journey. Their support has lifted me in more ways than I can express.

I am especially grateful to my therapist, Ayesha Seddiqa, for guiding me through some of the most difficult moments in my life. Her care and support have been crucial in helping me navigate challenges and stay focused on my

goals.

I would also like to acknowledge the countless mathematicians and authors whose works have inspired me to think more deeply and creatively. The beauty and depth of mathematical research have constantly reminded me why I chose this path. Their contributions to the field have not only enriched my studies but have also motivated me to pursue further exploration and understanding.

Lastly, I extend my heartfelt appreciation to all my friends and everyone at the Department of Mathematics and Natural Sciences (MNS) at BRAC University for inspiring me to grow both as a student and as a person.

To all who have been part of this journey—thank you.

Contents

1 Elliptic Curves

Definition 1.1 (Elliptic curve)**.** An **elliptic curve** E defined over a field K is a curve of the form

$$E : y^2 = x^3 + ax + b, \tag{1.1}$$

with $a, b \in K$ and $\Delta = -16\left(4a^3 + 27b^2\right) \neq 0$.

The condition $-16\left(4a^3 + 27b^2\right) \neq 0$ ensures that the curve is non-singular, i.e. it has no cusps (like $y^2 = x^3$) and it has no self-intersections. The set of K-points of an elliptic curve is denoted as $E(K)$.

Although we are often interested in the behavior of a curve over $\mathbb{Q}$, it's helpful to look at the picture in $\mathbb{C}$. Because we have many nice structures on $\mathbb{C}$ (for example, being algebraically closed). Suppose $f(x, y) = 0$ is a curve. We shall study this in the projective space

$$\mathbb{P}^2 = \left(\mathbb{C}^3 - \{\mathbf{0}\}\right) / \sim, \tag{1.2}$$

where $\sim$ is the equivalence relation on $\mathbb{C}^3 - \{\mathbf{0}\}$ given by

$$(x, y, z) \sim \lambda\,(x, y, z) \text{ for } \lambda \in \mathbb{C}^\times. \tag{1.3}$$

The coordinates of $\mathbb{P}^2$ are called homogenous coordinates. In $\mathbb{P}^2$, if $z = 0$, we rescale a point (x, y, z) to $(x, y, 1)$, and consider it in $\mathbb{C}^2$. The points corresponding to $z = 0$ are called **points at infinity**. The coordinates of $\mathbb{P}^2$ are denoted as $(x : y : z)$, with

$$(x : y : z) = (\lambda x : \lambda y : \lambda z)$$

In order for a curve $f(x, y, z)$ to be well-defined in $\mathbb{P}^2$, it needs to be **homogenous**, i.e. the degree of all the terms have to be the same. So, an elliptic curve $y^2 = x^3 + ax + b$ is considered as

$$y^2 z = x^3 + axz^2 + bz^3. \tag{1.4}$$

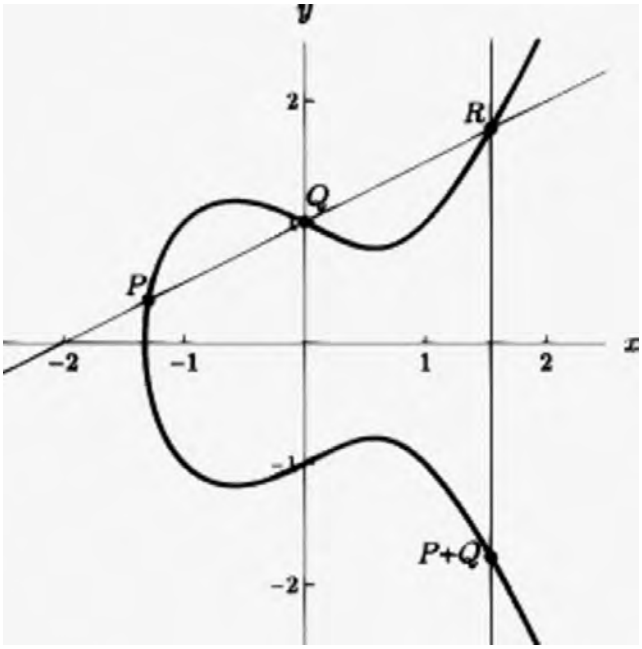
Note that an elliptic curve has exactly one point at infinity. Indeed, for $z = 0$, the equation gives us that $x = 0$. But $z = x = 0$ corresponds to a point $(0 : y : 0)$ in $\mathbb{P}^2$, which is equal to $(0 : 1 : 0)$ in $\mathbb{P}^2$. So the point at infinity on an elliptic curve is the point $(0 : 1 : 0)$.

1.1 Group structure

One can define a group structure on an elliptic curve.

> **Theorem 1.1** (Bezout's theorem)
> Given two algebraic projective plane curves of degrees d_1 and d_2, if they don't share a common component (equivalently, the defining polynomials are relatively prime), then counting with multiplicity they have exactly $d_1 d_2$ intersection points.

To define a group from an elliptic curve, we take the identity as the point at infinity, which is the point $\mathcal{O} = (0 : 1 : 0)$. If we take two points P and Q on the curve, we can draw a straight line between them. This line has degree 1, and the elliptic curve has degree 3, so they will intersect in 3 points. Let's call the third intersection point R. Then we define $P + Q$ to be the reflection of R with respect to the x-axis.

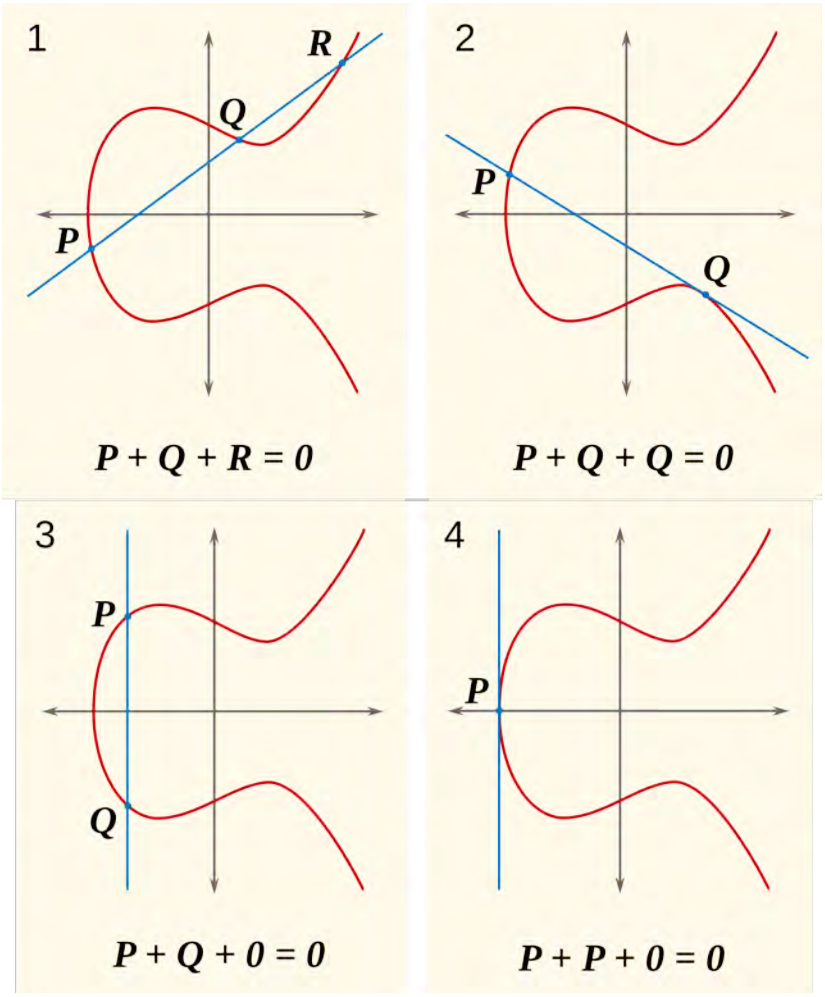


Although this looks geometric, its secretly completely algebraic. That is, one could write down equations down for these intersection points, and then these equations would be valid over any field, regardless of whether one can draw a picture.

Proposition 1.2

The above operation defines an abelian group over any field.

This is one of the rare scenarios where proving associativity is the hardest.



1.2 Lattice

Definition 1.2 (Lattice)**.** Given two complex numbers ω_1, ω_2 that are R-linearly independent, the **lattice** generated by ω_1, ω_2 is the additive subgroup $\omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ of $\mathbb{C}$.

If Λ is a lattice of $\mathbb{C}$, then the quotient group $\mathbb{C}/\Lambda$ can be thought of as a complex torus. We can think of it as a complex lie group (a group which is also a complex manifold). Given a lattice Λ, we can define the weight k Eisenstein series corresponding to Λ:

$$G_k(\Lambda) = \sum_{\substack{\lambda \in \Lambda, \\ \lambda \neq 0}} \lambda^{-k}. \tag{1.5}$$

The Weierstrass-$\wp$ function corresponding to Λ is defined as

$$\wp_\Lambda(z) := \frac{1}{z^2} + \sum_{\lambda \in \Lambda \setminus \{0\}} \left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right). \tag{1.6}$$

Proposition 1.3

Let Λ be a lattice. The function $\wp(z) = \wp_\Lambda(z)$ satisfies the differential equation

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

where $g_2(\Lambda) = 60G_4(\Lambda)$ and $g_3(\Lambda) = 140G_6(\Lambda)$.

Sketch of proof. We start with the geometric series

$$\frac{1}{1-x} = 1 + x + x^2 + \dots.$$

Differentiating and substituting $x = \frac{z}{\lambda}$ gives

$$\frac{1}{\left(1 - \frac{z}{\lambda}\right)^2} = 1 + \frac{2z}{\lambda} + \frac{3z^2}{\lambda^2} + \dots.$$

Subtracting 1, dividing by λ^2, and using the definition of $\wp(z)$ (after a tiny bit of algebra), we find

$$\wp(z) = \frac{1}{z^2} + \sum_{\lambda \in \Lambda \setminus \{0\}} \left(\frac{2z}{\lambda^3} + \frac{3z^2}{\lambda^4} + \frac{4z^3}{\lambda^5} + \dots \right).$$

The defining sum of $\wp(z)$ is absolutely convergent, this expression is too, and we have

$$\wp(z) = \frac{1}{z^2} + 3G_4 z^2 + 5G_6 z^4 + 7G_8 z^6 + \dots,$$

where

$$G_k = G_k(\Lambda) := \sum_{\lambda \in \Lambda}{}' \lambda^{-k}$$

are the **weight** k **Eisenstein series** (the $'$ on the sum will always mean to omit 0). Note that the odd powers went away as $G_k = 0$ for k odd upon letting $\lambda \mapsto -\lambda$. Thus, we can build a table

$$\begin{aligned}
\wp(z) &= \frac{1}{z^2} + 3G_4 z^2 + 5G_6 z^4 + 7G_8 z^6 + \dots, \\
\wp'(z) &= -\frac{2}{z^3} + 6G_4 z + 20G_6 z^3 + 42G_8 z^5 + \dots, \\
\left(\wp'(z)\right)^2 &= \frac{4}{z^6} - 24G_4 \cdot z^{-2} - 80G_6 + \left(36G_4^2 - 168G_8\right) z^2 + \dots, \\
\wp(z)^2 &= \frac{1}{z^4} + 6G_4 + 10G_6 z^2 + \dots, \\
\wp(z)^3 &= \frac{1}{z^6} + 9G_4 \cdot z^{-2} + 15G_6 + \left(21G_8 + 27G_4^2\right) z^2 + \dots.
\end{aligned}$$

Taking the notation

$$g_2 := 60G_4, \quad g_3 := 140G_6,$$

we have

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

■

Then a lattice Λ gives rise to an elliptic curve over $\mathbb{C}$

$$E_\Lambda : y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda). \tag{1.7}$$

(Although this is not technically an elliptic curve by our definition, after a suitable change of variables, we can turn it into an elliptic curve.) In homogenous coordinates of the elliptic curve E_Λ, the map $\mathbb{C}/\Lambda \to E_\Lambda$ is given by

$$\begin{aligned}
z &\mapsto (\wp(z) : \wp'(z) : 1) \\
0 &\mapsto (0 : 1 : 0)\,.
\end{aligned} \tag{1.8}$$

Theorem 1.4

(1.8) is an isomorphism of groups.

Proof. [7], Lecture 7 ■

Definition 1.3. Lattices Λ and Λ' are said to be **homothetic** if $\Lambda' = \lambda\Lambda$ for some $\lambda \in \mathbb{C}^\times$.

Theorem 1.5

Two lattices Λ and Λ' are homothetic if and only if their corresponding elliptic curves E_Λ and $E_{\Lambda'}$ are isomorphic.

Proof. [7], Lecture 13 ■

Theorem 1.6

For every elliptic curve E over $\mathbb{C}$, there exist a lattice Λ such that $E(\mathbb{C})$ is isomorphic to E_Λ. Such a Λ is unique up to homothety by Theorem 1.5.

Proof. [7], Lecture 13 ■

1.3 Complex multiplication

Definition 1.4. For any elliptic curve E, we denote the **n-torsion subgroup** $E[n]$ to be the set of points on an elliptic curve of order dividing n, i.e.

$$E[n] = \{P \in E \mid nP = \mathcal{O}\}, \tag{1.9}$$

where $\mathcal{O}$ is the point at infinity—the identity element under elliptic curve group law.

Proposition 1.7

For any n, $E[n]$ is isomorphic to the direct sum$(\mathbb{Z}/n\mathbb{Z}) \oplus (\mathbb{Z}/n\mathbb{Z})$.

Proof. Recall that every elliptic curve E can be identified with a complex torus $\mathbb{C}/\Lambda$, where Λ is a lattice in the complex plane, and this identification is made such that the group law on the elliptic curve corresponds to adding the corresponding elements on the torus (that is, adding the cosets of Λ in $\mathbb{C}$). Thus, any point in $E[n]$ corresponds to a point $p \in \mathbb{C}/\Lambda$ such that $np \in \Lambda$. If Λ is generated by ω_1, ω_2, it is clear that any such element is of the form $p = \frac{a\omega_1}{n} + \frac{b\omega_2}{n}$ for integers $0 \leq a, b < n$, showing the desired result. ■

Definition 1.5 (Isogeny)**.** An **isogeny** of elliptic curves E_1, E_2 is a nonzero holomorphic group homomorphism (equivalently, an algebraic homomorphism) $\phi : E_1 \to E_2$ (considering E_1 and E_2 as tori $\mathbb{C}/\Lambda_1$. and $\mathbb{C}/\Lambda_2$, so the holomorphicity is defied by the complex lie group structure).

Definition 1.6. An **endomorphism** of an elliptic curve E is an isogeny from E to itself. The endomorphism ring of E, denoted $\mathrm{End}(E)$, is the set of all endomorphisms of E, with addition being defined pointwise and multiplication being defined by composition.

Example 1.1. For any elliptic curve E and any $n \in \mathbb{Z}$, the multiplication-by-n map that sends $P \in E$ to $nP \in E$ is an endomorphism.

Therefore, $\mathrm{End}(E)$ contains a subring isomorphic to $\mathbb{Z}$. By abuse of notation, we shall denote the subring with $\mathbb{Z}$.

Example 1.2. Consider the elliptic curve $E : y^2 = x^3 + x$ and the endomorphism

$$\phi\left(x, y\right) = \left(-x, iy\right). \tag{1.10}$$

This is a well-defined endomorphism since $\left(-iy\right)^2 = \left(-x\right)^3 + \left(-x\right)$. Then ϕ^4 is the identity. But ϕ is not the multiplication-by-n map for any $n \in \mathbb{Z}$.

Definition 1.7. An elliptic curve E is said to have **complex multiplication** if $\mathrm{End}\left(E\right) \neq \mathbb{Z}$.

2 Elliptic Curves as Projective Curves

So far we've been working mostly in $\mathbb{C}$. Now we'll take a look in the case of a general field K. We'll define isogeny in context of a general field.

Definition 2.1. A **plane projective curve** over K is a curve of the form $f(x, y, z) = 0$ where f is a homogeneous polynomial in $K[x, y, z]$.

Definition 2.2. Let C be a plane projective curve over K defined by the equation $f(x, y, z) = 0$ with f a nonconstant homogeneous polynomial in $K[x, y, z]$ that is irreducible in $\bar{K}[x, y, z]$. The **function field** $K(C)$ is the set of equivalence classes of rational functions g/h such that:

(a) g and h are homogeneous polynomials in $k[x, y, z]$ of the same degree;

(b) h is not divisible by f, equivalently, h is not an element of the ideal (f);

(c) g_1/h_1 and g_2/h_2 are considered equivalent whenever $g_1h_2 - g_2h_1 \in (f)$.

If L is any algebraic extension of K (including $L = \bar{K}$), the function field $L(C)$ is similarly defined with $g, h \in L[x, y, z]$. $K(C)$ is a field under addition and multiplication of rational functions.

$$\frac{g_1}{h_1} + \frac{g_2}{h_2} = \frac{g_1h_2 + g_2h_1}{h_1h_2} \quad \text{and} \quad \frac{g_1}{h_1} \cdot \frac{g_2}{h_2} = \frac{g_1g_2}{h_1h_2}. \tag{2.1}$$

The multiplicative inverse of $\frac{g}{h}$ is $\frac{h}{g}$, except when $g \in (f)$. But in that case $g/h = 0/1$, since $g \cdot 1 - h \cdot 0 = g \in (f)$. Therefore, $K(C)$ is a field.

Remark 2.1. $K(C)$ and $C(K)$ are not the same. The former is the function field, and the latter is the set of K-rational points of the curve C.

Definition 2.3. Let C be a projective curve over K with $\alpha \in K(C)$. We say that α is defined at a point $P \in C(\bar{K})$ if α can be represented as g/h for some $g, h \in K[x, y, z]$ with $h(P) \neq 0$.

Recall that for any field F, we use $\mathbb{P}^2(F)$ to denote the set of projective triples $(x : y : z)$, with $x, y, z \in F$ not all zero, modulo the equivalence relation $(x : y : z) \sim (\lambda x : \lambda y : \lambda z)$ for $\lambda \in F^\times$.

Definition 2.4. We say that $\alpha \in K(C)$ is defined at $P \in C\left(\bar{K}\right)$, if $\alpha = g/h$ with $h(P) \neq 0$.

Evaluating g/h at a point in $\mathbb{P}^2\left(\bar{K}\right)$ makes sense, because g and h are homogeneous, and have the same degree. Indeed,

$$\frac{g(\lambda x, \lambda y, \lambda z)}{h(\lambda x, \lambda y, \lambda z)} = \frac{\lambda^{\deg g} g(x, y, z)}{\lambda^{\deg h} h(x, y, z)} = \frac{g(x, y, z)}{h(x, y, z)}. \tag{2.2}$$

Alternatively, we could've defined the function field $K(C)$ as follows: first form the quotient ring

$$\bar{K}[C] = \frac{K[x, y]}{\langle f \rangle}. \tag{2.3}$$

This ring is an integral domain. Then we take its field of fractions, which is the function field $K(C)$.

Then for every point P on the curve C, we define a map

$$\begin{aligned} \operatorname{ord}_P : \bar{K}[C] &\to \mathbb{Z}_{\geq 0} \cup \{\infty\} \\ g &\mapsto \sup\left\{d \in \mathbb{Z} \mid g \in M_P^d\right\}, \end{aligned} \tag{2.4}$$

where M_P is the ideal of $\bar{K}[C]$ with

$$M_P = \left\{g \in \bar{K}[C] \mid g(P) = 0\right\}. \tag{2.5}$$

Now, if we now set $\operatorname{ord}_P(g/h) = \operatorname{ord}_P g - \operatorname{ord}_P h$, then we have the map

$$\operatorname{ord}_P : \bar{K}(C) \to \mathbb{Z} \cup \{\infty\}. \tag{2.6}$$

Definition 2.5. Let C_1 and C_2 be plane projective curves defined over K. A **rational map** $\varphi : C_1 \to C_2$ is a projective triple $(\varphi_x : \varphi_y : \varphi_z) \in \mathbb{P}^2(K(C_1))$, such that for every $P \in C_1(\bar{K})$ where $\varphi_x, \varphi_y, \varphi_z$ are defined and not all zero, the projective point $(\varphi_x(P) : \varphi_y(P) : \varphi_z(P))$ lies in $C_2(\bar{K})$. The map φ is defined (or regular) at P if there exists $\lambda \in K(C_1)^\times$ such that $\lambda\varphi_x, \lambda\varphi_y, \lambda\varphi_z$ are all defined at P and not all zero at P.

Definition 2.6. A **morphism of curves** is a rational map $\varphi : C_1 \to C_2$ that is defined at every $P \in C_1\left(\bar{K}\right)$.

2.1 Isogeny

Definition 2.7. Let E_1, E_2 be elliptic curves over K, with distinguished points O_1, O_2. An **isogeny** $\varphi : E_1 \to E_2$ is a morphism that is also a group homomorphism.

Definition 2.8. The **divisor group** of a curve C, denoted by $\mathrm{Div}(C)$, is the free abelian group generated by the points of C. Thus a divisor $D \in \mathrm{Div}(C)$ is a formal sum

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

where $n_P \in \mathbb{Z}$ and $n_P = 0$ for all but finitely many $P \in C$. The **degree** of D is defined by

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

The divisors of degree 0 form a subgroup of $\mathrm{Div}(C)$, which we denote by

$$\mathrm{Div}^0(C) = \{D \in \mathrm{Div}(C) : \deg D = 0\}.$$

For a smooth elliptic curve E, the number of $P \in E$ such that $\mathrm{ord}_P\, g \neq 0$ is finite, for $g \neq 0$ ([4], I.6.5). So we can associate $g \in K(E)^*$ to the divisor $\mathrm{div} f$ given by

$$\mathrm{div} f = \sum_{P \in E} (\mathrm{ord}_P\, g)\,(P)\,. \tag{2.7}$$

Definition 2.9. A divisor $D \in \mathrm{Div}(C)$ is **principal** if it has the form $D = \mathrm{div}(f)$ for some $f \in \bar{K}(C)^*$. Two divisors are **linearly equivalent**, written $D_1 \sim D_2$, if $D_1 - D_2$ is principal. The **divisor class group** (or **Picard group**) of C, denoted by $\mathrm{Pic}(C)$, is the quotient of $\mathrm{Div}(C)$ by its subgroup of principal divisors.

By [4], II.6.10, $\deg(\mathrm{div} g) = 0$, so that the principal divisors form a subgroup of $\mathrm{Div}^0(C)$.

Definition 2.10. We define the **degree-0 part of the divisor class group** of C to be the quotient of $\mathrm{Div}^0(C)$ by the subgroup of principal divisors. We denote this group by $\mathrm{Pic}^0(C)$.

Any map between curves $\varphi : E_1 \to E_2$ induces group homomorphism ([8], II.3.7)

$$\varphi_* : \mathrm{Pic}^0(E_1) \longrightarrow \mathrm{Pic}^0(E_2)$$

defined by

$$\varphi_*\left(\text{class of } \sum n_i(P_i)\right) = \text{class of } \sum n_i(\varphi P_i).$$

Furthermore, we have a group isomorphism ([8], III.3.4)

$$\kappa_i : E_i \longrightarrow \mathrm{Pic}^0(E_i), \quad P \mapsto \text{class of } (P) - (O).$$

Given an isogeny $\varphi : E_1 \to E_2$, there is a corresponding injection of function fields

$$\varphi^* : \bar{K}(E_2) \to \bar{K}(E_1), \tag{2.8}$$

defined by

$$\varphi^*(f) = f \circ \varphi. \tag{2.9}$$

Then $\bar{K}(E_1)$ is a finite extension of $\varphi^*\left(\bar{K}(E_2)\right)$, since both are finite extensions of transcendental extensions of $\bar{K}$. Then we define the degree of φ to be the degree of this field extension, i.e.

$$\deg \varphi = \left[\bar{K}(E_1) : \varphi^*\left(\bar{K}(E_2)\right)\right]. \tag{2.10}$$

If this extension is separable, then we say φ to be a separable isogeny. Furthermore, let $[0]$ be the zero isogeny, and we define

$$\deg [0] = 0. \tag{2.11}$$

Then we have, for every chain of isogenies

$$E_1 \xrightarrow{\varphi} E_2 \xrightarrow{\psi} E_3$$

we have

$$\deg (\psi \circ \varphi) = \deg \psi \cdot \deg \varphi. \tag{2.12}$$

We denote the set of all isogenies from E_1 to E_2 as $\mathrm{Hom}(E_1, E_2)$. $\mathrm{Hom}(E_1, E_2)$ is a group under addition, with addition being defined pointwise:

$$(\varphi + \psi)(P) = \varphi(P) + \psi(P). \tag{2.13}$$

For $E_1 = E_2 = E$, we can also compose the isogenies, so as to form the ring $\mathrm{End}(E)$.

Example 2.1. For $m \in \mathbb{Z}$, we can define the **multiplication-by-m** isogeny:

$$[m] : E \to E \tag{2.14}$$

in the natural way. For $m > 0$,

$$[m](P) = \underbrace{P + P + \cdots + P}_{m\text{-fold sum}}. \tag{2.15}$$

For $m < 0$, we define

$$[m](P) = [-m](-P). \tag{2.16}$$

Let $\varphi : C_1 \to C_2$ be a nonconstant map of smooth curves. As we have seen, φ induces maps on the function fields of C_1 and C_2,

$$\varphi^* : \bar{K}(C_2) \longrightarrow \bar{K}(C_1)$$

We similarly define maps of divisor groups as follows:

$$\varphi^* : \mathrm{Div}(C_2) \longrightarrow \mathrm{Div}(C_1), \quad (Q) \mapsto \sum_{P \in \varphi^{-1}(Q)} e_\varphi(P)(P),$$

where $e_\varphi(P)$ is the **ramification index**, which is defined by the inseparable degree of the field extension $\bar{K}(C_1) \leq \varphi^* \bar{K}(C_2)$. We also write it as $\deg_i \varphi$. and

$$\varphi_* : \mathrm{Div}(C_1) \longrightarrow \mathrm{Div}(C_2), \quad (P) \mapsto (\varphi P),$$

and extend $\mathbb{Z}$-linearly to arbitrary divisors.

Theorem 2.1

Let E_1, E_2 be elliptic curves over K. A morphism $\varphi : E_1 \to E_2$ is an isogeny if and only if $\varphi(O_1) = O_2$.

Proof. One direction is clear. So we prove that $\varphi(O) = O$ implies that φ is an isogeny. As discussd earlier, we have a group homomorphism

$$\varphi_* : \mathrm{Pic}^0(E_1) \longrightarrow \mathrm{Pic}^0(E_2)$$

defined by

$$\varphi_*\left(\text{class of } \sum n_i(P_i)\right) = \text{class of } \sum n_i(\varphi P_i).$$

Furthermore, we have a group isomorphism

$$\kappa_i : E_i \longrightarrow \mathrm{Pic}^0(E_i), \quad P \mapsto \text{class of } (P) - (O).$$

$\varphi(O) = O$, we get the following commutative diagram

$$\begin{array}{ccc} E_1 & \xrightarrow{\kappa_1} & \mathrm{Pic}^0(E_1) \\ \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \varphi_*} \\ E_2 & \xrightarrow[\kappa_2]{} & \mathrm{Pic}^0(E_2) \end{array}$$

Since κ_1, κ_2, and φ_* are all group homomorphisms and κ_2 is injective, it follows that φ is also a homomorphism. ■

Theorem 2.2

For a separable isogeny $\varphi : E_1 \to E_2$,

$$|\mathrm{Ker}\,\varphi| = \deg \varphi. \tag{2.17}$$

Sketch of proof. Let $\deg_s \varphi$ denote the separable degree of φ, i.e. $\deg_s \varphi$ is the separable degree of the field extension $\bar{K}(E_1) \leq \varphi^*\left(\bar{K}(E_2)\right)$. Then, by [8] II.2.6,

$$\left|\varphi^{-1}(Q)\right| = \deg_s \varphi \quad \text{for all but finitely many } Q \in E_2.$$

But for any $Q, Q' \in E_2$, if we choose some $R \in E_1$ with $\varphi(R) = Q' - Q$, then the fact that φ is a homomorphism implies that there is a one-to-one correspondence

$$\varphi^{-1}(Q) \longrightarrow \varphi^{-1}(Q'), \quad P \mapsto P + R.$$

Hence

$$\left|\varphi^{-1}(Q)\right| = \deg_s \varphi \quad \text{for all } Q \in E_2.$$

For a separable isogeny, $\deg_s = \deg$, so that choosing $Q = O$ gives us the result. ■

Lemma 2.3

Given an isogeny $\varphi : E_1 \to E_2$, the map

$$\operatorname{Ker}\varphi \longrightarrow \operatorname{Aut}(\bar{K}(E_1)/\varphi^*\bar{K}(E_2)), \quad T \mapsto \tau_T^*,$$

is an isomorphism. (Here τ_T is the translation-by-T map and τ_T^* is the automorphism that τ_T induces on $\bar{K}(E_1)$.)

Proof. If $T \in \operatorname{Ker}\varphi$ and $f \in \bar{K}(E_2)$, then

$$\tau_T^*(\varphi^* f) = (\varphi \circ \tau_T)^* f = \varphi^* f,$$

since $\varphi \circ \tau_T = \varphi$. Hence as an automorphism of $\bar{K}(E_1)$, the map τ_T^* fixes $\varphi^*\bar{K}(E_2)$, so the map in (b) is well-defined. Next, since

$$\tau_S \circ \tau_T = \tau_{S+T} = \tau_T \circ \tau_S,$$

the map in (b) is a homomorphism. Finally, from (a) we have

$$|\operatorname{Ker}\varphi| = \deg_s \varphi,$$

while a basic result from Galois theory says that

$$\left|\operatorname{Aut}(\bar{K}(E_1)/\varphi^*\bar{K}(E_2))\right| \le \deg_s \varphi.$$

Hence to prove that the map $T \mapsto \tau_T^*$ is an isomorphism, it suffices to show that it is injective. But if τ_T^* fixes $\bar{K}(E_1)$, then in particular every function on E_1 takes the same value at T and O. This clearly implies that $T = O$. ■

Theorem 2.4

For a separable isogeny $\varphi : E_1 \to E_2$, $\bar{K}(E_1)$ is a Galois extension of $\varphi^*\bar{K}(E_2)$.

Proof. If φ is separable, $\deg_s \varphi = \deg \varphi$. So

$$\begin{aligned}\left|\mathrm{Aut}(\bar{K}(E_1)/\varphi^*\bar{K}(E_2))\right| &= |\mathrm{Ker}\,\varphi| \\ &= \deg\varphi \\ &= \left[\bar{K}(E_1) : \varphi^*\bar{K}(E_2)\right].\end{aligned}$$

Therefore, $\bar{K}(E_1) \le \varphi^*\bar{K}(E_2)$ is a Galois extension. ■

Proposition 2.5

Let

$$\varphi : E_1 \to E_2 \text{ and } \psi : E_1 \to E_3 \tag{2.18}$$

be nonconstant isogenies, and φ is separable. If

$$\mathrm{Ker}\,\varphi \subseteq \mathrm{Ker}\,\psi, \tag{2.19}$$

then there exists a unique isogeny

$$\lambda : E_2 \to E_3 \tag{2.20}$$

such that

$$\psi = \lambda \circ \varphi. \tag{2.21}$$

Proof. Since φ is separable, $\bar{K}(E_1)$ is a Galois extension of $\varphi^*\bar{K}(E_2)$. Then the inclusion $\mathrm{Ker}\,\varphi \subset \mathrm{Ker}\,\psi$ and the identification

$$\mathrm{Ker}\,\varphi \longrightarrow \mathrm{Aut}(\bar{K}(E_1)/\varphi^*\bar{K}(E_2)), \quad T \mapsto \tau_T^*,$$

imply that every element of $\mathrm{Gal}(\bar{K}(E_1)/\varphi^*\bar{K}(E_2))$ fixes $\psi^*\bar{K}(E_3)$. Hence by Galois theory, there are field inclusions

$$\psi^*\bar{K}(E_3) \subset \varphi^*\bar{K}(E_2) \subset \bar{K}(E_1).$$

Now the injection of function fields $\psi^*\bar{K}(E_3) \to \varphi^*\bar{K}(E_2)$ gives rise to a map ([8], II.2.4)

$$\lambda : E_2 \to E_3$$

satisfying

$$\varphi^*(\lambda^*\bar{K}(E_3)) = \psi^*\bar{K}(E_3),$$

and this in turn implies that

$$\lambda \circ \varphi = \psi.$$

Finally, λ is an isogeny, since

$$\lambda(O) = \lambda(\varphi(O)) = \psi(O) = O.$$

■

Proposition 2.6

$\mathrm{Hom}\,(E_1, E_2)$ is a torsion-free $\mathbb{Z}$-module.

Proof. Suppose $[m] \circ \varphi = [0]$ for some $m \in \mathbb{Z}$. Taking degree, we get

$$\deg[m] \cdot \deg\varphi = 0. \tag{2.22}$$

This means either $\deg[m] = 0$ or $\deg\varphi = 0$. The degree is 0 only when the isogeny is trivial, so $m = 0$ or $\varphi = 0$, proving that $\mathrm{Hom}\,(E_1, E_2)$ is a torsion-free $\mathbb{Z}$-module. ■

Definition 2.11. Let E be an elliptic curve and $m \in \mathbb{Z}$ with $m \geq 1$. The **m-torsion subgroup** of E, denoted by $E[m]$, is the set of points of E of order m:

$$E[m] = \{P \in E \mid [m]P = O\}. \tag{2.23}$$

The **torsion subgroup** of E, denoted by E_{tors} is the set of all points of finite order:

$$E_{\mathrm{tors}} = \bigcup_{m=1}^{\infty} E[m]. \tag{2.24}$$

2.2 Differentials

Definition 2.12. Let C be a curve. The space of (meromorphic) differential forms on C, denoted by Ω_C, is the $\bar{K}$-vector space generated by symbols of the form dx for $x \in \bar{K}(C)$, subject to the usual relations:

(a) $d(x+y) = dx + dy$ for all $x, y \in \bar{K}(C)$.

(b) $d(xy) = xdy + ydx$ for all $x, y \in \bar{K}(C)$.

(c) $da = 0$ for all $a \in \bar{K}$.

Let $\phi : C_1 \to C_2$ be a nonconstant map of curves. The associated function field map $\phi^* : \bar{K}(C_2) \to \bar{K}(C_1)$ induces a map on differentials,

$$\phi^* : \Omega_{C_2} \longrightarrow \Omega_{C_1}, \quad \phi^*\left(\sum f_i dx_i\right) = \sum (\phi^* f_i)\, d(\phi^* x_i)$$

This map provides a useful criterion for determining when ϕ is separable.

Theorem 2.7

Let $\phi : C_1 \to C_2$ be a nonconstant map of curves. Then ϕ is separable if and only if the map

$$\phi^* : \Omega_{C_2} \longrightarrow \Omega_{C_1}$$

is injective (equivalently, nonzero).

Sketch of proof. Choose $y \in \bar{K}(C_2)$ such that $\Omega_{C_2} = \bar{K}(C_2)\, dy$ and such that $\bar{K}(C_2)/\bar{K}(y)$ is a separable extension. Note that $\phi^*\bar{K}(C_2)$ is then separable over $\phi^*\bar{K}(y) = \bar{K}(\phi^* y)$. Now

$$\begin{aligned}
\phi^* \text{ is injective} &\iff d(\phi^* y) \neq 0 \\
&\iff d(\phi^* y) \text{ is a basis for } \Omega_{C_1}, \\
&\iff \bar{K}(C_1)/\bar{K}(\phi^* y) \text{ is separable}, \\
&\iff \bar{K}(C_1)/\phi^*\bar{K}(C_2) \text{ is separable},
\end{aligned}$$

where the last equivalence follows because we already know that $\phi^*\bar{K}(C_2)/\bar{K}(\phi^* y)$ is separable. ∎

Theorem 2.8

If $\operatorname{char} K \nmid m$, then $[m] : E \to E$ is separable.

Proof. $\operatorname{char} K \nmid m$, so that $m \neq 0$ in our field. Hence, the map $[m]^*$ is a nonzero map between the spaces of differential forms. Therefore, by Theorem 2.7, $[m]$ is separable. ■

2.3 Dual isogeny

Definition 2.13. Given any isogeny $\varphi : E_1 \to E_2$ with $\deg \varphi = m$, there exists a unique isogeny $\widehat{\varphi} : E_2 \to E_1$ satisfying

$$\widehat{\varphi} \circ \varphi = [m]\,. \tag{2.25}$$

$\widehat{\varphi}$ is called the dual isogeny of φ.

If $\varphi = [0]$, then $\widehat{\varphi} = [0]$.

Theorem 2.9

As a group homomorphism, $\widehat{\varphi}$ equals the composition

$$E_2 \longrightarrow \operatorname{Div}^0(E_2) \xrightarrow{\varphi^*} \operatorname{Div}^0(E_1) \xrightarrow{\text{sum}} E_1,$$

$$Q \longmapsto (Q) - (O) \qquad \sum n_P(P) \longmapsto \sum [n_P]P.$$

Sketch of proof. Let $Q \in E_2$. Then the image of Q under the indicated composition is

$$\begin{aligned}
\operatorname{sum}(\varphi^*((Q) - (O))) &= \sum_{P \in \varphi^{-1}(Q)} [e_\varphi(P)]P - \sum_{T \in \varphi^{-1}(O)} [e_\varphi(T)]T \\
&= [\deg_i \varphi] \left(\sum_{P \in \varphi^{-1}(Q)} P - \sum_{T \in \varphi^{-1}(O)} T \right) \\
&= [\deg_i \varphi] \circ [\#\varphi^{-1}(Q)]P \\
&= [\deg_i \varphi] \circ [\deg_s \varphi]P \\
&= [\deg \varphi]P.
\end{aligned}$$

■

Proposition 2.10

$\varphi \circ \widehat{\varphi} = [m]$ on E_2.

Proof. Let $\varphi \circ \widehat{\varphi} = \lambda$.

$$\begin{aligned} \lambda \circ \varphi &= \varphi \circ (\widehat{\varphi} \circ \varphi) \\ &= \varphi \circ [m] \\ &= [m] \circ \varphi. \end{aligned} \tag{2.26}$$

Therefore, $(\lambda - [m]) \circ \varphi = 0$. So either $\lambda = [m]$ or $\varphi = 0$. In the latter case, $m = 0$, so that $\varphi \circ \widehat{\varphi} = [0] = [m]$. ■

Proposition 2.11

Let $\varphi : E_1 \to E_2$ and $\lambda : E_2 \to E_3$ be isogenies. Then

$$\widehat{\lambda \circ \varphi} = \widehat{\varphi} \circ \widehat{\lambda}. \tag{2.27}$$

Proof. Let $m = \deg \varphi$ and $n = \deg \lambda$.

$$\begin{aligned} \left(\widehat{\varphi} \circ \widehat{\lambda}\right) \circ (\lambda \circ \varphi) &= \widehat{\varphi} \circ [n] \circ \varphi \\ &= [n] \circ \widehat{\varphi} \circ \varphi \\ &= [n] \circ [m] \\ &= [nm] \\ &= [\deg(\lambda \circ \varphi)]\,. \end{aligned} \tag{2.28}$$

■

Theorem 2.12

Let $\varphi, \psi : E_1 \to E_2$ be isogenies. Then

$$\widehat{\varphi + \psi} = \widehat{\varphi} + \widehat{\psi}. \tag{2.29}$$

Proof. Let $x_1, y_1 \in K(E_1)$ and $x_2, y_2 \in K(E_2)$ be Weierstrass coordinates. We start by looking at E_2 considered as an elliptic curve defined over the field $K(E_1) = K(x_1, y_1)$.[1] Then another way of saying that $\varphi : E_1 \to E_2$ is an

isogeny is to note that $\varphi(x_1, y_1) \in E_2(K(x_1, y_1))$, and similarly for $\psi(x_1, y_1)$ and $(\varphi + \psi)(x_1, y_1)$.

Now consider the divisor

$$D = \mathrm{div}((\varphi+\psi)(x_1, y_1))-\mathrm{div}(\varphi(x_1, y_1))+\mathrm{div}(\psi(x_1, y_1))+(O) \in \mathrm{Div}_{K(x_1,y_1)}(E_2).$$

The definition of $\varphi + \psi$ implies that D sums to O, so (III.3.5) tells us that D is linearly equivalent to 0. Thus there is a function

$$f \in K(x_1, y_1)(E_2) = K(x_1, y_1, x_2, y_2)$$

that, when considered as a function of x_2 and y_2, has divisor D.
We now switch perspective and look at f as a function of x_1 and y_1. In other words, we treat f as a function on E_1 considered as an elliptic curve defined over $K(x_2, y_2)$. Suppose that $P_1 \in E_1(K(x_2, y_2))$ is a point satisfying $\varphi(P_1) = (x_2, y_2)$. Then examining D, specifically the term $-\mathrm{div}(\varphi(x_1, y_1))$, we see that f has a pole at P_1, i.e., the function $f(x_1, y_1; x_2, y_2)$ has a pole if x_1, y_1, x_2, y_2 satisfy $(x_2, y_2) = \varphi(x_1, y_1)$. Further,

$$\mathrm{ord}_{P_1}(f) = e_\varphi(P_1).$$

Similarly, f has a pole at P_1 if $(x_2, y_2) = \psi(P_1)$, and it has a zero at P_1 if $(x_2, y_2) = (\varphi + \psi)(P_1)$. It follows that as a function of x_1 and y_1, the divisor of f has the form

$$(\varphi + \psi)^*((x_2, y_2)) - \varphi^*((x_2, y_2)) - \psi^*((x_2, y_2)) + \sum n_i(P_i) \in \mathrm{Div}_{K(x_2,y_2)}(E_1),$$

where the P_i's are in $E_1(\bar{K})$, i.e., $\sum n_i(P_i) \in \mathrm{Div}_{\bar{K}}(E_1)$. Since this is the divisor of a function, it sums to O, so using Theorem 2.9, we conclude that the point

$$\widehat{(\varphi + \psi)}(x_2, y_2) - \widehat{\varphi}(x_2, y_2) - \widehat{\psi}(x_2, y_2)$$

does not depend on (x_2, y_2), i.e., it is in $E_1(\bar{K})$. Putting $(x_2, y_2) = O$ shows that it is equal to O, which completes the proof that

$$\widehat{(\varphi + \psi)} = \widehat{\varphi} + \widehat{\psi}.$$

■

Proposition 2.13
For all $m \in \mathbb{Z}$, $\widehat{[m]} = [m]$, and $\deg [m] = m^2$.

Proof. Clearly it's true for $m = 1$, because $[1]$ is the identity map. Now,

$$\begin{aligned} \widehat{[m+1]} &= \widehat{[m] + [1]} \\ &= \widehat{[m]} + \widehat{[1]}. \end{aligned} \tag{2.30}$$

Now, by induction, we get $\widehat{[m]} = [m]$ for every m.
Let $d = \deg [m]$. Then

$$\begin{aligned} [d] &= \widehat{[m]} \circ [m] \\ &= [m] \circ [m] \\ &= \left[m^2\right]. \end{aligned} \tag{2.31}$$

Hence, $d = m^2$. ■

Proposition 2.14
$\deg \widehat{\varphi} = \deg \varphi$.

Proof. Let $m = \deg \varphi$.

$$m^2 = \deg [m] \tag{2.32}$$
$$= \deg (\widehat{\varphi} \circ \varphi) \tag{2.33}$$
$$= \deg \widehat{\varphi} \cdot \deg \varphi. \tag{2.34}$$

Therefore, $\deg \widehat{\varphi} = m = \deg \varphi$. ■

Proposition 2.10 along with Proposition 2.14 implies that $\widehat{\widehat{\varphi}} = \varphi$.

Theorem 2.15
If $\operatorname{char} K \nmid m$,

$$E[m] \cong \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}} \tag{2.35}$$

Proof. Since $\operatorname{char} K \nmid m$,

$$|E[m]| = |\operatorname{Ker}[m]| = \deg[m] = m^2. \tag{2.36}$$

Similarly, for every $d \mid m$,

$$|E[d]| = d^2. \tag{2.37}$$

Now let $m = \prod p^e$. Since $E[m]$ is abelian,

$$E[m] = \prod E\left[p^e\right]. \tag{2.38}$$

$|E[p^e]| = p^{2e}$.

$$|E[p]| = p^2 \implies E[p] = \frac{\mathbb{Z}}{p^2\mathbb{Z}} \text{ or } \frac{\mathbb{Z}}{p\mathbb{Z}} \times \frac{\mathbb{Z}}{p\mathbb{Z}}. \tag{2.39}$$

If $E[p] = \frac{\mathbb{Z}}{p^2\mathbb{Z}}$, then the order of all the elements in $E[p]$ does not divide p. So we must have $E[p] = \frac{\mathbb{Z}}{p\mathbb{Z}} \times \frac{\mathbb{Z}}{p\mathbb{Z}}$. Now suppose, $E\left[p^i\right] = \frac{\mathbb{Z}}{p^i\mathbb{Z}} \times \frac{\mathbb{Z}}{p^i\mathbb{Z}}$ for every $i = 1, 2, \ldots, e-1$. Since $|E[p^e]| = p^{2e}$, we have

$$E[p^e] = \frac{\mathbb{Z}}{p^{a_1}\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{p^{a_k}\mathbb{Z}}. \tag{2.40}$$

Let's now calculate how many elements of order p are in $E[p^e]$. The number is p in each component $\frac{\mathbb{Z}}{p^{a_i}\mathbb{Z}}$, hence the total number of order p elements is p^k. But we know it's p^2, so $k = 2$.

$$E[p^e] = \frac{\mathbb{Z}}{p^{a_1}\mathbb{Z}} \times \frac{\mathbb{Z}}{p^{a_2}\mathbb{Z}}, \tag{2.41}$$

with $a_1 + a_2 = 2e$. But $E[p^e]$ contains a copy of $E\left[p^{e-1}\right] = \frac{\mathbb{Z}}{p^{e-1}\mathbb{Z}} \times \frac{\mathbb{Z}}{p^{e-1}\mathbb{Z}}$. This is only possible when both $a_1 = a_2 = e$, or $a_1 = e-1, a_2 = e+1$. In the latter case, $E[p^e] = \frac{\mathbb{Z}}{p^{e-1}\mathbb{Z}} \times \frac{\mathbb{Z}}{p^{e+1}\mathbb{Z}}$, and the number of elements whose order divides p^e is $p^{e-1}p^e = p^{2e-1}$. But as we know the number is $2e$. Therefore, $E[p^e] = \frac{\mathbb{Z}}{p^e\mathbb{Z}} \times \frac{\mathbb{Z}}{p^e\mathbb{Z}}$. As a result,

$$\begin{aligned} E[m] &= \prod E[p^e] \\ &= \prod \left(\frac{\mathbb{Z}}{p^e\mathbb{Z}} \times \frac{\mathbb{Z}}{p^e\mathbb{Z}} \right) \\ &= \prod \frac{\mathbb{Z}}{p^e\mathbb{Z}} \times \prod \frac{\mathbb{Z}}{p^e\mathbb{Z}} \\ &= \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}}. \end{aligned} \tag{2.42}$$

■

3 Tate module

As we have proved earlier,

$$E[m] = \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}}, \tag{3.1}$$

when $\operatorname{char} K \nmid m$. We now mimic the construction of p-adic integers $\mathbb{Z}_p$, and construct the Tate module.

3.1 Inverse limits

Given a suitable "compatible system" of objects, the inverse limit of this system is an object that packages together the data of the system.

Definition 3.1. Let I be a set with a partial order $\leq$. An inverse system (also called a projective system) indexed by I is a collection of sets (or groups or rings or topological spaces) $\{A_i\}_{i\in I}$ together with maps (of sets, groups, rings, or topological spaces)

$$\varphi_{ij} : A_i \to A_j \quad \text{for all } j \leq i \tag{3.2}$$

such that $\varphi_{ii} = \mathrm{id}_{A_i}$ for all $i \in I$ and $\varphi_{jk} \circ \varphi_{ij} = \varphi_{ik}$ for all $k \leq j \leq i$. The φ_{ij} are called transition maps.

Definition 3.2. The inverse limit of the system $(\{A_i\}, \{\varphi_{ij}\})$ is the set/ group/ ring/ topological space

$$\varprojlim_i A_i = \left\{ (a_i)_{i\in I} \in \prod_{i\in I} A_i : \varphi_{ij}(a_i) = a_j \text{ for all } j \leq i \right\} \tag{3.3}$$

of compatible systems of elements of the inverse system.

Example 3.1. Let p be prime and consider the inverse system of rings

$$A_i = \mathbb{Z}/p^i\mathbb{Z} \quad \text{for } i \in \mathbb{Z}_{>0} \tag{3.4}$$

with transition maps

$$\mathbb{Z}/p^i\mathbb{Z} \xrightarrow{\bmod p^j} \mathbb{Z}/p^j\mathbb{Z} \tag{3.5}$$

for all $j \leq i$. Then $\varprojlim \mathbb{Z}/p^i\mathbb{Z}$ consists of systems $a = \left(a_i \bmod p^i\right)$ such that $a_i \bmod p^j = a_j$ whenever $j \leq i$. Intuitively, an element $a \in \lim \mathbb{Z}/p^i\mathbb{Z}$ is a "number" which can be taken mod p^i for any $i \geq 1$, subject to the obvious compatibilities. This is the ring of p-adic integers, $\mathbb{Z}_p$.

3.2 Construction of Tate module

Let E be an elliptic curve. In this section, we let p be a prime number different from $\operatorname{char} K$. Consider the groups $E\left[p^n\right]$, and the group homomorphisms

$$E\left[p^{n+1}\right] \xrightarrow{[p]} E\left[p^n\right]. \tag{3.6}$$

Then we take the inverse limit of this system so as to get

$$T_p(E) = \varprojlim_n E\left[p^n\right]. \tag{3.7}$$

Each $E\left[p^n\right]$ is a $\mathbb{Z}/p^n\mathbb{Z}$-module. Therefore, $T_p(E)$ has the structure of a $\mathbb{Z}_p$-module, where $\mathbb{Z}_p$ is the ring of p-adic integers.

Theorem 3.1

$$T_p(E) \cong \mathbb{Z}_p \times \mathbb{Z}_p. \tag{3.8}$$

Proof. $E\left[p^n\right] = \mathbb{Z}/p^n\mathbb{Z} \times \mathbb{Z}/p^n\mathbb{Z}$. Taking the inverse limit, we have

$$\begin{aligned} T_p(E) &= \varprojlim_n E\left[p^n\right] \\ &= \varprojlim_n \left(\frac{\mathbb{Z}}{p^n\mathbb{Z}} \times \frac{\mathbb{Z}}{p^n\mathbb{Z}}\right) \\ &= \varprojlim_n \frac{\mathbb{Z}}{p^n\mathbb{Z}} \times \varprojlim_n \frac{\mathbb{Z}}{p^n\mathbb{Z}} \\ &= \mathbb{Z}_p \times \mathbb{Z}_p. \end{aligned} \tag{3.9}$$

■

The Tate module can be a useful tool for studying isogenies. Let

$$\varphi : E_1 \to E_2 \tag{3.10}$$

be an isogeny. Then φ induces maps

$$\varphi^n : E_1 [p^n] \to E_2 [p^n] . \tag{3.11}$$

Hence, we have a $\mathbb{Z}_p$-linear map

$$\varphi_p : T_p (E_1) \to T_p (E_2) . \tag{3.12}$$

Thus we have a map

$$\begin{aligned} \operatorname{Hom}(E_1, E_2) &\to \operatorname{Hom}(T_p(E_1), T_p(E_2)) \\ \varphi &\mapsto \varphi_p. \end{aligned} \tag{3.13}$$

Proposition 3.2
The map in (3.13) is injective.

Proof. Suppose $\varphi_p = 0$, i.e. φ is in the kernel of the map. Then for every $n \geq 1$,

$$\varphi^n : E_1 [p^n] \to E_2 [p^n] . \tag{3.14}$$

is the zero map. In other words, $E_1 [p^n] \subseteq \operatorname{Ker} \varphi$. Let $m = \deg \varphi$. Then

$$[m] = \widehat{\varphi} \circ \varphi. \tag{3.15}$$

As a result, we have

$$\operatorname{Ker} [p^n] = E_1 [p^n] \subseteq \operatorname{Ker} \varphi \subseteq \operatorname{Ker} [m] . \tag{3.16}$$

By Proposition 2.5, since $[p^n]$ is separable (Theorem 2.8) there exists an isogeny $\lambda_n : E_1 \to E_1$ such that

$$[m] = \lambda_n \circ [p^n] . \tag{3.17}$$

By taking degree,

$$m^2 = \deg \lambda_n \cdot p^{2n}. \tag{3.18}$$

So $p^{2n} \mid m^2$, i.e. $p^n \mid m$. This holds for every n. Hence, $m = 0$, and $\varphi = 0$. ∎

3.3 Main result

So we have proved that

$$\begin{aligned} \operatorname{Hom}(E_1, E_2) &\to \operatorname{Hom}(T_p(E_1), T_p(E_2)) \\ \varphi &\mapsto \varphi_p. \end{aligned} \tag{3.19}$$

is an injection. But $\operatorname{Hom}(T_p(E_1), T_p(E_2))$ is a lot larger than $\operatorname{Hom}(E_1, E_2)$. $\operatorname{Hom}(E_1, E_2)$ is a torsion-free $\mathbb{Z}$-module, whereas $\operatorname{Hom}(T_p(E_1), T_p(E_2))$ is a $\mathbb{Z}_p$-module. We can make $\operatorname{Hom}(E_1, E_2)$ into a $\mathbb{Z}_p$-module by tensoring with $\mathbb{Z}_p$. Then we get the following map:

$$\begin{aligned} \operatorname{Hom}(E_1, E_2) \otimes \mathbb{Z}_p &\to \operatorname{Hom}(T_p(E_1), T_p(E_2)) \\ \varphi \otimes a &\mapsto a \cdot \varphi_p. \end{aligned} \tag{3.20}$$

Theorem 3.3

Let E_1, E_2 be elliptic curves, and $p \neq \operatorname{char} K$ be a prime number. Then the map

$$\begin{aligned} \operatorname{Hom}(E_1, E_2) \otimes \mathbb{Z}_p &\to \operatorname{Hom}(T_p(E_1), T_p(E_2)) \\ \varphi \otimes a &\mapsto a \cdot \varphi_p. \end{aligned} \tag{3.21}$$

is injective.

To prove this, we need to prove some results first.

Lemma 3.4

et E_1 and E_2 be elliptic curves. Then the degree map $\deg : \operatorname{Hom}(E_1, E_2) \to \mathbb{Z}$ is a positive-definite quadratic form.

Proof. We need to show that the pairing $\langle \cdot, \cdot \rangle$ given by

$$\langle \varphi, \psi \rangle = \deg(\varphi + \psi) - \deg(\varphi) - \deg(\psi) \tag{3.22}$$

is bilinear. This is clear, as

$$[\langle \varphi, \psi \rangle] = [\deg(\varphi + \psi)] - [\deg(\varphi)] - [\deg(\psi)] \tag{3.23}$$

$$= \widehat{(\varphi + \psi)} \circ (\varphi + \psi) - \widehat{\varphi} \circ \varphi - \widehat{\psi} \circ \psi \tag{3.24}$$

$$= \widehat{\varphi} \circ \psi + \widehat{\psi} \circ \varphi. \tag{3.25}$$

Therefore, $\langle \cdot, \cdot \rangle$ is bilinear. Furthermore,

$$\deg(n\varphi) = \deg([n] \circ \varphi) = n^2 \deg \varphi. \tag{3.26}$$

Therefore, deg is a quadratic form. ■

Lemma 3.5

Let G be a discrete subgroup of $\mathbb{R}^n$. Then G is finitely generated.

Proof. First, we can replace $\mathbb{R}^n$ with the $\mathbb{R}$-vector space generated by the set G, i.e. we can form a basis of $\mathbb{R}^n$ with $x_1, x_2, \ldots, x_n \in G$. Let G' be the subgroup generated by the x_i's, i.e.

$$G' = \mathbb{Z}x_1 \oplus \mathbb{Z}x_2 \oplus \cdots \oplus \mathbb{Z}x_n. \tag{3.27}$$

Now, consider the quotient $\mathbb{R}^n/G'$:

$$\frac{\mathbb{R}^n}{G'} = \frac{\mathbb{R}x_1 \oplus \mathbb{R}x_2 \oplus \cdots \oplus \mathbb{R}x_n}{\mathbb{Z}x_1 \oplus \mathbb{Z}x_2 \oplus \cdots \oplus \mathbb{Z}x_n} = S^1x_1 \oplus S^1x_2 \oplus \cdots \oplus S^1x_n. \tag{3.28}$$

This is compact as it's the direct sum of n-copies of S^1.

Since G is discrete, its image in $\frac{\mathbb{R}^n}{G'}$ has to be discrete as well. Since $\frac{\mathbb{R}^n}{G'}$ is compact, the image of G in $\frac{\mathbb{R}^n}{G'}$ has to be finite. Therefore, G/G' is finite. If $|G/G'| \neq 1$, we can find $g \in G$ that is a $\mathbb{Q}$-linear combination of x_i's, which contradicts the discreteness of G. Therefore, $G = G'$. ■

Lemma 3.6

Let $M \subseteq \mathrm{Hom}(E_1, E_2)$ be a finitely generated subgroup, and let

$$M' = \{\varphi \in \mathrm{Hom}(E_1, E_2) \mid [m] \circ \varphi \in M \text{ for some } m \in \mathbb{Z}_{>0}\}. \tag{3.29}$$

Then M' is finitely generated.

Proof. We'll see M' as a subgroup of $M \otimes \mathbb{R}$, and show that it's a discrete subgroup. Since $M \otimes \mathbb{R}$ is a finite dimensional real vector space, we can equip it with the natural topology inherited from $\mathbb{R}$. The degree map is clearly continuous: Since the degree map is a quadratic form on $\mathrm{Hom}(E_1, E_2)$, it is a quadratic form on M. Since M is finitely generated, we can think of it

being given by a quadratic polynomial in the coefficients of each generator. Therefore, it extends naturally to a quadratic form on $M \otimes \mathbb{R}$, which is automatically continuous.

As a result,

$$U = \{\varphi \otimes x \in M \otimes \mathbb{R} \mid \deg(\varphi \otimes x) < 1\} \tag{3.30}$$

is a neighborhood of origin in $M \otimes \mathbb{R}$. Furthermore,

$$M' \cap U = \{0\}, \tag{3.31}$$

because every nonzero isogeny has degree at least 1. Hence, M' is a discrete subgroup of $M \otimes \mathbb{R}$. Hence, by Lemma 3.5, M' is finitely generated. ■

Proof of Theorem 3.3. Suppose that

$$\varphi_p := a_1 (\varphi_1)_p + \cdots + a_k (\varphi_k)_p = 0 \tag{3.32}$$

where $a_1, \ldots, a_k \in \mathbb{Z}_p$ and $\varphi_1, \ldots, \varphi_k \in \mathrm{Hom}(E_1, E_2)$. In other words, if we denote the map by F,

$$\begin{aligned} F : \mathrm{Hom}(E_1, E_2) \otimes \mathbb{Z}_p &\to \mathrm{Hom}(T_p(E_1), T_p(E_2)) \\ \varphi \otimes a &\mapsto a \cdot \varphi_p. \end{aligned} \tag{3.33}$$

then

$$F(\varphi_1 \otimes a_1 + \cdots + \varphi_k \otimes a_k) = 0, \tag{3.34}$$

i.e. $\varphi := \varphi_1 \otimes a_1 + \cdots + \varphi_k \otimes a_k \in \mathrm{Ker}\, F$.

Let M be the submodule of $\mathrm{Hom}(E_1, E_2)$ generated by $\varphi_1, \ldots, \varphi_k$. By Lemma 3.6, M' is finitely generated, and hence free. Let $\psi_1, \ldots, \psi_m$ be a basis for M'. Then there exist $b_1, \ldots, b_m \in \mathbb{Z}_p$ such that

$$\varphi = \psi_1 \otimes b_1 + \cdots + \psi_m \otimes b_m, \tag{3.35}$$

so that

$$\varphi_p = b_1 (\psi_1)_p + \cdots + b_m (\psi_m)_p = 0. \tag{3.36}$$

We will show that each b_i is zero by showing that its $\mathbb{Z}/p^n\mathbb{Z}$ part is zero for each n. For $n \geq 1$, there is a $c_i \in \mathbb{Z}$ such that $b_i \equiv c_i \pmod{p^n}$. Hence,

$$\psi = c_1 (\psi_1)_p + \cdots + c_m (\psi_m)_p \tag{3.37}$$

agrees with

$$\varphi_p = b_1 (\psi_1)_p + \cdots + b_m (\psi_m)_p \tag{3.38}$$

up to the level of p^n. Since φ_p acts as 0 on $T_p(E_1), \psi$ acts as 0 on $E_1[p^n]$. Since $[p^n]$ is separable (because $p \neq \operatorname{char} K$), and since its kernel is contained in the kernel of ψ, we can factor ψ as $[p^n] \circ \psi'$ (Proposition 2.5). Since $\psi \in M', \psi' \in M'$ also, so

$$\psi' = d_1 (\psi_1)_p + \cdots + d_m (\psi_m)_p \tag{3.39}$$

for some $d_1, \ldots, d_m \in \mathbb{Z}$. But the ψ_i are a basis for M', so $c_i = d_i p^n$. Hence $b_i \equiv 0 \pmod{p^n}$. Since n was chosen arbitrarily, the b_i are 0 in $\mathbb{Z}_p$, so $\varphi = 0$ as desired. ■

4 Future Directions

The results of this thesis open several avenues for further research in the arithmetic geometry of elliptic curves. A natural extension of this work is to investigate whether the map

$$\mathrm{Hom}\left(E_1, E_2\right) \otimes \mathbb{Z}_p \to \mathrm{Hom}\left(T_p\left(E_1\right), T_p\left(E_2\right)\right) \tag{4.1}$$

is an isomorphism. Our guess is that it's not always an isomorphism, but for special cases of K it is an isomorphism. Exploring the surjectivity or bijectivity of the map in specific cases, such as supersingular elliptic curves or curves defined over particular fields, might reveal richer structural information. Another promising direction involves leveraging this injection to study congruences between elliptic curves and their associated Galois representations.

Another possible future research direction would be to investigate if similar injection results hold for other families of abelian varieties or higher-dimensional analogs. Understanding how the morphism spaces of these varieties interact with their associated Tate modules could provide deeper insights into the general relationship between geometric morphisms and p-adic representations.

Finally, computational approaches to verifying this injectivity in explicit examples might lead to practical tools in number theory and cryptography, where elliptic curves play a pivotal role. These directions highlight the intersection of pure mathematics and applications, emphasizing the broad potential impact of the ideas explored in this thesis.

Bibliography

[1] M. F. Atiyah and I. G. McDonald. *Introduction To Commutative Algebra*. Westview Press, 1994. ISBN: 978-0201407518.

[2] C. Brookes and Q. Kuang. *Lecture Notes on Galois Theory*. 2017. URL: https://qk206.user.srcf.net/notes/galois_theory.pdf.

[3] D. A. Cox. *Galois Theory*. Wiley, 2012. ISBN: 978-1118072059.

[4] R. Hartshorne. *Algebraic Geometry*. Springer, 1977. ISBN: 978-1-4419-2807-8.

[5] N. Koblitz. *Introduction to Elliptic Curves and Modular Forms*. Springer, 1993. ISBN: 978-1-4612-6942-7.

[6] S. Marks. *Galois Representations*. 2020. URL: https://people.math.harvard.edu/~smarks/mod-forms-tutorial/mf-notes/galois-reps.pdf.

[7] L. Rolen. *Lecture Notes on Modular Forms and Elliptic Curves*. 2020. URL: https://math.vanderbilt.edu/rolenl/ModularForms.html.

[8] J. H. Silverman. *The Arithmetic of Elliptic Curves*. Springer, 2009. ISBN: 978-1-4419-1858-1.

[9] J. H. Silverman and J. T. Tate. *Rational Points on Elliptic Curves*. Springer, 2015. ISBN: 978-3-319-18587-3.

[10] A. Sutherland. *18.783 - Elliptic Curves, Lecture Notes*. 2022. URL: https://math.mit.edu/classes/18.783/2022/lectures.html.