THE UNIVERSITY OF CALGARY

# Isomorphism and Isogeny of Elliptic Curves, With Examples

by

Brendan Oseen

A THESIS
SUBMITTED TO THE FACULTY OF GRADUATE STUDIES
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE
DEGREE OF MASTER OF SCIENCE

DEPARTMENT OF MATHEMATICS AND STATISTICS

CALGARY, ALBERTA
December, 2003

## THE UNIVERSITY OF CALGARY

## FACULTY OF GRADUATE STUDIES

The undersigned certify that they have read, and recommend to the Faculty of Graduate Studies for acceptance, a thesis entitled "Isomorphism and Isogeny of Elliptic Curves, With Examples" submitted by Brendan Oseen in partial fulfillment of the requirements for the degree of MASTER OF SCIENCE.

Renate S

Chair/Supervisor, Dr. Renate Scheidler
Department of Mathematics and Statistics

Clifton Cunningham

Co-supervisor, Dr. Clifton Cunningham
Department of Mathematics and Statistics

Dr. Aiden Bruen
Department of Mathematics and Statistics

T.R.B. Cockett

Dr. Robin Cockett
Department of Computer Science

Dec. 11, 2003

Date

# Abstract

This thesis is a survey of isogeny and isomorphism of elliptic curves. We first introduce the reader to elliptic curves, and show that the points of an elliptic curve form a group. We then deal with isogeny and isomorphism of elliptic curves, and analyze the properties thereof. There are also many examples, both throughout the thesis, as well as in the penultimate chapter, to give the reader a clearer understanding of elliptic curves.

This thesis is intended to be accessible to the reader with little or no knowledge of elliptic curves, and assumes only that the reader has a basic mathematical background. While some readers may be more familiar with affine models of elliptic curves, we prefer to consider them only projectively because from the perspective of algebraic geometry, we believe that that is the proper way of discussing them.

# Acknowledgements

I would like to acknowledge Clifton L.R. Cunningham and Renate Scheidler for their time and support, their painstaking work, and their sufferance of my manifold eccentricities; and Hugh Cowie Williams for his inimitable humour. I would also like to thank all three of these individuals for the enjoyable company, stimulating conversation and political debate they have afforded me; their tolerance of my endemic tardiness (and, of course, their funding :-).

In addition, I am grateful to the department for its financial support, and to various members thereof, in particular — but not limited to — Richard A. Mollin, Kalathoor Varadarajan and Jonathan Schaer.

Finally, I would like to recognize Don, Larry, The Huffer and everyone from NHS for making the last two years more fun; and above all, the ZD's for their patience and generosity (you know who you are).

# Dedication

For FTF, MF, BS, SO, SF, EW, PTT, DD, TKC, WG and TCA.

# Table of Contents

# List of Tables

# List of Figures

# Chapter 1

# Introduction and Motivation

This thesis is an exposition of algebraic curves and function fields with special reference to elliptic curves. Elliptic curves are of interest for several reasons. One justification for their study is that they are used in cryptographic implementations. While this has put them in the limelight in recent years, it is not our primary motivation for studying them. On the contrary, we believe elliptic curves are worth studying for aesthetic reasons alone. They are imbued with a natural group structure which is found on very few algebraic curves.

The study of elliptic curves is also of use in finding solutions of certain diophantine equations. Given an equation of an elliptic curve, for instance, the equation $y^2 = x^3 + 17$, and two known points on the curve, one can generate other points on the curve through point addition.

Another example is the proof of Fermat's Last Theorem (FLT) which makes use of the Taniyama-Shimura-Weil (TSW) theorem relating elliptic curves and modular forms. Recall that FLT states that for $n \in \mathbb{N}, n \geq 3$, there do not exist $a, b, c \in \mathbb{N}$ such that $a^n + b^n = c^n$ and $abc \neq 0$. The TSW conjecture asserts that all elliptic curves over $\mathbb{Q}$ are modular. Serre conjectured in [21] that if there is such a solution $(a, b, c, n)$ which contradicts FLT, then the elliptic curve $y^2 = x(x - a^p)(x + b^p)$ (for $p$ some prime divisor of $n$) is non-modular. (See also [8].) Ribet later proved Serre's conjecture in [19], which effectively established that the TSW conjecture implies

FLT. Wiles and Taylor proved a special case of TSW in [26] and [28] which was sufficient to prove FLT. The TSW was finally proven in its entirety in [3].

In addition, some current cryptosystems are based on elliptic curves. Their security depends on the presumed difficulty of the elliptic curve discrete log problem. Briefly, given a finite cyclic group $G$ with generator $g$, and some element $h \in G$, one would like to find the exponent $e = \log_g h$, called the *discrete log of $h$ to the base $g$*, such that $g^e = h$. In the case of elliptic curves, the group is additive, so if $P, Q$ are points on $E$ with $Q \in< P >$, the cyclic subgroup generated by $P$, then the goal is to find $n \in \mathbb{N}$ such that $nP = Q$. On some elliptic curves, the discrete log problem may be difficult, especially if $P$ generates a large cyclic subgroup of the group of points on the curve, while on others, it may be tractable. The purpose of finding an isogeny, therefore, is to map points on a "harder" curve to those on an "easier" curve, where it is less difficult to solve the discrete log problem. For if $E$ is a "hard" elliptic curve generated as an additive group by $P$, and $E'$ an "easy" elliptic curve, and if $\alpha : E \longrightarrow E'$ is a non-trivial isogeny, then for any $Q \in E$, $\log_P(Q)$ is equal to $\log_{\alpha(P)}(\alpha(Q))$, which is easier to find. The United States National Institute for Standards and Technology (NIST) recommends certain "hard" elliptic curves for cryptographic implementation. For details, see [17].

Our goal is to give a relatively self-contained treatment of the subject of isomorphism and isogeny of elliptic curves. This thesis endeavours to bring together much of the material on the subject into one cohesive, readable unit. Above all, we attempt to give a complete account of isogeny and the theory thereof, which is ostensibly lacking in the current literature. The comprehensive handling of the curve-function field duality, as well as the many examples, also distinguish this thesis from many other bodies of work on the subject. In particular, Chapter 6 gives numerous examples relating point counting of elliptic curves over finite fields to isogeny and isomorphism of these curves.

The thesis is organized as follows. The second chapter consists of background material on algebraic curves and function fields. The third chapter deals with maps of curves and their function fields. In Chapter 4, we define elliptic curves and carefully establish the abelian group structure, while the fifth chapter is devoted entirely to isogeny. The sixth chapter gives some practical basis to the preceding chapters. To be more precise, we look at elliptic curves over finite fields of three different characteristics (2,3 and 11). In each case, we determine the Weierstrass curves in a given isomorphism class, and classify the isomorphism and isogeny subclasses thereof by using the theory and techniques developed in the first five chapters. The final chapter consists of some concluding remarks and a statement of open problems.

# Chapter 2

# Curves and Function Fields

This chapter lays the groundwork for our study of elliptic curves. We introduce projective space, general algebraic curves and the function fields thereof. In some treatments of elliptic curves, projective space is not discussed at all; on the other hand, we choose to adopt the projective (rather than affine) point of view for the bulk of this thesis. Our reason for doing so is that this approach is more natural, and leads the reader to a clearer understanding of elliptic curves. Additionally, an elliptic curve is really a subset of the projective plane and so, presenting it as a subset of the affine plane gives an incomplete picture of the curve.

## 2.1 Projective Space

Prior to our exposition of elliptic curves, it is necessary to introduce a few concepts central to their theory. Throughout this thesis, let $K$ be a field, $\bar{K}$ its algebraic closure. We write $\bar{K}^{\times} = \bar{K}\backslash\{0\}$ and $K^{\times} = K\backslash\{0\}$ .

**Definition 2.1.1** *Let n be a positive integer.* Affine $n$-space over $\bar{K}$, *written* $\mathbb{A}^n(\bar{K})$, *is the set* $\{(a_1, a_2, \cdots, a_n) : a_1, \cdots, a_n \in \bar{K}\}$. *Elements of affine n-space over* $\bar{K}$ *are called* (affine) points. Affine $n$-space over $K$, *written* $\mathbb{A}^n(K)$, *is the subset of* $\mathbb{A}^n(\bar{K})$ *consisting of points with coordinates in* $K$. *We call the set* $\mathbb{A}^2(\bar{K})$ *the* affine plane over $\bar{K}$.

**Example 2.1.2** *Let* $K = \mathbb{Q}$. *Then* $\mathbb{A}^2(\bar{\mathbb{Q}}) = \bar{\mathbb{Q}} \times \bar{\mathbb{Q}}$, *called the affine plane over* $\bar{\mathbb{Q}}$.

**Definition 2.1.3** *Let $f(x,y) \in \bar{K}[x,y]$ be a polynomial. We call a set of the form $\{(x_0,y_0) \in \mathbb{A}^2(\bar{K}) : f(x_0,y_0) = 0\}$ an* affine plane curve over $\bar{K}$ *and write $f : f(x,y) = 0$ for short to denote this set. Elements of this set are called* points on $f$ *and the curve $f$ is called the* locus *of $f(x,y)$.*

**Example 2.1.4** *Let $\bar{K} = \mathbb{C}$; let $f(x,y) = y^2 - x^3$. Then $f$ is an affine complex plane curve. The point $(\zeta, 1)$, where $\zeta$ is a cube root of unity, is a point on this curve.*

**Definition 2.1.5** *Consider the following equivalence relation on the set $\mathbb{A}^{n+1}(\bar{K})^{\times}$ of* non-zero *elements in affine $(n+1)$-space over $\bar{K}$:*

$$(x_0, \cdots, x_n) \sim (y_0, \cdots, y_n) \Leftrightarrow (x_0, \cdots, x_n) = \lambda(y_0, \cdots, y_n), \exists \lambda \in \bar{K}^{\times}.$$

*Let $[x_0 : x_1 : \cdots : x_n]$ denote the equivalence class of $(x_0, x_1, \cdots, x_n) \in \mathbb{A}^{n+1}(\bar{K}) \setminus \{0\}$ and let $\mathbb{P}^n(\bar{K})$ denote the set of such equivalence classes as $(x_0, \cdots, x_n)$ ranges over $\mathbb{A}^{n+1}(\bar{K}) \setminus \{0\}$; thus,*

$$\mathbb{P}^n(\bar{K}) := \{[x_0 : x_1 : \cdots : x_n] | (x_0, x_1, \cdots, x_n) \in \mathbb{A}^{n+1}(\bar{K}) \setminus \{0\}\}.$$

*We call $\mathbb{P}^n(\bar{K})$* projective $n$-space over $\bar{K}$ *and its elements are called* (projective) points. *We define* projective $n$-space over $K$ *to be the subset of $\mathbb{P}^n(\bar{K})$ of equivalence classes with a representative having coordinates in $K$, and denote it by $\mathbb{P}^n(K)$.*

Note that $[x_0 : \cdots : x_n] \in \mathbb{P}^n(K)$ does not imply that $x_i \in K$ for all $i$. It simply means that the class has a representative with this property.

**Definition 2.1.6** *For $n = 2, \mathbb{P}^2(\bar{K})$ is called the* projective plane over $\bar{K}$.

**Example 2.1.7** *If $K = \mathbb{Q}$, then $[1:2:3] = [\sqrt{2}:\sqrt{8}:\sqrt{18}] \in \mathbb{P}^2(\mathbb{Q})$ since*

$$(\sqrt{2}, \sqrt{8}, \sqrt{18}) = \sqrt{2}(1, 2, 3).$$

**Definition 2.1.8** *Let $a, b, c \in \bar{K}$, at least one nonzero. A* line *in $\mathbb{P}^2(\bar{K})$ is a set of the form*

$$\ell = \{[x_0 : y_0 : z_0] \in \mathbb{P}^2(\bar{K}) \mid ax_0 + by_0 + cz_0 = 0\}.$$

*We write for short*

$$\ell : ax + by + cz = 0.$$

**Definition 2.1.9** *The line $\ell : z = 0$ is called the* line at infinity *in $\mathbb{P}^2(\bar{K})$, and denoted $\ell_\infty$.*

## 2.2 Irreducible Projective Plane Curves

In this section, we relate homogeneous polynomials and subsets of the projective plane. In particular, we will see that such subsets are completely determined by their irreducible factors.

**Definition 2.2.1** *Let $f(x, y, z) \in \bar{K}[x, y, z]$. The polynomial $f(x, y, z)$ is said to be* irreducible *if $f(x, y, z) = g(x, y, z)h(x, y, z)$ (with $g(x, y, z), h(x, y, z) \in \bar{K}[x, y, z]$) implies $g(x, y, z)$ or $h(x, y, z)$ is a unit in $\bar{K}[x, y, z]$.*

**Example 2.2.2** *The polynomial $f(x, y, z) = x^3 + y^3 - 1729z^3 \in \bar{K}[x, y, z]$ is irreducible if and only if the characteristic of $K$ is not equal to $3, 7, 13$ or $19$.*

**Proof.** Suppose $f(x,y,z) = g(x,y,z)h(x,y,z)$, with $g(x,y,z), h(x,y,z) \in \bar{K}[x,y,z]$. If $f(x,y,z)$ factors non-trivially, then it must factor as a product of homogeneous polynomials whose degrees sum to the degree of $f(x,y,z)$, in this case 3. For if $d_1$ is the degree of the highest degree term of $g(x,y,z)$ and $d_2$ that of the lowest degree; and if $d_3$ is the degree of the highest degree term of $h(x,y,z)$ and $d_4$ of the lowest, then $d_1 + d_3 = d_2 + d_4 = 3$, which forces $d_1 = d_2, d_3 = d_4$. Since the degree of $f(x,y,z)$ is 3, this means that it must factor as the product of linear and quadratic homogeneous polynomials. Suppose this was the case. Then

$$x^3 + y^3 - 1729z^3 = (a_0x^2 + a_1y^2 + a_2z^2 + a_3xy + a_4xz + a_5yz)(b_0x + b_1y + b_2z)$$

for $a_0, a_1, a_2, a_3, a_4, a_5, b_0, b_1, b_2 \in \bar{K}$. This yields the following system of equations:

$$\begin{aligned}
a_0b_0 &= 1 && (2.1)\\
a_1b_1 &= 1 && (2.2)\\
a_2b_2 &= -1729 && (2.3)\\
a_0b_1 + a_3b_0 &= 0 && (2.4)\\
a_0b_2 + a_4b_0 &= 0 && (2.5)\\
a_1b_0 + a_3b_1 &= 0 && (2.6)\\
a_2b_0 + a_4b_2 &= 0 && (2.7)\\
a_1b_2 + a_5b_1 &= 0 && (2.8)\\
a_2b_1 + a_5b_2 &= 0 && (2.9)\\
a_3b_2 + a_4b_1 + a_5b_0 &= 0. && (2.10)
\end{aligned}$$

First, observe that equations 2.1 through 2.3 imply that $a_0, a_1, a_2, b_0, b_1, b_2$ are all non-zero and the remaining equations imply that $a_3, a_4$ and $a_5$ are also non-zero. We can express all coefficients in terms of $a_0$. Equations 2.4 and 2.6 force $a_0^3 = a_1^3$, i.e. $a_1 = ua_0$, where $u$ is a cube root of unity. To see this, note that multiplying equation 2.4 by $a_0$ gives $a_3 = -a_0^2 b_1 = \frac{-a_0^2}{a_1}$. Likewise, equation 2.6 gives $a_3 = -a_1^2 b_0 = \frac{-a_1^2}{a_0}$. Therefore, $b_1 = \frac{u^2}{a_0}$ and $a_3 = -u^2 a_0$. Using the same line of reasoning, equation 2.5 forces $b_2 = -a_4 b_0^2 = \frac{-a_4}{a_0^2}$ and equation 2.7 forces $a_2 = -a_0 a_4 b_2 = \frac{a_4^2}{a_0}$. Since $a_2 b_2 = -1729$, this means that $\frac{-a_4^3}{a_0^3} = -1729$ so $a_4 = (v1729^{\frac{1}{3}})a_0$, $v$ a cube root of unity, and $a_2 = (v^2 1729^{\frac{2}{3}})a_0, b_2 = \frac{-1729}{a_2} = \frac{-v1729^{\frac{1}{3}}}{a_0}$. Finally, equation 2.8 forces $a_5 = \frac{-a_1 b_2}{b_1} = -a_1^2 b_2 = u^2 v 1729^{\frac{1}{3}} a_0$.

The first 9 equalities hold when substituting these values for $a_0, \cdots, a_5, b_0, b_1, b_2$. However, the final expression $a_3 b_2 + a_4 b_1 + a_5 b_0$ evaluates to $3u^2 v 1729^{\frac{1}{3}}$. If $char(K) = 3$, this expression is equal to 0. Similarly, since $1729 = 7 * 13 * 19$, it is equal to 0 when the characteristic of $K$ is $7, 13$ or 19. Otherwise, this expression is non-zero. Hence, the polynomial $x^3 + y^3 - 1729z^3$ is irreducible over any field of characteristic not equal to $3, 7, 13$ or 19. □

**Definition 2.2.3** *An* affine plane curve $C$ *over* $\bar{K}$ *is a subset of* $\mathbb{A}^2(\bar{K})$ *of the form*

$$\{(x_0, y_0) \in \mathbb{A}^2(\bar{K}) \mid C(x_0, y_0) = 0\}$$

*for some polynomial* $C(x, y) \in \bar{K}[x, y]$.

**Definition 2.2.4** *An* irreducible projective plane curve $C$ *over* $\bar{K}$ *is a subset of* $\mathbb{P}^2(\bar{K})$ *of the form*

$$\{[x_0 : y_0 : z_0] \in \mathbb{P}^2(\bar{K}) \mid C(x_0, y_0, z_0) = 0\}$$

*for some irreducible homogeneous polynomial* $C(x,y,z) \in \bar{K}[x,y,z]$. *We write* $C : C(x,y,z) = 0$ *for short. Elements of* $C$ *are called* points on the curve $C$ *and* $C$ *is called the* locus *of the polynomial* $C(x,y,z)$.

**Example 2.2.5** *Assume the characteristic of* $\bar{K}$ *is not 3, 7, 13, or 19 and let* $C(x,y,z) = x^3 + y^3 - 1729z^3$. *Since* $C(x,y,z) \in \bar{K}[x,y,z]$ *is irreducible, as shown in the proof of Example 2.2.2, the locus* $C \subset \mathbb{P}^2(\bar{K})$ *of* $C(x,y,z)$ *is an irreducible projective plane curve over* $\bar{K}$.

Removing a finite number of points from an irreducible projective plane curve, we get a bijective correspondence between the remaining points and the points of an affine plane curve, as the next lemma shows.

**Lemma 2.2.6** *The points of an irreducible projective plane curve* $C : C(x,y,z) = 0$, *minus the points on the line at infinity, are in bijective correspondence with the points on the affine plane curve* $C_{\mathit{aff}} \colon C_{\mathit{aff}}(\bar{x},\bar{y}) = 0$, *where* $C_{\mathit{aff}}(\bar{x},\bar{y}) = C(\frac{x}{z},\frac{y}{z},1), \bar{x} = \frac{x}{z}$ *and* $\bar{y} = \frac{y}{z}$. *The correspondence is given by* $[x_0 : y_0 : 1] \longrightarrow (x_0, y_0)$.

**Proof.** Suppose that $[x_0 : y_0 : 1] \in C \setminus \ell_\infty$. Then $C(x_0, y_0, 1) = 0$. Thus, $\frac{C(x_0,y_0,1)}{1^d} = 0$, so $C_{\mathit{aff}}(x_0, y_0) = 0$, since by definition, $C_{\mathit{aff}}(\bar{x},\bar{y}) = C(\frac{x}{z},\frac{y}{z},1) = \frac{C(x,y,z)}{z^d}$. Likewise, if $C_{\mathit{aff}}(x_0,y_0) = 0$, then $\frac{C(x_0,y_0,1)}{1^d} = 0$, so $[x_0 : y_0 : 1] \in C \setminus \ell_\infty$. That the correspondence is bijective is clear. □

**Definition 2.2.7** *Let* $C(x,y,z) \in \bar{K}[x,y,z]$ *be irreducible and let* $C \subset \mathbb{P}^2(\bar{K})$ *be the locus of* $C(x,y,z)$. *The irreducible projective plane curve* $C$ *is* defined over $K$ *if there exists* $C'(x,y,z) \in K[x,y,z]$ *such that the locus of the image of* $C'(x,y,z)$ *under the* *inclusion* $K[x,y,z] \hookrightarrow \bar{K}[x,y,z]$ *equals* $C$. *We write* $C/K$ *when* $C \subset \mathbb{P}^2(\bar{K})$ *is defined over* $K$.

**Example 2.2.8** *The curve* $C : \sqrt{2}x^3 + \sqrt{2}y^3 - 1729\sqrt{2}z^3 = 0$ *over* $\bar{\mathbb{Q}}$ *is defined over* $\mathbb{Q}$ *because the locus* $C \subset \mathbb{P}^2(\bar{\mathbb{Q}})$ *of* $C(x,y,z) = \sqrt{2}x^3 + \sqrt{2}y^3 - 1729\sqrt{2}z^3 \in \bar{\mathbb{Q}}[x,y,z]$ *is equal to the locus* $C'$ *of* $C'(x,y,z) = x^3 + y^3 - 1729z^3 \in \mathbb{Q}[x,y,z]$.

**Definition 2.2.9** *Let* $f(x,y,z) \in \bar{K}[x,y,z]$ *be a homogeneous polynomial. We define* $V(f(x,y,z))$ *to be the set* $\{[x_0 : y_0 : z_0] \in \mathbb{P}^2(\bar{K}) : f(x_0, y_0, z_0) = 0\}$.

An irreducible projective plane curve $C$ is a subset of the projective plane of the form $V(f(x,y,z))$, for $f(x,y,z) \in \bar{K}[x,y,z]$ some irreducible homogeneous polynomial. The example just given shows that this polynomial need not be unique; in other words, the set $C$ can be equal to $V(f'(x,y,z))$ for some $f'(x,y,z) \neq f(x,y,z) \in \bar{K}[x,y,z]$. However, the polynomials $f'(x,y,z)$ for which $C = V(f'(x,y,z))$ are quite limited, as the next theorem shows; namely, they are all multiples of $f(x,y,z)$ in $\bar{K}[x,y,z]$.

**Theorem 2.2.10 (Nullstellensatz for irreducible projective plane curves)** *Let* $f(x,y,z) \in \bar{K}[x,y,z]$ *be an irreducible homogeneous polynomial and let* $(f(x,y,z))$ *be the principal* $\bar{K}[x,y,z]$*-ideal generated by* $f(x,y,z)$. *If* $g(x,y,z) \in \bar{K}[x,y,z]$ *is a homogeneous polynomial such that* $g(x_0, y_0, z_0) = 0$ *for all* $[x_0 : y_0 : z_0] \in V(f(x,y,z))$, *then* $g(x,y,z) \in (f(x,y,z))$, *i.e.* $f(x,y,z)$ *divides* $g(x,y,z)$.

**Proof.** See [4, Theorem 2, II.4.3]. □

**Corollary 2.2.11** *Let $C : C(x,y,z) = 0$ be an irreducible projective plane curve. If $C = \{[x_0 : y_0 : z_0] \in \mathbb{P}^2(\bar{K}) : C'(x_0, y_0, z_0) = 0\}$ for some irreducible homogeneous polynomial $C'(x,y,z) \in \bar{K}[x,y,z]$, then $C'(x,y,z) = kC(x,y,z)$, where $k \in \bar{K}[x,y,z]^*$, the group of units of $\bar{K}[x,y,z]$, i.e. $k \in \bar{K}^\times$.*

**Proof.** By the Nullstellensatz, $C(x,y,z)$ divides $C'(x,y,z)$ and $C'(x,y,z)$ divides $C(x,y,z)$. In other words, $C'(x,y,z) = kC(x,y,z)$ for some $k \in \bar{K}[x,y,z]^*$, because $C'(x,y,z)$ is irreducible. □

Observe that the locus of *any* homogeneous polynomial in $\bar{K}[x,y,z]$ is completely determined by its irreducible factors. Hence, for any polynomial $C(x,y,z) \in \bar{K}[x,y,z]$, $V(C(x,y,z)) = V(C(x,y,z)^n)$ for all $n \in \mathbb{N}$. In Chapter 3 we will see — via Bézout's theorem — that the loci of two homogeneous polynomials are equal if and only if the polynomials have the same irreducible factors.

Henceforth, for convenience, when we speak of a curve, we will be speaking only of an irreducible projective plane curve over the algebraically closed field $\bar{K}$.

**Definition 2.2.12** *Let $C$ be a curve defined over $K$. We denote by $C(K)$ the subset $C \cap \mathbb{P}^2(K)$ of $C$. A point $P \in C$ in $C(K)$ is called a $K$-*rational point.

**Example 2.2.13** *Let $C \subset \mathbb{P}^2(\bar{\mathbb{Q}})$ be the curve $C : x^3 + y^3 - 1729z^3 = 0$.* $[12 : 1 : 1]$ *is a $\mathbb{Q}$-rational point on $C$ since* $[12 : 1 : 1] \in \mathbb{P}^2(\mathbb{Q})$ *and*

$$12^3 + 1^3 - 1729(1)^3 = 1728 + 1 - 1729 = 0,$$

*so* $[12 : 1 : 1] \in C$.

**Proposition 2.2.14** *Let $C = V(C(x,y,z)) = V(C'(x,y,z))$ be a curve, where $C(x,y,z)$ and $C'(x,y,z) \in \bar{K}[x,y,z]$ are distinct irreducible homogeneous polynomials. Let $P \in C$. Then*

$$\frac{\partial C'(x,y,z)}{\partial x}(P) = 0 \Leftrightarrow \frac{\partial C(x,y,z)}{\partial x}(P) = 0$$
$$\frac{\partial C'(x,y,z)}{\partial y}(P) = 0 \Leftrightarrow \frac{\partial C(x,y,z)}{\partial y}(P) = 0$$
$$\frac{\partial C'(x,y,z)}{\partial z}(P) = 0 \Leftrightarrow \frac{\partial C(x,y,z)}{\partial z}(P) = 0.$$

**Proof.** By Corollary 2.2.11, $C'(x,y,z) = kC(x,y,z)$ for some $k \in \bar{K}^{\times}$. The result now follows since

$$\begin{aligned} \frac{\partial C'(x,y,z)}{\partial x} &= k\frac{\partial C(x,y,z)}{\partial x} \\ \frac{\partial C'(x,y,z)}{\partial y} &= k\frac{\partial C(x,y,z)}{\partial y} \\ \frac{\partial C'(x,y,z)}{\partial z} &= k\frac{\partial C(x,y,z)}{\partial z}. \end{aligned}$$

□

**Definition 2.2.15** *For a curve $C : C(x,y,z) = 0$, we say that $C$ is* singular *at a point $P \in C$ if the partial derivatives at $P$ are all 0, i.e.*

$$\frac{\partial C(x,y,z)}{\partial x}(P) = \frac{\partial C(x,y,z)}{\partial y}(P) = \frac{\partial C(x,y,z)}{\partial z}(P) = 0.$$

*In this case, we say that $P$ is a* singular point. *A curve with no singular points is called* non-singular *or* smooth*; otherwise, it is called* singular.

**Remark 2.2.16** *The fact that singularity is a well-defined notion follows immediately from the preceding proposition, as well as Corollary 2.2.11. In other words,* *singularity does not depend on the model of the curve used (i.e. the polynomial for which we take the curve $C$ to be the locus).*

**Example 2.2.17** *Let $C/\mathbb{F}_2$ be the curve which is the locus of the polynomial $y^2z-x^3$ (i.e. $C : y^2z - x^3 = 0$) over $\bar{\mathbb{F}}_2$, where $\mathbb{F}_2$ is the finite field of 2 elements. Then $C$ is singular because it has a singular point at $[0:0:1]$, for*

$$\begin{aligned} \frac{\partial C(x,y,z)}{\partial x} &= -3x^2 \\ &= x^2 \\ \frac{\partial C(x,y,z)}{\partial y} &= 2yz \\ &= 0 \\ \frac{\partial C(x,y,z)}{\partial z} &= y^2, \end{aligned}$$

*and all three of these partial derivatives are 0 at $[0:0:1]$.*

Having introduced the partial derivatives of a curve, we may now introduce the notion of the tangent line to a point on a curve. Such a definition will be indispensable in our treatment of elliptic curves in the third chapter and beyond.

**Definition 2.2.18** *Let $C$ be a curve and $P$ a point on $C$. The* tangent line to $C$ at *$P$ is the line*

$$\ell_P : \frac{\partial C(x,y,z)}{\partial x}(P)x + \frac{\partial C(x,y,z)}{\partial y}(P)y + \frac{\partial C(x,y,z)}{\partial z}(P)z = 0.$$

**Example 2.2.19** *Consider our favourite curve, $C : x^3 + y^3 - 1729z^3 = 0$, over a field of characteristic not equal to 3,7,13, or 19, which we introduced in Example*

*2.2.2. If $P = [x_0 : y_0 : z_0]$ is a point on $C$, then the tangent line to $C$ at $P$ is given by the equation*

$$x_0^2 x + y_0^2 y - 1729 z_0^2 z = 0, \tag{2.11}$$

*because*

$$\begin{aligned} \frac{\partial C(x,y,z)}{\partial x} &= 3x^2 \\ \frac{\partial C(x,y,z)}{\partial y} &= 3y^2 \\ \frac{\partial C(x,y,z)}{\partial z} &= -5187z^2, \end{aligned}$$

*so dividing the partial derivatives by 3 gives Equation 2.11.*

**Remark 2.2.20** *It should be clear that a point $P$ on a curve $C$ will always lie on the tangent line to $C$ at $P$. For if $C$ is the locus of an nth degree irreducible homogeneous polynomial $C(x, y, z)$, then $\ell_P(P) = nC(P) = 0$.*

## 2.3 The Coordinate Ring and Function Field

In this section, we introduce the function field of a curve. An understanding of the function field of a curve is key to an understanding of the curve itself, because a function field essentially determines the curve, in the sense that if two curves have the same function field (up to isomorphism), then their points are in bijective correspondence.

**Proposition 2.3.1** *Let $C$ be a curve and suppose that*

$$C = V(C(x, y, z)) = V(C'(x, y, z)),$$

*where* $C(x,y,z) \neq C'(x,y,z)$ *are irreducible homogeneous polynomials in* $\bar{K}[x,y,z]$. *Further, suppose that* $f(x,y,z), g(x,y,z) \in \bar{K}[x,y,z]$. *Then*

$$f(x,y,z) + (C(x,y,z)) = g(x,y,z) + (C(x,y,z))$$

*in the factor ring* $\bar{K}[x,y,z]/(C(x,y,z))$ *if and only if*

$$f(x,y,z) + (C'(x,y,z)) = g(x,y,z) + (C'(x,y,z))$$

*in the factor ring* $\bar{K}[x,y,z]/(C'(x,y,z))$.

**Proof.** If $f(x,y,z)+(C(x,y,z)) = g(x,y,z)+(C(x,y,z))$, then $f(x,y,z)-g(x,y,z) \in (C(x,y,z))$, i.e. $f(x,y,z) - g(x,y,z) = h(x,y,z)C(x,y,z)$ for some $h(x,y,z) \in \bar{K}[x,y,z]$. By Corollary 2.2.11, $f(x,y,z) - g(x,y,z) = kh(x,y,z)C'(x,y,z)$, for some $k \in \bar{K}^{\times}$, so $f(x,y,z) + (C'(x,y,z)) = g(x,y,z) + (C'(x,y,z))$. The proof of the converse is analogous. □

**Definition 2.3.2** *Let* $C$ *be a curve.* The coordinate ring $\bar{K}[C]$ *of* $C$ *is the ring of all polynomials in* $\bar{K}[x,y,z]$ *modulo* $(C(x,y,z))$, *where* $(C(x,y,z))$ *is the principal* $\bar{K}[x,y,z]$*-ideal generated by* $C(x,y,z)$, *i.e. the factor ring* $\bar{K}[x,y,z]/(C(x,y,z))$. *If* $C(x,y,z) \in K[x,y,z]$, *then* $K[C]$ *is the subring* $K[x,y,z]/(C(x,y,z))$ *of* $\bar{K}[C]$ *where here,* $(C(x,y,z))$ *is the principal* $K[x,y,z]$*-ideal generated by* $C(x,y,z)$.

**Remark 2.3.3** *By Proposition 2.3.1, the coordinate ring is well-defined since it is independent of the model of the curve used (i.e. which polynomial we take to be* $C(x,y,z)$*). Moreover,* $\bar{K}[C]$ *is an integral domain because* $C(x,y,z)$ *is irreducible in* $\bar{K}[x,y,z]$.

**Lemma 2.3.4** *Let $C : C(x,y,z) = 0$ be a curve and consider the set consisting of quotients $\frac{f(x,y,z)}{g(x,y,z)}$ of homogeneous polynomials $f(x,y,z), g(x,y,z)$ in $\bar{K}[x,y,z]$ such that $g(x,y,z) \notin (C(x,y,z))$ and either $f(x,y,z)$ and $g(x,y,z)$ have the same degree or $f(x,y,z)$ is the $0$ polynomial. Define the relation $\sim$ on this set by $\frac{f(x,y,z)}{g(x,y,z)} \sim \frac{f'(x,y,z)}{g'(x,y,z)}$ if $f(x,y,z)g'(x,y,z) - f'(x,y,z)g(x,y,z) \in (C(x,y,z))$. Then $\sim$ is an equivalence relation.*

**Proof.** For the sake of brevity, denote by $f$ and $g$ the polynomials $f(x,y,z)$ and $g(x,y,z)$, respectively. Once again, the equivalence is well-defined because it is independent of the model used for the curve. For if $C = V(C'(x,y,z))$, where $C'(x,y,z) \neq C(x,y,z)$, then $fg' - f'g \in (C(x,y,z))$ if and only if $fg' - f'g \in (C'(x,y,z))$, by Corollary 2.2.11. The relation is clearly reflexive and symmetric. Transitivity follows as well: if $\frac{f}{g} \sim \frac{f'}{g'}$ and $\frac{f'}{g'} \sim \frac{f''}{g''}$, then

$$fg'' - f''g = \frac{(fg' - f'g)g'' + (f'g'' - g'f'')g}{g'},$$

and since $[(fg' - f'g)g'' + (f'g'' - g'f'')g] \in (C(x,y,z))$ and $g'$ is not in $(C(x,y,z))$, $fg'' - f''g \in (C(x,y,z))$, so $\frac{f}{g} \sim \frac{f''}{g''}$. □

**Example 2.3.5** *Let $C : x^3 + y^3 - 1729z^3 = 0$ over $\bar{\mathbb{Q}}$. Then $\frac{x^2-xy+y^2}{z^2} \sim \frac{1729z}{x+y}$, since $(x^2 - xy + y^2)(x+y) - (z^2)(1729z) \in (C(x,y,z))$. Similarly, $\frac{x^3+y^3-1729z^3}{x^3} \sim \frac{0}{y^2}$, since $[(x^3 + y^3 - 1729z^3)(y^2) - (0)(x^3)] \in (C(x,y,z))$.*

Henceforth, we will only use upper case letters such as $C$ and $E$ to denote affine or projective plane curves. Since there will be no ambiguity, we will, for instance, sometimes use $f$ or $g$ to denote $f(x,y,z)$ and $g(x,y,z)$, respectively, as in the proof of Lemma 2.3.4.

**Proposition 2.3.6** *Let $C$ be a curve and denote by $\bar{K}(C)$ the set of equivalence classes under the equivalence described in Lemma 2.3.4. Then $\bar{K}(C)$ is a field, where multiplication of the class of $\frac{f}{g}$ by that of $\frac{f'}{g'}$ gives the class of $\frac{ff'}{gg'}$, and addition of the classes of $\frac{f}{g}$ and $\frac{f'}{g'}$ gives the class of $\frac{fg'+f'g}{gg'}$.*

**Proof.** Multiplication is well-defined. To see this, note that if $\frac{f}{g} \sim \frac{f'}{g'}$ then

$$\frac{f}{g}\frac{f''}{g''} \sim \frac{f'}{g'}\frac{f''}{g''}$$

because

$$fg'f''g'' - f'gf''g'' = f''g''(fg' - f'g) \in (C(x,y,z)),$$

since by assumption,

$$fg' - f'g \in (C(x,y,z)).$$

Similarly, addition is well-defined. Commutativity, distributivity and associativity clearly hold in $\bar{K}(C)$ for both addition and multiplication. The additive identity is just the class of $\frac{C(x,y,z)}{z^d}$, where $d$ is the degree of $C(x,y,z)$, for $\frac{f(x,y,z)}{g(x,y,z)} + \frac{C(x,y,z)}{z^d} \sim \frac{f(x,y,z)}{g(x,y,z)}$ for any quotient $\frac{f(x,y,z)}{g(x,y,z)}$. The multiplicative identity is the class of the constant quotient $1 = \frac{1}{1}$. The additive inverse of the class of $\frac{f(x,y,z)}{g(x,y,z)}$ is just the class of $\frac{-f(x,y,z)}{g(x,y,z)}$, since $\frac{f(x,y,z)}{g(x,y,z)} + \frac{-f(x,y,z)}{g(x,y,z)} \sim \frac{C(x,y,z)}{z^d}$. Finally, for any non-zero quotient $\frac{f(x,y,z)}{g(x,y,z)}$, i.e. $f(x,y,z) \notin (C(x,y,z))$, the multiplicative inverse is just the class of $\frac{g(x,y,z)}{f(x,y,z)}$. □

**Remark 2.3.7** *It should be apparent why we needed to include quotients of the form $\frac{0}{g}$, $g \notin C(x,y,z)$ in the set of Lemma 2.3.4, and not merely quotients of homogeneous polynomials of the same degree. For consider $\frac{f}{g}$, $f$ and $g$ non-constant. The additive inverse of the class of $\frac{f}{g}$ is the class of $\frac{-f}{g}$. Adding these together gives $\frac{fg-fg}{g^2} = \frac{0}{g^2}$. This is not a quotient of homogeneous polynomials of the same degree, so the* *set of quotients of homogeneous polynomials of the same degree is not closed under addition. If we did not define the equivalence relation for quotients of the form $\frac{0}{g}$, then addition of certain classes would not be well-defined — because for a suitable choice of elements in these classes (such as $\frac{f}{g}$ and $\frac{-f}{g}$ above), their sum would not reside in an equivalence class.*

**Definition 2.3.8** *The field $\bar{K}(C)$ is called the* function field of $C$. *Elements of $\bar{K}(C)$ are called* rational functions.

We call elements of $\bar{K}(C)$ rational functions for the following reason. If $\frac{f}{g}$ is a quotient of homogeneous polynomials of the same degree, we can regard $\frac{f}{g}$ as a function from $\mathbb{P}^2(\bar{K})$ to $\bar{K}$. If $\frac{f}{g} \sim \frac{f'}{g'}$, for another quotient $\frac{f'}{g'}$, then $\frac{f}{g}(P) = \frac{f'}{g'}(P)$ at all points $P$ on $C$ where both $g(P)$ and $g'(P)$ are non-zero. In other words, each nonzero equivalence class consists of quotients of homogeneous polynomials of the same degree which are equal as rational functions on the curve $C$, when restricted to all but finitely many points on $C$ (where the denominators of both quotients are non-zero). One may think of the constant functions as the elements of $\bar{K}$ and the non-constant functions as those elements which are transcendental over $\bar{K}$.

**Proposition 2.3.9** *Denote by $X \in \bar{K}[C]$ the image of $x \in \bar{K}[x, y, z]$ under the quotient map $\bar{K}[x, y, z] \hookrightarrow \bar{K}[C]$, i.e. $X = x + (C(x, y, z))$, and similarly, $Y$ the image of $y$ and $Z$ the image of $z$. Then $\bar{K}(C)$ is the set of quotients $\frac{f(X,Y,Z)}{g(X,Y,Z)}$, where $f(x, y, z)$ and $g(x, y, z)$ are homogeneous polynomials, $g(x, y, z) \notin (C(x, y, z))$, and $f(x, y, z)$ and $g(x, y, z)$ have the same degree if $f(x, y, z) \neq 0$. Furthermore, $\frac{f(X,Y,Z)}{g(X,Y,Z)}$ is the equivalence class of $\frac{f(x,y,z)}{g(x,y,z)}$, and $\frac{f(X,Y,Z)}{g(X,Y,Z)} = \frac{f'(X,Y,Z)}{g'(X,Y,Z)}$ if and only if $f(X, Y, Z)g'(X, Y, Z) - f'(X, Y, Z)g(X, Y, Z) = 0 \in \bar{K}[C]$.*

**Proof.** Suppose $\frac{f(x,y,z)}{g(x,y,z)} \sim \frac{f'(x,y,z)}{g'(x,y,z)}$. Then $f(x,y,z)g'(x,y,z) - f'(x,y,z)g(x,y,z) \in (C(x,y,z))$, so $C(x,y,z) \mid f(x,y,z)g'(x,y,z) - f'(x,y,z)g(x,y,z)$ and hence

$$f(X,Y,Z)g'(X,Y,Z) - f'(X,Y,Z)g(X,Y,Z) = 0.$$

Conversely, if $\frac{f(X,Y,Z)}{g(X,Y,Z)} = \frac{f'(X,Y,Z)}{g'(X,Y,Z)}$, then

$$f(X,Y,Z)g'(X,Y,Z) - f'(X,Y,Z)g(X,Y,Z) = 0 \in \bar{K}[C],$$

so $C(x,y,z) \mid f(x,y,z)g'(x,y,z) - f'(x,y,z)g(x,y,z)$. Thus, $f(x,y,z)g'(x,y,z) - f'(x,y,z)g(x,y,z) \in (C(x,y,z))$ and

$$\frac{f(x,y,z)}{g(x,y,z)} \sim \frac{f'(x,y,z)}{g'(x,y,z)}.$$

□

**Remark 2.3.10** *Note that $\frac{f(X,Y,Z)}{g(X,Y,Z)}$ need not in general be a quotient of homogeneous polynomials in $X, Y, Z$ of the same degree. Consider, for instance, the curve $C : y^2z - x^3 = 0$. Then*

$$\begin{aligned} \frac{X}{Y} &= \frac{x + (C(x,y,z))}{y + (C(x,y,z))} \\ &= \frac{y^2z - x^3 + x + (C(x,y,z))}{y + (C(x,y,z))} \\ &= \frac{Y^2Z - X^3 + X}{Y}. \end{aligned}$$

*(In fact, the numerator of the latter quotient is not even a homogeneous polynomial in $X, Y, Z$.) Nevertheless, we can — and will — always write elements of the function field as quotients of the form $\frac{f(X,Y,Z)}{g(X,Y,Z)}$, where $f(X,Y,Z)$ and $g(X,Y,Z)$ are homogeneous in $X, Y, Z$, and of the same degree when $f(X,Y,Z) \neq 0$.*

For the remainder of this thesis, if $C : C(x,y,z) = 0$ is a curve, let $X, Y$ and $Z$ be as in Proposition 2.3.9, so that $\frac{f(X,Y,Z)}{g(X,Y,Z)} \in \bar{K}(C)$ denotes the equivalence class of $\frac{f(x,y,z)}{g(x,y,z)}$. (In general, we will use the upper case $U$ to denote the residue class of lower case $u$, i.e. $U = u + (C(u,v,w))$.)

**Definition 2.3.11** *We denote by $K(C)$ the subset of $\bar{K}(C)$ consisting of equivalence classes containing a quotient $\frac{f(x,y,z)}{g(x,y,z)}$, where $f(x,y,z), g(x,y,z) \in K[x,y,z]$. Elements of $K(C)$ are called* rational functions defined over $K$.

**Proposition 2.3.12** *The set $K(C)$ is a subfield of $\bar{K}(C)$.*

**Proof.** $K(C)$ clearly contains both 0 and 1. It suffices, then, to show that $K(C)$ is closed under addition, multiplication and inverses. If $\frac{f_1(X,Y,Z)}{g_1(X,Y,Z)}$ and $\frac{f_2(X,Y,Z)}{g_2(X,Y,Z)} \in K(C)$, then the sum $\frac{f_1(X,Y,Z)g_2(X,Y,Z)+f_2(X,Y,Z)g_1(X,Y,Z)}{g_1(X,Y,Z)g_2(X,Y,Z)}$ is clearly also in $K(C)$. Similarly, the product $\frac{f_1(X,Y,Z)f_2(X,Y,Z)}{g_1(X,Y,Z)g_2(X,Y,Z)}$ must be in $K(C)$. If $\frac{f(X,Y,Z)}{g(X,Y,Z)} \in K(C)$, then $\frac{-f(X,Y,Z)}{g(X,Y,Z)}$ and $\frac{g(X,Y,Z)}{f(X,Y,Z)}$ are in $K(C)$. □

Note that $\frac{f(X,Y,Z)}{g(X,Y,Z)} \in K(C)$ does not necessarily imply that $f(x,y,z), g(x,y,z) \in K[x,y,z]$, as the next example shows.

**Example 2.3.13** *Consider $C/\mathbb{Q} : x^3 + y^3 - 1729z^3 = 0$. Then $\frac{\sqrt{2}X}{\sqrt{2}Y} \in K(C)$, since $\frac{\sqrt{2}X}{\sqrt{2}Y} = \frac{X}{Y}$, the class of $\frac{x}{y}$.*

The next result gives a precise characterization of function fields of curves. We will use this fact throughout the rest of this thesis.

**Proposition 2.3.14** *Let $C : C(x,y,z) = 0$ be a curve and let $a = \frac{X}{Z}$ and $b = \frac{Y}{Z}$. Then $\bar{K}(C) = \bar{K}(a,b)$. In particular, $\bar{K}(C)$ is a finitely generated extension of $\bar{K}$ of transcendence degree one.*

**Proof.** It is easily seen that any quotient of homogeneous polynomials $\frac{f(x,y,z)}{g(x,y,z)}$, where $f$ and $g$ are of the same degree, can be expressed as a rational function in $\frac{x}{z}$ and $\frac{y}{z}$. Therefore, $\frac{f(X,Y,Z)}{g(X,Y,Z)}$ is a rational function of $a$ and $b$. Furthermore, $a$ and $b$ are algebraically dependent because $C(a,b,1) = 0$. Since $a$ is transcendental over $\bar{K}$, the transcendence degree of $\bar{K}(C)$ over $\bar{K}$ is 1. □

**Remark 2.3.15** *The generating set in the proposition above is not unique. That is,* $\bar{K}(C) = \bar{K}(\frac{a}{b}, \frac{1}{b})$ *and* $\bar{K}(C) = \bar{K}(\frac{b}{a}, \frac{1}{a})$*, since* $\bar{K}(a,b) = \bar{K}(\frac{a}{b}, \frac{1}{b}) = \bar{K}(\frac{b}{a}, \frac{1}{a})$.

## 2.4 Valuation Theory and Orders

We now recall some facts regarding valuation theory. Subsequently, we discuss the local ring of a smooth curve at a point. While it may not be immediately apparent why we need the local ring, it will become obvious in the section on divisors at the beginning of Chapter 4.

**Definition 2.4.1** *Let $K$ be a field. A* discrete valuation *on $K$ is a function $v : K \longrightarrow \mathbb{Z} \cup \infty$ with the following properties:*

1. $v(ab) = v(a) + v(b)$
2. $v(a+b) \geq min\{v(a), v(b)\}$
3. *$v$ is surjective*
4. $v(a) = \infty \Leftrightarrow a = 0$.

*By convention, we define $\infty + v(a)$ to be $\infty$ whence $v(0) = v(0 * a) = v(0) + v(a)$.*

**Proposition 2.4.2** *The set*

$$R_v = \{a \in K \mid v(a) \geq 0\}$$

*is a subring of $K$ with identity.*

**Proof.** Since $v(0) = \infty$, we have $0 \in R_v$, so we need only show that $R_v$ contains 1, is closed under addition, multiplication and additive inverses. Note that from property (1) above, $v(1) = v(1 * 1) = v(1) + v(1)$, so $v(1) = 0$ and $1 \in R_v$. Applying this same property again, we find that $R_v$ is closed under multiplication and property (2) gives us closure under addition. Finally, by property (1), we find that $0 = v(1) = v((-1) * (-1)) = v(-1) + v(-1) = 2v(-1)$, from which we conclude that $v(-1) = 0$. Thus, for any $a \in R_v$, $v(-a) = v(-1) + v(a) = v(a) \geq 0$. Hence, $-a \in R_v$ and $R_v$ is closed under additive inverses. □

**Definition 2.4.3** *The ring $R_v$ is called the* valuation ring of $v$.

**Proposition 2.4.4** *Let $v$ be a discrete valuation on a field $K$. Then for all $a \in K$, either $a \in R_v$ or $a^{-1} \in R_v$.*

**Proof.** Applying property (1) from Definition 2.4.1, we find that $0 = v(1) = v(aa^{-1}) = v(a) + v(a^{-1})$. Hence, either $v(a) \geq 0$ or $v(a^{-1}) \geq 0$. □

In fact, the valuation ring $R_v$ of a discrete valuation $v$ is a principal ideal domain with a unique maximal ideal, as the next proposition states.

**Proposition 2.4.5** *Let $v : K \longrightarrow \mathbb{Z} \cup \infty$ be a discrete valuation on a field $K$, with discrete valuation ring $R_v$. Then $R_v$ is a principal ideal domain with a unique* *maximal ideal $M_v$. The ideal $M_v$ is the set*

$$M_v = \{a \in K \mid v(a) > 0\}.$$

*Furthermore, if $M_v = (t)$, with $(t)$ the principal $R_v$-ideal generated by an element $t \in R_v$, then every non-zero $R_v$-ideal is of the form $(t^n)$ for some $n \in \mathbb{Z}$.*

**Proof.** See [6, Proposition 5, Section 16.2]. □

**Definition 2.4.6** *A generator $t$ of $M_v$ at the end of Proposition 2.4.5 is called a* uniformizing parameter *for $v$.*

**Proposition 2.4.7** *Let $C$ be a smooth curve and $P \in C$. Then the set*

$$\bar{K}(C)_P = \left\{ f \in \bar{K}(C) \mid f = \frac{g}{h}, h(P) \neq 0, \exists\, \frac{g}{h} \in \bar{K}(C) \right\}$$

*is a ring with identity.*

**Proof.** This set clearly contains 0 and 1. We need only establish closure under addition, multiplication and additive inverses. If $f, f' \in \bar{K}(C)_P$ such that $f = \frac{g}{h}, f' = \frac{g'}{h'}$, with $h(P) \neq 0, h'(P) \neq 0$, then obviously $f + f'$ and $ff'$ are in $\bar{K}(C)_P$, since $h(P)h'(P) \neq 0$. Likewise, $-f = \frac{-g}{h} \in \bar{K}(C)_P$. □

**Remark 2.4.8** *If $\frac{g}{h} \in \bar{K}(C)_P$, it does not follow that $h(P) \neq 0$. It simply means that there exists $\frac{g'}{h'} \in \bar{K}(C)$ such that $h'(P) \neq 0$ and $\frac{g}{h} = \frac{g'}{h'}$.*

**Definition 2.4.9** *The ring $\bar{K}(C)_P$ is called the* local ring of $C$ at $P$.

**Definition 2.4.10** *Let $C$ be a smooth curve and $P \in C$. Define $M_P$ to be the set*

$$M_P = \left\{ f \in \bar{K}(C)_P \mid f(P) = 0 \right\}.$$

**Example 2.4.11** *Consider $C/\mathbb{Q} : y^2z - x^3 - z^3 = 0, P = [0 : 1 : 0] \in C$, and let $\ell_1, \ell_2$ be the lines*

$$\begin{aligned} \ell_1 : z &= 0 \\ \ell_2 : x &= 0. \end{aligned}$$

*Then $\frac{\ell_1(X,Y,Z)}{\ell_2(X,Y,Z)} = \frac{Z}{X} = \frac{X^2}{Y^2-Z^2}$, since $(Y^2 - Z^2)(Z) - (X)(X^2) = Y^2Z - X^3 - Z^3 = 0$. Now $\frac{X^2}{Y^2-Z^2}(P) = \frac{0}{1} = 0$, so $\frac{Z}{X} \in M_P$. The function field of $C$ is $\bar{\mathbb{Q}}(a, \sqrt{a^3+1})$, where $a = \frac{X}{Z}$ and $\sqrt{a^3+1} = \frac{Y}{Z}$. The local ring $\bar{\mathbb{Q}}(C)_P$ of $C$ at $P$ is $\bar{\mathbb{Q}}[\frac{X}{Y}]$ and $M_P = (\frac{X}{Y})\bar{\mathbb{Q}}(C)_P$.*

**Proposition 2.4.12** *The set $M_P$ is a $\bar{K}(C)_P$-ideal.*

**Proof.** The set $M_P$ contains 0 and is obviously closed under addition and additive inverses. Hence, $M_P$ is an additive subgroup of $\bar{K}(C)_P$. Moreover, if $f \in M_P$ and $r \in \bar{K}(C)_P$ then it follows that $fr \in M_P$, so $M_P$ is an ideal in $\bar{K}(C)_P$. □

Not coincidentally, $M_P$ is a maximal $\bar{K}(C)_P$-ideal, which is easily seen, since $\bar{K}(C)_P/M_P$ is a field isomorphic to $\bar{K}$, with the isomorphism given by

$$f + M_P \longrightarrow f(P).$$

This motivates the following proposition.

**Proposition 2.4.13** *Let $C$ be a smooth curve and $P \in C$. For any $f \in \bar{K}(C)^\times$, define $ord_P(f)$ , called the* order of $f$ at $P$, *by*

$$ord_P(f) = \begin{cases} max\{d \mid f \in M_P^d\} & \text{if } f \in \bar{K}(C)_P \\ -max\{d \mid \frac{1}{f} \in M_P^d\} & \text{otherwise.} \end{cases}$$

*The value $ord_P(0)$ is defined to be $\infty$. Then the function $ord_P$ is a discrete valuation on $\bar{K}(C)$ with discrete valuation ring $\bar{K}(C)_P$, whose unique maximal ideal is $M_P$.*

**Proof.** See [24, Proposition I.1.7], [2, Proposition 9.2]. □

Note that for any $f, g \in \bar{K}(C)$, $ord_P(f) = -ord_P(\frac{1}{f})$ and $ord_P(fg) = ord_P(f) + ord_P(g)$. We will exploit this fact at the outset of Chapter 4.

**Definition 2.4.14** *Let $f \in \bar{K}(C)^{\times}$, $P$ a point on $C$ and $d = ord_P(f)$. If $d > 0$, we say that $f$ has a* zero of order $d$ *at $P$; if $d < 0$, we say that $f$ has a* pole of order $-d$ *at $P$.*

We will see later that a non-zero rational function can only have finitely many zeros and poles.

**Proposition 2.4.15** *Let $C$ be a curve and $f \in \bar{K}(C)^{\times}$. Then*

$$\sum_{P \in C, ord_P(f) \neq 0} ord_P(f) = 0.$$

**Proof.** See [18, Theorem 11.3]. □

**Example 2.4.16** *Recall the curve $C/\mathbb{Q} : y^2z - x^3 - z^3 = 0$ from Example 2.4.11. Then the rational function $\frac{X}{Y}$ has zeros at the points*

$$\begin{aligned} P_1 &= [0:1:0] \\ P_2 &= [0:1:1] \\ P_3 &= [0:1:-1] \end{aligned}$$

*and poles at the points*

$$\begin{aligned} P_4 &= [1:0:-1] \\ P_5 &= [1:0-\xi] \\ P_6 &= [1:0:-\xi^2], \end{aligned}$$

*where* $\xi$ *is a primitive cube root of unity. We have* $ord_{P_1}(\frac{X}{Y}) = ord_{P_2}(\frac{X}{Y}) = ord_{P_3}(\frac{X}{Y}) = 1$ *and* $ord_{P_4}(\frac{X}{Y}) = ord_{P_5}(\frac{X}{Y}) = ord_{P_6}(\frac{X}{Y}) = -1$, *so*

$$\sum_{P \in C, ord_P(\frac{X}{Y}) \neq 0} ord_P\left(\frac{X}{Y}\right) = 3 \cdot 1 + 3 \cdot -1 = 0.$$

# Chapter 3

# Rational maps

In this chapter, we examine relationships between curves defined over the same field. In particular, we establish the duality between function field embeddings and maps of curves before moving on to isomorphism and a short discussion of separability. Unless otherwise stated, we continue to let $K$ be a field and $\bar{K}$ its algebraic closure.

## 3.1 Field Homomorphisms

This section deals with homomorphisms of function fields. Prior to this, we remind the reader of an elementary fact.

**Lemma 3.1.1** *A ring homomorphism between fields is either injective or trivial.*

**Proof.** If $E$ and $F$ are fields and $\Gamma : E \longrightarrow F$ is a homomorphism, then $ker(\Gamma)$ is an $E$-ideal, so $aE \subset ker(\Gamma)$ for any $a \in ker(\Gamma)$. But if $a \neq 0$, $aE = E$ and so the homomorphism must be identically zero. Furthermore, if $\Gamma$ is non-zero then it must be injective, because $\Gamma(a) = \Gamma(b), a \neq b$ implies $\Gamma(a - b) = 0$, so $ker(\Gamma) \neq \{0\}$. □

**Remark 3.1.2** *Since we will only consider function field homomorphisms which fix $\bar{K}$, we will be dealing exclusively with non-trivial (i.e. non-zero) homomorphisms. In light of Proposition 2.3.14, it follows that for curves $C_1, C_2$, such a homomorphism from $\bar{K}(C_2)$ into $\bar{K}(C_1)$ is completely determined by its action on $\frac{U}{W}$ and $\frac{V}{W}$, since*

$\bar{K}(C_2) = \bar{K}(\frac{U}{W}, \frac{V}{W})$. *(This holds if* $C_2 \neq \ell_\infty : w = 0$. *If not, then* $\frac{U}{W}$ *and* $\frac{V}{W}$ *are undefined, since* $\frac{W}{U} = \frac{W}{V} = 0 \in \bar{K}(C_2)$. *In this case:*

$$\begin{aligned} \bar{K}(C_2) &= \bar{K}(\ell_\infty) \\ &= \bar{K}\left(\frac{U}{V}, \frac{W}{V}\right) \\ &= \bar{K}\left(\frac{U}{V}\right), \end{aligned}$$

*which is to say that* $\bar{K}(\ell_\infty)$ *is a purely transcendental extension of* $\bar{K}$. *As a matter of fact, the function field of any line can easily be shown to be such an extension field.)*

The next result will be of use later on.

**Proposition 3.1.3** *Let* $C_1$ *and* $C_2$ *be curves and let* $\Gamma : \bar{K}(C_2) \longrightarrow \bar{K}(C_1)$ *be a* $\bar{K}$*-homomorphism of function fields. Then* $\bar{K}(C_1)/\Gamma(\bar{K}(C_2))$ *is a finite extension of fields.*

**Proof.** $\bar{K}(C_1)$ is a finitely generated transcendental extension of $\bar{K}$ of transcendence degree one. For $\frac{X}{Z} \in \bar{K}(C_1)$ is transcendental over $\bar{K}$ while $\frac{Y}{Z} \in \bar{K}(C_1)$ is algebraic over $\bar{K}(\frac{X}{Z})$ and every function in $\bar{K}(C_1)$ is a rational function of $\frac{X}{Z}$ and $\frac{Y}{Z}$. (One can derive a polynomial in $\bar{K}(\frac{X}{Z})[t]$ for which $\frac{Y}{Z}$ is a root from the equation defining the curve $C_1$.) Since $\Gamma$ is a non-zero $\bar{K}$-homomorphism, every non-constant rational function $F(\frac{U}{W}, \frac{V}{W}) \in \bar{K}(C_2)$ is mapped by $\Gamma$ to a non-constant rational function $G(\frac{X}{Z}, \frac{Y}{Z}) \in \bar{K}(C_1)$. That is, $\Gamma(\bar{K}(C_2))$ is a transcendental extension of $\bar{K}$ of transcendence degree one contained in $\bar{K}(C_1)$. $\bar{K}(C_1)$ is also algebraic over $\Gamma(\bar{K}(C_2))$, since an element of $\bar{K}(C_1)$ being transcendental over $\Gamma(\bar{K}(C_2))$ would imply that $\bar{K}(C_1)$ has transcendence degree 2 over $\bar{K}$. The result now follows, because $\bar{K}(C_1)$ is a finitely generated algebraic extension of $\Gamma(\bar{K}(C_2))$. □

**Definition 3.1.4** *Let $\Gamma : \bar{K}(C_2) \longrightarrow \bar{K}(C_1)$ be a $\bar{K}$-homomorphism of function fields of curves $C_1 : C_1(x, y, z) = 0, C_2 : C_2(u, v, w) = 0$. If $C_2 \neq \ell_\infty$, the set $R_\Gamma \subseteq C_1$ is defined to be the set of $P \in C_1$ such that there exist homogeneous polynomials $\gamma_1(X, Y, Z), \gamma_2(X, Y, Z), \gamma_3(X, Y, Z) \in \bar{K}[C_1]$ of the same degree for which*

$$\begin{aligned} \Gamma\left(\frac{U}{W}\right) &= \frac{\gamma_1(X,Y,Z)}{\gamma_3(X,Y,Z)} \\ \Gamma\left(\frac{V}{W}\right) &= \frac{\gamma_2(X,Y,Z)}{\gamma_3(X,Y,Z)}, \end{aligned}$$

*and at least one of $\gamma_1, \gamma_2, \gamma_3$ is non-zero at $P$, i.e. $\gamma_i(x_0, y_0, z_0) \neq 0$, for some $i, 1 \leq i \leq 3$. If $C_2 = \ell_\infty$, then $R_\Gamma$ is the set of $P \in C_1$ such that there exist homogeneous polynomials $\gamma_1(X, Y, Z), \gamma_2(X, Y, Z) \in \bar{K}[C_1]$ of the same degree for which*

$$\Gamma\left(\frac{U}{V}\right) = \frac{\gamma_1(X,Y,Z)}{\gamma_2(X,Y,Z)}$$

*and $\gamma_1(P) \neq 0$ or $\gamma_2(P) \neq 0$.*

In order to simplify the exposition during the rest of this chapter, we will often implicitly assume that the curve $C_2$ ($C_1$) is not $\ell_\infty$, so that the rational functions $\frac{U}{W}$ and $\frac{V}{W}$ (respectively $\frac{X}{Z}, \frac{Y}{Z}$) are defined. All of the major results contained herein generalize to curves whose function fields are purely transcendental (such as lines and conics).

**Proposition 3.1.5** *Switching $W$ and $V$ or $W$ and $U$ in Definition 3.1.4 leaves the set $R_\Gamma$ unchanged.*

**Proof.** Recall that we saw at the end of Section 2.2 that $\bar{K}(C_2) = \bar{K}(\frac{U}{V}, \frac{W}{V}) = \bar{K}(\frac{V}{U}, \frac{W}{U})$, so $\Gamma$ is completely determined by $\Gamma(\frac{U}{V}), \Gamma(\frac{W}{V})$ (and also, by $\Gamma(\frac{V}{U}), \Gamma(\frac{W}{U})$).

In the former case, $\Gamma(\frac{U}{V}) = \frac{\gamma_1(X,Y,Z)}{\gamma_2(X,Y,Z)}, \Gamma(\frac{W}{V}) = \frac{\gamma_3(X,Y,Z)}{\gamma_2(X,Y,Z)}$. Thus, $P \in R_\Gamma$ if and only if there exist $\gamma_1(X,Y,Z), \gamma_2(X,Y,Z), \gamma_3(X,Y,Z) \in \bar{K}[C_1]$ for which

$$\begin{aligned} \Gamma\left(\frac{U}{V}\right) &= \frac{\gamma_1(X,Y,Z)}{\gamma_2(X,Y,Z)} \\ \Gamma\left(\frac{W}{V}\right) &= \frac{\gamma_3(X,Y,Z)}{\gamma_2(X,Y,Z)}, \end{aligned}$$

and at least one of $\gamma_1, \gamma_2, \gamma_3$ is non-zero at $P$, i.e. $\gamma_i(x_0, y_0, z_0) \neq 0$, for some $i, 1 \leq i \leq 3$. The third case with $\gamma_1(X,Y,Z)$ in the denominator (i.e. $\bar{K}(C_2) = \bar{K}(\frac{V}{U}, \frac{W}{U})$) is the exact analogue of the first two. □

**Example 3.1.6** *Let*

$$\begin{aligned} C_1 : y^2z - x^3 - xz^2 &= 0, \\ C_2 : v^2w - u^3 + 4uw^2 &= 0, \end{aligned}$$

*be curves over any field. The map of function fields $\Gamma : \bar{K}(C_2) \longrightarrow \bar{K}(C_1)$ determined by*

$$\begin{aligned} \Gamma\left(\frac{U}{W}\right) &= \frac{Y^2}{X^2} \\ \Gamma\left(\frac{V}{W}\right) &= \frac{YZ^2 - X^2Y}{X^2Z}, \end{aligned}$$

*is a $\bar{K}$-homomorphism. To show this, we need to show that $\Gamma$ defined above gives a well-defined embedding of $\bar{K}(C_2)$ into $\bar{K}(C_1)$. Note that since $\Gamma(\frac{U}{W}), \Gamma(\frac{V}{W}) \in \bar{K}(C_1)$, the image $\bar{K}(\Gamma(\frac{U}{W}), \Gamma(\frac{V}{W}))$ of $\bar{K}(C_2)$ under $\Gamma$ is contained in $\bar{K}(C_1)$. It suffices, then, to show that $\Gamma$ is well-defined, i.e. that $\Gamma$ takes $0$ in $\bar{K}(C_2)$ to $0$ in $\bar{K}(C_1)$. For if $f, f'$ are two different representatives of the same equivalence class in $\bar{K}(C_2)$ (i.e. $f \sim f'$), then $\Gamma(0) = 0$ if and only if $\Gamma(f - f') = 0$, or equivalently $\Gamma(f) = \Gamma(f')$.*

*This follows from the fact that* $f \sim f'$ *if and only if* $f(\frac{U}{W}, \frac{V}{W}) = f'(\frac{U}{W}, \frac{V}{W})$, *so* $\Gamma(f(\frac{U}{W}, \frac{V}{W})) = \Gamma(f'(\frac{U}{W}, \frac{V}{W}))$ *if and only if* $0 = \Gamma(f(\frac{U}{W}, \frac{V}{W}) - f'(\frac{U}{W}, \frac{V}{W})) = \Gamma(0)$. *Given that*

$$\begin{aligned}\Gamma(0) &= \Gamma\left(C_2\left(\frac{U}{W}, \frac{V}{W}, 1\right)\right)\\ &= C_2\left(\Gamma\left(\frac{U}{W}\right), \Gamma\left(\frac{V}{W}\right), 1\right),\end{aligned}$$

*where the second equality follows from the fact that* $\Gamma$ *preserves addition and multiplication, we need only show that* $C_2(\Gamma(\frac{U}{W}), \Gamma(\frac{V}{W}), 1) = 0$*:*

$$\begin{aligned}& C_2\left(\Gamma\left(\frac{U}{W}\right), \Gamma\left(\frac{V}{W}\right), 1\right)\\ =\ & C_2\left(\frac{Y^2}{X^2}, \frac{YZ^2 - X^2Y}{X^2Z}, 1\right)\\ =\ & \frac{-Y^6Z^2 + X^6Y^2 + 2X^4Y^2Z^2 + X^2Y^2Z^4}{X^6Z^2}\\ =\ & \frac{Y^2Z - X^3 - XZ^2}{X^3} \cdot \frac{-Y^4Z - X^3Y^2 - XY^2Z^2}{X^3Z^2}\\ =\ & 0,\end{aligned}$$

*so* $\Gamma$ *is indeed well-defined. Moreover,* $\Gamma\left(\frac{U}{W}\right) = \frac{Y^2}{X^2}$ *and* $\Gamma\left(\frac{V}{W}\right) = \frac{YZ^2 - X^2Y}{X^2Z}$ *are transcendental over* $\bar{K}$ *and algebraically dependent via the relation*

$$C_2\left(\frac{Y^2}{X^2}, \frac{YZ^2 - X^2Y}{X^2Z}, 1\right) = 0,$$

*so* $\bar{K}(C_2) = \bar{K}(\frac{U}{W}, \frac{V}{W}) \cong \bar{K}(\frac{Y^2}{X^2}, \frac{YZ^2 - X^2Y}{X^2Z}) \subseteq \bar{K}(C_1)$.

*We now show that* $[0:1:0] \in R_\Gamma$*:*

$$\begin{aligned}\Gamma\left(\frac{U}{W}\right) &= \frac{XY^2}{X^3}\\ \Gamma\left(\frac{V}{W}\right) &= \frac{2XYZ - Y^3}{X^3},\end{aligned}$$

*since* $\frac{XY^2}{X^3} = \frac{Y^2}{X^2}$ *and* $(YZ^2-X^2Y)(X^3)-(2XYZ-Y^3)(X^2Z) = (X^2Y)(Y^2Z-X^3-XZ^2) = 0 \in \bar{K}[C_1]$. *Hence,* $[0:1:0] \in R_\Gamma$ *because* $\gamma_1(X,Y,Z) = XY^2, \gamma_2(X,Y,Z) = 2XYZ - Y^3$, $\gamma_3(X,Y,Z) = X^3$, *and* $\gamma_2(0,1,0) = -1 \neq 0$.

**Proposition 3.1.7** *Let* $\Gamma, C_1$ *and* $C_2$ *be as in Definition 3.1.4. The complement of* $R_\Gamma$ *in* $C_1$ *(the set* $\{P \in C_1 \mid P \notin R_\Gamma\}$*) is finite.*

**Proof.** This is a consequence of Bézout's theorem, which we will encounter in Section 4.1. Briefly, this theorem states that the loci of two relatively prime homogeneous polynomials have only finitely many points in common. Given that

$$\begin{aligned} \Gamma\left(\frac{U}{W}\right) &= \frac{\gamma_1(X,Y,Z)}{\gamma_3(X,Y,Z)} \\ \Gamma\left(\frac{V}{W}\right) &= \frac{\gamma_2(X,Y,Z)}{\gamma_3(X,Y,Z)}, \end{aligned}$$

it follows that there are only finitely many points $P \in C_1$ for which $\gamma_3(P) = 0$, since $\gamma_3(X,Y,Z) \neq 0$ in $\bar{K}[C_1]$ and $C_1(x,y,z)$ is irreducible, so $C_1(x,y,z)$ and $\gamma_3(x,y,z)$ are coprime in $\bar{K}[x,y,z]$. □

## 3.2 Rational Maps

In this section, we define a rational map of curves. We will also see that a $\bar{K}$-homomorphism of function fields from $\bar{K}(C_2)$ into $\bar{K}(C_1)$ induces a rational map from the curve $C_1$ to the curve $C_2$.

**Theorem 3.2.1** *Let* $C_1 : C_1(x,y,z) = 0, C_2 : C_2(u,v,w) = 0$ *be curves with function fields* $\bar{K}(C_1)$ *and* $\bar{K}(C_2)$ *and suppose that* $\Gamma : \bar{K}(C_2) \longrightarrow \bar{K}(C_1)$ *is a* $\bar{K}$*-homomorphism of function fields. For each* $P \in R_\Gamma$*, let* $\gamma_{1,P}(X,Y,Z), \gamma_{2,P}(X,Y,Z)$

*and* $\gamma_{3,P}(X,Y,Z) \in \bar{K}[C_1]$ *be such that*

$$\Gamma\left(\frac{U}{W}\right) = \frac{\gamma_{1,P}(X,Y,Z)}{\gamma_{3,P}(X,Y,Z)}$$
$$\Gamma\left(\frac{V}{W}\right) = \frac{\gamma_{2,P}(X,Y,Z)}{\gamma_{3,P}(X,Y,Z)},$$

*and at least one of* $\gamma_{1,P}, \gamma_{2,P}$ *and* $\gamma_{3,P}$ *is non-zero at* $P$. *Then* $\Gamma$ *induces a map of curves* $\Gamma^{\#} : R_\Gamma \subseteq C_1 \longrightarrow C_2$, *given by*

$$\Gamma^{\#}(P) = \begin{cases} [\Gamma(\frac{U}{W})(P) : \Gamma(\frac{V}{W})(P) : 1] & \text{if } \gamma_{3,P}(P) \neq 0 \\ [\Gamma(\frac{U}{V})(P) : 1 : \Gamma(\frac{W}{V})(P)] & \text{if } \gamma_{2,P}(P) \neq 0 \\ [1 : \Gamma(\frac{V}{U})(P) : \Gamma(\frac{W}{U})(P)] & \text{if } \gamma_{1,P}(P) \neq 0 \end{cases}$$

*for all* $P \in R_\Gamma$.

**Proof.** First, we show that such a map is well-defined. Observe that $\gamma_{1,P}, \gamma_{2,P}$ and $\gamma_{3,P}$ need not be unique. We need to show that $\Gamma^{\#}(P)$ is independent of the representation chosen for $\Gamma(\frac{U}{W})$ and $\Gamma(\frac{V}{W})$. To that end, suppose that

$$\Gamma\left(\frac{U}{W}\right) = \frac{\beta_{1,P}(X,Y,Z)}{\beta_{3,P}(X,Y,Z)}$$
$$\Gamma\left(\frac{V}{W}\right) = \frac{\beta_{2,P}(X,Y,Z)}{\beta_{3,P}(X,Y,Z)},$$

where as usual, $\beta_{1,P}, \beta_{2,P}$ and $\beta_{3,P} \in \bar{K}[C_1]$ are homogeneous polynomials in $X, Y$ and $Z$ of the same degree such that at least one is non-zero at $P$. Without loss of generality, suppose that $\gamma_{3,P}(P)$ and $\beta_{3,P}(P)$ are both non-zero — that is, suppose that there are two different representatives $\frac{\alpha_1(X,Y,Z)}{\alpha_3(X,Y,Z)}$ and $\frac{\beta_1(X,Y,Z)}{\beta_3(X,Y,Z)}$ for $\Gamma(\frac{U}{W})$ which are both defined at $P$. Then

$$\frac{\gamma_{1,P}}{\gamma_{3,P}}(P) = \frac{\beta_{1,P}}{\beta_{3,P}}(P)$$

because

$$\frac{\gamma_{1,P}}{\gamma_{3,P}} = \frac{\beta_{1,P}}{\beta_{3,P}}$$

in $\bar{K}(C_1)$. Consequently, $\Gamma(\frac{U}{W})(P)$ is well-defined and the same argument tells us that $\Gamma(\frac{V}{W})(P)$ is also well-defined.

Next, we need to show that if $P$ falls under two or more of the three cases in the definition of $\Gamma^{\#}$, all relevant maps take the point $P$ to the same point in $\mathbb{P}^2(\bar{K})$. We will only cover one case, namely, the case $\gamma_{2,P}(P) \neq 0, \gamma_{3,P}(P) \neq 0$, since the other two cases can be proven analogously. Since $\Gamma$ is a field homomorphism, $\Gamma(\frac{U}{V}) = \Gamma(\frac{U}{W}\frac{W}{V}) = \Gamma(\frac{U}{W})\Gamma(\frac{W}{V})$ and $\Gamma(\frac{W}{V}) = \frac{1}{\Gamma(\frac{V}{W})}$, so

$$\begin{aligned}
\left[\Gamma\left(\frac{U}{V}\right)(P) : 1 : \Gamma\left(\frac{W}{V}\right)(P)\right] &= \left[\Gamma\left(\frac{U}{W}\right)(P)\Gamma\left(\frac{W}{V}\right)(P) : 1 : \Gamma\left(\frac{W}{V}\right)(P)\right] \\
&= \Gamma\left(\frac{W}{V}\right)(P)\left[\Gamma\left(\frac{U}{W}\right)(P) : \Gamma\left(\frac{V}{W}\right)(P) : 1\right] \\
&= \left[\Gamma\left(\frac{U}{W}\right)(P) : \Gamma\left(\frac{V}{W}\right)(P) : 1\right].
\end{aligned}$$

It now remains to show that the image of $\Gamma^{\#}$ is a subset of $C_2$. Let $d_2$ the degree of $C_2(x,y,z)$, let $P = [x_0 : y_0 : z_0] \in R_\Gamma$, with $\gamma_{1,P}, \gamma_{2,P}, \gamma_{3,P}$ as above, and without loss of generality, let $z_0 \neq 0$. We only consider the case $\gamma_{3,P}(P) \neq 0$. (The other two cases can be proven in an analogous manner). We need to show that $\Gamma^{\#}(P) \in C_2$, i.e. $C_2(\Gamma^{\#}(P)) = 0$. Then since $C_2(\frac{U}{W}, \frac{V}{W}, 1) = \frac{C_2(U,V,W)}{W^{d_2}} = 0 \in \bar{K}(C_2)$, we have

$$\begin{aligned}
C_2(\Gamma^{\#}(P)) &= C_2\left(\Gamma\left(\frac{U}{W}\right), \Gamma\left(\frac{V}{W}\right), 1\right)(P) \\
&= \Gamma\left(C_2\left(\frac{U}{W}, \frac{V}{W}, 1\right)\right)(P) \\
&= \Gamma\left(\frac{C_2(U,V,W)}{W^{d_2}}\right)(P) \\
&= \Gamma(0_{\bar{K}(C_2)})(P) \\
&= 0_{\bar{K}(C_1)}(P) \\
&= 0,
\end{aligned}$$

where the second equality follows from the fact that $\Gamma$ is a $\bar{K}$-homomorphism. □

Observe that if $\Gamma$ is given by

$$\begin{aligned}
\Gamma\left(\frac{U}{W}\right) &= \frac{\gamma_1(X,Y,Z)}{\gamma_3(X,Y,Z)} \\
\Gamma\left(\frac{V}{W}\right) &= \frac{\gamma_2(X,Y,Z)}{\gamma_3(X,Y,Z)},
\end{aligned}$$

then since

$$\begin{aligned}
\frac{C_2(\gamma_1(X,Y,Z), \gamma_2(X,Y,Z), \gamma_3(X,Y,Z))}{\gamma_3(X,Y,Z)^{d_2}} &= C_2\left(\frac{\gamma_1(X,Y,Z)}{\gamma_3(X,Y,Z)}, \frac{\gamma_2(X,Y,Z)}{\gamma_3(X,Y,Z)}, 1\right) \\
&= C_2\left(\Gamma\left(\frac{U}{W}\right), \Gamma\left(\frac{V}{W}\right), 1\right) \\
&= \Gamma\left(C_2\left(\frac{U}{W}, \frac{V}{W}, 1\right)\right) \\
&= \Gamma(0) \\
&= 0,
\end{aligned}$$

we must have

$$C_2(\gamma_1(x,y,z), \gamma_2(x,y,z), \gamma_3(x,y,z)) = C_1(x,y,z)f(x,y,z)$$

for some $f(x, y, z) \in \bar{K}[x, y, z]$.

**Proposition 3.2.2** *Let $\Gamma : \bar{K}(C_2) \longrightarrow \bar{K}(C_1)$ be a $\bar{K}$-homomorphism of function fields. Then $\Gamma^{\#}$ is non-constant.*

**Proof.** Suppose $\Gamma^{\#}$ is constant, i.e. $\Gamma^{\#}(P) = [u_0 : v_0 : w_0]$ for some $[u_0 : v_0 : w_0] \in C_2$, and without loss of generality, let $w_0 \neq 0$. From the definition of $\Gamma^{\#}$, we must have

$$\begin{aligned} \Gamma\left(\frac{U}{W}\right) &= \frac{u_0}{w_0}, \\ \Gamma\left(\frac{V}{W}\right) &= \frac{v_0}{w_0}. \end{aligned}$$

Then from

$$\begin{aligned} \Gamma\left(\frac{U}{W}\right) &= \frac{u_0}{w_0}, \\ \Gamma\left(\frac{u_0}{w_0}\right) &= \frac{u_0}{w_0}, \end{aligned}$$

and the fact that $\Gamma$ is injective, we must have $\frac{U}{W} = \frac{u_0}{w_0}$, so $C_2(u, v, w) \mid (w_0 u - u_0 w)$ and $C_2$ is a line. Using the same reasoning, we find that $C_2(u, v, w) \mid (w_0 v - v_0 w)$ as well. However, this means that $w_0 u - u_0 w$ and $w_0 v - v_0 w$ are associates in $\bar{K}[u, v, w]$ — a contradiction. Hence, $\Gamma^{\#}$ is non-constant. □

**Example 3.2.3** *Consider the curves*

$$\begin{aligned} C_1/K : y^2 z - x^3 - xz^2 &= 0 \\ C_2/K : v^2 w - u^3 + 4uw^2 &= 0. \end{aligned}$$

*The $\bar{K}$-homomorphism of function fields $\Gamma : \bar{K}(C_2) \longrightarrow \bar{K}(C_1)$ from Example 3.1.6 given by*

$$\begin{aligned}\Gamma\left(\frac{U}{W}\right) &= \frac{Y^2}{X^2}\\ \Gamma\left(\frac{V}{W}\right) &= \frac{2XYZ - Y^3}{X^3},\end{aligned}$$

*induces a non-constant map of curves $\Gamma^{\#}$ which is given by*

$$\Gamma^{\#}(P) = \begin{cases} \left[\frac{y_0^2}{x_0^2} : \frac{2x_0y_0z_0 - y_0^3}{x_0^3} : 1\right] & \textit{if } x_0 \neq 0 \\ \left[\frac{x_0y_0^2}{2x_0y_0z_0 - y_0^3} : 1 : \frac{x_0^3}{2x_0y_0z_0 - y_0^3}\right] = [0:1:0] & \textit{if } P = [0:1:0]. \end{cases}$$

*We see that $\Gamma^{\#}$is defined for all $P \in C_1$ for which $x_0 \neq 0$ or $x_0 = 0$ and $y_0 \neq 0$, i.e. everywhere except at $P = [0:0:1]$. Therefore, $C_1 \setminus \{[0:0:1]\} \subseteq R_\Gamma$. In fact, $[0:0:1]$ also belongs to $R_\Gamma$, as we will see in Chapter 5, so $R_\Gamma = C_1$.*

In light of the fact that $\Gamma(\frac{U}{W})$ and $\Gamma(\frac{V}{W})$ are just quotients of homogeneous polynomials of the same degree, we may express the map $\Gamma^{\#}$ induced by $\Gamma$ strictly in terms of homogeneous polynomials in the ring $\bar{K}[C_1]$. For if $\Gamma(\frac{U}{W}) = \frac{\gamma_1(X,Y,Z)}{\gamma_3(X,Y,Z)}$ and $\Gamma(\frac{V}{W}) = \frac{\gamma_2(X,Y,Z)}{\gamma_3(X,Y,Z)}$, then multiplying out by $\gamma_3(X,Y,Z)$ gives the same map of curves. That is, the map $\Gamma^{\#}$ takes the point $[x_0 : y_0 : z_0] \in C_1$ to $[\gamma_1(x_0,y_0,z_0) : \gamma_2(x_0,y_0,z_0) : \gamma_3(x_0,y_0,z_0)] \in C_2$.

**Example 3.2.4** *Consider the $\bar{K}$-homomorphism $\Gamma : \bar{K}(C_2) \longrightarrow \bar{K}(C_1)$ of function fields from Example 3.2.3, given by*

$$\begin{aligned}\Gamma\left(\frac{U}{W}\right) &= \frac{Y^2}{X^2}\\ \Gamma\left(\frac{V}{W}\right) &= \frac{2XYZ - Y^3}{X^3}.\end{aligned}$$

*By Example 3.2.3, the map* $\Gamma^{\#} : R_\Gamma \longrightarrow C_2$ *induced by* $\Gamma$ *is given by*

$$\Gamma^{\#}(P) = \begin{cases} \left[\frac{y_0^2}{x_0^2} : \frac{2x_0y_0z_0 - y_0^3}{x_0^3} : 1\right] & \text{if } x_0 \neq 0 \\ \\ \left[\frac{x_0y_0^2}{2x_0y_0z_0 - y_0^3} : 1 : \frac{x_0^3}{2x_0y_0z_0 - y_0^3}\right] = [0:1:0] & \text{if } P = [0:1:0], \end{cases}$$

*which, after clearing denominators, yields the map*

$$\Gamma^{\#}(P) = [x_0y_0^2 : 2x_0y_0z_0 - y_0^3 : x_0^3],$$

*for* $P \neq [0:0:1]$.

This naturally motivates a definition of a map of curves which is not related to function field homomorphisms.

**Definition 3.2.5** *Let* $C_1, C_2$ *be curves and let* $f_1, f_2, f_3$ *in* $\bar{K}[C_1]$ *be homogeneous polynomials such that all nonzero* $f_i$ *have the same degree and* $f_i \neq 0 \in \bar{K}[C_1]$ *for some* $i = 1, 2, 3$. *Set* $U_f = \{P \in C_1 \mid f_i(P) \neq 0 \text{ for some } i = 1, 2, 3\}$. *Then a map of the form* $f : U_f \longrightarrow C_2$ *given by*

$$f(P) = [f_1(P) : f_2(P) : f_3(P)]$$

*is said to be a* partial map.

**Remark 3.2.6** *Note that by Bézout's Theorem, the set* $U_f$ *in Definition 3.2.5 is a cofinite subset of* $C_1$.

**Definition 3.2.7** *Let* $f : U_f \rightarrow C_2, g : U_g \rightarrow C_2$ *be partial maps of curves* $C_1, C_2$ *given by*

$$\begin{aligned} f(P) &= [f_1(P) : f_2(P) : f_3(P)] \\ g(P) &= [g_1(P) : g_2(P) : g_3(P)]. \end{aligned}$$

*Then $f$ and $g$ are said to be* equivalent, *written $f \sim g$, if $f(P) = g(P)$ for all $P \in U_f \cap U_g$.*

**Lemma 3.2.8** *Let $f, g$ be partial maps of curves $C_1, C_2$ as in Definition 3.2.7. Then $f \sim g$ if and only if for $1 \leq i, j \leq 3$,*

$$f_i(x,y,z)g_j(x,y,z) - f_j(x,y,z)g_i(x,y,z) \in (C_1(x,y,z)).$$

**Proof.** Suppose that $f \sim g$. If $f_i = g_i = 0$ for some $i$, assume without loss of generality that $i = 3$. Then $f_1g_3 - f_3g_1 = f_2g_3 - f_3g_2 = 0 \in (C_1(x,y,z))$. Clearly, we must have $f_1 \neq 0$ or $f_2 \neq 0$. Suppose $f_2 \neq 0$. Then we must have $g_2 \neq 0$ also, so for all but finitely many $P \in C_1$, $f_2(P) \neq 0, g_2(P) \neq 0$. Hence, for all but finitely many $P \in C_1$, $\frac{f_1(P)}{f_2(P)} = \frac{g_1(P)}{g_2(P)}$, and we conclude (by the irreducibility of $C_1(x,y,z)$ and Bézout's Theorem) that $f_1g_2 - f_2g_1 \in (C(x,y,z))$. On the other hand, suppose $f_i \neq 0$ for all $i$, so $g_i \neq 0$ for all $i$. Then for all but finitely many $P \in C_1$, $f_j(P) \neq 0$ and $g_j(P) \neq 0$ for $1 \leq j \leq 3$. Hence, for all but finitely many $P \in C_1$,

$$\frac{f_i(P)}{f_j(P)} = \frac{g_i(P)}{g_j(P)},$$

for $1 \leq i \leq 3$. Thus, the homogeneous polynomials $C_1(x,y,z)$ and $f_i(x,y,z)g_j(x,y,z) - f_j(x,y,z)g_i(x,y,z)$ have infinitely many common zeros, from which we again conclude that

$$f_i(x,y,z)g_j(x,y,z) - f_j(x,y,z)g_i(x,y,z) \in (C_1(x,y,z)).$$

Conversely, suppose that for $1 \leq i, j \leq 3$,

$$f_i(x,y,z)g_j(x,y,z) - f_j(x,y,z)g_i(x,y,z) \in (C_1(x,y,z)).$$

If $f_i = 0$ for some $i$, assume without loss of generality that $i = 3$. From the equations

$$\begin{aligned} 0 \in \bar{K}[C_1] &= f_1 g_2 - f_2 g_1 &(2.1)\\ &= f_1 g_3 - f_3 g_1 &(2.2)\\ &= f_2 g_3 - f_3 g_2, &(2.3)\end{aligned}$$

we see that $f_1 g_3 = f_2 g_3 = 0$. If $f_2 = 0$, we must have $f_1 \neq 0$ so $g_3 = 0$, from which we deduce that $g_2 = 0$ and $g_1 \neq 0$. Similarly, if $f_1 = 0$, then $f_2 \neq 0$, so $g_1 = 0$ and $g_2 \neq 0$. If $f_1, f_2 \neq 0$, we find that $g_3 = 0$, so if $g_2 = 0$, $g_1 \neq 0$ and $f_1 g_2 - f_2 g_1 = -f_2 g_1 \neq 0$ — a contradiction. Therefore, if $f_1, f_2 \neq 0$ we must have $g_1, g_2 \neq 0$. In all cases $(1 \leq i \leq 3)$, we find that $f_i = 0$ if and only if $g_i = 0$. Therefore, for all $1 \leq i \leq 3$, $\frac{f_i(P)}{f_j(P)} = \frac{g_i(P)}{g_j(P)}$ for some $j$, for all but finitely many $P \in C_1$. Moreover, if $f_j(P) = 0$ and $g_j(P) \neq 0$ for some $P$, we see from Equations 2.1-2.3 that $f_i(P) = 0$ for $1 \leq i \leq 3$ — that is, $P \notin U_f$. □

**Lemma 3.2.9** *The relation $\sim$ is an equivalence relation.*

**Proof.** Reflexivity and symmetry are obvious. Transitivity follows from the fact that a finite intersection of cofinite subsets of a set is again a cofinite subset. □

**Definition 3.2.10** *Let $C_1, C_2$ be curves and let $R$ denote the set of partial maps $f : U_f \to C_2$ from $C_1$ into $C_2$. We denote by $Rat_{\bar{K}}(C_1, C_2)$ the set of equivalence classes under the equivalence relation of Definition 3.2.7. An element of $Rat_{\bar{K}}(C_1, C_2)$ is called a* rational map from $C_1$ to $C_2$.

**Definition 3.2.11** *Let $\gamma$ be a rational map of curves $C_1, C_2$. Then $\gamma$ is* regular at *$P \in C_1$ if $P \in U_f$ for some partial map $f \in \gamma$.*

**Example 3.2.12** *Consider the circle $C/\mathbb{Q} : x^2 + y^2 = z^2$ and the line at infinity $\ell_\infty/\mathbb{Q} : w = 0$, and the partial map $f : U_f \to \ell_\infty$ given by $f([x_0 : y_0 : z_0]) = [y_0 : x_0 - z_0 : 0]$. Then $U_f = C \setminus \{[1 : 0 : 1]\}$. The map $g : U_g \to \ell_\infty$ given by $g([x_0 : y_0 : z_0]) = [x_0+z_0 : -y_0 : 0]$ is equivalent to $f$ because $(x+z)(x-z)-(-y)(y) = x^2 + y^2 - z^2 \in (C(x, y, z))$. Therefore, since $U_g = C \setminus \{[1 : 0 : -1]\}$, we have $U_f \cup U_g = C$, and the class $\gamma$ of $f, g$ is regular on all of $C$.*

Given a rational map $\gamma$, we can give an alternate characterization of $\gamma$ as an extended map of curves, as the next proposition demonstrates.

**Proposition 3.2.13** *Let $C_1, C_2$ be curves and let $\gamma \in Rat_{\overline{K}}(C_1, C_2)$. Then the map given by $\gamma(P) = f(P)$ for all $f \in \gamma$ for which $P \in U_f$ gives a well-defined map of curves whose domain is the set*

$$\bigcup_{f\in\gamma} U_f,$$

*which we denote by $U_\gamma$.*

**Proof.** Let $P \in C_1$ and let $f, g \in \gamma$ such that $P \in U_f \cap U_g$. Suppose without loss of generality that $f_3(P) \neq 0$ and $g_2(P) \neq 0$. Then

$$\begin{aligned}
[f_1(P) : f_2(P) : f_3(P)] &= \left[\frac{f_1(P)}{f_3(P)} : \frac{f_2(P)}{f_3(P)} : 1\right] \\
&= \left[\frac{f_2(P)}{f_3(P)}\frac{g_1(P)}{g_2(P)} : \frac{f_2(P)}{f_3(P)} : \frac{f_2(P)}{f_3(P)}\frac{g_3(P)}{g_2(P)}\right] \\
&= \left[\frac{g_1(P)}{g_2(P)} : 1 : \frac{g_3(P)}{g_2(P)}\right] \\
&= [g_1(P) : g_2(P) : g_3(P)] .
\end{aligned}$$

We can multiply the second line above by $\frac{f_3(P)}{f_2(P)}$ to get the third for the following reason. Since

$$\begin{aligned} 1 &= \frac{f_2}{f_3} \cdot \frac{f_3}{f_2} \\ &= \frac{f_2}{f_3} \cdot \frac{g_3}{g_2} \end{aligned}$$

as rational functions on $C_1$, and since $f_3(P)g_2(P) \neq 0$ (i.e. $\frac{f_2 g_3}{f_3 g_2}$ is defined at $P$), we must have $f_2(P)g_3(P) \neq 0$. Hence, $\frac{f_2(P)}{f_3(P)} \neq 0$. □

For the remainder of this thesis, we will usually regard a rational map $\gamma$ as the map of curves described in Proposition 3.2.13, rather than as an equivalence class of partial maps. Furthermore, for a rational map $\gamma$, when we write $\gamma(P) = f(P) = [f_1(P) : f_2(P) : f_3(P)]$, we will mean that $f \in \gamma$, i.e. $f$ is a partial map residing in the equivalence class $\gamma$ with $U_f \subseteq U_\gamma$. In some cases, we may write $\gamma(P) = [\gamma_1(P) : \gamma_2(P) : \gamma_3(P)]$. In these instances, we mean that $\gamma_i$ ranges over $f_i$ for $i = 1, 2, 3$ for all $f \in \gamma$; that is, $\gamma_i$ can be taken to be $f_i$ for $i = 1, 2, 3$ when $P \in U_f$.

For any $\bar{K}$-homomorphism of function fields $\Gamma, \Gamma^{\#}$ is a rational map from some cofinite subset of $C_1$ into $C_2$. The following definition addresses this.

**Definition 3.2.14** *Let* $\Gamma : \bar{K}(C_2) \longrightarrow \bar{K}(C_1)$ *be a* $\bar{K}$*-homomorphism of function fields. Then* $\Gamma^{\#}$ *is called the* rational map induced by $\Gamma$.

**Remark 3.2.15** *Observe that Definition 3.2.10 does not preclude constant rational maps. However, we saw in Proposition 3.2.2 that constant rational maps do not arise as rational maps induced by function field* $\bar{K}$*-homomorphisms.*

The next proposition gives a necessary and sufficient condition for a point $P$ to be in $R_\Gamma$ for a $\bar{K}$-homomorphism $\Gamma$.

**Proposition 3.2.16** *Let $C_1, C_2$ be curves, $\Gamma : \bar{K}(C_2) \longrightarrow \bar{K}(C_1)$ a $\bar{K}$-homomorphism of function fields, and $\Gamma^\#$ the rational map induced by $\Gamma$ given by*

$$\Gamma^\#(P) = [\gamma_1(P) : \gamma_2(P) : \gamma_3(P)],$$

*for homogeneous polynomials $\gamma_1, \gamma_2, \gamma_3 \in \bar{K}[C_1]$. Then for all $P \in C_1, P \in R_\Gamma$ if and only if $\Gamma^\#$ is regular at $P$.*

**Proof.** Suppose $P \in R_\Gamma$. Then $\Gamma(\frac{U}{W}) = \frac{\gamma_1}{\gamma_3}, \Gamma(\frac{V}{W}) = \frac{\gamma_2}{\gamma_3}$ and since $P \in R_\Gamma$, there exist $\beta_1, \beta_2, \beta_3$ of the same degree such that $\Gamma(\frac{U}{W}) = \frac{\beta_1}{\beta_3}, \Gamma(\frac{V}{W}) = \frac{\beta_2}{\beta_3}$ and $\beta_i(P) \neq 0$ for some $i \in \{1,2,3\}$. (It follows that $\Gamma(\frac{U}{V}) = \frac{\gamma_1}{\gamma_2} = \frac{\beta_1}{\beta_2}$.) This means that $\gamma_i\beta_j - \gamma_j\beta_i = 0 \in \bar{K}[C_1]$ for $i, j \in \{1,2,3\}$, so $\gamma_i(x,y,z)\beta_j(x,y,z) - \gamma_j(x,y,z)\beta_i(x,y,z) \in (C_1(x,y,z))$. By Lemma 3.2.8, the partial maps $\gamma, \beta$ given by

$$\begin{aligned} \gamma(P) &= [\gamma_1(P) : \gamma_2(P) : \gamma_3(P)] \\ \beta(P) &= [\beta_1(P) : \beta_2(P) : \beta_3(P)] \end{aligned}$$

are equivalent, so $\beta \in \Gamma^\#$ with $P \in U_\beta$. Thus, $\Gamma^\#$ is regular at $P$.

Conversely, suppose $\Gamma^\#$ is regular at $P$; that is, there exists a partial map $\beta \in \Gamma^\#$ such that $P \in U_\beta$. Then we conclude again by Lemma 3.2.8 that $\gamma_i(x,y,z)\beta_j(x,y,z) - \gamma_j(x,y,z)\beta_i(x,y,z) \in (C_1(x,y,z))$, so $\frac{\gamma_i}{\gamma_j} = \frac{\beta_i}{\beta_j}$ for $i, j \in \{1,2,3\}$. Since $\Gamma(\frac{U}{W}) = \frac{\gamma_1}{\gamma_3}, \Gamma(\frac{V}{W}) = \frac{\gamma_2}{\gamma_3}$, it follows that $P \in R_\Gamma$. $\square$

**Corollary 3.2.17** *The domain of $\Gamma^\#$ in Proposition 3.2.16 is $R_\Gamma$, i.e. $U_{\Gamma^\#} = R_\Gamma$.*

**Example 3.2.18** *Consider the rational map $\Gamma^{\#} : R_\Gamma \longrightarrow C_2$ induced by the $\bar{K}$-homomorphism from Example 3.1.6, for the curves*

$$\begin{aligned} C_1 : y^2z - x^3 - xz^2 &= 0 \\ C_2 : v^2w - u^3 + 4uw^2 &= 0, \end{aligned}$$

*and given by $\Gamma^{\#}(P) = [y_0^2z_0 : y_0z_0^2 - x_0^2y_0 : x_0^2z_0]$, if $P \neq [0:1:0], [0:0:1]$, i.e. $C_1 \setminus \{[0:1:0],[0:0:1]\} \subseteq U_{\Gamma^{\#}}$. Then for the partial map $g([x_0 : y_0 : z_0]) = [x_0y_0^2 : 2x_0y_0z_0 - y_0^3 : x_0^3]$, we find that $g \in \Gamma^{\#}$ and $[0:1:0] \in U_g$, so $\Gamma^{\#}$ is regular at $[0:1:0]$. Similarly,*

$$\begin{aligned} \Gamma\left(\frac{U}{W}\right) &= \frac{g_1(X,Y,Z)}{g_3(X,Y,Z)} \\ &= \frac{XY^2}{X^3} \\ \Gamma\left(\frac{V}{W}\right) &= \frac{g_2(X,Y,Z)}{g_3(X,Y,Z)} \\ &= \frac{2XYZ - Y^3}{X^3}, \end{aligned}$$

*and $g_2(0,1,0) = -1 \neq 0$, so $[0:1:0] \in R_\Gamma$.*

Although the rational map from the previous example is actually regular everywhere, the set $R_\Gamma$ is not always equal to the curve $C_1$, as we will soon see.

**Proposition 3.2.19** *Let $C_1 : C_1(x,y,z) = 0, C_2 : C_2(u,v,w) = 0$ be curves and let $\Gamma : \bar{K}(C_2) \longrightarrow \bar{K}(C_1)$ be a $\bar{K}$-homomorphism of function fields. Then for all singular $P \in R_\Gamma$, $\Gamma^{\#}(P)$ is singular.*

**Proof.** Let $P$ be a singular point on $C_1$, and let $\Gamma^{\#}([x_0 : y_0 : z_0])$ be given by $[\gamma_1(x_0,y_0,z_0) : \gamma_2(x_0,y_0,z_0) : \gamma_3(x_0,y_0,z_0)]$ as usual. Then from the fact that

$$C_2(\gamma_1(x,y,z), \gamma_2(x,y,z), \gamma_3(x,y,z)) = C_1(x,y,z)f(x,y,z),$$

for some $f(x,y,z) \in \bar{K}[x,y,z]$, we have:

$$\begin{aligned}\frac{\partial C_2(u,v,w)}{\partial u} &= \frac{\partial C_2(\gamma_1(x,y,z),\gamma_2(x,y,z),\gamma_3(x,y,z))}{\partial x}\frac{\partial x}{\partial u} \\ &= \left(\frac{\partial C_1(x,y,z)}{\partial x}f(x,y,z) + C_1(x,y,z)\frac{\partial f(x,y,z)}{\partial x}\right)\frac{\partial x}{\partial u}.\end{aligned}$$

Hence,

$$\frac{\partial C_2(u,v,w)}{\partial u}(\Gamma^{\#}(P)) = \left(\frac{\partial C_1(x,y,z)}{\partial x}(P)f(P) + C_1(P)\frac{\partial f(x,y,z)}{\partial x}(P)\right)\frac{\partial x}{\partial u}(P).$$

Since $\frac{\partial C_1(x,y,z)}{\partial x}(P) = C_1(P) = 0$, $\frac{\partial C_2(u,v,w)}{\partial u}(\Gamma^{\#}(P)) = 0$ and it can similarly shown that $\frac{\partial C_2(u,v,w)}{\partial v}(\Gamma^{\#}(P)) = \frac{\partial C_2(u,v,w)}{\partial w}(\Gamma^{\#}(P)) = 0$, so $\Gamma^{\#}(P)$ is singular. □

**Example 3.2.20** *Consider the curves*

$$C_1/\mathbb{Q} : y^2z - x^3 - 8xz^2 = 0$$

$$C_2/\mathbb{Q} : v^2w^2 - 2u^4 + w^4 = 0,$$

*with a $\bar{K}$-homomorphism $\Gamma : \bar{K}(C_1) \longrightarrow \bar{K}(C_2)$ given by*

$$\begin{aligned}\Gamma\left(\frac{X}{Z}\right) &= \frac{2(VW + 2U^2 - W^2)}{(U-W)^2} \\ \Gamma\left(\frac{Y}{Z}\right) &= \frac{8UVW - 4VW^2 + 8U^3 - 4W^3}{(U-W)^3}.\end{aligned}$$

*Then $\Gamma^{\#} : R_\Gamma \longrightarrow C_1$ is given by*

$$\Gamma^{\#}([u_0 : v_0 : w_0]) = [2(v_0w_0+2u_0^2-w_0^2)(u_0-w_0) : 8u_0v_0w_0-4v_0w_0^2+8u_0^3-4w_0^3 : (u_0-w_0)^3].$$

*A quick check confirms that $C_2 \setminus \{[0:1:0],[1:-1:1]\} \subseteq R_\Gamma$. However, $[0:1:0]$ is the only singular point of $C_2$. The curve $C_1$ is easily seen to be non-singular, so $[0:1:0]$ cannot lie in $R_\Gamma$. Thus, $R_\Gamma \subseteq C_2 \setminus \{[0:1:0]\}$.*

On the other hand, the converse is not true: Non-singular points can be mapped to singular points, as the next example shows.

**Example 3.2.21** *Consider the same two curves from the previous example and the $\bar{K}$-homomorphism $\Gamma' : \bar{K}(C_2) \longrightarrow \bar{K}(C_1)$ given by*

$$\begin{aligned}\Gamma'\left(\frac{U}{W}\right) &= \frac{Y - 2X - 8Z}{Y - 4X + 8Z}\\ \Gamma'\left(\frac{V}{W}\right) &= \frac{Y^2 - 24X^2 + 48YZ - 16XZ - 64Z^2}{(Y - 4X + 8Z)^2},\end{aligned}$$

*so that $(\Gamma')^{\#} : C_1 \longrightarrow C_2$ is given by*

$$\begin{aligned}&(\Gamma')^{\#}([x_0 : y_0 : z_0])\\ = \;&[(y_0 - 2x_0 - 8z_0)(y_0 - 4x_0 + 8z_0) : y_0^2 - 24x_0^2 + 48y_0z_0 - 16x_0z_0 - 64z_0^2 :\\ &(y_0 - 4x_0 + 8z_0)^2].\end{aligned}$$

*Then $(\Gamma')^{\#}([x_0 : 4x_0 - 8 : 1]) = [0 : 1 : 0]$, where $x_0$ is a root of $x^3 - 16x^2 + 72x - 64$. (Note that $C_1(x_0, 4x_0 - 8, 1) = -x_0^3 + 16x_0^2 - 72x_0 + 64 = 0$, so $[x_0 : 4x_0 - 8 : 1] \in C_1$.) We just saw that $[0 : 1 : 0] \in C_2$ is singular.*

**Definition 3.2.22** *Let $C_1, C_2$ be curves and let $\Gamma^{\#} : R_\Gamma \longrightarrow C_2$ be a rational map induced by a $\bar{K}$-homomorphism $\Gamma : \bar{K}(C_2) \longrightarrow \bar{K}(C_1)$. Then $\Gamma^{\#}$ is said to be* defined over $K$ *if there exist homogeneous polynomials $\gamma_1(X, Y, Z), \gamma_2(X, Y, Z), \gamma_3(X, Y, Z) \in K[C_1]$ of the same degree such that*

$$\Gamma\left(\frac{U}{W}\right) = \frac{\gamma_1(X, Y, Z)}{\gamma_3(X, Y, Z)}$$

$$\Gamma\left(\frac{V}{W}\right) = \frac{\gamma_2(X, Y, Z)}{\gamma_3(X, Y, Z)}.$$

**Example 3.2.23** *Consider the curves and field homomorphism from Example 3.2.18, with $K = \mathbb{Q}$. Then*

$$\Gamma^{\#}(P) = [\sqrt{2}x_0y_0^2 : 2\sqrt{2}x_0y_0z_0 - \sqrt{2}y_0^3 : \sqrt{2}x_0^3],$$

*for $P \neq [0:0:1]$. But $\Gamma^{\#}$ is defined over $\mathbb{Q}$, because this is the same map of points as $\Gamma^{\#} : R_\Gamma \longrightarrow C_2$, given by*

$$\Gamma^{\#}(P) = [x_0y_0^2 : 2x_0y_0z_0 - y_0^3 : x_0^3],$$

*for $P \neq [0:0:1]$, i.e.*

$$\begin{aligned}\Gamma\left(\frac{U}{W}\right) &= \frac{XY^2}{X^3}\\ \Gamma\left(\frac{V}{W}\right) &= \frac{2XYZ - Y^3}{X^3}.\end{aligned}$$

## 3.3 Isomorphism

In this section, we deal with isomorphism of curves, an important topic vis-à-vis the last three chapters of this thesis. The meaning of isomorphism of curves is different from that of rings or fields. However, we will see that isomorphism of curves is tied to that of fields, just as non-constant rational maps are tied to $\bar{K}$-homomorphisms of function fields. First, we introduce a related notion.

**Definition 3.3.1** *Let $\gamma$ be a rational map of curves $C_1; C_2$. If $\gamma$ is regular at $P$ for all $P \in C_1$, we call $\gamma$ a* morphism *and write $\gamma : C_1 \longrightarrow C_2$.*

The next theorem gives an important result for non-constant morphisms.

**Proposition 3.3.2** *Let $C_1$ and $C_2$ be curves. A non-constant morphism $\gamma = [\gamma_1 : \gamma_2 : \gamma_3]$ from $C_1$ to $C_2$ is surjective.*

**Proof.** See [18, Corollary 8.10]. □

The following provides an example of a morphism of curves whose defining homogeneous polynomials each have degree three.

**Example 3.3.3** *Let*

$$C_1/\mathbb{Q} : x^3 + y^3 - 27z^3 = 0$$
$$C_2/\mathbb{Q} : 3u^2w - 3vw^2 + w^3 - 27u^3 = 0$$

*be curves defined over the rational numbers. The map $\alpha : C_2 \longrightarrow C_1$ given by*

$$\alpha([u_0 : v_0 : w_0]) = [v_0 : w_0 - v_0 : u_0]$$

*is a rational map because*

$$v_0^3 + (w_0 - v_0)^3 - 27u_0^3 = 3v_0^2w_0 - 3v_0w_0^2 + w_0^3 - 27u_0^3 = 0$$

*for all $[u_0 : v_0 : w_0] \in C_2$, and it is a morphism because $\alpha$ is regular at all points $[u_0 : v_0 : w_0] \in C_2$.*

*The following fact will be useful later: Let $C_3$ be given by*

$$C_3/\mathbb{Q} : 108s^2t + t^3 - 108r^3 = 0.$$

*Then the map*

$$\beta([u_0 : v_0 : w_0]) = [6u_0 : 2v_0 - w_0 : 6w_0]$$

*is a morphism from $C_2$ to $C_3$ defined over $\mathbb{Q}$.*

*Checking that this is a rational map amounts to substituting the values* $6u_0, 2v_0 - w_0$ *and* $6w_0$ *for* $r, s$ *and* $t$, *respectively, in the equation for* $C_3$, *and verifying that* $C_3(6u_0, 2v_0 - w_0, 6w_0) = 0$ *for all* $[u_0 : v_0 : w_0] \in C_2$. *This rational map must be a morphism because* $\beta$ *is regular at all points* $[u_0 : v_0 : w_0]$ *on* $C_2$.

**Lemma 3.3.4** *Let* $\gamma$ *be a non-constant rational map of curves* $C_1, C_2$, *and let* $C_1$ *be smooth. Then* $\gamma$ *is a morphism.*

**Proof.** See [24, Proposition II.2.1]. □

**Definition 3.3.5** *Let* $C_1, C_2$ *be curves over some algebraically closed field* $\bar{K}$ *and* $\alpha : C_1 \longrightarrow C_2$ *a non-constant rational map. If* $\alpha' : C_2 \longrightarrow C_1$ *is a rational map such that* $\alpha \circ \alpha'$ *and* $\alpha' \circ \alpha$, *where defined, give the identity maps on* $C_2$ *and* $C_1$, *respectively, then we say that* $C_1$ *and* $C_2$ *are* birationally equivalent *and we denote* $\alpha'$ *by* $\alpha^{-1}$ .

**Example 3.3.6** *Consider again the curves*

$$C_1/\mathbb{Q} : y^2z - x^3 - 8xz^2 = 0$$

$$C_2/\mathbb{Q} : v^2w^2 - 2u^4 + w^4 = 0$$

*from Example 3.2.20 and the maps* $\Gamma^{\#} : R_{\Gamma} \longrightarrow C_1, (\Gamma')^{\#} : R_{\Gamma'} \longrightarrow C_2$ *given by*

$$\begin{aligned}
& \Gamma^{\#}([u_0 : v_0 : w_0]) \\
= \; & [2(v_0w_0 + 2u_0^2 - w_0^2)(u_0 - w_0) : 8u_0v_0w_0 - 4v_0w_0^2 + 8u_0^3 - 4w_0^3 : (u_0 - w_0)^3] \\
& (\Gamma')^{\#}([x_0 : y_0 : z_0]) \\
= \; & [(y_0 - 2x_0 - 8z_0)(y_0 - 4x_0 + 8z_0) : y_0^2 - 24x_0^2 + 48y_0z_0 - 16x_0z_0 - 64z_0^2 : \\
& (y_0 - 4x_0 + 8z_0)^2].
\end{aligned}$$

*Then*

$$\begin{aligned}
&(\Gamma')^{\#} \circ \Gamma^{\#}([u_0 : v_0 : w_0]) \\
= \ & [u_0w_0(4v_0w_0 + 32u_0w_0 - 20w_0^2 - 8u_0^2)^2 : v_0w_0(4v_0w_0 + 32u_0w_0 - 20w_0^2 - 8u_0^2)^2 : \\
& w_0^2(4v_0w_0 + 32u_0w_0 - 20w_0^2 - 8u_0^2)^2] \\
= \ & [u_0 : v_0 : w_0],
\end{aligned}$$

*and it can similarly be shown that* $\Gamma^{\#} \circ (\Gamma')^{\#}([x_0 : y_0 : z_0]) = [x_0 : y_0 : z_0]$*, so* $C_1$ *and* $C_2$ *are birationally equivalent.*

Observe that while $(\Gamma')^{\#} = (\Gamma^{\#})^{-1}$ in the previous example, the map $\Gamma^{\#}$ is not a morphism, since $C_2$ is singular at $[0 : 1 : 0]$ while $C_1$ is non-singular. The next definition addresses this point.

**Definition 3.3.7** *Let* $C_1, C_2$ *be curves over some algebraically closed field* $\bar{K}$ *and* $\alpha : C_1 \longrightarrow C_2$*,* $\alpha^{-1} : C_2 \longrightarrow C_1$ *as in Definition 3.3.5. If* $\alpha, \alpha^{-1}$ *are morphisms then we say that* $C_1$ *and* $C_2$ *are* isomorphic *and we write* $C_1 \simeq C_2$ *. We call* $\alpha$ *(and* $\alpha^{-1}$*) an* isomorphism*. The curves* $C_1$ *and* $C_2$ *are* isomorphic over $K$ *(*$C_1 \simeq_K C_2$*) if* $\alpha, \alpha^{-1}$ *are morphisms defined over* $K$*.*

**Example 3.3.8** *Consider once more the circle* $C/\mathbb{Q} : x^2 + y^2 = z^2$ *and the line at infinity* $\ell_\infty/\mathbb{Q} : w = 0$ *from Example 3.2.12 and the rational map* $\beta : U_\beta \to C$ *given by* $\beta([u_0 : v_0 : w_0]) = [u_0^2 - v_0^2 : -2u_0v_0 : u_0^2 + v_0^2]$*. The map* $\beta$ *is clearly a morphism, and one may verify via simple algebra that* $\beta$ *and the morphism* $\gamma : C \to \ell_\infty$ *given by*

$$\gamma(P) = \begin{cases} f(P) & \text{if } P \neq [1 : 0 : 1] \\ g(P) & \text{if } P \neq [1 : 0 : -1], \end{cases}$$

*with $f, g$ given by*

$$\begin{aligned} f([x_0 : y_0 : z_0]) &= [y_0 : x_0 - z_0 : 0] \\ g([x_0 : y_0 : z_0]) &= [x_0 + z_0 : -y_0 : 0], \end{aligned}$$

*are inverses of each other, hence $\beta = \gamma^{-1}$ and the circle and the line at infinity (in fact* all *lines) are isomorphic to one another.*

**Example 3.3.9** *Consider again the curves $C_1 : x^3 + y^3 - 27z^3 = 0, C_2 : 3u^2w - 3v^2 + w^3 - 27u^3 = 0$ and $C_3 : 108s^2t + t^3 - 108r^3 = 0$ and the morphisms $\alpha : C_2 \longrightarrow C_1$ and $\beta : C_2 \longrightarrow C_3$ from Example 3.3.3 given by*

$$\begin{aligned} \alpha([u_0 : v_0 : w_0]) &= [v_0 : w_0 - v_0 : u_0] \\ \beta([u_0 : v_0 : w_0]) &= [6u_0 : 2v_0 - w_0 : 6w_0]. \end{aligned}$$

*Then $\alpha$ and $\beta$ are isomorphisms over $\mathbb{Q}$ via $\alpha^{-1} : C_1 \longrightarrow C_2$ and $\beta^{-1} : C_3 \longrightarrow C_2$ given by*

$$\begin{aligned} \alpha^{-1}([x_0 : y_0 : z_0]) &= [z_0 : x_0 : x_0 + y_0] \\ \beta^{-1}([r_0 : s_0 : t_0]) &= [2r_0 : 6s_0 + t_0 : 2t_0]. \end{aligned}$$

*In fact,*

$$\begin{aligned} \alpha^{-1} \circ \alpha([u_0 : v_0 : w_0]) &= \alpha^{-1}([v_0 : w_0 - v_0 : u_0]) \\ &= [u_0 : v_0 : v_0 + (w_0 - v_0)] \\ &= [u_0 : v_0 : w_0] \\ \alpha \circ \alpha^{-1}([x_0 : y_0 : z_0]) &= \alpha([z_0 : x_0 : x_0 + y_0]) \\ &= [x_0 : (x_0 + y_0) - x_0 : z_0] \\ &= [x_0 : y_0 : z_0]. \end{aligned}$$

*Likewise,*

$$\begin{aligned}
\beta^{-1}\circ\beta([u_0 : v_0 : w_0]) &= \beta^{-1}([6u_0 : 2v_0 - w_0 : 6w_0]) \\
&= [12u_0 : 6(2v_0 - w_0) + 6w_0 : 2(6w_0)] \\
&= [12u_0 : 12v_0 + : 12w_0] \\
&= [u_0 : v_0 : w_0] \\
\beta\circ\beta^{-1}([r_0 : s_0 : t_0]) &= \beta([2r_0 : 6s_0 + t_0 : 2t_0]) \\
&= [6(2r_0) : 2(6s_0 + t_0) - 2t_0 : 6(2t_0)] \\
&= [12r_0 : 12s_0 : 12t_0] \\
&= [r_0 : s_0 : t_0].
\end{aligned}$$

*Therefore, $C_1$ and $C_3$ are isomorphic over $\mathbb{Q}$ via $\beta\circ\alpha^{-1} : C_1 \longrightarrow C_3$ and $\alpha\circ\beta^{-1} : C_3 \longrightarrow C_1$.*

**Remark 3.3.10** *Observe that the isomorphisms $\alpha$ and $\alpha^{-1}$ from Example 3.3.9 can alternately be expressed in terms of invertible matrices. To be exact:*

$$\alpha([u_0 : v_0 : w_0]) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & -1 & 1 \\ 1 & 0 & 0 \end{pmatrix} [u_0 : v_0 : w_0]^T$$

*and*

$$\alpha^{-1}([x_0 : y_0 : z_0]) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix} [x_0 : y_0 : z_0]^T.$$

*Here, we regard $[u_0 : v_0 : w_0]$ and $[x_0 : y_0 : z_0]$ as row vectors.*

**Proposition 3.3.11** *Let $A \in GL_3(\bar{K})$ and $C$ a curve. Then the image of the curve $C$ under the map $\alpha_A : C \longrightarrow \mathbb{P}^2(\bar{K})$, where $\alpha_A(P) = AP$, is a curve $C'$ to which $C$ is isomorphic, i.e. $\alpha_A : C \longrightarrow C'$ is an isomorphism with inverse $\alpha_{A^{-1}}$.*

**Proof.** Since $A$ is invertible, $\alpha_A$ is regular on all of $C$, and $\alpha_A$ is given by linear homogeneous polynomials, so it is a morphism. Furthermore, $\alpha_A^{-1} : C' \longrightarrow C$ is given by $\alpha_{A^{-1}}(Q) = A^{-1}Q$. Composing the two morphisms gives

$$\alpha_{A^{-1}} \circ \alpha_A(P) = A^{-1}AP = (A^{-1}A)P = I_3P = P$$

$$\alpha_A \circ \alpha_{A^{-1}}(Q) = AA^{-1}Q = (AA^{-1})Q = I_3Q = Q$$

and $\alpha_A$ is an isomorphism, as required. □

Two isomorphic curves defined over a given field need not be isomorphic over this same field, as the following example illustrates.

**Example 3.3.12** *Taking $K = \mathbb{F}_{13}$, consider the two curves*

$$C_1/\mathbb{F}_{13} : y^2z = x^3 + 7xz^2 + 3z^3,$$

$$C_2/\mathbb{F}_{13} : v^2w = u^3 + 5uw^2 + 11w^3.$$

*Then*

$$\alpha : [x_0 : y_0 : z_0] \rightarrow [6x_0 : r^{-3}y_0 : z_0],$$

*is an isomorphism from $C_1$ to $C_2$ with inverse*

$$\alpha^{-1} : [u_0 : v_0 : w_0] \rightarrow [11u_0 : r^3v_0 : w_0],$$

*where $r^2 = 11$.*

*Since 11 is a quadratic non-residue modulo 13, the isomorphism is not defined over $\mathbb{F}_{13}$.*

**Theorem 3.3.13** *Isomorphism induces an equivalence relation on the set of curves defined over a given field.*

**Proof.** Every curve is isomorphic to itself via the identity map. Symmetry is obvious since the inverse of an isomorphism is again an isomorphism. The composition of two morphisms gives another morphism, such that the composition of the inverse morphisms gives the inverse of the first composition. □

## 3.4 The Category Theoretic Perspective

Up to this point, we showed that a $\bar{K}$-homomorphism implies the existence of a non-constant rational map. It is possible to go the other way. Given a non-constant rational map, there is a $\bar{K}$-homomorphism of the corresponding function fields (in the opposite direction) which corresponds to this map. That is, the map of curves is in fact a non-constant rational map induced by a suitable $\bar{K}$-homomorphism, and there is a 1-to-1 correspondence between the non-constant rational maps of curves (if such exist) and the $\bar{K}$-homomorphisms of their function fields, as we will see.

**Definition 3.4.1** *Let $\gamma$ be a non-constant rational map of curves $C_1, C_2$, given by $\gamma([x_0 : y_0 : z_0]) = [\gamma_1(x_0, y_0, z_0) : \gamma_2(x_0, y_0, z_0) : \gamma_3(x_0, y_0, z_0)]$, for homogeneous polynomials $\gamma_1, \gamma_2, \gamma_3 \in \bar{K}[C_1]$. Then we define $\gamma^* : \bar{K}(C_2) \longrightarrow \bar{K}(C_1)$ by*

$$\begin{aligned} \gamma^*\left(\frac{U}{W}\right) &= \frac{\gamma_1(X,Y,Z)}{\gamma_3(X,Y,Z)} \\ \gamma^*\left(\frac{V}{W}\right) &= \frac{\gamma_2(X,Y,Z)}{\gamma_3(X,Y,Z)}, \end{aligned}$$

*and extend $\gamma^*$ canonically to $\bar{K}(C_2)$ so that $\gamma^*$ preserves addition and multiplication.*

**Proposition 3.4.2** *Let $\gamma$ be a non-constant rational map of curves $C_1, C_2$. Then $\gamma^*$ is a $\bar{K}$-homomorphism of function fields.*

**Proof.** $\gamma^*$ obviously fixes $\bar{K}$. Suppose $\gamma$ is given by

$$\gamma(P) = [\gamma_1(P) : \gamma_2(P) : \gamma_3(P)],$$

where $\gamma_1, \gamma_2, \gamma_3 \in \bar{K}[C_1]$ are homogeneous polynomials of the same degree. Then $\gamma^*(\frac{U}{W}) = \frac{\gamma_1(X,Y,Z)}{\gamma_3(X,Y,Z)}$ and $\gamma^*(\frac{V}{W}) = \frac{\gamma_2(X,Y,Z)}{\gamma_3(X,Y,Z)}$. Clearly, $\gamma^*(\bar{K}(C_2)) \subseteq \bar{K}(C_1)$. From the discussion in Example 3.1.6, it suffices to show $\gamma^*(0) = 0$ to establish that $\gamma^*$ is well-defined. We have

$$\begin{aligned}
\gamma^*(0) &= \gamma^*\left(C_2\left(\frac{U}{W}, \frac{V}{W}, 1\right)\right) \\
&= C_2\left(\gamma^*\left(\frac{U}{W}\right), \gamma^*\left(\frac{V}{W}\right), 1\right) \\
&= C_2\left(\frac{\gamma_1(X,Y,Z)}{\gamma_3(X,Y,Z)}, \frac{\gamma_2(X,Y,Z)}{\gamma_3(X,Y,Z)}, 1\right) \\
&= \frac{C_2(\gamma_1(X,Y,Z), \gamma_2(X,Y,Z), \gamma_3(X,Y,Z))}{\gamma_3(X,Y,Z)^{d_2 d_3}},
\end{aligned}$$

where $d_2$ is the degree of $C_2(x,y,z)$ and $d_3$ is the degree of the homogeneous polynomials $\gamma_1(x,y,z), \gamma_2(x,y,z), \gamma_3(x,y,z)$. Now $C_2(\gamma_1(P), \gamma_2(P), \gamma_3(P)) = 0$ for all $P$ at which $\gamma$ is regular, because $[\gamma_1(P) : \gamma_2(P) : \gamma_3(P)] \in C_2$ for all $P$ where $\gamma$ is regular; in the event that $\gamma$ is not regular at $P$, we have $\gamma_1(P) = \gamma_2(P) = \gamma_3(P) = 0$ and $C_2(0,0,0) = 0$. Since $C_2(\gamma_1(P), \gamma_2(P), \gamma_3(P)) = 0$ for all points $P$ on the curve $C_1$, we may conclude (by the irreducibility of $C_1(x,y,z)$ and Bézout's Theorem) that $C_2(\gamma_1(x,y,z), \gamma_2(x,y,z), \gamma_3(x,y,z)) \in (C_1(x,y,z))$. Hence, $\gamma^*(0) = 0$ and $\gamma^*$ is well-defined, as required. □

**Example 3.4.3** *Consider again the curves from Example 3.1.6:*

$$\begin{aligned} C_1 : y^2z - x^3 - xz^2 &= 0 \\ C_2 : v^2w - u^3 + 4uw^2 &= 0, \end{aligned}$$

*and the rational map $\gamma$ from Example 3.2.18 given by $\gamma(P) = f(P) = [y_0^2z_0 : y_0z_0^2 - x_0^2y_0 : x_0^2z_0] \in C_2$ for all $P \in U_f \subseteq U_\gamma$. Then $\gamma^* : \bar{K}(C_2) \longrightarrow \bar{K}(C_1)$ is given by*

$$\begin{aligned} \gamma^*\left(\frac{U}{W}\right) &= \frac{Y^2}{X^2} \\ \gamma^*\left(\frac{V}{W}\right) &= \frac{YZ^2 - X^2Y}{X^2Z}. \end{aligned}$$

This map $\gamma^*$ of function fields may look very familiar to the reader. (See Example 3.1.6.) This is not a coincidence, as the next few results reveal.

**Theorem 3.4.4** *Let $\Gamma : \bar{K}(C_2) \longrightarrow \bar{K}(C_1)$ be a $\bar{K}$-homomorphism of function fields. Then $(\Gamma^{\#})^* = \Gamma$.*

**Proof.** This follows directly from the definitions of # and *. For $\Gamma^{\#} : R_\Gamma \longrightarrow C_2$ is given by

$$\Gamma^{\#}([x_0 : y_0 : z_0]) = [\gamma_1(x_0, y_0, z_0) : \gamma_2(x_0, y_0, z_0) : \gamma_3(x_0, y_0, z_0)],$$

where

$$\begin{aligned} \Gamma\left(\frac{U}{W}\right) &= \frac{\gamma_1(X,Y,Z)}{\gamma_3(X,Y,Z)} \\ \Gamma\left(\frac{V}{W}\right) &= \frac{\gamma_2(X,Y,Z)}{\gamma_3(X,Y,Z)}. \end{aligned}$$

□

**Proposition 3.4.5** *Let $C_1$ and $C_2$ be curves and let $\Gamma : \bar{K}(C_2) \longrightarrow \bar{K}(C_1)$ be a $\bar{K}$-homomorphism. Then there exists a unique non-constant rational map $\gamma$ such that $\gamma^* = \Gamma$.*

**Proof.** We have already established existence: Simply define $\gamma = \Gamma^{\#}$. Then $\gamma^* = (\Gamma^{\#})^* = \Gamma$ by Theorem 3.4.4 and therefore $(\gamma^*)^{\#} = \Gamma^{\#} = \gamma$. It thus only remains to prove uniqueness. Suppose $\beta$ is another rational map such that $\beta^* = \Gamma$ and write

$$\begin{aligned} \gamma(P) &= f(P) \\ &= [f_1(P) : f_2(P) : f_3(P)] \\ \beta(P) &= g(P) \\ &= [g_1(P) : g_2(P) : g_3(P)], \end{aligned}$$

where $f \in \gamma, g \in \beta$. Then

$$\begin{aligned} \frac{g_1(X,Y,Z)}{g_3(X,Y,Z)} &= \beta^* \left( \frac{U}{W} \right) \\ &= \Gamma \left( \frac{U}{W} \right) \\ &= \frac{f_1(X,Y,Z)}{f_3(X,Y,Z)} \\ \frac{g_2(X,Y,Z)}{g_3(X,Y,Z)} &= \beta^* \left( \frac{V}{W} \right) \\ &= \Gamma \left( \frac{V}{W} \right) \\ &= \frac{f_2(X,Y,Z)}{f_3(X,Y,Z)}. \end{aligned}$$

That is, for $1 \le i, j \le 3$, $\frac{f_i(X,Y,Z)}{f_j(X,Y,Z)}$ and $\frac{g_i(X,Y,Z)}{g_j(X,Y,Z)}$ are equal as rational functions on the curve $C_1$. By Lemma 3.2.8, we may conclude that $f \sim g$, so $\beta = \gamma$. □

**Theorem 3.4.6** *Let $\gamma$ be a non-constant rational map of curves $C_1, C_2$. Then $(\gamma^*)^\# = \gamma$.*

**Proof.** Set $\Gamma = \gamma^*$. By Theorem 3.4.4,

$$\begin{aligned}\Gamma &= (\Gamma^\#)^* \\ &= ((\gamma^*)^\#)^*.\end{aligned}$$

Also, by Proposition 3.4.5, $\gamma$ is the unique rational map with $\gamma^* = \Gamma$, so $(\gamma^*)^\# = \gamma$.□

**Proposition 3.4.7** *Let $\alpha$ be a non-constant rational map of curves $C_1, C_2$ and $\beta$ a non-constant rational map of curves $C_2, C_3$. Then $(\beta \circ \alpha)^* = \alpha^* \circ \beta^*$.*

**Proof.** This follows from the definition of $^*$. The homomorphism $(\beta \circ \alpha)^* : \bar{K}(C_3) \longrightarrow \bar{K}(C_1)$ takes $\frac{R}{T} \in \bar{K}(C_3)$ to $\frac{\beta_1(\alpha_1(X,Y,Z),\alpha_2(X,Y,Z),\alpha_3(X,Y,Z))}{\beta_3(\alpha_1(X,Y,Z),\alpha_2(X,Y,Z),\alpha_3(X,Y,Z))}$. The homomorphism $\beta^* : \bar{K}(C_3) \longrightarrow \bar{K}(C_2)$ takes $\frac{R}{T}$ to $\frac{\beta_1(U,V,W)}{\beta_3(U,V,W)}$ while $\alpha^*$ takes $\frac{U}{W}$ to $\frac{\alpha_1(X,Y,Z)}{\alpha_3(X,Y,Z)}$ and $\frac{V}{W}$ to $\frac{\alpha_2(X,Y,Z)}{\alpha_3(X,Y,Z)}$. Composing $\alpha^*$ with $\beta^*$ gives:

$$\begin{aligned}\alpha^* \circ \beta^* \left(\frac{R}{T}\right) &= \alpha^* \left(\frac{\beta_1(U,V,W)}{\beta_3(U,V,W)}\right) \\ &= \alpha^* \left(\frac{\beta_1(\frac{U}{W},\frac{V}{W},1)}{\beta_3(\frac{U}{W},\frac{V}{W},1)}\right) \\ &= \frac{\beta_1(\frac{\alpha_1(X,Y,Z)}{\alpha_3(X,Y,Z)},\frac{\alpha_2(X,Y,Z)}{\alpha_3(X,Y,Z)},1)}{\beta_3(\frac{\alpha_1(X,Y,Z)}{\alpha_3(X,Y,Z)},\frac{\alpha_2(X,Y,Z)}{\alpha_3(X,Y,Z)},1)} \\ &= \frac{\beta_1(\alpha_1(X,Y,Z),\alpha_2(X,Y,Z),\alpha_3(X,Y,Z))}{\beta_3(\alpha_1(X,Y,Z),\alpha_2(X,Y,Z),\alpha_3(X,Y,Z))} \\ &= (\beta \circ \alpha)^* \left(\frac{R}{T}\right).\end{aligned}$$

The proof for $\frac{S}{T}$ is completely analogous. □

To what extent is a curve $C$ over a field $\bar{K}$ determined by its function field $\bar{K}(C)$? We just saw that curves and their function fields are closely related. To be more precise, isomorphism of function fields of curves (over a given field) induces an equivalence relation on the set of curves over this field and vice versa, as the following theorem states.

**Theorem 3.4.8** *Let $C_1$ and $C_2$ be smooth curves. Then $\bar{K}(C_1) \cong \bar{K}(C_2)$ if and only $C_1 \simeq C_2$.*

**Proof.** Assume $\bar{K}(C_1) \cong \bar{K}(C_2)$. Then there exists $\Gamma : \bar{K}(C_2) \longrightarrow \bar{K}(C_1)$ such that

$$\begin{aligned}
\Gamma\left(\frac{U}{W}\right) &= \frac{\gamma_1(X,Y,Z)}{\gamma_3(X,Y,Z)}\\
\Gamma\left(\frac{V}{W}\right) &= \frac{\gamma_2(X,Y,Z)}{\gamma_3(X,Y,Z)}\\
\Gamma^{-1}\left(\frac{X}{Z}\right) &= \frac{\lambda_1(U,V,W)}{\lambda_3(U,V,W)}\\
\Gamma^{-1}\left(\frac{Y}{Z}\right) &= \frac{\lambda_2(U,V,W)}{\lambda_3(U,V,W)},
\end{aligned}$$

with $\gamma_1, \gamma_2, \gamma_3$ homogeneous polynomials of the same degree and $\lambda_1, \lambda_2, \lambda_3$ also homogeneous polynomials of the same degree. Then

$$\begin{aligned}
\Gamma^{-1}\left(\frac{\gamma_1(X,Y,Z)}{\gamma_3(X,Y,Z)}\right) &= \frac{U}{W}\\
\Gamma^{-1}\left(\frac{\gamma_2(X,Y,Z)}{\gamma_3(X,Y,Z)}\right) &= \frac{V}{W}\\
\Gamma\left(\frac{\lambda_1(U,V,W)}{\lambda_3(U,V,W)}\right) &= \frac{X}{Z}\\
\Gamma\left(\frac{\lambda_2(U,V,W)}{\lambda_3(U,V,W)}\right) &= \frac{Y}{Z}.
\end{aligned}$$

Thus, for all $P = [x_0 : y_0 : z_0] \in C_1$ and $Q = [u_0 : v_0 : w_0] \in C_2$,

$$\begin{aligned}\Gamma^{\#}([x_0 : y_0 : z_0]) &= [\gamma_1(x_0, y_0, z_0) : \gamma_2(x_0, y_0, z_0) : \gamma_3(x_0, y_0, z_0)] \\ (\Gamma^{-1})^{\#}([u_0 : v_0 : w_0]) &= [\lambda_1(u_0, v_0, w_0) : \lambda_2(u_0, v_0, w_0) : \lambda_3(u_0, v_0, w_0)].\end{aligned}$$

We claim that $\Gamma^{\#} : C_1 \longrightarrow C_2$ is an isomorphism with inverse $(\Gamma^{-1})^{\#}$. We must show that for all $P = [x_0 : y_0 : z_0] \in C_1$, $(\Gamma^{-1})^{\#}(\Gamma^{\#}(P)) = P$ and for all $Q = [u_0 : v_0 : w_0] \in C_2$, $\Gamma^{\#}((\Gamma^{-1})^{\#}(Q)) = Q$. Now

$$\begin{aligned}\frac{X}{Z} &= \Gamma\left(\frac{\lambda_1(U, V, W)}{\lambda_3(U, V, W)}\right) \\ &= \frac{\lambda_1(\Gamma(\frac{U}{W}), \Gamma(\frac{V}{W}), 1)}{\lambda_3(\Gamma(\frac{U}{W}), \Gamma(\frac{V}{W}), 1)} \\ &= \frac{\lambda_1(\frac{\gamma_1(X,Y,Z)}{\gamma_3(X,Y,Z)}, \frac{\gamma_2(X,Y,Z)}{\gamma_3(X,Y,Z)}, 1)}{\lambda_3(\frac{\gamma_1(X,Y,Z)}{\gamma_3(X,Y,Z)}, \frac{\gamma_2(X,Y,Z)}{\gamma_3(X,Y,Z)}, 1)} \\ &= \frac{\lambda_1(\gamma_1(X, Y, Z), \gamma_2(X, Y, Z), \gamma_3(X, Y, Z))}{\lambda_3(\gamma_1(X, Y, Z), \gamma_2(X, Y, Z), \gamma_3(X, Y, Z))}.\end{aligned}$$

Similarly,

$$\frac{Y}{Z} = \frac{\lambda_2(\gamma_1(X, Y, Z), \gamma_2(X, Y, Z), \gamma_3(X, Y, Z))}{\lambda_3(\gamma_1(X, Y, Z), \gamma_2(X, Y, Z), \gamma_3(X, Y, Z))}.$$

From Lemma 3.2.8, it follows that for all $[x_0 : y_0 : z_0] \in U_{(\Gamma^{-1})^{\#} \circ \Gamma^{\#}}$,

$$\begin{aligned}[x_0 : y_0 : z_0] &= [\lambda_1(\gamma_1(x_0, y_0, z_0), \gamma_2(x_0, y_0, z_0), \gamma_3(x_0, y_0, z_0)) : \\ &\quad \lambda_2(\gamma_1(x_0, y_0, z_0), \gamma_2(x_0, y_0, z_0), \gamma_3(x_0, y_0, z_0)) : \\ &\quad \lambda_3(\gamma_1(x_0, y_0, z_0), \gamma_2(x_0, y_0, z_0), \gamma_3(x_0, y_0, z_0))],\end{aligned}$$

so $(\Gamma^{-1})^{\#}(\Gamma^{\#}(P)) = P$. By the same reasoning, $\Gamma^{\#}((\Gamma^{-1})^{\#}(Q)) = Q$. Furthermore, we know from Lemma 3.3.4 that $\Gamma^{\#}$ and $(\Gamma^{-1})^{\#}$ are morphisms, since both $C_1$ and $C_2$ are smooth. Thus, $(\Gamma^{-1})^{\#} = (\Gamma^{\#})^{-1}$ and $C_1 \simeq C_2$.

Conversely, suppose that $C_1$ and $C_2$ are isomorphic via $\gamma : C_1 \longrightarrow C_2$ and $\gamma^{-1} : C_2 \longrightarrow C_1$ and let $\gamma$ and $\gamma^{-1}$ be given by

$$\begin{aligned}\gamma(P) &= [\gamma_1(P) : \gamma_2(P) : \gamma_3(P)] \\ \gamma^{-1}(Q) &= [\lambda_1(Q) : \lambda_2(Q) : \lambda_3(Q)].\end{aligned}$$

Then $\gamma^* : \bar{K}(C_2) \longrightarrow \bar{K}(C_1)$ and $(\gamma^{-1})^* : \bar{K}(C_1) \longrightarrow \bar{K}(C_2)$ are $\bar{K}$-embeddings of function fields. We claim that $\gamma^*$ is an isomorphism, with $(\gamma^*)^{-1} = (\gamma^{-1})^*$. To prove this, we need to show that

$$\begin{aligned}\gamma^*\left((\gamma^{-1})^*\left(\frac{X}{Z}\right)\right) &= \frac{X}{Z} \\ \gamma^*\left((\gamma^{-1})^*\left(\frac{Y}{Z}\right)\right) &= \frac{Y}{Z} \\ (\gamma^{-1})^*\left(\gamma^*\left(\frac{U}{W}\right)\right) &= \frac{U}{W} \\ (\gamma^{-1})^*\left(\gamma^*\left(\frac{V}{W}\right)\right) &= \frac{V}{W}.\end{aligned}$$

We only establish the first equality, since the other three can be proven analogously. From the definitions of $\gamma^*$ and $(\gamma^{-1})^*$, we see that

$$\gamma^*\left((\gamma^{-1})^*\left(\frac{X}{Z}\right)\right) = \frac{\lambda_1(\gamma_1(X,Y,Z),\gamma_2(X,Y,Z),\gamma_3(X,Y,Z))}{\lambda_3(\gamma_1(X,Y,Z),\gamma_2(X,Y,Z),\gamma_3(X,Y,Z))}.$$

But for all $P = [x_0 : y_0 : z_0] \in C_1$, we have

$$\begin{aligned}[x_0 : y_0 : z_0] = {} & [\lambda_1(\gamma_1(x_0,y_0,z_0),\gamma_2(x_0,y_0,z_0),\gamma_3(x_0,y_0,z_0)) : \\ & \lambda_2(\gamma_1(x_0,y_0,z_0),\gamma_2(x_0,y_0,z_0),\gamma_3(x_0,y_0,z_0)) : \\ & \lambda_3(\gamma_1(x_0,y_0,z_0),\gamma_2(x_0,y_0,z_0),\gamma_3(x_0,y_0,z_0))].\end{aligned}$$

Since for all but finitely many $P \in C_1$, $z_0 \neq 0$, it follows that for all but finitely many $P \in C_1$,

$$\frac{x_0}{z_0} = \frac{\lambda_1(\gamma_1(x_0, y_0, z_0), \gamma_2(x_0, y_0, z_0), \gamma_3(x_0, y_0, z_0))}{\lambda_3(\gamma_1(x_0, y_0, z_0), \gamma_2(x_0, y_0, z_0), \gamma_3(x_0, y_0, z_0))}.$$

This means that the rational functions $\frac{X}{Z}$ and $\frac{\lambda_1(\gamma_1(X,Y,Z),\gamma_2(X,Y,Z),\gamma_3(X,Y,Z))}{\lambda_3(\gamma_1(X,Y,Z),\gamma_2(X,Y,Z),\gamma_3(X,Y,Z))}$ are equal as rational functions on some cofinite subset of $C_1$. Hence,

$$\begin{aligned} \frac{X}{Z} &= \frac{\lambda_1(\gamma_1(X,Y,Z), \gamma_2(X,Y,Z), \gamma_3(X,Y,Z))}{\lambda_3(\gamma_1(X,Y,Z), \gamma_2(X,Y,Z), \gamma_3(X,Y,Z))} \\ &= \gamma^*\left((\gamma^{-1})^*\left(\frac{X}{Z}\right)\right) \end{aligned}$$

and thus, $\gamma^*$ is an isomorphism, as claimed. □

**Remark 3.4.9** *Note that we can establish a weaker result by removing the condition that $C_1$ and $C_2$ above be smooth. In this case, isomorphism of function fields of* all *curves induces an equivalence relation on the curves themselves; the equivalence class of a curve is the set of curves to which it is birationally equivalent.*

We are now almost ready to establish the most important result of this chapter, an equivalence of categories which relates curves and function fields. Just prior to doing this, however, we require two more definitions.

**Definition 3.4.10** *Let $S$ denote the set of non-constant rational maps of curves over $\bar{K}$. We say that $\alpha : U_\alpha \subseteq C_1 \to C_2$ and $\beta : U_\beta \subseteq C_3 \to C_4$ are* similar, *if $C_1$ and $C_3$ are birationally equivalent and $C_2$ are $C_4$ are birationally equivalent.*

**Lemma 3.4.11** *Similarity of rational maps is an equivalence relation.*

**Proof.** This is clear from the definition of similarity, since birational equivalence of curves is an equivalence relation. □

There is an analogous notion of similarity for function fields, which we now define.

**Definition 3.4.12** *Let $T$ denote the set of $\bar{K}$-homomorphisms of function fields (i.e. $\bar{K}$-homomorphisms of transcendence degree one extensions of $\bar{K}$). Recall that we saw in Proposition 2.3.14 that every function field is of the form $\bar{K}(a,b)$, with $a,b$ algebraically dependent. We say that two such homomorphisms $\Gamma_1 : \bar{K}(a_1,b_1) \to \bar{K}(a_2,b_2), \Gamma_2 : \bar{K}(a_3,b_3) \to \bar{K}(a_4,b_4)$ are* similar *if $\bar{K}(a_1,b_1) \cong \bar{K}(a_3,b_3)$ and $\bar{K}(a_2,b_2) \cong \bar{K}(a_4,b_4)$.*

**Lemma 3.4.13** *Similarity of function field $\bar{K}$-homomorphisms is an equivalence relation.*

**Proof.** Again, this is clear, since isomorphism of fields is an equivalence relation. □

**Theorem 3.4.14** *Let $A$ be the category whose objects are equivalence classes of curves over $\bar{K}$ modulo birational equivalence, and whose maps are equivalence classes of non-constant rational maps modulo similarity. (In other words, maps take birational equivalence classes of curves to birational equivalence classes of curves.) Let $B$ be the category whose objects are equivalence classes of transcendence degree one extensions of $\bar{K}$ modulo isomorphism of fields, and whose maps are equivalence classes of $\bar{K}$-homomorphisms modulo similarity. (The maps on $B$ take isomorphism classes of function fields to isomorphism classes of function fields.) Then $A$ and $B$ are* *equivalent via the functors $F_1 : A \longrightarrow B$ and $F_2 : B \longrightarrow A$, which are given by:*

$$\begin{aligned} F_1(\textit{class of } C) &= \textit{class of } \bar{K}(C) \\ F_1(\textit{class of } \gamma) &= \textit{class of } \gamma^* \\ F_2(\textit{class of } \bar{K}(a,b)) &= \textit{class of } C \\ F_2(\textit{class of } \Gamma) &= \textit{class of } \Gamma^{\#}, \end{aligned}$$

*where $C$ is obtained in the third line above in the following way. We know that $a$ and $b$ are algebraically dependent over $\bar{K}$; let $C(x,y)$ be the unique monic irreducible polynomial $\in \bar{K}[x,y]$ such that $C(a,b) = 0$, and let $d$ be the degree of $C(x,y)$. Then we set $C$ to be the locus of the irreducible homogeneous polynomial $z^d C(\frac{x}{z}, \frac{y}{z})$. Additionally, $F_1$ and $F_2$ are contravariant.*

**Proof.** We first observe that $F_1$ and $F_2$ are well-defined by Remark 3.4.9. Specifically, two curves are in the same birational equivalence class if and only if their function fields are in the same isomorphism class. By the same token, two rational maps $\gamma, \beta$ are in the same similarity class if and only if $\gamma^*$ and $\beta^*$ reside in the same similarity class. The contravariance of the functors $F_1, F_2$ was established earlier in this chapter: see Theorem 3.2.1 and Proposition 3.4.2. It is clear that the identities in both categories are maps in their respective categories. Likewise, it is clear that composition of maps in each category, where defined, gives another map in that category. Finally, it suffices to show that $F_2 = F_1^{-1}$, i.e. that $F_2 \circ F_1 = Id_A$ and $F_1 \circ F_2 = Id_B$. For maps, this is just a consequence of Theorems 3.4.4, 3.4.6 and

Proposition 3.4.5. More formally:

$$\begin{aligned} F_2 \circ F_1(class\ of\ \gamma) &= F_2(class\ of\ \gamma^*) \\ &= class\ of\ (\gamma^*)^\# \\ &= class\ of\ \gamma \\ F_1 \circ F_2(class\ of\ \Gamma) &= F_1(class\ of\ \Gamma^\#) \\ &= class\ of\ (\Gamma^\#)^* \\ &= class\ of\ \Gamma. \end{aligned}$$

For objects, it is clear that $F_2$ and $F_1$ are inverses of each other. Hence, $F_1$ is a full-and-faithful (bijective) contravariant functor with inverse $F_2$. □

**Remark 3.4.15** *It should be clear to the reader why it is necessary to take the objects to be* all *curves modulo birational equivalence rather than only smooth curves modulo isomorphism. Recall the curves $C_1, C_2$ of Example 3.3.6. The curve $C_1$ is smooth, while $C_2$ is not, yet they are birationally equivalent. This example illustrates that by choosing different generators for our function field, we encounter difficulty if we restrict ourselves to smooth curves in the categorical treatment above. To wit, suppose we are given a function field $\bar{K}(a_1, b_1)$ such that the curve $C$ obtained from $\bar{K}(a_1, b_1)$ as described in Theorem 3.4.14 is a smooth curve. On the other hand, by choosing different generators $a_2, b_2$ for the same field, it could happen that we obtain a curve $C'$ which is singular (yet which is birationally equivalent to $C$).*

## 3.5 Separability

In this section, we remind the reader of some facts regarding separability. We will need these facts in Chapter 5.

**Definition 3.5.1** *Let $K/F$ be a finite extension of fields. We define the* separable degree of *$K/F$, written $[K : F]_s$, to be the number of $F$-automorphisms of $K$, that is, the number of isomorphisms from $K$ to $K$, with fixed field $F$.*

**Example 3.5.2** *Consider the extension $\mathbb{F}_p(\mu)/\mathbb{F}_p$, $p \equiv 3 \,(mod\ 4)$ a prime, and $\mu$ a root of the irreducible polynomial $x^2 + 1 \in \mathbb{F}_p[x]$. Then the only $\mathbb{F}_p$-automorphisms of $\mathbb{F}_p(\mu)$ are the automorphisms determined by $\mu \mapsto \mu$ and $\mu \mapsto -\mu$. Hence, the separable degree of this extension is 2, the same as the degree $[\mathbb{F}_p(\mu) : \mathbb{F}_p]$.*

In Section 5.2, we will see an example of an extension $K/F$ where $[K : F]_s = 1 \neq [K : F]$.

**Remark 3.5.3** *Observe that the separable degree of an extension is bounded above by the degree of the extension (and below by 1, since the identity map is an $F$-automorphism) because an $F$-automorphism must take an element to one of its conjugates, and there are at most $[K : F]$ distinct conjugates. In the case where the fields have characteristic 0, the separable degree and the degree always coincide.*

**Definition 3.5.4** *Let $C_1, C_2$ be curves and $\gamma : C_1 \longrightarrow C_2$ a rational map. Then $\gamma$ is said to be* separable *if the separable degree of $\bar{K}(C_1)/\gamma^*(\bar{K}(C_2))$ is equal to the degree of this extension, i.e. $[\bar{K}(C_1) : \gamma^*(\bar{K}(C_2))]_s = [\bar{K}(C_1) : \gamma^*(\bar{K}(C_2))]$. We denote this degree by $\gamma_s$ . If $\gamma$ is not separable, it is said to be* inseparable.

**Theorem 3.5.5** *Let $C_1$ and $C_2$ be smooth curves and let $\gamma : C_1 \longrightarrow C_2$ be a non-constant rational map. Then for all but finitely many $Q \in C_2$, $|\gamma^{-1}(Q)| = \gamma_s$.*

**Proof.** See [24, Proposition II.2.6.(b)]. □

# Chapter 4

# Elliptic Curves

In this chapter, we at last introduce elliptic curves. We will need to establish that they have the inherent (additive) group structure which we alluded to previously. This property will follow from the fact that an elliptic curve is the locus of an irreducible cubic. Unless otherwise stated, let $K$ and $\bar{K}$ be as in the previous chapters.

## 4.1 Weierstrass Curves

The goal of this section is to give a brief overview of Weierstrass curves, and to examine some of their properties. For a more comprehensive treatment, see [24, III.1].

**Definition 4.1.1** *A* Weierstrass curve *is an irreducible projective plane curve described by a third degree homogeneous equation of the form*

$$E : y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3, \tag{1.1}$$

*where* $a_1, a_2, a_3, a_4, a_6 \in \bar{K}$*. The above equation is called a* Weierstrass equation *and* $E$ *is said to be in* Weierstrass form.

**Remark 4.1.2** *The coefficients are labelled in such a way for the following reason. Define an additive weight function* $wt$ *on each term of (1.1) such that*

$$wt(a_ix^my^nz^{3-m-n}) = i + m \cdot wt(x) + n \cdot wt(y) + (3 - m - n) \cdot wt(z).$$

*If we set $wt(x) = 2$, $wt(y) = 3$, and $wt(z) = 0$, then $wt(a_i x^m y^n z^{3-m-n}) = 6$ for each term in (1.1). For example, the coefficient of the $y^2z$ term is 1, so we set $a_0 = 1$, so $i = 0, m = 0, n = 2, 3 - m - n = 1$, and we get $i + 2m + 3n = 0 + 0 \cdot 2 + 2 \cdot 3 = 6$.*

**Example 4.1.3** *The curve $E : y^2z - x^3 - xz^2 = 0$ over any field is a Weierstrass curve.*

**Lemma 4.1.4** *If $char(K) \neq 2$, the Weierstrass curve $E$ given in Equation 1.1 is isomorphic to the curve*

$$E' : v^2w = 4u^3 + b_2u^2w + 2b_4uw^2 + b_6w^3,$$

*where*

$$\begin{aligned} b_2 &= a_1^2 + 4a_2 \\ b_4 &= 2a_4 + a_1a_3 \\ b_6 &= a_3^2 + 4a_6. \end{aligned} \tag{1.2}$$

**Proof.** Consider the morphism $\alpha : E \longrightarrow E'$ given by

$$\alpha([x_0 : y_0 : z_0]) = [x_0 : 2y_0 + a_1x_0 + a_3z_0 : z_0],$$

with inverse $\alpha^{-1} : E' \longrightarrow E$ given by

$$\alpha^{-1}([u_0 : v_0 : w_0]) = [2u_0 : v_0 - a_1u_0 - a_3w_0 : 2w_0].$$

Suppose that $[x_0 : y_0 : z_0]$ is any point on $E$ and $[u_0 : v_0 : w_0]$ is any point on $E'$. One must first check that $E'(x_0, 2y_0 + a_1x_0 + a_3z_0, z_0) = 0$ and $E(2u_0, v_0 - a_1u_0 -$

$a_3w_0, 2w_0) = 0$:

$$
\begin{aligned}
& E'(x_0, 2y_0 + a_1x_0 + a_3z_0, z_0) \\
= \; & (2y_0 + a_1x_0 + a_3z_0)^2z_0 - 4x_0^3 - b_2x_0^2z_0 - 2b_4x_0z_0^2 - b_6z_0^3 \\
= \; & 4y_0^2z_0 + a_1^2x_0^2z_0 + a_3^2z_0^3 + 4a_1x_0y_0z_0 + 4a_3y_0z_0^2 + 2a_1a_3x_0z_0^2 - 4x_0^3 - b_2x_0^2z_0 \\
& -2b_4x_0z_0^2 - b_6z_0^3 \\
= \; & 4(y_0^2z_0 + a_1x_0y_0z_0 + a_3y_0z_0^2 - x_0^3 - a_2x_0^2z_0 - a_4x_0z_0^2 - a_6z_0^3) \\
= \; & 0.
\end{aligned}
$$

A similar computation reveals that the same holds in the opposite direction:

$$
\begin{aligned}
& E(2u_0, v_0 - a_1u_0 - a_3w_0, 2w_0) \\
= \; & (v_0 - a_1u_0 - a_3w_0)^2 2w_0 + a_1(2u_0)(v_0 - a_1u_0 - a_3w_0)2w_0 \\
& + a_3(v_0 - a_1u_0 - a_3w_0)(2w_0)^2 - (2u_0)^3 - a_2(2u_0)^2 2w_0 - a_4(2u_0)(2w_0)^2 \\
& - a_6(2w_0)^3 \\
= \; & (2v_0^2w_0 + 2a_1^2u_0^2w_0 + 2a_3^2w_0^3 - 4a_1u_0v_0w_0 - 4a_3v_0w_0^2 + 4a_1a_3u_0w_0^2) \\
& + (4a_1u_0v_0w_0 - 4a_1^2u_0^2w_0 - 4a_1a_3u_0w_0^2) + (4a_3v_0w_0^2 - 4a_1a_3u_0w_0^2 - 4a_3^2w_0^3) \\
& - 8u_0^3 - 8a_2u_0^2w_0 - 8a_4u_0w_0^2 - 8a_6w_0^3 \\
= \; & 2[v_0^2w_0 - (a_1^2 + 4a_2)u_0^2w_0 - (a_3^2 + 4a_6)w_0^3 - (2a_1a_3 + 4a_4)u_0w_0^2 - 4u_0^3] \\
= \; & 2(v_0^2w_0 - b_2u_0^2w_0 - b_6w_0^3 - 2b_4u_0w_0^2 - 4u_0^3) \\
= \; & 0.
\end{aligned}
$$

It is not difficult to see that both rational maps $\alpha$ and $\alpha^{-1}$ are regular everywhere.

The rational map $\alpha$ is not regular at some point $[x_0 : y_0 : z_0] \in E$ if and only if

$$\begin{aligned} x_0 &= 0 \\ 2y_0 + a_1x_0 + a_3z_0 &= 0 \\ z_0 &= 0. \end{aligned}$$

But the three preceding conditions hold only when $x_0 = y_0 = z_0 = 0$. By the same token, $\alpha^{-1}$ is not regular at some point $[u_0 : v_0 : w_0] \in E'$ if and only if

$$\begin{aligned} 2u_0 &= 0 \\ v_0 - a_1u_0 - a_3w_0 &= 0 \\ 2w_0 &= 0. \end{aligned}$$

Again, the previous conditions hold only for $u_0 = v_0 = w_0 = 0$. Composing the two morphisms with one another gives the identity on both curves, so the curves are indeed isomorphic. □

**Remark 4.1.5** *If $char(K) \neq 2$, we can write $E'$ in the form*

$$E' : (v')^2w = u^3 + c_2u^2w + c_4uw^2 + c_6w^3,$$

*where $v' = \frac{v}{2}$ and*

$$\begin{aligned} c_2 &= \frac{b_2}{4} \\ c_4 &= \frac{b_4}{2} \\ c_6 &= \frac{b_6}{4}. \end{aligned}$$

**Lemma 4.1.6** *If $char(K) \neq 2$ and $char(K) \neq 3$, then $E'$ is isomorphic to*

$$E'' : s^2t = r^3 + Art^2 + Bt^3,$$

*where*

$$\begin{aligned} A &= \frac{b_4}{2} - \frac{b_2^2}{48} \\ B &= \frac{b_2^3}{864} - \frac{b_2b_4}{24} + \frac{b_6}{4}. \end{aligned}$$

**Proof.** Consider the rational maps $\beta : E' \longrightarrow E''$ given by

$$\beta([u_0 : v_0 : w_0]) = [12u_0 + b_2w_0 : 6v_0 : 12w_0],$$

with inverse $\beta^{-1} : E'' \longrightarrow E'$ given by

$$\beta^{-1}([r_0 : s_0 : t_0]) = [12r_0 - b_2t_0 : 24s_0 : 12t_0].$$

Let $[u_0 : v_0 : w_0]$ be any point on $E'$ and let $[r_0 : s_0 : t_0]$ be any point on $E''$. Then

$$\begin{aligned} & E''(12u_0 + b_2w_0, 6v_0, 12w_0) \\ = \; & (6v_0)^2 12w_0 - (12u_0 + b_2w_0)^3 - \left(\frac{b_4}{2} - \frac{b_2^2}{48}\right)(12u_0 + b_2w_0)(12w_0)^2 \\ & - \left(\frac{b_2^3}{864} - \frac{b_2b_4}{24} + \frac{b_6}{4}\right)(12w_0)^3 \\ = \; & 432v_0^2w_0 - 1728u_0^3 - 432b_2u_0^2w_0 - 36b_2^2u_0w_0^2 - b_2^3w_0^3 + (36b_2^2 - 864b_4)u_0w_0^2 \\ & +(3b_2^3 - 72b_2b_4)w_0^3 + (-2b_2^3 + 72b_2b_4 - 432b_6)w_0^3 \\ = \; & 432v_0^2w_0 - 1728u_0^3 - 432b_2u_0^2w_0 - 864b_4u_0w_0^2 - 432b_6w_0^3 \\ = \; & 432(v_0^2w_0 - 4u_0^3 - b_2u_0^2w_0 - 2b_4u_0w_0^2 - b_6w_0^3) \\ = \; & 0. \end{aligned}$$

Similarly,

$$\begin{aligned}
& E'(12r_0 - b_2t_0, 24s_0, 12t_0) \\
= \ & (24s_0)^2 12t_0 - 4(12r_0 - b_2t_0)^3 - b_2(12r_0 - b_2t_0)^2 12t_0 - 2b_4(12r_0 - b_2t_0)(12t_0)^2 \\
& -b_6(12t_0)^3 \\
= \ & 6912s_0^2t_0 - 6912r_0^3 + 1728b_2r_0^2t_0 - 144b_2^2r_0t_0^2 + 4b_2^3t_0^3 - 1728b_2r_0^2t_0 + 288b_2^2r_0t_0^2 \\
& -12b_2^3t_0^3 - 3456b_4r_0t_0^2 + 288b_2b_4t_0^3 - 1728b_6t_0^3 \\
= \ & 6912s_0^2t_0 - 6912r_0^3 - (3456b_4 - 144b_2^2)r_0t_0^2 - (8b_2^3 - 288b_2b_4 + 1728b_6)t_0^3 \\
= \ & 6912\left[s_0^2t_0 - r_0^3 - \left(\frac{b_4}{2} - \frac{b_2^2}{48}\right)r_0t_0^2 - \left(\frac{b_2^3}{864} - \frac{b_2b_4}{24} + \frac{b_6}{4}\right)t_0^3\right] \\
= \ & 6912(s_0^2t_0 - r_0^3 - Ar_0t_0^2 - Bt_0^3) \\
= \ & 0.
\end{aligned}$$

Both maps are clearly defined everywhere, so they are morphisms, and they are in fact isomorphisms since $\beta \circ \beta^{-1}([r_0 : s_0 : t_0]) = [144r_0 : 144s_0 : 144t_0] = [r_0 : s_0 : t_0]$ for any point $[r_0 : s_0 : t_0]$ on $E''$, and $\beta^{-1} \circ \beta([u_0 : v_0 : w_0]) = [144u_0 : 144v_0 : 144w_0] = [u_0 : v_0 : w_0]$ for any point $[u_0 : v_0 : w_0]$ on $E'$. □

We now describe two other interesting quantities associated with Weierstrass curves.

**Definition 4.1.7** *(i) The* discriminant $\Delta(E)$ *of a Weierstrass curve $E$ as in (1.1) is given by*

$$\Delta(E) = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6,$$

*where $b_2, b_4, b_6$ are given as in (1.2) and*

$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2.$$

*(ii)If $E$ is smooth, then the $j$-*invariant *$j(E)$ is given by*

$$j(E) = (b_2^2 - 24b_4)^3/\Delta(E).$$

Often, we will simply write $\Delta$ in place of $\Delta(E)$ or $j$ in place of $j(E)$, when the Weierstrass curve $E$ we are speaking of is clear from the context.

**Theorem 4.1.8** *A Weierstrass curve is non-singular if and only if its discriminant is non-zero.*

**Proof.** See [24, Proposition III.1.4.(a)]. □

**Example 4.1.9** *The Weierstrass curve $E : y^2z - x^3 = 0$ over any field is singular since $\Delta(E) = 0$.*

## 4.2 Elliptic Curves

We now define an elliptic curve. As the following definition demonstrates, an elliptic curve is not merely determined by its set of points; it is the extra condition (the basepoint) which gives the elliptic curve its group structure, as we will see later.

**Definition 4.2.1** *An* elliptic curve *is a pair $(E, O_E)$, where $E$ is a smooth, irreducible projective plane curve which is isomorphic to a smooth Weierstrass curve (called a* Weierstrass model *of $E$) and $O_E$ is a point on $E$. $O_E$ is called the* basepoint *of the curve $E$.*

We will sometimes just write $E$ in place of $(E, O_E)$, especially when $O_E$ is clear from the context. (We will return to this point in Section 4.4.)

**Example 4.2.2** *The curve $C_3/\mathbb{Q} : 108s^2t - 108r^3 + t^3 = 0$ from Example 3.3.3, taken together with $O_{C_3} = [0 : 1 : 0]$, is an elliptic curve.*

**Theorem 4.2.3** *Two elliptic curves are isomorphic (over $\bar{K}$) if and only if their Weierstrass models have the same $j$-invariant.*

**Proof.** In Chapter 5, we will see that every isomorphism of elliptic curves in Weierstrass form has a certain form. This form preserves $j$-invariants. See [24, Proposition III.1.4.(b)]. □

This is a useful test for isomorphism, as we will see in the Chapter 5 examples.

The next theorem has far-reaching consequences for the rest of this thesis. It enables us to endow an elliptic curve with a natural group structure, where point addition is a morphism.

**Theorem 4.2.4** *Every elliptic curve is the locus of a smooth, irreducible cubic projective plane curve. Conversely, every smooth, irreducible cubic projective plane curve is the locus of an elliptic curve.*

**Proof.** For the proof of the first statement, see [18, Theorems 12.5,13.1]. For the converse, see [24, Proposition III.3.1.(a)]. □

## 4.3 Bézout's Theorem

In the previous section, we saw that an elliptic curve is a smooth irreducible cubic curve. We now establish the number of common points of two curves which are the loci of relatively prime homogeneous polynomials, specifically when the aforementioned polynomials are cubic and linear, respectively. This will prepare much of the work needed to show that an elliptic curve carries the structure of an additive abelian group.

**Definition 4.3.1** *Let $\ell : ax + by + cz = 0$ be a line, $C$ a projective plane curve and $n$ the degree of $C(x, y, z)$. We define the* intersection multiplicity $i_{C,\ell}(P)$ *of $C, \ell$ at $P = [x_0 : y_0 : z_0]$ as follows. Suppose first that $\ell \neq \ell_\infty$. If $b \neq 0$, $i_{C,\ell}([x_0 : y_0 : 1])$ is the multiplicity of $x_0$ as a root of $C(x, \frac{-ax-c}{b}, 1)$. If $b = 0$ then $a \neq 0$ and $i_{C,\ell}([x_0 : y_0 : 1])$ is the multiplicity of $y_0$ as a root of $C(\frac{-c}{a}, y, 1)$. Furthermore,*

$$i_{C,\ell}([x_0 : y_0 : 0]) = n - \sum_{[x_0:y_0:1] \in C \cap \ell} i_{C,\ell}([x_0 : y_0 : 1]).$$

*Finally, if $\ell = \ell_\infty$, then $i_{C,\ell_\infty}([x_0 : 1 : 0])$ is the multiplicity of $x_0$ as a root of $C(x, 1, 0)$ and*

$$i_{C,\ell_\infty}([1 : 0 : 0]) = n - \sum_{[x_0:1:0] \in C \cap \ell_\infty} i_{C,\ell_\infty}([x_0 : 1 : 0]).$$

**Example 4.3.2** *Consider the curve $C/\mathbb{Q} : x^3 + y^3 - 1729z^3 = 0$. The tangent line to $C$ at $P = [1 : -1 : 0]$ is the line $\ell_P : x + y = 0$. Applying the definition of intersection multiplicity, we find that $C(x, -x, 1) = x^3 + (-x)^3 - 1729 = -1729$. Since this constant polynomial has no roots, there are no other points of intersection of $\ell_P$ and $C$, so the intersection multiplicity of $C$ and $\ell_P$ at $[1 : -1 : 0]$ is $3 - 0 = 3$.*

The next theorem is the foundation of everything that follows. It allows us to define an abelian group structure on an elliptic curve.

**Theorem 4.3.3 (Bézout)** *Let $C_1$ and $C_2$ be irreducible projective plane curves of degree $m$ and $n$, respectively, such that $C_1 \neq C_2$ (so $C_1(x, y, z)$ and $C_2(x, y, z)$ are relatively prime). Then $C_1$ and $C_2$ intersect in at least one point and in at most $mn$ points.*

We will not prove Bézout's theorem, but rather a special case which will suffice for our purposes. For a proof of the more general case, see [13, Theorem 2.18].

**Proposition 4.3.4** *A line $\ell \subset \mathbb{P}^2(\bar{K})$ and a curve $C$ intersect in at most $n$ points, where $n$ is the degree of $C(x, y, z)$.*

**Proof.** Given the preceding discussion of coordinate systems, we may assume without loss of generality that $\ell$ is the line at infinity. (Recall that this is the line $\ell_\infty : z = 0$.) For there exists an isomorphism $\alpha_A$ from $C$ to another curve $C'$ given by a non-singular matrix $A$ in $GL_3(\bar{K})$ which takes the line $\ell$ to $\ell_\infty$. (See Proposition 3.3.11.) If $\ell$ is given by

$$\ell : ax + by + cz = 0,$$

let $B$ be any non-singular matrix such that

$$[a\ b\ c]B = [0\ 0\ 1],$$

and set $A = B^{-1}$. Then we see that for any $P \in C \cap \ell$, the point $\alpha_A(P)$ is on $\ell_\infty$

since:

$$\begin{aligned}0 &= [a\ b\ c]P^T \\ &= ([a\ b\ c]A^{-1})AP^T \\ &= ([a\ b\ c]B)AP^T \\ &= [0\ 0\ 1]AP^T \\ &= [0\ 0\ 1][\alpha_A(P)]^T.\end{aligned}$$

Similarly, if $Q \in C' \cap \ell_\infty$, then $\alpha_{A^{-1}}(Q) \in C \cap \ell$. In other words, $P \in \ell$ if and only if $\alpha_A(P) \in \ell_\infty$. Since $\alpha_A$ is an isomorphism, it gives a bijection between the points of $C$ and $C'$. Thus, we see that $C$ and $\ell$ intersect in the same number of points as $C'$ and $\ell_\infty$. Therefore, $C' \cap \ell_\infty$ is the locus of the polynomial $C'(x, y, 0)$, which is homogeneous and of degree $n$, but in two variables rather than three. There are two cases.

**Case 1:** $C'(x, y, 0)$ contains an $x^n$ term with a non-zero coefficient. Then clearly, the point $[1 : 0 : 0]$ does not lie on $C' \cap \ell_\infty$. On the other hand, $C'(x, 1, 0) \in \bar{K}[x]$ is an $n$th degree polynomial in the variable $x$, so it has $n$ (not necessarily distinct) roots in $\bar{K}$ (because $\bar{K}$ is algebraically closed). For each root $x_i, 1 \leq i \leq n$, $[x_i : 1 : 0] \in C' \cap \ell_\infty$.

**Case 2:** The coefficient of $x^n$ in $C'(x, y, 0)$ is 0. In this case, let $d < n$ be the largest value $d$ such that the coefficient of $x^d y^{n-d}$ in $C'(x, y, 0)$ is non-zero. Then $C'(x, 1, 0) \in \bar{K}[x]$ is a $d$th degree polynomial which has roots $x_i, 1 \leq i \leq d$. Again, for each root $x_i$, $[x_i : 1 : 0] \in C' \cap \ell_\infty$. The point $[1 : 0 : 0]$ also belongs to $C' \cap \ell_\infty$. Therefore, there are $d + 1$ points of intersection. □

## 4.4 The Group of Points of an Elliptic Curve

In this section, we define a group structure on the points of an elliptic curve $(E, O_E)$. Before we proceed, however, we require the following result.

**Lemma 4.4.1** *Let $(E, O_E)$ be an elliptic curve and $P = [x_0 : y_0 : z_0]$ a point on $E$ with tangent line $\ell_P$ to $E$ at $P$. Then $\ell_P$ intersects the curve $E$ in at most 2 distinct points. Moreover, the intersection multiplicity of $\ell_P$ and $E$ at $P$ is at least 2.*

**Proof.** We establish the result for elliptic curves in Weierstrass form. (The general case can be similarly shown since $E$ is given by a cubic equation by Theorem 4.2.4.) The only point $P = [x_0 : y_0 : z_0]$ with $z_0 = 0$ that lies on $E$ is $P = [0 : 1 : 0]$. Then $\ell_P = \ell_\infty$. Since the intersection of $E(x, y, z)$ and $\ell_P$ is the curve $x^3 = 0$, we see that the intersection multiplicity at $P$ is 3, and $\ell_P$ and $E$ intersect in only one point, the point $P$. Adding the intersection multiplicities of all points of intersection of $\ell_\infty$ and $E$ gives 3.

Now let $P = [x_0 : y_0 : z_0]$ with $z_0 \neq 0$, so we may assume that $z_0 = 1$. We break the rest of the proof down into three cases.

**Case 1:** $Char(K) = 2$. Then the tangent line at $E$ to $P$ is the line

$$\ell_P : (a_1 y_0 + x_0^2 + a_4)x + (a_1 x_0 + a_3)y + (y_0^2 + a_1 x_0 y_0 + a_2 x_0^2 + a_6)z = 0.$$

Observe that if $a_1x_0 + a_3 = 0$, then the tangent line has equation $x + x_0 z = 0$. This line intersects the curve $E$ at the point $[0 : 1 : 0]$ and by assumption at $P = [x_0 : y_0 : 1]$. Substituting $x = x_0$ in $E$, we find that the only solution of the equation

$$y^2 + a_1 x_0 y + a_3 y = x_0^3 + a_2 x_0^2 + a_4 x_0 + a_6$$

is $y_0$, since the right-hand side is by definition equal to $y_0^2 + a_1x_0y_0 + a_1y_0 = y_0^2 + y_0(a_1x_0 + a_3) = y_0^2$, and the left-hand side simplifies to $y^2$. Hence, the only points of intersection are the points $[0 : 1 : 0]$, with intersection multiplicity 1, and $[x_0 : y_0 : 1]$, with intersection multiplicity 2. Note that $1 + 2 = 3$.

For the case where $a_1x_0 + a_3 \neq 0$, we substitute $z = 1$ into the equation for $\ell_P$ to get the equation

$$y = \left(\frac{a_1y_0 + x_0^2 + a_4}{a_1x_0 + a_3}\right)x + \frac{y_0^2 + a_1x_0y_0 + a_2x_0^2 + a_6}{a_1x_0 + a_3}.$$

Substituting the value of the right hand side above for $y$ in the equation for $E$, we get a cubic equation in $x$:

$$\begin{aligned}
&\left(\left(\frac{a_1y_0 + x_0^2 + a_4}{a_1x_0 + a_3}\right)x + \frac{y_0^2 + a_1x_0y_0 + a_2x_0^2 + a_6}{a_1x_0 + a_3}\right)^2 \\
+a_1x &\left(\left(\frac{a_1y_0 + x_0^2 + a_4}{a_1x_0 + a_3}\right)x + \frac{y_0^2 + a_1x_0y_0 + a_2x_0^2 + a_6}{a_1x_0 + a_3}\right) \\
+a_3 &\left(\left(\frac{a_1y_0 + x_0^2 + a_4}{a_1x_0 + a_3}\right)x + \frac{y_0^2 + a_1x_0y_0 + a_2x_0^2 + a_6}{a_1x_0 + a_3}\right) = x^3 + a_2x^2 + a_4x + a_6.
\end{aligned}$$

Adding the left-hand side to the right, we get an equation of the form $f(x) = 0$. The coefficient of $x^2$ is equal to

$$\frac{a_2a_1^2x_0^2 + a_2a_3^2 + a_1^2y_0^2 + x_0^4 + a_4^2 + a_1^3x_0y_0 + a_1^2x_0^3 + a_1^2a_4x_0 + a_1^2a_3y_0 + a_1a_3x_0^2 + a_1a_3a_4}{a_1^2x_0^2 + a_3^2}.$$

This simplifies to

$$\frac{a_1^2a_6 + a_2a_3^2 + x_0^4 + a_4^2 + a_1a_3x_0^2 + a_1a_3a_4}{a_1^2x_0^2 + a_3^2}.$$

The coefficient of $x$ is equal to

$$\frac{a_1a_4x_0 + a_3a_4 + a_1y_0^2 + a_1^2x_0y_0 + a_1a_2x_0^2 + a_1a_6 + a_1a_3y_0 + a_3x_0^2 + a_3a_4}{a_1x_0 + a_3},$$

which simplifies to

$$\frac{a_1x_0^3 + a_3x_0^2}{a_1x_0 + a_3} = x_0^2.$$

The constant term is equal to

$$\underline{y_0^4 + a_1^2x_0^2y_0^2 + a_2^2x_0^4 + a_6^2 + a_1a_3x_0y_0^2 + a_1^2a_3x_0^2y_0 + a_1a_2a_3x_0^3 + a_1a_3a_6x_0 + a_3^2y_0^2}$$

$$\frac{+a_1a_3^2x_0y_0 + a_2a_3^2x_0^2 + a_3^2a_6 + a_1^2a_6x_0^2 + a_3^2a_6}{a_1^2x_0^2 + a_3^2}.$$

The numerator of this coefficient further simplifies to

$$(x_0^6+a_1^2x_0^2y_0^2+a_3^2y_0^2+a_2^2x_0^4+a_4^2x_0^2+a_6^2)+a_1^2x_0^2y_0^2+a_2^2x_0^4+a_6^2+(a_1^2a_3x_0^2y_0+a_1a_3^2x_0y_0+a_1a_3x_0^4$$

$$+a_1a_2a_3x_0^3+a_1a_3a_4x_0^2+a_1a_3a_6x_0)+a_1^2a_3x_0^2y_0+a_1a_2a_3x_0^3+a_1a_3a_6x_0+(a_1a_3^2x_0y_0+a_3^3y_0$$

$$+a_2a_3^2x_0^2 + a_3^2a_4x_0 + a_3^2a_6) + a_1a_3^2x_0y_0 + a_2a_3^2x_0^2 + a_1^2a_6x_0^2$$

which is equal to

$$x_0^6+(a_1a_3^2x_0y_0+a_3^3y_0+a_2a_3^2x_0^2+a_3^2a_4x_0+a_3^2a_6)+a_4^2x_0^2+a_1a_3x_0^4+a_1a_3a_4x_0^2+a_3^3y_0+a_3^2a_4x_0$$

$$+a_3^2a_6 + a_1a_3^2x_0y_0 + a_1^2a_6x_0^2,$$

so the constant term is equal to

$$\frac{x_0^6 + a_2a_3^2x_0^2 + a_4^2x_0^2 + a_1a_3x_0^4 + a_1a_3a_4x_0^2 + a_1^2a_6x_0^2}{a_1^2x_0^2 + a_3^2}.$$

It remains to show that $x_0$ is at least a double root of the cubic polynomial

$$x^3 + \left(\frac{a_1^2a_6 + a_2a_3^2 + x_0^4 + a_4^2 + a_1a_3x_0^2 + a_1a_3a_4}{a_1^2x_0^2 + a_3^2}\right)x^2 + x_0^2x$$

$$+\frac{x_0^6 + a_2a_3^2x_0^2 + a_4^2x_0^2 + a_1a_3x_0^4 + a_1a_3a_4x_0^2 + a_1^2a_6x_0^2}{a_1^2x_0^2 + a_3^2}.$$

This polynomial factors as

$$(x^2+x_0^2)\left(x+\frac{a_1^2a_6+a_2a_3^2+x_0^4+a_4^2+a_1a_3x_0^2+a_1a_3a_4}{a_1^2x_0^2+a_3^2}\right)$$

so $x_0$ is a double root of this polynomial. Thus, $\ell_P$ and $E$ intersect at $P=[x_0:y_0:1]$ with multiplicity 2, and at $P'=[x_1:y_1:1]$ with multiplicity 1, where

$$\begin{aligned} x_1 &= \frac{a_1^2a_6+a_2a_3^2+x_0^4+a_4^2+a_1a_3x_0^2+a_1a_3a_4}{a_1^2x_0^2+a_3^2} \\ y_1 &= \left(\frac{a_1y_0+x_0^2+a_4}{a_1x_0+a_3}\right)x_1+\frac{y_0^2+a_1x_0y_0+a_2x_0^2+a_6}{a_1x_0+a_3}. \end{aligned}$$

**Case 2:** $Char(K)=3$. In this case, the Weierstrass curve is isomorphic to

$$E: y^2z = x^3+a_2x^2z+a_4xz^2+a_6z^3,$$

and the isomorphism given in Lemma 4.1.4 does not change the number of points of intersection or the intersection multiplicities, since the isomorphism is a linear map. As before, we consider the tangent line to $E$ at a point $P=[x_0:y_0:1]$. The tangent line at this point is given by the equation

$$(a_2x_0+2a_4)x+(2y_0)y+(y_0^2+2a_2x_0^2+a_4x_0)z=0.$$

If $y_0=0$, then the equation of the tangent line is given by $x-x_0z=0$. This line once again intersects $E$ in the points $[0:1:0]$ and $P$. Setting $z=1, x=x_0$ in $E$, we see that the only root of the equation

$$y^2=x_0^3+a_2x_0^2+a_4x_0+a_6$$

is $y=y_0=0$, because the right-hand side is by definition equal to $y_0^2=0$, so $\ell_P$ intersects $E$ at $P=[x_0:0:1]$ with multiplicity 2 and at $[0:1:0]$ with multiplicity 1.

Now suppose that $y_0 \neq 0$. Then setting $z = 1$ as in the characteristic 2 case, we see that $x$ and $y$ satisfy the relation

$$y = \left(\frac{2a_2x_0 + a_4}{2y_0}\right)x + \frac{2y_0^2 + a_2x_0^2 + 2a_4x_0}{2y_0}.$$

As before, we want to show that $x_0$ is a double root of

$$\left(\left(\frac{2a_2x_0 + a_4}{2y_0}\right)x + \frac{2y_0^2 + a_2x_0^2 + 2a_4x_0}{2y_0}\right)^2 = x^3 + a_2x^2 + a_4x + a_6,$$

that is, that $x_0$ is a double root of the equation

$$x^3 + \left(\frac{2a_2^2x_0^2 + 2a_2a_4x_0 + 2a_4^2 + a_2y_0^2}{y_0^2}\right)x^2 + \left(\frac{a_2x_0y_0^2 + 2a_2^2x_0^3 + 2a_2a_4x_0^2 + 2a_4^2x_0}{y_0^2}\right)x + \\ \frac{2y_0^4 + 2a_2x_0^2y_0^2 + a_4x_0y_0^2 + 2a_2^2x_0^4 + 2a_2a_4x_0^3 + 2a_4^2x_0^2 + a_6y_0^2}{y_0^2} = 0.$$

The constant coefficient can be rewritten as

$$\begin{aligned} & \frac{2(y_0^4 + a_2x_0^2y_0^2 + 2a_4x_0y_0^2 + a_2^2x_0^4 + a_2a_4x_0^3 + a_4^2x_0^2 + 2a_6y_0^2)}{y_0^2} \\ = & \frac{2(y_0^2(y_0^2 + a_2x_0^2 + 2a_4x_0) + a_2^2x_0^4 + a_2a_4x_0^3 + a_4^2x_0^2 + 2a_6y_0^2)}{y_0^2} \\ = & \frac{2(y_0^2(x_0^3 + 2a_2x_0^2 + a_6) + a_2^2x_0^4 + a_2a_4x_0^3 + a_4^2x_0^2 + 2a_6y_0^2)}{y_0^2} \\ = & \frac{2x_0^3y_0^2 + a_2x_0^2y_0^2 + 2a_2^2x_0^4 + 2a_2a_4x_0^3 + 2a_4^2x_0^2}{y_0^2}. \end{aligned}$$

The polynomial

$$x^3 + \left(\frac{2a_2^2x_0^2 + 2a_2a_4x_0 + 2a_4^2 + a_2y_0^2}{y_0^2}\right)x^2 + \left(\frac{a_2x_0y_0^2 + 2a_2^2x_0^3 + 2a_2a_4x_0^2 + 2a_4^2x_0}{y_0^2}\right)x + \\ \frac{2x_0^3y_0^2 + a_2x_0^2y_0^2 + 2a_2^2x_0^4 + 2a_2a_4x_0^3 + 2a_4^2x_0^2}{y_0^2}$$

factors as

$$(x^2 + x_0x + x_0^2)\left(x + \frac{2a_2^2x_0^2 + 2a_2a_4x_0 + 2a_4^2 + a_2y_0^2 + 2x_0y_0^2}{y_0^2}\right),$$

so $x_0$ is a double root, as required. Hence, $\ell_P$ intersects $E$ at the point $P$ with multiplicity 2, and at the point $[x_1 : y_1 : 1]$ with multiplicity 1, where

$$\begin{aligned} x_1 &= -\frac{2a_2^2x_0^2 + 2a_2a_4x_0 + 2a_4^2 + a_2y_0^2 + 2x_0y_0^2}{y_0^2} \\ y_1 &= \left(\frac{2a_2x_0 + a_4}{2y_0}\right)x_1 + \frac{2y_0^2 + a_2x_0^2 + 2a_4x_0}{2y_0}. \end{aligned}$$

**Case 3:** Finally, we cover the case where the characteristic of $\bar{K}$ is not 2 or 3. In this case, we may assume from Lemma 4.1.6 that $E$ is given by the equation

$$E : y^2z = x^3 + Axz^2 + Bz^3,$$

because the transformation is linear and thus once again does not affect intersection multiplicities. The tangent line at a point $P = [x_0 : y_0 : 1]$ is given by the equation

$$(-3x_0^2 - A)x + (2y_0)y + (y_0^2 - 2Ax_0 - 3B)z = 0.$$

If $y_0 = 0$, the equation of the tangent line is $x - x_0z = 0$. The proof that this line intersects the curve $E$ in only two points is identical to the proof of the characteristic 2 and 3 cases, so we omit it.

Suppose, then, that $y_0 \neq 0$ and set $z = 1$. Then $x$ and $y$ are related via

$$y = \left(\frac{3x_0^2 + A}{2y_0}\right)x + \frac{-y_0^2 + 2Ax_0 + 3B}{2y_0},$$

which we choose to write as

$$y = \left(\frac{3x_0^2 + A}{2y_0}\right)x + \frac{-x_0^3 + Ax_0 + 2B}{2y_0}.$$

As in the previous two cases, we will prove that $x_0$ is a double root of the equation

$$\left(\left(\frac{3x_0^2 + A}{2y_0}\right)x + \frac{-x_0^3 + Ax_0 + 2B}{2y_0}\right)^2 = x^3 + Ax + B,$$

i.e. of the equation

$$\begin{aligned}
x^3 - &\left(\frac{9x_0^4 + 6Ax_0^2 + A^2}{4y_0^2}\right) x^2 + \left(\frac{4Ay_0^2 + 6x_0^5 - 6Ax_0^3 - 12Bx_0^2 + 2Ax_0^3 - 2A^2x_0 - 4AB}{4y_0^2}\right) x \\
&+ \frac{4By_0^2 - x_0^6 + 2Ax_0^4 + 4Bx_0^3 - A^2x_0^2 - 4ABx_0 - 4B^2}{4y_0^2} \\
&= x^3 - \left(\frac{9x_0^4 + 6Ax_0^2 + A^2}{4y_0^2}\right) x^2 \\
&+ \left(\frac{4A(x_0^3 + Ax_0 + B) + 6x_0^5 - 6Ax_0^3 - 12Bx_0^2 + 2Ax_0^3 - 2A^2x_0 - 4AB}{4y_0^2}\right) x \\
&+ \frac{4B(x_0^3 + Ax_0 + B) - x_0^6 + 2Ax_0^4 + 4Bx_0^3 - A^2x_0^2 - 4ABx_0 - 4B^2}{4y_0^2} \\
&= x^3 - \left(\frac{9x_0^4 + 6Ax_0^2 + A^2}{4y_0^2}\right) x^2 \\
&+ \left(\frac{6x_0^5 - 12Bx_0^2 + 2A^2x_0}{4y_0^2}\right) x \\
&+ \frac{8Bx_0^3 - x_0^6 + 2Ax_0^4 - A^2x_0^2}{4y_0^2} \\
&= (x^2 - 2x_0x + x_0^2)\left(x + \frac{8x_0y_0^2 - 9x_0^4 - 6Ax_0^2 - A^2}{4y_0^2}\right)
\end{aligned}$$

and $x_0$ is once again a double root. □

Since a line in projective space has degree one and an elliptic curve has degree three, by Bézout's Theorem, the elliptic curve will intersect the given line in three points, when the points are counted with their intersection multiplicities. This is important. The fact that the line and curve intersect in three points means that one *can* define an additive identity as well as a group law without ambiguity. First, define the basepoint $O_E$ to be the additive identity. The rest is given by the following definition.

**Definition 4.4.2** *Let $(E, O_E)$ be an elliptic curve. The following three properties fully describe point addition on the curve $E$.*

- *$-P$ is defined as the third point of intersection of $E$ and the line through $P$ and $O_E$.*
- *If $P \neq Q$, $P + Q = -R$, where $R$ is the third point of intersection of $E$ and the line through $P$ and $Q$.*
- *In the event that $P = Q$, $P+Q$ is defined to be $-R$, where $R$ is the third point of intersection of $E$ and the tangent line at $P$.*

The formulae for point addition on a Weierstrass curve with basepoint $O_E = [0 : 1 : 0]$ are as follows:

$$\begin{aligned} & [x_0 : y_0 : 1] + [x_0 : y_0 : 1] \\ = \; & [m^2 + a_1 mb - (a_2 + 2x_0)b^2 : mb(x_0 - x_2) - y_0 b^2 - (a_1 x_2 + a_3)b^2 : b^2], \end{aligned}$$

$$\begin{cases} m = 3x_0^2 + 2a_2 x_0 + a_4 - a_1 y_0 \\ b = 2y_0 + a_1 x_0 + a_3, \end{cases}$$

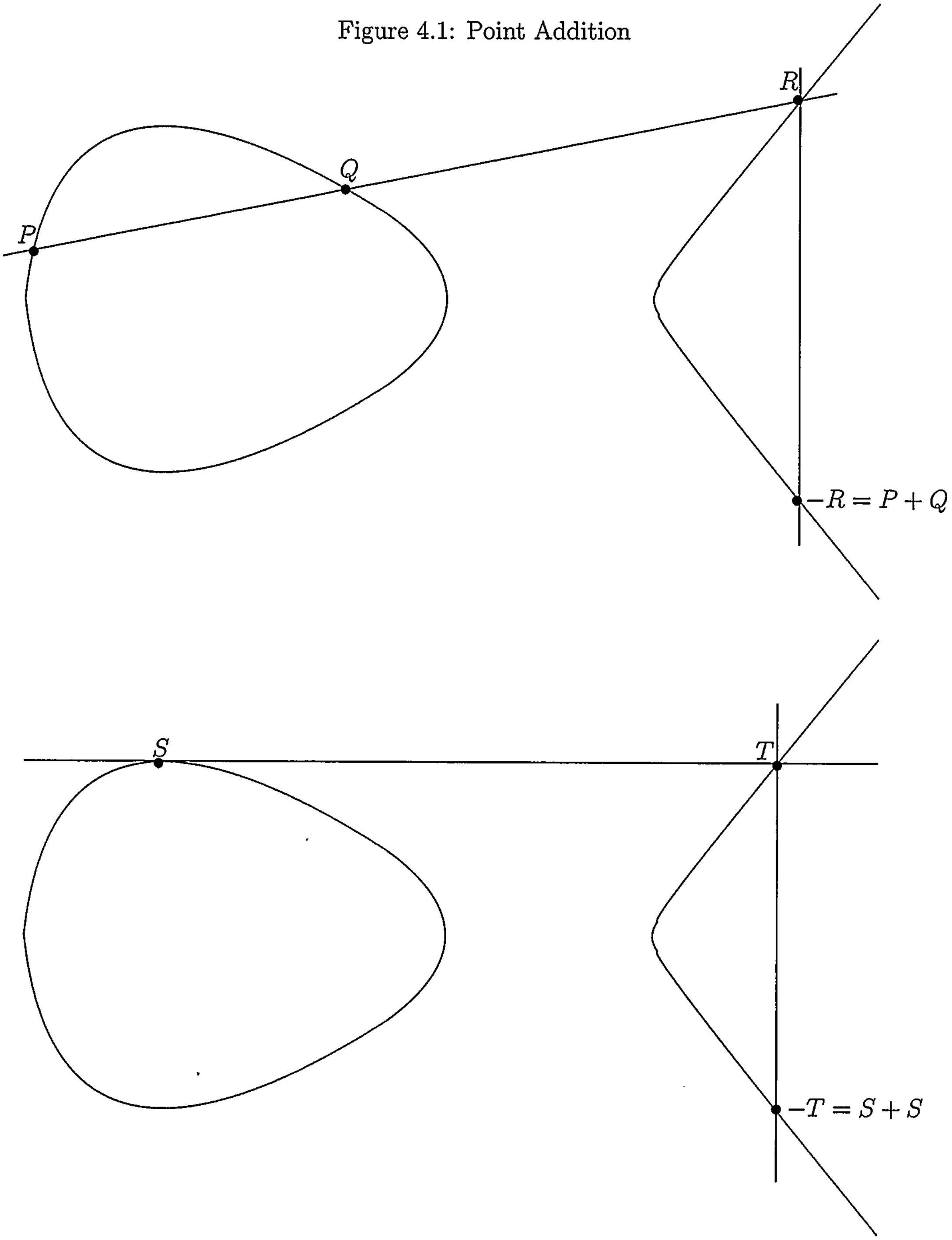
and if $(x_0, y_0) \neq (x_1, y_1)$:

$$\begin{aligned} & [x_0 : y_0 : 1] + [x_1 : y_1 : 1] \\ = \; & [\delta_2^2 + a_1\delta_2\delta_1 - (a_2 + x_0 + x_1)\delta_1^2 : \delta_2\delta_1(x_0 - x_2) - y_0\delta_1^2 - (a_1 x_2 + a_3)\delta_1^2 : \delta_1^2], \end{aligned}$$

$$\begin{cases} \delta_1 = & x_1 - x_0 \\ \delta_2 = & y_1 - y_0. \end{cases}$$

The following figure gives the reader a pictorial idea of point addition.

Figure 4.1: Point Addition



It is not difficult to see that if we have an irreducible projective plane curve $C$ which is isomorphic to a smooth Weierstrass curve, we can make $C$ into an elliptic curve $(E = C, O_E)$ by letting $O_E$ be some arbitrary point $P$ on the curve $C$. By convention, the chosen point $O_E$ of a Weierstrass curve is the point $[0 : 1 : 0]$ because it is always a point on the curve, regardless of the coefficients of the equation of the curve or the underlying field. We will therefore not state the basepoint whenever the curve is in Weierstrass form and simply assume that $O_E = [0 : 1 : 0]$. The Weierstrass form is just one 'model', however, and the next example shows an elliptic curve with a different model and basepoint.

**Example 4.4.3** *$E/\mathbb{Q} : x^3 + y^3 = 1729z^3$ (with basepoint $[1 : -1 : 0]$) is an elliptic curve because it is isomorphic to the curve $E'/\mathbb{Q} : u^3 + v^3 = 27w^3$, which itself was shown in Example 3.3.9 to be isomorphic to the Weierstrass curve $E''/\mathbb{Q} : 108s^2t = 108r^3 - t^3$. The isomorphism from E to E′ is given by*

$$\alpha([x_0 : y_0 : z_0]) = \left[x_0 : y_0 : \frac{\sqrt[3]{1729}}{3} z_0\right]$$

*with inverse*

$$\alpha^{-1}([u_0 : v_0 : w_0]) = \left[u_0 : v_0 : \frac{3}{\sqrt[3]{1729}} w_0\right].$$

*We claim that for any point $P = [x_0 : y_0 : z_0]$ on $E$ above, $-P = [y_0 : x_0 : z_0]$. The assertion is that $[x_0 : y_0 : z_0] + [y_0 : x_0 : z_0] = [1 : -1 : 0]$. It suffices to show that the three points are collinear. The line*

$$ax + ay + cz = 0$$

*where $(a, c) = (1, 0)$, if $x_0 + y_0 = 0$ and $(a, c) = \left(\frac{-z_0}{x_0+y_0}, 1\right)$, otherwise, contains all three points, so the three points are indeed collinear. Applying the definition of point* *addition to the 2 points* $[10:9:1]$ *and* $[12:1:1]$ *on* $E$ *yields*

$$[10:9:1]+[12:1:1]=[-37:46:3]$$

*since* $[46:-37:3]$ *is the third point of intersection of the line through* $P$ *and* $Q$*, which has equation* $4x+y-49z=0$.

**Theorem 4.4.4** *Let* $(E, O_E)$ *be an elliptic curve and let* $A$ *and* $B$ *be points on* $E$*. Then there is an isomorphism (of curves)* $\tau : E \longrightarrow E$ *which takes* $A$ *to* $B$*.*

**Proof.** Let $Q = B - A \in E$. Then $\tau(P) = P + Q$ is clearly an isomorphism of curves which takes $A$ to $B$. □

**Remark 4.4.5** *Note that* $\tau$ *is not unique. Regarding* $E$ *just as a curve for a moment, there are infinitely many points* $P \in E$ *which, taken as the basepoint, make* $E$ *into an elliptic curve. Therefore, there are infinitely many possible values of* $Q = B - A$ *— since* $-A$ *is different for different values of* $O_E$ *— and so infinitely many isomorphisms of curves that take* $A$ *to* $B$*.*

**Definition 4.4.6** *Let* $E$ *be an elliptic curve. The subset of those points defined over (i.e. with coordinates in) the subfield* $K$ *of* $\bar{K}$ *is denoted by* $E(K)$ .

**Example 4.4.7** *Consider* $E/\mathbb{F}_{11}$ *given by*

$$E : y^2z = x^3 + xz^2 + 2z^3.$$

$$\begin{aligned} E(\mathbb{F}_{11}) &= \{[0:1:0],[1:2:1],[1:9:1],[2:1:1],\\ &\quad [2:10:1],[4:2:1],[4:9:1],[5:0:1],\\ &\quad [6:2:1],[6:9:1],[7:0:1],[8:4:1],\\ &\quad [8:7:1],[9:5:1],[9:6:1],[10:0:1]\}. \end{aligned}$$

**Theorem 4.4.8** *Let $(E, O_E)$ be an elliptic curve over $\bar{K}$ with $O_E \in E(K)$. Then the points on $E$ form an additive abelian group and $E(K)$ is a subgroup thereof.*

**Proof.** The identity is $O_E$, and the commutative property, closure and the existence of inverses clearly hold. Associativity requires somewhat more effort (we show this in Proposition 5.1.19). □

The structure and order of the subgroup $E(K)$ of $E(\bar{K})$ of $K$-rational points are of particular interest, especially as they pertain to $K = \mathbb{F}_q$, the finite field of $q$ elements. The following two theorems give information about this.

**Theorem 4.4.9** *(Hasse) Let $E$ be an elliptic curve over a finite field $\mathbb{F}_q$. Then $|E(\mathbb{F}_q)| = q + 1 - t$, where*

$$|t| \leq 2\sqrt{q}.$$

**Proof.** See [7, Theorem 3.61]. □

**Theorem 4.4.10** *(Rück) For $E$ an elliptic curve over a finite field $\mathbb{F}_q$, there exist $m, n \in \mathbb{N}$ with*

$$E(\mathbb{F}_q) \cong \mathbb{Z}_m \times \mathbb{Z}_n$$

*such that $m \mid n$ and $m \mid q - 1$.*

**Proof.** See [7, Theorem 3.76]. □

**Example 4.4.11** *Consider again $E/\mathbb{F}_{11}$ given by*

$$E : y^2 z = x^3 + xz^2 + 2z^3.$$

*Then we see from Example 4.4.7 that* $|E(\mathbb{F}_{11})| = 16$, *so* $E(\mathbb{F}_{11}) \cong \mathbb{Z}_{16}$ *or* $E(\mathbb{F}_{11}) \cong \mathbb{Z}_2 \times \mathbb{Z}_8$ *or* $E(\mathbb{F}_{11}) \cong \mathbb{Z}_4 \times \mathbb{Z}_4$. *The group* $E(\mathbb{F}_{11})$ *has 3 points of order 2 (which one can verify from the point addition formulae — they are* $[5:0:1], [7:0:1], [10:0:1]$*) while* $\mathbb{Z}_{16}$ *has but one, so* $E(\mathbb{F}_{11})$ *cannot be isomorphic to* $\mathbb{Z}_{16}$. *Since* $4 \nmid 10$, *we conclude that* $E(\mathbb{F}_{11}) \cong \mathbb{Z}_2 \times \mathbb{Z}_8$. *Additionally, we find that the value t from Theorem 4.4.9 is* $11 + 1 - 16 = -4$, *so* $|t| = 4 < 2 \cdot \sqrt{11}$.

# Chapter 5

# Isogeny

This chapter is devoted to isogeny. According to the definition of isogeny, it would seem that an isogeny is just a particular type of morphism. However, an isogeny is much more than that. An isogeny is a very special type of morphism, given that it is a morphism not just between *any* curves, but rather, between elliptic curves. Recall that such curves have a natural group structure embedded within them. As we will soon see, the isogenies thereof also have special properties. Amongst other things, isogenies are group homomorphisms. As always, let $K$ be a field with algebraic closure $\bar{K}$.

## 5.1 Divisors

We begin with a discussion of divisors. Divisors facilitate an understanding of elliptic curves. They enable one to establish the associative law in the group of points of an elliptic curve in a clean fashion, without resorting to tedious calculations.

**Definition 5.1.1** *Let $E$ be an elliptic curve. The* divisor group $\mathrm{Div}(E)$ of $E$ *is the abelian group of finite formal sums of points of $E$. Elements of Div(E) are called* divisors *and take the form*

$$\sum_{P\in E} n_P(P),$$

*where $n_P \in \mathbb{Z}$ and $n_P = 0$ for all but finitely many $P \in E$.*

**Remark 5.1.2** *In other words, a divisor $D$ can be interpreted as a function $D : E \longrightarrow \mathbb{Z}$ with finite support given by $D(P) = n_P$ for all $P \in E$.*

**Example 5.1.3** *Let $E$ be an elliptic curve and let $P, Q \in E$. Then $2(P) + (-1)(Q)$ is a divisor.*

**Remark 5.1.4** *The divisor above is not to be confused with the point $R = P+P-Q$ on the curve $E$.*

**Definition 5.1.5** *Let $E$ be an elliptic curve. The* degree *of a divisor*

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

*is the sum*

$$\sum_{P \in E} n_P$$

*and is denoted by* $\deg(D)$.

**Example 5.1.6** *For $P$ any point on an elliptic curve $E$, the degree of $(P) - (O_E)$ is 0. Likewise, the degree of the divisor $2(P)+(-1)(Q)$ from Example 5.1.3 is* $2-1 = 1$.

**Definition 5.1.7** *Let $Div(E)$ be the divisor group of an elliptic curve $E$. We denote by $Div^0(E)$ the subset of $Div(E)$ consisting of divisors of degree 0.*

Note that $Div^0(E)$ is actually a subgroup of $Div(E)$, since the degree zero divisors are closed under addition and inverses, and $Div^0(E)$ contains the zero divisor.

**Remark 5.1.8** *The degree map* $\deg : Div(E) \longrightarrow \mathbb{Z}$ *is a group homomorphism whose kernel is $Div^0(E)$.*

The next definition deals with the order of a rational function $f$ at a point $P$ on the curve $E$. Recall that we introduced this notion in Proposition 2.4.13.

**Lemma 5.1.9** *Let $E$ be an elliptic curve and let $f \in \bar{K}(E)^\times$. Then the function $E \longrightarrow \mathbb{Z}$ defined by $P \longrightarrow ord_P(f)$ is a divisor.*

**Proof.** It suffices to show that this function is zero for all but finitely many points $P \in E$. By definition, $f = \frac{g}{h}$ is just a quotient of homogeneous polynomials $g, h$ of the same degree in $X, Y, Z$. The claim now follows, since by Bézout's theorem, $g(x, y, z)$ and $h(x, y, z)$ can each intersect $E(x, y, z)$ in only finitely many points, and thus, there are only finitely many $P \in E$ such that $g(P) = 0$ or $h(P) = 0$, i.e. for which $ord_P(f) \neq 0$. □

**Definition 5.1.10** *Let $E$ be an elliptic curve and $f \in \bar{K}(E)^\times$. We denote by $div(f)$ the divisor $\sum_{P \in E} ord_P(f)(P)$.*

**Example 5.1.11** *Let $f$ be the image of $k \in \bar{K}^\times$ under the inclusion map $\bar{K}^\times \hookrightarrow \bar{K}(E)^\times$. Then $div(f) = 0 = \sum_{P \in E} 0(P)$, since $ord_P(f) = 0$ for any point $P \in E$.*

**Definition 5.1.12** *Let $E$ be an elliptic curve. We say that a divisor $D$ is a* principal divisor *if $D = div(f)$ for some $f \in \bar{K}(E)^\times$.*

**Definition 5.1.13** *Let $E$ be an elliptic curve. Two divisors $D_1, D_2$ are said to be* linearly equivalent, *written $D_1 \sim D_2$, if $D_1 - D_2$ is a principal divisor.*

**Proposition 5.1.14** *The relation $\sim$ is an equivalence relation.*

**Proof.** The relation $\sim$ is clearly reflexive, since $0 = div(f)$, for any constant rational function $f \in \bar{K}(E)^{\times}$. The relation is symmetric, because $D_1 - D_2 = div(f)$ implies $D_2 - D_1 = div(\frac{1}{f})$, so $D_2 \sim D_1$. Finally, the relation is transitive, since

$$\begin{aligned} D_1 - D_3 &= (D_1 - D_2) + (D_2 - D_3) \\ &= \sum_{P \in E} ord_P(f)(P) + \sum_{P' \in E} ord_{P'}(g)(P') \\ &= \sum_{P \in E} ord_P(fg)(P) \\ &= div(fg). \end{aligned}$$

□

**Proposition 5.1.15** *The set of principal divisors is a subgroup of $Div^0(E)$.*

**Proof.** The fact that the degree of a principal divisor is 0 follows from Proposition 2.4.15. Adding $div(f)$ to $div(g)$ gives $div(fg)$ — this gives closure. The (additive) inverse of $div(f)$ is $div(\frac{1}{f})$. □

**Definition 5.1.16** *We denote by $Pic^0(E)$ the factor group of $Div^0(E)$ modulo the subgroup of principal divisors, or equivalently, the group of divisor classes under linear equivalence. The group $Pic^0(E)$ is called the* Picard group of $E$.

Henceforth, we will use the notation $\overline{D}$ to denote the divisor class of a divisor $D \in Div^0(E)$.

**Lemma 5.1.17** *Let $\overline{D} \in Pic^0(E)$. Then there exists a unique point $P$ on $E$ such that $(P) - (O_E) \in \overline{D}$.*

**Proof.** See [24, Proposition III.3.4(a)]. □

**Corollary 5.1.18** *The map $\theta : E \longrightarrow Pic^0(E)$ given by $P \longrightarrow \overline{(P)-(O_E)}$ is a bijection with inverse $\theta^{-1} : Pic^0(E) \longrightarrow E$ given by $\overline{D} \longrightarrow P$, where $P$ is the unique point such that $\overline{(P)-(O_E)} = \overline{D}$.*

We now come to one of the most important results of this thesis. We show, among other things, that the points of an elliptic curve are associative under point addition and hence really do form an abelian group.

**Proposition 5.1.19** *Let $\theta : E \longrightarrow Pic^0(E)$ be the bijection given in Corollary 5.1.18. Then $\theta$ preserves addition on $E$, so $E$ is an additive abelian group and $\theta$ is a group isomorphism.*

**Proof.** Let $P, Q \in E$. We claim that $\theta(P+Q) = \theta(P) + \theta(Q)$. Now $\theta(P+Q) = \overline{(P+Q)-(O_E)}$ and $\theta(P)+\theta(Q) = \overline{(P)-(O_E)} + \overline{(Q)-(O_E)} = \overline{(P)+(Q)-2(O_E)}$. Hence, we need to show that $\overline{(P+Q)-(O_E)} = \overline{(P)+(Q)-2(O_E)}$. In other words, we need to show that $(P+Q)-(P)-(Q)+(O_E)$ is principal, i.e. of the form $div(f)$, for some $f \in \bar{K}(E)^{\times}$. Let $\ell_1$ be the line through $P+Q, -(P+Q)$ and $O_E$, and $\ell_2$ the line through $P, Q$ and $-(P+Q)$. Consider the rational function $\frac{\ell_1(X,Y,Z)}{\ell_2(X,Y,Z)}$. Then $\ell_1$ intersects $E$ in exactly the three points $P+Q, -(P+Q)$ and $O_E$. Similarly, $\ell_2$ intersects $E$ only in the three points $P, Q$ and $-(P+Q)$. There are several cases to consider. We show only two cases, since the others can be established similarly.

**Case 1:** Suppose that $P+Q, -(P+Q), O_E, P$ and $Q$ are distinct. Then $\frac{\ell_1(X,Y,Z)}{\ell_2(X,Y,Z)}$ has order 1 at $P+Q$ and $O_E$, order $1-1=0$ at $-(P+Q)$ and order -1 at $P$ and $Q$. So

$$div\left(\frac{\ell_1(X,Y,Z)}{\ell_2(X,Y,Z)}\right) = (P+Q)-(P)-(Q)+(O_E).$$

**Case 2:** Suppose that $P, Q, -(P+Q)$ and $O_E$ are again distinct, but that $P+Q = -(P+Q)$. Then $\ell_1 = \ell_{P+Q}$, the tangent line to $E$ at $P+Q$. Thus, $\frac{\ell_1(X,Y,Z)}{\ell_2(X,Y,Z)}$ has order $2-1=1$ at $P+Q$, order 1 at $O_E$ and order -1 at $P$ and $Q$. (See [18, Proposition 4.6] for details.) Once again, we see that

$$div\left(\frac{\ell_1(X,Y,Z)}{\ell_2(X,Y,Z)}\right) = (P+Q) - (P) - (Q) + (O_E).$$

In all other cases, we come to the same conclusion — that

$$div\left(\frac{\ell_1(X,Y,Z)}{\ell_2(X,Y,Z)}\right) = (P+Q) - (P) - (Q) + (O_E),$$

(which may simplify if, for instance, $P = Q$) and we omit the proofs of these cases.

Now that we have proved that $\theta$ preserves addition, it remains to show that the points of $E$ form an additive abelian group which is isomorphic to $Pic^0(E)$. We proved all but the associative law in the previous chapter. For associativity, consider that

$$\begin{aligned}
\theta((P+Q)+R) &= \theta(P+Q)+\theta(R)\\
&= (\theta(P)+\theta(Q))+\theta(R)\\
&= \theta(P)+(\theta(Q)+\theta(R))\\
&= \theta(P)+\theta(Q+R)\\
&= \theta(P+(Q+R)),
\end{aligned}$$

where the third equality follows from the fact that $Pic^0(E)$ is a group and thus associative. The result follows, since $\theta$ is one-to-one (from Lemma 5.1.17). □

## 5.2 Isogeny

We have now come to the topic that is central to our entire discussion: isogeny. We begin by defining an isogeny of elliptic curves, give examples and analyze some of the properties of isogenies.

**Definition 5.2.1** *Let $E_1$ and $E_2$ be elliptic curves defined over $K$. An* isogeny *$\alpha : E_1 \to E_2$ is a morphism such that $\alpha(O_{E_1}) = O_{E_2}$, where $O_{E_1}$ and $O_{E_2}$ are the basepoints of $E_1$ and $E_2$, respectively. An isogeny which is defined over $K$ is called a $K$*-isogeny.

**Remark 5.2.2** *If $E_1$ and $E_2$ are elliptic curves defined over $K$, an isogeny from $E_1$ to $E_2$ need not be a $K$-isogeny, as the following example shows.*

**Example 5.2.3** *Taking $K = \mathbb{F}_{13}$, consider the elliptic curves we saw previously in Example 3.3.12:*

$$E_1/\mathbb{F}_{13} : y^2z = x^3 + 7xz^2 + 3z^3,$$

$$E_2/\mathbb{F}_{13} : v^2w = u^3 + 5uw^2 + 11w^3.$$

*The isomorphism from $E_1$ to $E_2$ from that example, given by*

$$\alpha : [x_0 : y_0 : z_0] \to [6x_0 : r^{-3}y_0 : z_0],$$

*where $r^2 = 11$, is in fact an isogeny, since $\alpha([0:1:0]) = [6 * 0 : r^{-3} * 1 : 0] = [0 : 1 : 0]$. However, it is not an $\mathbb{F}_{13}$-isogeny, since $E_1$ has 13 points over $\mathbb{F}_{13}$ while $E_2$ has 15 points over $\mathbb{F}_{13}$ (see Theorem 5.2.16).*

The requirement that the map takes the identity to the identity does not seem restrictive. However, this has major ramifications as the following theorem shows.

**Theorem 5.2.4** *Let $E_1$ and $E_2$ be elliptic curves defined over $K$. An isogeny $\alpha : E_1 \to E_2$ is a group homomorphism from $E_1$ to $E_2$.*

**Proof.** By Proposition 5.1.19, $E_1$ is isomorphic to $Pic^0(E_1)$ and $E_2$ is isomorphic to $Pic^0(E_2)$. Consider the $\mathbb{Z}$-linear map $\alpha_* : Div(E_1) \longrightarrow Div(E_2)$ given by

$$\sum n_P(P) \longmapsto \sum n_P(\alpha(P)).$$

Then $\alpha_*$ is a group homomorphism. The map $\alpha_*$ can also be shown to preserve linear equivalence (see [24, Proposition II.3.6(d)]) — thus, $\alpha_*$ can be extended to a homomorphism from $Pic^0(E_1)$ to $Pic^0(E_2)$. If we denote by $\theta_1 : E_1 \longrightarrow Pic^0(E_1)$ the isomorphism from $E_1$ to $Pic^0(E_1)$ and by $\theta_2 : E_2 \longrightarrow Pic^0(E_2)$ the isomorphism from $E_2$ to $Pic^0(E_2)$, then we see that $\theta_2^{-1} \circ \alpha_* \circ \theta_1(P) = \alpha(P)$ for all $P$ on $E_1$. Since $\alpha$ is the composition of three group homomorphisms, $\alpha$ must also be a group homomorphism. □

We now give three examples of isogenies, two of them from a curve $E$ to itself.

**Definition 5.2.5** *Let $E$ be an elliptic curve. Define the* multiplication-by-$m$ map *$[m] : E \longrightarrow E$, where $m \in \mathbb{Z}$, by*

$$m[P] = \begin{cases} P + \cdots + P & \text{if } m > 0 \\ -[-m]P & \text{if } m < 0 \\ O_E & \text{if } m = 0 \end{cases}$$

**Proposition 5.2.6** *For all $m \in \mathbb{Z}$, $[m]$ is an isogeny.*

**Proof.** The fact that $[m]$ is given by homogeneous polynomials of the same degree follows from the point addition formulae in Section 4.4. (We only gave the point addition formulae for Weierstrass curves; nonetheless, such formulae can be derived for *any* elliptic curve.) The map $[m]$ is obviously a morphism, since it is defined at all points $P \in E$. It suffices, then, to show that $[m]$ takes $O_E$ to $O_E$. Since we clearly have $O_E + O_E = O_E$, it follows by induction on $m$, for $m > 0$, that adding $O_E$ to itself $m$ times gives $O_E$. In the second case, we see that $-[-m]O_E = -O_E = O_E$. □

**Example 5.2.7** *Let $E/\mathbb{Q} : x^3 + y^3 = 1729z^3$ and $P = [x_0 : y_0 : z_0]$ any point on $E$. Then $[2]P = -R$, where $-R$ is the point $[-y_0(x_0^3 + 1729z_0^3) : x_0(y_0^3 + 1729z_0^3) : z_0(x_0^3 - y_0^3)]$. Note that the tangent line to $E$ at $P$ is the line*

$$\ell_P : x_0^2x + y_0^2y - 1729z_0^2z = 0,$$

*as we saw in Example 2.2.19, and the point*

$$R = [x_0(y_0^3 + 1729z_0^3) : -y_0(x_0^3 + 1729z_0^3) : z_0(x_0^3 - y_0^3)]$$

*certainly lies on this line and the curve $E$, so $R$ is the second point of intersection of $\ell_P$ and $E$ — in other words, $-R = 2[P]$. (Recall that we saw in Example 4.4.3 that the inverse of $[x_0 : y_0 : z_0]$ is the point $[y_0 : x_0 : z_0]$.) For instance,*

$$2([10 : 9 : 1]) = [-24561 : 24580 : 271].$$

**Example 5.2.8** *Take $E_1 = (C_1/\mathbb{Q} : x^3 + y^3 - 27z^3 = 0, [1 : -1 : 0])$, $E_2 = (C_2/\mathbb{Q} : 3u^2w - 3vw^2 + w^3 - 27u^3 = 0, [0 : 1 : 0])$ and $E_3 = (C_3/\mathbb{Q} : 108s^2t + t^3 - 108r^3 =$*

$0, [0:1:0])$ *to be the curves from Example 3.3.3 and* $\alpha : E_2 \longrightarrow E_1, \beta : E_2 \longrightarrow E_3$ *the maps from the same example, given by*

$$\begin{aligned} \alpha([u_0 : v_0 : w_0]) &= [v_0 : w_0 - v_0 : u_0] \\ \beta([u_0 : v_0 : w_0]) &= [6u_0 : 2v_0 - w_0 : 6w_0]. \end{aligned}$$

*Then* $\alpha$ *is an isomorphism with inverse* $\alpha^{-1} : E_1 \longrightarrow E_2$ *given by*

$$\alpha^{-1}([x_0 : y_0 : z_0]) = [z_0 : x_0 : x_0 + y_0].$$

*Consequently, the morphism* $\beta \circ \alpha^{-1} : E_1 \longrightarrow E_3$ *given by*

$$\beta \circ \alpha^{-1}([x_0 : y_0 : z_0]) = [6z_0 : x_0 - y_0 : 6(x_0 + y_0)],$$

*is an isogeny, since it maps* $[1 : -1 : 0]$ *to* $[0 : 1 : 0]$.

**Proposition 5.2.9** *Let* $(E, O_E)$ *be any elliptic curve defined over a finite field* $\mathbb{F}_q$*, such that* $O_E \in E(\mathbb{F}_q)$*. Then the* Frobenius map $\varphi : E \to E$ *given by* $\varphi([x_0 : y_0 : z_0]) = [x_0^q : y_0^q : z_0^q]$ *is an isogeny which fixes* $E(\mathbb{F}_q)$ *pointwise.*

**Proof.** $\varphi$ certainly is a morphism from $E$ to $E$, since $E(x^q, y^q, z^q) = E(x, y, z)^q$ (because $E$ is by assumption defined over $\mathbb{F}_q$). Let $[x_0 : y_0 : z_0] \in E(\mathbb{F}_q)$, so that we may assume without loss of generality that $x_0, y_0, z_0 \in \mathbb{F}_q$. Since the group of units $\mathbb{F}_q^\times$ of $\mathbb{F}_q$ has cardinality $q-1$, we know that the order of each element of $\mathbb{F}_q^\times$ divides $q-1$, whence $x_0^q = x_0, y_0^q = y_0, z_0^q = z_0$. The fact that $\varphi$ takes $O_E$ to $O_E$ follows from $O_E \in E(\mathbb{F}_q)$. □

Now if $\phi$ is a non-zero isogeny with corresponding function field $\bar{K}$-homomorphism $\phi^*$, then $\phi^*(\bar{K}(C_2))$ is a subfield of $\bar{K}(C_1)$, and $\bar{K}(C_1)/\phi^*(\bar{K}(C_2))$ is a finite extension by Proposition 3.1.3. This motivates the following definition.

**Definition 5.2.10** *Let $E_1, E_2$ be elliptic curves and let $\phi : E_1 \longrightarrow E_2$ be an isogeny. If $\phi$ is non-zero, we define the* degree *of $\phi$ to be the degree of the finite extension $\bar{K}(E_1)/\phi^*(\bar{K}(E_2))$ and denote it by* $\deg(\phi)$ *. By convention,* $\deg[0]$ *is set to be 0.*

**Theorem 5.2.11** *The degree of the Frobenius map is $q$.*

**Proof.** We need to show that $[\bar{\mathbb{F}}_q(E) : \varphi^*(\bar{\mathbb{F}}_q(E))] = q$. Denote as before by $\frac{X}{Z}$ the equivalence class of $\frac{x}{z}$ in $\bar{\mathbb{F}}_q(E)$ and by $\frac{Y}{Z}$ the equivalence class of $\frac{y}{z}$. Set $a = \frac{X}{Z}$ and $b = \frac{Y}{Z}$ and recall from Proposition 2.3.14 that $\bar{\mathbb{F}}_q(E) = \bar{\mathbb{F}}_q(a, b)$. Then $\varphi^*(a) = a^q$ and $\varphi^*(b) = b^q$, so $\varphi^*(\bar{\mathbb{F}}_q(E)) = \bar{\mathbb{F}}_q(a^q, b^q)$. Now $[\bar{\mathbb{F}}_q(a^q, b^q) : \bar{\mathbb{F}}_q(a^q)] = 2, [\bar{\mathbb{F}}_q(a) : \bar{\mathbb{F}}_q(a^q)] = q$ and $[\bar{\mathbb{F}}_q(a, b) : \bar{\mathbb{F}}_q(a)] = 2$. $\bar{\mathbb{F}}_q(a^q, b^q)$ is a subfield of $\bar{\mathbb{F}}_q(a, b)$, so applying the tower law for finite field extensions gives $[\bar{\mathbb{F}}_q(a, b) : \bar{\mathbb{F}}_q(a^q, b^q)] = q$, as required.□

**Proposition 5.2.12** *The degree of the multiplication-by-m map [m] is $m^2$.*

**Proof.** See [5, Lemma 7.2]. □

**Theorem 5.2.13** *Let $\alpha : E_1 \to E_2, \beta : E_2 \to E_3$ be isogenies (all three curves over the same field). Then* $\deg(\beta \circ \alpha) = \deg(\beta) \deg(\alpha)$.

**Proof.** By Definition 5.2.10, $\deg(\beta \circ \alpha) = [\bar{K}(E_1) : (\beta \circ \alpha)^*(\bar{K}(E_3))]$. Since $(\beta \circ \alpha)^* = \alpha^* \circ \beta^*$ (from Proposition 3.4.7), this means that $[\bar{K}(E_1) : (\beta \circ \alpha)^*(\bar{K}(E_3))] = [\bar{K}(E_1) : \alpha^*(\beta^*(\bar{K}(E_3)))]$. It only remains to apply the tower law for finite extensions:

$$[\bar{K}(E_1) : \alpha^*(\beta^*(\bar{K}(E_3)))] = [\bar{K}(E_1) : \bar{K}(E_2)][\bar{K}(E_2) : \alpha^*(\beta^*(\bar{K}(E_3)))].$$

The value of the first term in the product is $\deg(\alpha)$, since

$$[\bar{K}(E_1) : \bar{K}(E_2)] = [\bar{K}(E_1) : \alpha^*(\bar{K}(E_2))][\alpha^*(\bar{K}(E_2)) : \bar{K}(E_2)],$$

$[\bar{K}(E_1) : \alpha^*(\bar{K}(E_2))] = \deg(\alpha)$ and $[\alpha^*(\bar{K}(E_2)) : \bar{K}(E_2)] = 1$ (because $\alpha^*$ is injective). Similarly, the value of the second term is $\deg(\beta)$ because

$$[\bar{K}(E_2) : \alpha^*(\beta^*(\bar{K}(E_3)))] = [\bar{K}(E_2) : \beta^*(\bar{K}(E_3))][\beta^*(\bar{K}(E_3)) : \alpha^*(\beta^*(\bar{K}(E_3)))],$$

$[\bar{K}(E_2) : \beta^*(\bar{K}(E_3))] = \deg(\beta)$ and $[\beta^*(\bar{K}(E_3)) : \alpha^*(\beta^*(\bar{K}(E_3)))] = 1$ ($\beta^*$ is also an injection). Hence, $\deg(\beta \circ \alpha) = \deg(\alpha)\deg(\beta)$. □

We conclude this section with an important result on the number of points which are mapped to $O_E$ by an isogeny.

**Proposition 5.2.14** *Let $\phi : E_1 \longrightarrow E_2$ be an isogeny of elliptic curves. Then $|\phi^{-1}(Q)| = \phi_s$ for all $Q \in E_2$. In particular, $|ker(\phi)| = |\phi^{-1}(O_E)| = \phi_s$.*

**Proof.** We saw in Theorem 3.5.5 that for all but finitely many points $Q \in E_2$, $|\phi^{-1}(Q)| = \phi_s$. Fix $Q, Q' \in E_2$ and let $Q' = Q + R$. Since $\phi$ is a morphism, by Proposition 3.3.2 there exists $P' \in E_1$ such that $\phi(P') = R$. Then for each $P \in E_1$ with $\phi(P) = Q$, we have $\phi(P + P') = Q + R = Q'$, because $\phi$ is a group homomorphism by Theorem 5.2.4. This shows that $|\phi^{-1}(Q')| \geq |\phi^{-1}(Q)|$. Using the same argument, we can show that $|\phi^{-1}(Q')| \leq |\phi^{-1}(Q)|$. It follows that every point $Q \in E_2$ must have $\phi_s$ points in its inverse image. Setting $Q = O_E$ gives the result on $ker(\phi)$. □

**Lemma 5.2.15** *Let $E$ be an elliptic curve over a finite field $\mathbb{F}_q$ of characteristic $p$, and $\varphi$ the Frobenius map on $E$. Then the map $[m] + [n]\varphi$ is separable if and only if $p \nmid m$.*

**Proof.** See [24, Corollary III.5.5]. □

When $K = \mathbb{F}_q$ a finite field, the $\mathbb{F}_q$-rational points of an elliptic curve form a finite group by Theorem 4.4.8. The following theorem relates orders of these groups to isogeny.

**Theorem 5.2.16** *Let $E_1, E_2$ be elliptic curves over a finite field $\mathbb{F}_q$. Then there exists an $\mathbb{F}_q$-isogeny $\phi : E_1 \longrightarrow E_2$ if and only if $|E_1(\mathbb{F}_q)| = |E_2(\mathbb{F}_q)|$.*

**Proof.** If such an $\mathbb{F}_q$-isogeny $\phi : E_1 \longrightarrow E_2$ exists, and $\varphi_1$ is the Frobenius map on $E_1$ and $\varphi_2$ the Frobenius map on $E_2$, then $\phi \circ ([1] - \varphi_1) = ([1] - \varphi_2) \circ \phi$, since $\phi$ is defined over $\mathbb{F}_q$. Hence, from Theorem 5.2.13, $\deg([1]-\varphi_1) = \deg([1]-\varphi_2)$. Since both $[1]-\varphi_1$ and $[1] - \varphi_2$ are separable by Lemma 5.2.15, it follows from Proposition 5.2.14 that both curves have the same number of $\mathbb{F}_q$-rational points, because $|ker(\alpha)| = \deg(\alpha)$ for any separable map $\alpha$ (Proposition 5.2.14), and $E_1(\mathbb{F}_q) = ker([1] - \varphi_1), E_2(\mathbb{F}_q) = ker([1] - \varphi_2)$. For the proof of the converse, see [25]. □

## 5.3 The Dual Isogeny

It is natural to ask if the existence of an isogeny from an elliptic curve $E_1$ to another, $E_2$, gives any information about the existence (or lack thereof) of isogenies from $E_2$ to $E_1$. In fact, it does, as the next theorem indicates.

**Theorem 5.3.1** *If $\phi : E_1 \to E_2$ is a non-constant isogeny of degree $m$, then there exists a unique isogeny $\hat{\phi} : E_2 \to E_1$ such that $\hat{\phi} \circ \phi = [m]$ on $E_1$.*

**Proof.** See [24, Theorem III.6.1]. □

The proof of the existence is non-trivial — in fact, it is beyond the scope of this thesis.

**Definition 5.3.2** *Let $\phi : E_1 \to E_2$ be an isogeny. Then the isogeny $\hat{\phi}$ in Theorem 5.3.1 is called the* dual isogeny.

**Theorem 5.3.3 (Properties of the dual isogeny)** *Let $\phi : E_1 \to E_2, \beta : E_1 \to E_2, \psi : E_2 \to E_3$ be non-zero isogenies of elliptic curves $E_1, E_2, E_3$ over some field $K$. Then*

1. $\widehat{\psi \circ \phi} = \hat{\phi} \circ \hat{\psi}$,
2. $\widehat{\phi + \beta} = \hat{\phi} + \hat{\beta}$,
3. $\deg(\hat{\phi}) = \deg(\phi)$,
4. $\hat{\hat{\phi}} = \phi$.

**Proof.** For 1, we want to show that $(\hat{\phi} \circ \hat{\psi}) \circ (\psi \circ \phi) = [m][n]$, where $m = \deg(\phi)$ and $n = \deg(\psi)$. We have

$$\begin{aligned}(\hat{\phi} \circ \hat{\psi}) \circ (\psi \circ \phi) &= \hat{\phi} \circ [n] \circ \phi \\ &= [n] \circ \hat{\phi} \circ \phi \\ &= [n] \circ [m] \\ &= [mn],\end{aligned}$$

where the second equality follows from the fact that $\hat{\phi}$ is a group homomorphism. Given that the dual is unique, this proves 1. For the proof of 2, see [5, Appendix C]. Since $\deg(\hat{\phi} \circ \phi) = \deg([m]) = m^2$ by Proposition 5.2.12, we can deduce by Theorem

5.2.13 that $\deg(\hat{\phi}) = m$ as well. This proves 3. Finally, we need to show that $\hat{\hat{\phi}} = \phi$. Observe that

$$\begin{aligned}(\phi \circ \hat{\phi}) \circ \phi &= \phi \circ (\hat{\phi} \circ \phi) \\ &= \phi \circ [m] \\ &= [m] \circ \phi,\end{aligned}$$

where the third equality follows from the fact that $\phi$ is a group homomorphism. Therefore, $(\phi \circ \hat{\phi} - [m]) \circ \phi = [0]$, and by Theorem 5.2.13, we conclude that $(\phi \circ \hat{\phi} - [m]) = [0]$ or $\phi = [0]$. By assumption, $\phi \neq [0]$, so we must have $\phi \circ \hat{\phi} = [m] = [\deg(\hat{\phi})]$. But by definition, $\hat{\hat{\phi}}$ is the unique isogeny from $E_1$ to $E_2$ such that $\hat{\hat{\phi}} \circ \hat{\phi} = [\deg(\hat{\phi})] = [m]$. Hence, we conclude that $\hat{\hat{\phi}} = \phi$. □

**Corollary 5.3.4** *Let $m \in \mathbb{Z}, m \neq 0$. Then $\widehat{[m]} = [m]$.*

**Proof.** Since $[m] \circ [m] = [m^2] = [\deg([m])]$ by Proposition 5.2.12, we conclude from the uniqueness of $\widehat{[m]}$ that $\widehat{[m]} = [m]$. □

**Corollary 5.3.5** *Let $\phi : E_1 \longrightarrow E_2$ be an isogeny with dual isogeny $\hat{\phi}$, so $\hat{\phi} \circ \phi = [\deg(\phi)]$ on $E_1$. Then $\phi \circ \hat{\phi} = [\deg(\phi)]$ on $E_2$.*

**Proof.** This is immediate from the proof of property 4 of Theorem 5.3.3. □

**Example 5.3.6** *Recall the isogeny $\alpha : E_1 \rightarrow E_2$ introduced in Example 5.2.3 given by*

$$\alpha : [x_0 : y_0 : z_0] \rightarrow [6x_0 : r^{-3}y_0 : z_0],$$

*where*

$$E_1/\mathbb{F}_{13} : y^2z = x^3 + 7xz^2 + 3z^3,$$

$$E_2/\mathbb{F}_{13} : v^2w = u^3 + 5uw^2 + 11w^3.$$

*Then the dual isogeny $\hat{\alpha} : E_2 \longrightarrow E_1$ is given by*

$$\hat{\alpha}([x_0 : y_0 : z_0]) = [11x_0 : r^3y_0 : z_0].$$

*Composing the two isogenies $\alpha, \hat{\alpha}$ gives the identity map. This means that $\alpha$ is in fact an isomorphism, $\alpha^{-1} = \hat{\alpha}$, and deg$(\alpha) = 1$.*

**Proposition 5.3.7** *Let $\phi : E_1 \longrightarrow E_2$ be a non-constant isogeny. Then $\phi$ is an isomorphism if and only if* $\deg(\phi) = 1$, *in which case $\hat{\phi} = \phi^{-1}$.*

**Proof.** Let $\hat{\phi} \circ \phi = [m]$, with $m = \deg(\phi)$. Suppose $\phi$ is an isomorphism. Then $m = 1$. Since $\phi^{-1} \circ \phi = [1]$ on $E_1$, and $\hat{\phi} \circ \phi = [m] = [1]$ on $E_1$, we conclude by uniqueness of the dual isogeny that $\hat{\phi} = \phi^{-1}$. Conversely, if $\deg(\phi) = 1$, then $m = 1$, so $\hat{\phi} \circ \phi = [1]$ on $E_1$ and $\phi \circ \hat{\phi} = [1]$ on $E_2$ by Corollary 5.3.5. Thus, $\phi$ is an isomorphism with inverse $\phi^{-1} = \hat{\phi}$. □

## 5.4 Isogeny Classes

We saw in Chapter 3 that isomorphism induces an equivalence relation on the set of elliptic curves defined over some field $\bar{K}$. The same holds in fact for isogeny.

**Theorem 5.4.1** *Define the relation $\sim$ on the set of elliptic curves over $\bar{K}$ by $E_1 \sim E_2$ if there exists a non-constant isogeny (over $\bar{K}$) $\phi : E_1 \longrightarrow E_2$. Then $\sim$ is an equivalence relation on the set of elliptic curves over $\bar{K}$.*

**Proof.** Certainly, the reflexive property is satisfied because the identity map from an elliptic curve to itself is always a $\bar{K}$-isogeny. Transitivity also holds because the composition of $\bar{K}$-isogenies is again a $\bar{K}$-isogeny. Finally, if $E_1 \sim E_2$, then there exists a $\bar{K}$-isogeny $\phi : E_1 \longrightarrow E_2$. Hence, $E_2 \sim E_1$ via the dual isogeny $\hat{\phi}$ by Theorem 5.3.1 and we have symmetry. □

**Definition 5.4.2** *Let $E$ be an elliptic curve over $\bar{K}$. Then the* isogeny class of *$E$ is the set*

$$\{E'/\bar{K} \mid E \sim E'\}.$$

*If $E \sim E'$, then $E$ and $E'$ are said to be* isogenous. *If $E \sim E'$ via $\phi : E \longrightarrow E'$ and $\hat{\phi} : E' \longrightarrow E$, with $\phi, \hat{\phi}$ defined over a subfield $K$ of $\bar{K}$, then $E, E'$ are said to be* $K$-isogenous, *and the* $K$-isogeny class *of $E$ is the set of $E'$ over $\bar{K}$ which are $K$-isogenous to $E$.*

It is natural to ask which elliptic curves are isogenous to a given elliptic curve. In general, this is a difficult question.

In the case of finite fields, we know from Theorem 5.2.16 that it is sufficient to find some extension field (of the ground field) over which both curves have the same number of points. At the same time, this approach cannot establish when two curves are not isogenous over some extension field — this would entail checking every extension field, of which there are infinitely many.

Of course, in the event that the curves in question are isogenous, it remains to find an isogeny from one curve to the other, which can be difficult. If two curves are isogenous, other questions arise: how many isogenies are there from one curve to the other? Are there finitely many? And what degrees do these isogenies have? These questions are addressed in [1] and [20].

Isomorphism is also an equivalence relation. While an isogeny need not be an isomorphism, or vice versa, the two are closely related if we restrict ourselves to Weierstrass curves.

**Lemma 5.4.3** *Every isomorphism between elliptic curves in Weierstrass form is of the form* $[x_0 : y_0 : z_0] \longmapsto [u^2x_0{+}rz_0 : u^3y_0{+}u^2sx_0{+}tz_0 : z_0]$ *where* $u \in \bar{K}^*, r, s, t \in \bar{K}$.

**Proof.** See [24, Proposition III.3.1.(b)]. □

Clearly, then, any isomorphism of Weierstrass curves takes $[0 : 1 : 0]$ to $[0 : 1 : 0]$ and is thus an isogeny of degree 1. Now an isogeny is a group homomorphism by Theorem 5.2.4, which yields the following.

**Corollary 5.4.4** *Every isomorphism between elliptic curves in Weierstrass form is an isogeny and thus an isomorphism of the groups of points.*

The following diagram illustrates the relationship between isogeny and isomorphism of elliptic curves $E_1, E_2$ in Weierstrass form over a finite field $\mathbb{F}_q$:

$$\begin{tikzcd}
\mathbb{F}_q - isogenous \arrow[r, Leftrightarrow, "Thm.\, 5.2.16"] & |E_1(\mathbb{F}_q)| = |E_2(\mathbb{F}_q)| \\
\mathbb{F}_q - isomorphic \arrow[u, Rightarrow, "Cor.\, 5.4.4"'] \arrow[r, Rightarrow] \arrow[d, Rightarrow, "Cor.\, 5.4.4"] & E_1(\mathbb{F}_q) \cong E_2(\mathbb{F}_q) \arrow[u, Rightarrow] \\
isomorphic \arrow[d, Rightarrow, "Cor.\, 5.4.4"'] & \\
isogenous \arrow[r, Rightarrow, "Thm.\ 5.2.4"'] & group\ homomorphism\ E_1 \longrightarrow E_2
\end{tikzcd}$$

**Remark 5.4.5** *If the groups of $\mathbb{F}_q$-rational points of two elliptic curves are isomorphic, the curves need not be isomorphic over $\mathbb{F}_q$ or indeed isomorphic at all.*

**Example 5.4.6** *Consider the curves*

$$\begin{aligned} E_1/\mathbb{F}_{11} : y^2 z &= x^3 + xz^2 \\ E_2/\mathbb{F}_{11} : y^2 z &= x^3 + 2z^3. \end{aligned}$$

*Both curves have twelve points over $\mathbb{F}_{11}$, and it is easily verified that $E_1(\mathbb{F}_{11}) \cong E_2(\mathbb{F}_{11}) \cong \mathbb{Z}_{12}$. Yet $j(E_1) = 1 \neq j(E_2) = 0$, so $E_1$ and $E_2$ are not isomorphic as curves by Theorem 4.2.3.*

The example above also constitutes an example of two curves which are $\mathbb{F}_q$-isogenous (and therefore isogenous) but not isomorphic (and therefore not $\mathbb{F}_q$-isomorphic either). For an example of curves which are isomorphic, but not isomorphic over the ground field $\mathbb{F}_q$, see Example 5.2.3.

Now suppose that two elliptic curves in Weierstrass form over a finite field are isomorphic (and therefore isogenous). We would like to determine the smallest field over which the curves are isomorphic as well as the smallest field over which they are isogenous. Clearly, the latter is a subfield of the former. If it is a proper subfield, then the isogeny must have degree 2 or higher by Proposition 5.3.7.

Determining whether the curves are isogenous over some finite field is equivalent to counting the number of points over that field (Theorem 5.2.16), which can be difficult if the field is large. Finding the smallest field over which they are isomorphic is less time-consuming. Due to the explicit form of the isomorphism given in Lemma 5.4.3, it is quite easy to compute the minimal field over which the isomorphism is defined. To rule out an extension field for isomorphism, one can also check the group structure of the curves' groups of points over the extension field — this is more involved, however, especially if the finite field and thus the groups of points are large.

## 5.5 The Endomorphism Ring

In this final section, we briefly discuss the set of all isogenies from a curve $E$ to itself. In fact, these isogenies form a ring. For a more detailed analysis, see [24, III.9].

**Definition 5.5.1** *Let $E, E_1, E_2$ be elliptic curves with the latter two defined over the* *same field. Denote by $Isog(E_1, E_2)$ the set of isogenies from $E_1$ to $E_2$, by $End(E)$ the set of isogenies from $E$ to itself, $Isog_K(E_1, E_2)$ the set of $K$-isogenies from $E_1$ to $E_2$, and $End_K(E)$ the set of $K$-isogenies from $E$ to itself.*

**Theorem 5.5.2** *Let $E$ be any elliptic curve over some field $K$. $End(E)$ is a ring with identity and no zero divisors, therefore, $End(E)$ is a torsion-free $\mathbb{Z}$-module, with the addition law induced by addition on the curve and multiplication given by composition.*

**Proof.** The additive identity is the multiplication-by-0 map while the multiplicative identity is the multiplication-by-1 map. There are no zero divisors, for if $\phi, \psi$ are two non-zero isogenies then $deg(\phi \circ \psi) = deg(\phi) deg(\psi) \neq 0$. We omit the verification of the other properties — this is quite straightforward but tedious. □

**Proposition 5.5.3** *Let $E$ be any elliptic curve. Then all the multiplication-by-m maps are distinct, i.e. if $m, n \in \mathbb{Z}$ with $m \neq n$, then $[m] \neq [n]$.*

**Proof.** It suffices to show that $[m] = [n]$ if and only if $m = n$. One direction is trivial. Conversely, suppose that $[m] = [n]$. Then from Proposition 5.2.12, we know that $\deg([m]) = m^2 = \deg([n]) = n^2$. Hence, $n = \pm m$. If $m = 0$ then $n = 0$. Suppose that $m \neq 0$ and $n = -m$. Since $[-m] = -[m]$, this means that $[m] = -[m]$, or $[m] + [m] = [2m] = 0$. But then $\deg([2m]) = 4m^2 = 0$, contradicting the fact that $m \neq 0$. Hence, $m = n$, as required. □

**Corollary 5.5.4** *$\mathbb{Z}$ is a subring of $End(E)$ for all elliptic curves $E$.*

**Proof.** Consider the ring homomorphism $\mathbb{Z} \longrightarrow End(E)$ given by $m \mapsto [m]$. From Proposition 5.5.3, we know that this map is injective. Hence, the rational integers can be embedded into $End(E)$. □

**Definition 5.5.5** *If $\mathbb{Z}$ is a proper subring of $End(E)$, then $End(E)$ is said to have* complex multiplication.

**Example 5.5.6** *For $K = \mathbb{F}_q$ of characteristic $p$ with $q$ an odd power of $p$, and $E$ defined over $K$ with $O_E \in E(K)$, $End(E)$ admits complex multiplication via the Frobenius map $\varphi$. Clearly, $\varphi$ is not equal to $[0]$, nor can it be the multiplication-by-1 map because it is the identity only for $\mathbb{F}_q$-rational points. If $m \neq 0, 1$ and $m$ is coprime to $p$, consider that by Lemma 5.2.15, $[m]$ is separable, so $[m]$ has a non-trivial kernel (i.e. $\deg_s([m]) = m^2$ and $|ker([m])| = m^2 > 1$) by Proposition 5.2.14, whereas $|ker(\varphi)| = 1$, since $\varphi(P) = O_E$ if and only if $P = O_E$. If $p$ divides $m$, then we still cannot have $\varphi = [m]$, since $\deg(\varphi) = q \neq \deg([m]) = m^2$, as $q$ is an odd power of $p$ (therefore not a perfect square).*

We now investigate the possible structure of $End(E)$. There are in fact only three different types of endomorphism ring and we will discuss these shortly.

**Definition 5.5.7** *Let $R$ be a finitely generated $\mathbb{Q}$-algebra. An* order *in $R$ is a subring of $R$ which is finitely generated as a $\mathbb{Z}$-module and contains a $\mathbb{Q}$-basis of $R$.*

We will give two examples of an order in an algebra, but first, we give examples of two such algebras.

**Definition 5.5.8** *Let $D_0 \in \mathbb{Z}$ be squarefree. A* quadratic field *is an extension field of $\mathbb{Q}$ of the form*

$$\mathbb{Q}(\sqrt{D_0}) = \{r + s\sqrt{D_0} \mid r, s \in \mathbb{Q}\}.$$

*If $D_0 < 0$, we call $\mathbb{Q}(\sqrt{D_0})$ an* imaginary quadratic field, *otherwise a* real quadratic field.

**Definition 5.5.9** *Associated with a quadratic field $\mathbb{Q}(\sqrt{D_0})$ is the* fundamental discriminant *$\Delta_0$ given by*

$$\Delta_0 = \begin{cases} D_0 & \textit{if } D_0 \equiv 1 \textit{ mod } 4 \\ 4D_0 & \textit{otherwise.} \end{cases}$$

**Example 5.5.10** *Consider $D_0 = -1$. Then $\Delta_0 = -4$ and $\mathbb{Q}(\sqrt{D_0}) = \mathbb{Q}(i)$, where $i \in \mathbb{C}, i^2 = -1$.*

**Definition 5.5.11** *Let $\mathbb{Q}(\sqrt{D_0})$ be a quadratic field. The* ring of integers of $\mathbb{Q}(\sqrt{D_0})$, *written $\mathcal{O}_{\Delta_0}$, is the subring $\{\mu \in \mathbb{Q}(\sqrt{D_0}) \mid \exists f(x) = x^2 + ax + b \in \mathbb{Z}[x], f(\mu) = 0\}$ of $\mathbb{Q}(\sqrt{D_0})$. Elements of $\mathcal{O}_{\Delta_0}$ are called* algebraic integers.

**Theorem 5.5.12** *Let $\mathbb{Q}(\sqrt{D_0})$ be a quadratic field. The ring of integers of $\mathbb{Q}(\sqrt{D_0})$ takes the form $\mathcal{O}_{\Delta_0} = \mathbb{Z}[\omega_{\Delta_0}] = \{r + s\omega_{\Delta_0} | r, s \in \mathbb{Z}\}$, where*

$$\omega_{\Delta_0} = \begin{cases} \frac{1+\sqrt{D_0}}{2} & \textit{if } D_0 \equiv 1 \textit{ mod } 4 \\ \sqrt{D_0} & \textit{otherwise.} \end{cases}$$

**Proof.** If $\mu = a + b\sqrt{D_0} \in \mathbb{Q}(\sqrt{D_0})$ is an algebraic integer, then $\mu$ is a root of the monic quadratic polynomial

$$(x - (a + b\sqrt{D_0}))(x - (a - b\sqrt{D_0})) = x^2 - 2ax + a^2 - b^2 D_0 \in \mathbb{Q}[x].$$

This polynomial resides in $\mathbb{Z}[x]$ if and only if $a$ is of the form $\frac{n}{2}, n \in \mathbb{Z}$, and $a^2 - b^2 D_0$ is an integer. In the case $D_0 \equiv 1 \bmod 4$, $a^2 - b^2 D_0$ is equal to

$$\frac{n^2}{4} - b^2 D_0 = \frac{n^2 - 4b^2 D_0}{4}.$$

This is an integer if and only if $n^2 - 4b^2 D_0 \equiv 0 \pmod 4$. Since $n \in \mathbb{Z}$, $4b^2 D_0$ must also be an integer, i.e. $b$ must be of the form $\frac{m}{2}$, $m \in \mathbb{Z}$. Then $\mu = \frac{n-m}{2} + m\frac{1+\sqrt{D_0}}{2}$ with $\frac{n^2-m^2 D_0}{4} \in \mathbb{Z}$. This proves that $m, n$ must have the same parity, so $\frac{n-m}{2} \in \mathbb{Z}$. Therefore, $\mathcal{O}_{\Delta_0} \subseteq \mathbb{Z}[\frac{1+\sqrt{D_0}}{2}]$. In addition, it is easily seen that $\mathbb{Z}[\frac{1+\sqrt{D_0}}{2}] \subseteq \mathcal{O}_{\Delta_0}$, so we have $\mathbb{Z}[\frac{1+\sqrt{D_0}}{2}] = \mathcal{O}_{\Delta_0}$. The case $D_0 \equiv 2, 3 \bmod 4$ can be proven in similar fashion.

□

**Example 5.5.13** *If $D_0 = -3$ then $\Delta_0 = D_0$, $\omega_{\Delta_0} = \frac{1+i\sqrt{3}}{2}$, and*

$$\begin{aligned} \mathcal{O}_{\Delta_0} &= \mathbb{Z}\left[\frac{1+i\sqrt{3}}{2}\right] \\ &= \mathbb{Z}[e^{\frac{i\pi}{3}}]. \end{aligned}$$

**Lemma 5.5.14** *Let $\mathbb{Q}(\sqrt{D_0})$ be an imaginary quadratic field with fundamental discriminant $\Delta_0$. The orders in $\mathbb{Q}(\sqrt{D_0})$ are exactly the subrings of the form $\mathbb{Z}[n\omega_{\Delta_0}]$, where $n \in \mathbb{Z}$.*

**Proof.** See [23, Proposition 4.11]. □

A quadratic field is an example of a $\mathbb{Q}$-algebra. In this case, an order in a field $\mathbb{Q}(\sqrt{D_0})$ is a subring of $\mathbb{Q}(\sqrt{D_0})$ which is a $\mathbb{Z}$-module of rank 2, for which the smallest field containing it and $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{D_0})$.

**Example 5.5.15** *Consider again the imaginary quadratic field* $\mathbb{Q}(\sqrt{-3})$ *from the previous example. Here,* $\omega_{\Delta_0} = \frac{1+i\sqrt{3}}{2}$. *The subring* $\mathbb{Z}[2\omega_{\Delta_0}] = \mathbb{Z}[1+i\sqrt{3}]$ *is an order in* $\mathbb{Q}(\sqrt{-3})$. *It has rank 2 as a* $\mathbb{Z}$*-module and it contains* $\sqrt{-3}$*, so the smallest field containing* $\mathbb{Q}$ *and this ring is* $\mathbb{Q}(\sqrt{-3})$. *Alternatively, we see that* $\mathbb{Z}[2\omega_{\Delta}]$ *is of the form given in Lemma 5.5.14.*

**Definition 5.5.16** *A* quaternion algebra *is a (non-commutative) ring of the form* $\mathbb{Q}[i,j] = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}ij$*, where* $i^2 = j^2 = -1$*,* $ij = -ji$*, and* $i, j$ *commute with the elements of* $\mathbb{Q}$.

An order in a quaternion algebra is analogous to an order in a quadratic field. If $R$ is a quaternion algebra, an order in $R$ is a subring of $R$ which has rank at most 4 as a $\mathbb{Z}$-module and contains a $\mathbb{Q}$-basis of $R$.

**Example 5.5.17** *The subring* $\mathbb{Z}[i+j, i-j]$ *is an order in* $\mathbb{Q}[i,j]$*, because it has rank 4 and contains* $2i, 2j$ *and* $2ji$*, which form a* $\mathbb{Q}$*-basis for* $\mathbb{Q}[i,j]$.

**Theorem 5.5.18** *Let* $E$ *be an elliptic curve over some field. End(*$E$*) is isomorphic to one of the following:* $\mathbb{Z}$*; an order in an imaginary quadratic field; or an order in a quaternion algebra.*

**Proof.** See [24, Corollary III.9.4]. □

**Example 5.5.19** *Consider the elliptic curve* $E/\mathbb{Q} : x^3 + y^3 = 1729z^3$ *with basepoint* $[1 : -1 : 0]$.

*The isogeny $\phi : E \longrightarrow E$ given by $\phi([x_0 : y_0 : z_0]) = [\xi x_0 : \xi y_0 : z_0]$, where $\xi$ is a root of $x^2+x+1$, is a cube root of unity in End(E) (i.e. $\phi^3 = [1]$). End(E) is of the form*

$$End(E) = \{[a] + [b] \circ \phi \mid a, b \in \mathbb{Z}\},$$

*so*

$$End(E) \cong \mathbb{Z}\left[\frac{-1+i\sqrt{3}}{2}\right],$$

*with the ring isomorphism given by*

$$[a] + [b] \circ \phi \longrightarrow a + b\frac{-1+\sqrt{3}i}{2}.$$

**Remark 5.5.20** *Note the importance of the definition that an isogeny maps $O_E$ to $O_E$. For the previous example, consider the map $\varphi$ defined by $\varphi([x_0 : y_0 : z_0]) = [\xi x_0 : \xi^2 y_0 : z_0]$. $\varphi$ is also a morphism which is a cube root of unity but it is not an isogeny because it does not map $[1 : -1 : 0]$ to $[1 : -1 : 0]$ but rather to $[\xi : -\xi^2 : 0] = [1 : -\xi : 0]$.*

# Chapter 6

# Isomorphism and Isogeny for Small Non-zero Characteristic

In this chapter, we explore isomorphism and isogeny of elliptic curves in Weierstrass form over certain finite fields. Specifically, each of our examples covers one of the three cases for the form of the Weierstrass equation ($\mathrm{char}(K) = 2$, $\mathrm{char}(K) = 3$ and $\mathrm{char}(K) \neq 2, 3$) given in Definition 4.1.1 and Lemmata 4.1.4 and 4.1.6. In the opening section, we classify the isogeny and isomorphism classes of all non-singular Weierstrass curves over $\mathbb{F}_2$. In the other two sections, we examine the non-singular Weierstrass curve $E_0$: $y^2z = x^3 + xz^2$ over the finite field $\mathbb{F}_q$, for $q = 3$ and $q = 11$. More accurately, we look at those Weierstrass curves which are defined over $\mathbb{F}_q$ and which reside in the $\bar{\mathbb{F}}_q$-isomorphism class of $E_0$, searching for isogenies and isomorphisms of curves in this class. In the process, we apply much of the theory from earlier chapters in classifying the aforementioned isomorphism class.

## 6.1 The case $K = \mathbb{F}_2$

Over $\mathbb{F}_2$, there are 32 Weierstrass curves. Of these, half are singular and half non-singular, with 8 of the latter curves having $j$-invariant 0 and the other half having $j$-invariant 1. The curves with $j$-invariant 0 are:

$$\begin{aligned}
E_0: &\ y^2z + yz^2 &&= x^3, \\
E_1: &\ y^2z + yz^2 &&= x^3 + z^3, \\
E_2: &\ y^2z + yz^2 &&= x^3 + xz^2, \\
E_3: &\ y^2z + yz^2 &&= x^3 + xz^2 + z^3, \\
E_4: &\ y^2z + yz^2 &&= x^3 + x^2z, \\
E_5: &\ y^2z + yz^2 &&= x^3 + x^2z + z^3, \\
E_6: &\ y^2z + yz^2 &&= x^3 + x^2z + xz^2, \\
E_7: &\ y^2z + yz^2 &&= x^3 + x^2z + xz^2 + z^3.
\end{aligned}$$

Using the form of an isomorphism of Weierstrass curves given in Lemma 5.4.3, we can easily compute the (smallest) field over which any two of these curves with the same $j$-invariant are isomorphic. For instance, an isomorphism from $E_0$ to $E_1$, being of the form $[u^2x_0 + rz_0 : u^3y_0 + u^2sx_0 + tz_0 : z_0]$, requires substituting $[u^2x_0 + rz_0 : u^3y_0 + u^2sx_0 + tz_0 : z_0]$ for $(x, y, z)$ in the equation of $E_1$ which gives

$$u^6y_0^2z_0 + u^3y_0z_0^2 + u^6x_0^3 + (u^4s^2 + u^4r)x_0^2z_0 + (u^2s + u^2r^2)x_0z_0^2 + (r^3 + t^2 + t + 1)z_0^3 = 0.$$

This is true for all $[x_0 : y_0 : z_0] \in E_0$ only if the equation above is a multiple of $E_0(x_0, y_0, z_0) = y_0^2z_0 + y_0z_0^2 + x_0^3$ which, when comparing coefficients and dividing out by $u^6$, gives the system of four equations

$$\begin{aligned} r^3+t^2+t+1 &= 0 \\ u^{-4}s^2+u^{-4}r &= 0 \\ u^{-2}s+u^{-2}r^2 &= 0 \\ u^3 &= 1, \end{aligned}$$

which over $\mathbb{F}_2$ has a unique solution $r=s=t=u=1$. Using this technique, we find that the $\mathbb{F}_2$-isomorphism classes are as follows:

$$\{E_0, E_1, E_6, E_7\}$$

$$\{E_2, E_4\}$$

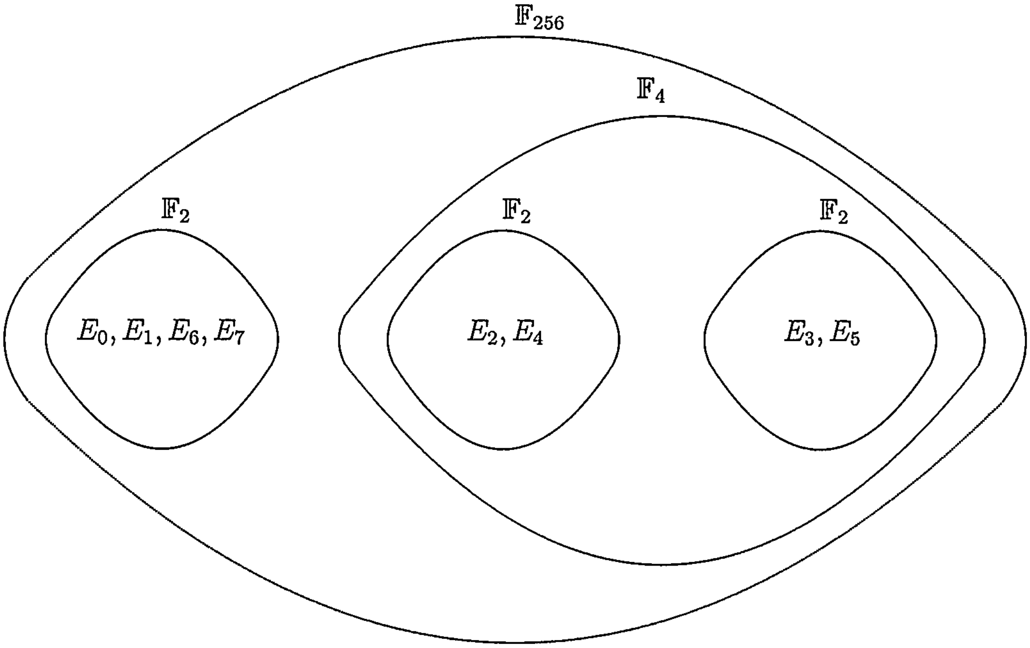
$$\{E_3, E_5\}.$$

Passing to $\mathbb{F}_4$, the isomorphism-classes of $E_2$ and $E_3$ merge into one. For an isomorphism between these two curves, the corresponding system of equations is

$$\begin{aligned} r^3+r+t^2+t+1 &= 0 \\ u^4s^2+u^4r &= 0 \\ r^2+s+1 &= u^4 \\ u^3 &= 1, \end{aligned}$$

which has the solution $r=s=0, u=1, t \in \mathbb{F}_4$ a root of $x^2+x+1$. (Another solution is $r=s=u=1, t^2+t+1=0$.) It is not until we reach $\mathbb{F}_{256}$, however, that all 8 curves reside in the same isomorphism class. The same line of reasoning as above yields the isomorphism from $E_0$ to $E_3$ given by $[x_0+s^2z_0 : y_0+sx_0+tz_0 : z_0]$, $s \in \mathbb{F}_{16}$ a root of $x^4+x+1$ and $t \in \mathbb{F}_{256}$ a root of the irreducible quadratic $x^2+x+s^3+1 \in \mathbb{F}_{16}[x]$.

Figure 6.1: Isomorphism (and isogeny) classes of Weierstrass curves over $\mathbb{F}_2$ with $j$-invariant 0



The question is then whether there exists any smaller field over which the four curves $E_0 - E_3$ have the same number of points as one of the other four curves. If this is the case, then there must be an isogeny of second degree or higher between the curves in question (since they could not be isomorphic over this field).

This problem aptly demonstrates the power of the Hasse bound given in Theorem 4.4.9. For rather than calculate the number of points of each $\mathbb{F}_2$-isogeny class of curve over each extension field from $\mathbb{F}_8$ up to $\mathbb{F}_{128}$, we can in some cases avoid such a computation. To see this, note that $|E_0(\mathbb{F}_4)| = 9$ and $|E_2(\mathbb{F}_4)| = |E_3(\mathbb{F}_4)| = 5$. Now $E_i(\mathbb{F}_4)$ is a subgroup of $E_i(\mathbb{F}_{16})$ for all $i$. So if, for instance, $E_0$ and $E_2$ are to have the same number of points over $\mathbb{F}_{16}$, it follows that they must both have a multiple of lcm(5,9)=45 points over $\mathbb{F}_{16}$. But the Hasse bound limits the number of points to the interval [9,25]. Using the same argument, one finds that $E_0$ does not have the same number of points over $\mathbb{F}_{64}$ as either of the other curves $E_1$ and $E_3$. One can count points over $\mathbb{F}_8$, $\mathbb{F}_{32}$ and $\mathbb{F}_{128}$ to verify that $E_0$ is not isogenous to the other curves over these fields either. Therefore, the $K$-isogeny classes are the same as the $K$-isomorphism classes for all $K \subseteq \mathbb{F}_{256}$.

The Weierstrass curves over $\mathbb{F}_2$ with $j$-invariant 1 are as follows:

$$\begin{aligned}
E_8 :&\quad y^2z + xyz &&= x^3 + z^3,\\
E_9 :&\quad y^2z + xyz &&= x^3 + xz^2,\\
E_{10} :&\quad y^2z + xyz &&= x^3 + x^2z + z^3,\\
E_{11} :&\quad y^2z + xyz &&= x^3 + x^2z + xz^2,\\
E_{12} :&\quad y^2z + xyz + yz^2 &&= x^3 + z^3,\\
E_{13} :&\quad y^2z + xyz + yz^2 &&= x^3 + xz^2 + z^3,\\
E_{14} :&\quad y^2z + xyz + yz^2 &&= x^3 + x^2z,\\
E_{15} :&\quad y^2z + xyz + yz^2 &&= x^3 + x^2z + xz^2.
\end{aligned}$$

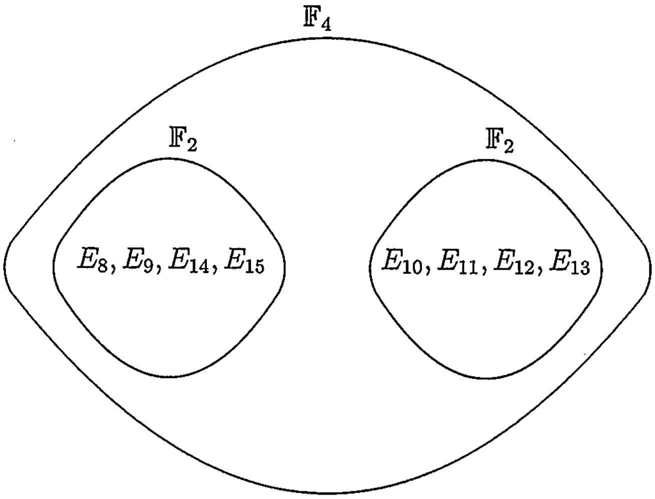
There are two $\mathbb{F}_2$-isomorphism classes here, namely:

$$\{E_8, E_9, E_{14}, E_{15}\}$$

$$\{E_{10}, E_{11}, E_{12}, E_{13}\}.$$

Over $\mathbb{F}_4$, all the curves are isomorphic, and the $\mathbb{F}_2$-isogeny classes are the same as the $\mathbb{F}_2$-isomorphism classes.

Figure 6.2: Isomorphism (and isogeny) classes of Weierstrass curves over $\mathbb{F}_2$ with $j$-invariant 1



## 6.2 The case $K = \mathbb{F}_3$

Moving on to characteristic 3, we find that the form of the isomorphism simplifies. To be more specific, since $E(x,y,z)$ does not contain an $xyz$ or $yz^2$ term, each isomorphism takes the form $[u^2x_0 + rz_0 : u^3y_0 : z_0]$, with $u \in \bar{K}^*$ and $r \in \bar{K}$. We will also discover that there are some curves which are isogenous over $\mathbb{F}_{3^n}$ for some $n \in \mathbb{N}$, but isomorphic only over a larger field. In other words, there is some higher degree (deg $\geq 2$) isogeny over the smaller field.

Consider first all elliptic curves defined over $\mathbb{F}_3$ which are isomorphic to

$$E_0 : y^2z = x^3 + xz^2.$$

Note that $j(E_0) = 0$. They are

$$\begin{aligned}
E_1 : \quad y^2z &= x^3 + xz^2 + z^3, \\
E_2 : \quad y^2z &= x^3 + xz^2 + 2z^3, \\
E_3 : \quad y^2z &= x^3 + 2xz^2, \\
E_4 : \quad y^2z &= x^3 + 2xz^2 + z^3, \\
E_5 : \quad y^2z &= x^3 + 2xz^2 + 2z^3.
\end{aligned}$$

Calculating the values of $u, r$ as before, we find that the $\mathbb{F}_3$-isomorphism classes are

$$\{E_0, E_1, E_2\}$$

$$\{E_3\}$$

$$\{E_4\}$$

$$\{E_5\}.$$

If we pass to the next field $\mathbb{F}_9$, we find that the system of equations for the isomorphism between $E_0$ and $E_3$ is

$$\begin{aligned} u^4 &= 2 \\ r^3 + r &= 0, \end{aligned}$$

for which $r = 0, u = \rho + 2$, $\rho$ a root of the irreducible equation $x^2 + 1 = 0$, is a solution. Hence, the isomorphism (over $\mathbb{F}_9$) is $[\rho x_0 : (2\rho+2)y_0 : z_0]$. In fact, the four $\mathbb{F}_3$-isomorphism classes combine into 2 over $\mathbb{F}_9$. They are:

$$\{E_0, E_1, E_2, E_3\}$$

$$\{E_4, E_5\}.$$

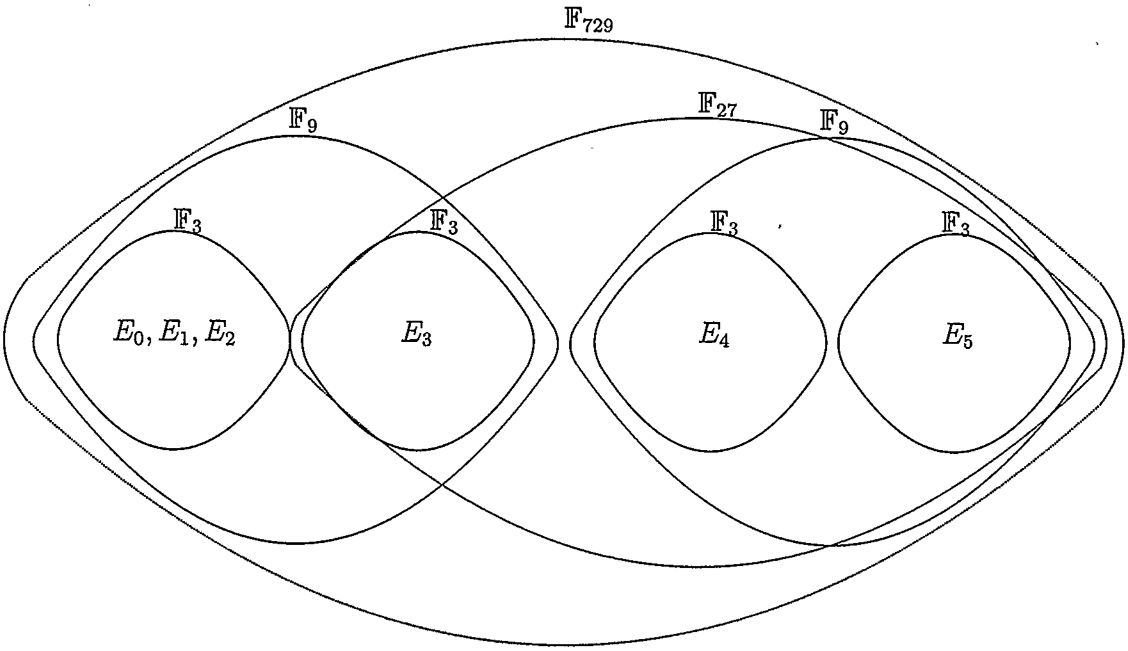
The $\mathbb{F}_{27}$-isomorphism classes are:

$$\{E_0, E_1, E_2\}$$

$$\{E_3, E_4, E_5\}.$$

At this point, we stop. We could continue with the isomorphism classes over $\mathbb{F}_{81}, \mathbb{F}_{243}$, etc. but this is not necessary. It turns out that the lowest field over which all six curves are isomorphic is $\mathbb{F}_{3^6} = \mathbb{F}_{729}$. We mention this fact because it will be important later on to compare the lowest field of isomorphism of two curves with the lowest field of isogeny thereof, which we do shortly. The isomorphism classes are pictorially represented in Figure 6.3.

Figure 6.3: Isomorphism classes of Weierstrass curves over $\mathbb{F}_3$ with $j$-invariant 0



Counting points over $\mathbb{F}_3$, we find that curves $E_0$ through $E_3$ have 4 points each, so they are all $\mathbb{F}_3$-isogenous by Theorem 5.2.16. This is the first case where two curves ($E_0$ and $E_3$) are isogenous over a proper subfield (namely $\mathbb{F}_3$) of the smallest field over which they are isomorphic (namely $\mathbb{F}_9$). We could also have deduced this from the fact that $E_0(\mathbb{F}_3)$ and $E_3(\mathbb{F}_3)$ are not isomorphic as groups. The curves $E_4$ and $E_5$ have 7 points and 1 point over $\mathbb{F}_3$, respectively, so they are not $\mathbb{F}_3$-isogenous to one another or to any of $E_0 - E_3$.

One isogeny from $E_0$ to $E_3$ is $[z_0y_0^2 : y_0(z_0^2 + 2x_0^2) : x_0^2z_0]$. (This is just the rational map $\Gamma^{\#}$ from Example 3.2.3, with $E_0 = (C_1, [0:1:0]), E_3 = (C_2, [0:1:0])$, and $K = \mathbb{F}_3$.) This map of curves is clearly regular at all points except possibly $[0:1:0]$ and $[0:0:1]$. In fact, we showed in Example 3.1.6 that the map is regular at $[0:1:0]$, since $[x_0y_0^2 : 2x_0y_0z_0 + 2y_0^3 : x_0^3]$ is regular at $[0:1:0]$.

We have yet to establish that the map is regular at $[0:0:1]$. Although we know from Lemma 3.3.4, since $E_0$ is smooth, that the map must be regular at $[0:0:1]$, we will explicitly show that this map is regular at $[0:0:1]$.

So how does one find an alternate 'representative' of the rational map, which demonstrates regularity at this point? There is no obvious method. However, noting that the partial map given above is given by third degree homogeneous polynomials defined over $\mathbb{F}_3$, one might ascertain that the missing representative is also of this form. Given that there are only finitely many possibilities for such a triple of homogeneous polynomials, one may determine by exhaustive search whether the solution (*if* it exists) is of this form. Omitting the tedious labour required of finding this representative, we observe that the map $[x_0^2 y_0 + y_0 z_0^2 : z_0^3 + z_0 x_0^2 + 2x_0 y_0^2 : x_0 y_0 z_0]$ is a map from $E_0$ to $E_3$ which is defined at $[0 : 0 : 1]$ (and maps this point to $[0 : 1 : 0]$).

As for the other curves, $E_4$ and $E_5$ each have 7 points over $\mathbb{F}_9$, so they are $\mathbb{F}_9$-isogenous.

Passing to $\mathbb{F}_{27}$ completes the picture: here, all six curves are isogenous (they have 28 points each). Once again, $E_0$ is $\mathbb{F}_{27}$-isogenous to $E_4$ and $E_5$ while not being isomorphic to either of them in any proper subfield of $\mathbb{F}_{27}$. An isogeny in this case is not so difficult to find: We compose the second degree isogeny from $E_0$ to $E_3$ with the $\mathbb{F}_{27}$-isomorphism from $E_3$ to $E_4$ to get a second degree isogeny from $E_0$ to $E_4$. We could also construct the sixth degree isogeny $[z_0^3 y_0^6 + \sigma x_0^6 z_0^3 : y_0^3(z_0^6 + 2x_0^6) : z_0^9]$, where $\sigma \in \mathbb{F}_{27}$ is a root of the irreducible polynomial $x^3 + x + 1 \in \mathbb{F}_3[x]$. This isogeny is obtained by composing the second degree isogeny from $E_0$ to $E_3$ with the third degree Frobenius map from $E_3$ to itself with the isomorphism (over $\mathbb{F}_{27}$) from $E_3$ to $E_4$. (In fact, we can construct isogenies of arbitrarily large degree by repeatedly composing any isogeny with the Frobenius map.)

Figure 6.4: Isogeny classes of Weierstrass curves over $\mathbb{F}_3$ with $j$-invariant 0

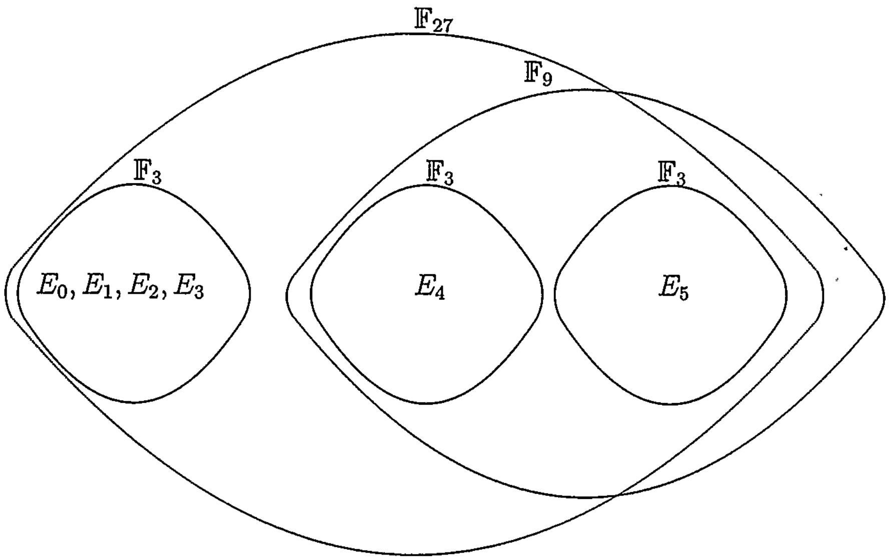


Table 6.1 lists isomorphisms from $E_i$ to $E_j$ $(0 \leq i, j \leq 5)$ over various extension fields of $\mathbb{F}_3$, where $\rho^2+1=0, \sigma^3+\sigma+1=0$. Subsequent tables give the isomorphisms in various isomorphism subclasses, where the isomorphisms go from $E_i$ in the left-hand column to $E_j$ in the top row.

Table 6.1: Various Isomorphisms

| | |
|---|---|
| $\alpha_1$ | $[x_0+z_0 : y_0 : z_0]$ |
| $\alpha_2$ | $[x_0+2z_0 : y_0 : z_0]$ |
| $\alpha_3$ | $[2\rho x_0 : (\rho+2)y_0 : z_0]$ |
| $\alpha_4$ | $[2\rho x_0+z_0 : (\rho+2)y_0 : z_0]$ |
| $\alpha_5$ | $[\rho x_0 : (2\rho+2)y_0 : z_0]$ |
| $\alpha_6$ | $[\rho x_0+2\rho z_0 : (\rho+1)y_0 : z_0]$ |
| $\alpha_7$ | $[\rho x_0+\rho z_0 : (\rho+1)y_0 : z_0]$ |
| $\alpha_8$ | $[2\rho x_0+2z_0 : (\rho+2)y_0 : z_0]$ |
| $\alpha_9$ | $[2x_0 : 2\rho y_0 : z_0]$ |
| $\alpha_{10}$ | $[2x_0 : \rho y_0 : z_0]$ |
| $\alpha_{11}$ | $[x_0+\sigma z_0 : y_0 : z_0]$ |
| $\alpha_{12}$ | $[x_0+2\sigma z_0 : y_0 : z_0]$ |
| $\alpha_{13}$ | $[2\rho x_0+\rho\sigma z_0 : (2\rho+1)y_0 : z_0]$ |
| $\alpha_{14}$ | $[2\rho x_0+(\rho\sigma+1)z_0 : (2\rho+1)y_0 : z_0]$ |
| $\alpha_{15}$ | $[2\rho x_0+2\rho\sigma z_0 : (2\rho+1)y_0 : z_0]$ |
| $\alpha_{16}$ | $[2\rho x_0+(2\rho\sigma+1)z_0 : (2\rho+1)y_0 : z_0]$ |
| $\alpha_{17}$ | $[2\rho x_0+(\rho\sigma+2)z_0 : (2\rho+1)y_0 : z_0]$ |
| $\alpha_{18}$ | $[2\rho x_0+(2\rho\sigma+2)z_0 : (2\rho+1)y_0 : z_0]$ |
| $\alpha_{19}$ | $[\rho x_0+\sigma z_0 : (2\rho+2)y_0 : z_0]$ |
| $\alpha_{20}$ | $[\rho x_0+2\sigma z_0 : (2\rho+2)y_0 : z_0]$ |
| $\alpha_{21}$ | $[\rho x_0+(2\rho+\sigma)z_0 : (2\rho+2)y_0 : z_0]$ |
| $\alpha_{22}$ | $[\rho x_0+(2\rho+2\sigma)z_0 : (2\rho+2)y_0 : z_0]$ |
| $\alpha_{23}$ | $[\rho x_0+(\rho+\sigma)z_0 : (2\rho+2)y_0 : z_0]$ |
| $\alpha_{24}$ | $[\rho x_0+(\rho+2\sigma)z_0 : (2\rho+2)y_0 : z_0]$ |

Table 6.2: Isomorphisms in the $\mathbb{F}_3$-class of $E_0$

| | $\mathbf{E}_0$ | $\mathbf{E}_1$ | $\mathbf{E}_2$ |
|---|---|---|---|
| $\mathbf{E}_0$ | Id | $\alpha_1$ | $\alpha_2$ |
| $\mathbf{E}_1$ | $\alpha_2$ | Id | $\alpha_1$ |
| $\mathbf{E}_2$ | $\alpha_1$ | $\alpha_2$ | Id |

Table 6.3: Isomorphisms in the $\mathbb{F}_9$-class of $E_0$

| | $\mathbf{E}_0$ | $\mathbf{E}_1$ | $\mathbf{E}_2$ | $\mathbf{E}_3$ |
|---|---|---|---|---|
| $\mathbf{E}_0$ | Id | $\alpha_1$ | $\alpha_2$ | $\alpha_5$ |
| $\mathbf{E}_1$ | $\alpha_2$ | Id | $\alpha_1$ | $\alpha_6$ |
| $\mathbf{E}_2$ | $\alpha_1$ | $\alpha_2$ | Id | $\alpha_7$ |
| $\mathbf{E}_3$ | $\alpha_3$ | $\alpha_4$ | $\alpha_8$ | Id |

Table 6.4: Isomorphisms in the $\mathbb{F}_9$-class of $E_4$

| | $\mathbf{E}_4$ | $\mathbf{E}_5$ |
|---|---|---|
| $\mathbf{E}_4$ | Id | $\alpha_9$ |
| $\mathbf{E}_5$ | $\alpha_{10}$ | Id |

Table 6.5: Isomorphisms in the $\mathbb{F}_{27}$-class of $E_0$

| | $\mathbf{E}_0$ | $\mathbf{E}_1$ | $\mathbf{E}_2$ |
|---|---|---|---|
| $\mathbf{E}_0$ | Id | $\alpha_1$ | $\alpha_2$ |
| $\mathbf{E}_1$ | $\alpha_2$ | Id | $\alpha_1$ |
| $\mathbf{E}_2$ | $\alpha_1$ | $\alpha_2$ | Id |

Table 6.6: Isomorphisms in the $\mathbb{F}_{27}$-class of $E_3$

| | $\mathbf{E}_3$ | $\mathbf{E}_4$ | $\mathbf{E}_5$ |
|---|---|---|---|
| $\mathbf{E}_3$ | Id | $\alpha_{11}$ | $\alpha_{12}$ |
| $\mathbf{E}_4$ | $\alpha_{12}$ | Id | $\alpha_{11}$ |
| $\mathbf{E}_5$ | $\alpha_{11}$ | $\alpha_{12}$ | Id |

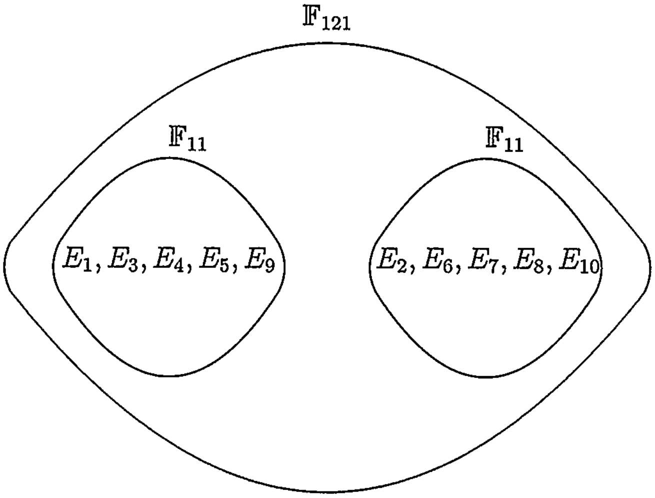
Table 6.7: Isomorphisms in the $\mathbb{F}_{729}$-class of $E_0$

| | $\mathbf{E}_0$ | $\mathbf{E}_1$ | $\mathbf{E}_2$ | $\mathbf{E}_3$ | $\mathbf{E}_4$ | $\mathbf{E}_5$ |
|---|---|---|---|---|---|---|
| $\mathbf{E}_0$ | Id | $\alpha_1$ | $\alpha_2$ | $\alpha_5$ | $\alpha_{19}$ | $\alpha_{20}$ |
| $\mathbf{E}_1$ | $\alpha_2$ | Id | $\alpha_1$ | $\alpha_6$ | $\alpha_{21}$ | $\alpha_{22}$ |
| $\mathbf{E}_2$ | $\alpha_1$ | $\alpha_2$ | Id | $\alpha_7$ | $\alpha_{23}$ | $\alpha_{24}$ |
| $\mathbf{E}_3$ | $\alpha_3$ | $\alpha_4$ | $\alpha_8$ | Id | $\alpha_{11}$ | $\alpha_{12}$ |
| $\mathbf{E}_4$ | $\alpha_{13}$ | $\alpha_{14}$ | $\alpha_{17}$ | $\alpha_{12}$ | Id | $\alpha_{11}$ |
| $\mathbf{E}_5$ | $\alpha_{15}$ | $\alpha_{16}$ | $\alpha_{18}$ | $\alpha_{11}$ | $\alpha_{12}$ | Id |

## 6.3 The case $K = \mathbb{F}_{11}$

Finally, we consider the same curve, $E_0 : y^2z = x^3 + xz^2$, this time over the field $\mathbb{F}_{11}$; in this case, $j(E_0) = 1$. The only curves over $\mathbb{F}_{11}$ with $j$-invariant 1 are those of the form $E_a : y^2z = x^3 + axz^2$, where $a \in \mathbb{F}_{11}^*$. All curves of this form have 12 $\mathbb{F}_{11}$-rational points, so they all reside in the same $\mathbb{F}_{11}$-isogeny class. A quick check shows that those curves of the form $E_r : y^2z = x^3 + rxz^2$, $r$ a quadratic residue modulo 11, have one point of order 2; those of the form $E_n : y^2z = x^3 + nxz^2$, $n$ a quadratic non-residue modulo 11, have three such points. It follows from Theorem 4.4.10 that $E_r(\mathbb{F}_{11}) \cong \mathbb{Z}_{12}$ and $E_n(\mathbb{F}_{11}) \cong \mathbb{Z}_2 \times \mathbb{Z}_6$, so that the $\mathbb{F}_{11}$-isogeny class of $E_0 = E_1$ (i.e. $a = 1$) contains two $\mathbb{F}_{11}$-isomorphism classes.

Figure 6.5: Isomorphism classes of Weierstrass curves over $\mathbb{F}_{11}$ with $j$-invariant 1



We would therefore like to find $\mathbb{F}_{11}$-isogenies to link the two isomorphism classes. We can do this in the following way. Consider $E_a$ and $E_{7a}$ (which lie in different $\mathbb{F}_{11}$-isomorphism classes since 7 is a quadratic non-residue modulo 11). Then the map $\phi : E_a \longrightarrow E_{7a}$ given by

$$\phi([x_0 : y_0 : z_0]) = [y_0^2 z_0 : y_0(10x_0^2 + az_0^2) : x_0^2 z_0]$$

is a second degree isogeny with dual $\hat{\phi} : E_{7a} \longrightarrow E_a$ given by

$$\hat{\phi}([u_0 : v_0 : w_0]) = [3v_0^2 w_0 : v_0(4u_0^2 + 5aw_0^2) : u_0^2 w_0].$$

(For $a = 1$, the isogeny $\phi$ is just the rational map $\Gamma^{\#}$ from Example 3.2.18.) One can thus form a second degree isogeny from a curve $E_r$ to $E_n$ — or vice versa — by composing the second degree $\mathbb{F}_{11}$-isogeny from $E_r$ to $E_{7r}$ with an $\mathbb{F}_{11}$-isomorphism from $E_{7r}$ to $E_n$.

# Chapter 7

# Conclusion

## 7.1 A Summary of Isogeny

Recall that we introduced general algebraic curves and function fields in Chapter 2. We then discussed the duality of projective algebraic curves and function fields (transcendence degree one extensions of given fields), and of non-constant rational maps of curves and $\bar{K}$-homomorphisms of function fields.

We then gave an exposition of elliptic curves, a special type of curve, and established the group structure of an elliptic curve. Subsequently, we discussed isomorphism and isogeny and documented their many interesting properties. In particular, we demonstrated that isogeny is a group homomorphism and that both isomorphism and isogeny induce equivalence relations on the set of elliptic curves over a given field.

We concluded with several computational examples which illustrated the theory developed in previous chapters. These examples served not only to illuminate the relationship between isogeny and isomorphism, but also underlined some of the problems which one encounters when attempting to deal with these notions in practice.

## 7.2 Open Problems

Inspite of all that is known about isogeny, there remain several open problems. We remind the reader of the most salient ones discussed.

Given two curves over a finite field $\mathbb{F}_q$, there is no easy way of determining whether they are in the same ($\bar{\mathbb{F}}_q$-) isogeny class. Of course, one can conclusively determine that they are, either by finding an explicit isogeny or by finding an extension field over which both curves have the same number of points. However, proving that they reside in separate isogeny classes amounts to proving that they do not have the same number of points over *any* finite extension field of $\mathbb{F}_q$.

Sometimes, it is not enough to have determined that two curves are isogenous. In the case where the goal is to reduce the discrete log problem on a "hard" elliptic curve $E$ to the discrete log problem on an "easy" curve $E'$, as described in Chapter 1, it is necessary to find an actual isogeny from $E$ to $E'$. There is no known method, given two isogenous curves, to quickly produce an isogeny between the two; while it could be of use to determine, for instance, the number of $\mathbb{F}_q$-isogenies between two isogenous curves, and the degrees of all such isogenies, there is also no known method for achieving either of these tasks.

Nonetheless, much is known about isogeny and isomorphism classes. For an elliptic curve $E$ in Weierstrass form, Schoof gives an explicit formula $N(t)$ for the number of $\mathbb{F}_q$-isomorphism classes in the $\mathbb{F}_q$-isogeny class of $E$. (See [20], in particular, [20, Section 4], for details.) For example, in the case of the curve $E_1/\mathbb{F}_{11} : y^2z = x^3 + xz^2$ given in the final section of Chapter 6, $|E(\mathbb{F}_{11})| = 12$, so that the value $t$ given in

Theorem 4.4.9 is 0. There are 20 nonsingular Weierstrass curves over $\mathbb{F}_{11}$ with $t = 0$ (i.e. with 12 points over $\mathbb{F}_{11}$), and we have $N(0) = 4$. Denoting by $QR_{11}$ the set of all quadratic residues modulo 11, and by $QN_{11}$ the set of all quadratic non-residues modulo 11, one finds that the four isogeny classes are:

$$\begin{aligned} I_1 &= \{E_r : y^2z = x^3 + rxz^2 \mid r \in QR_{11}\} \\ I_2 &= \{E_n : y^2z = x^3 + nxz^2 \mid n \in QN_{11}\} \\ I_3 &= \{E_{r'} : y^2z = x^3 + r'z^3 \mid r' \in QR_{11}\} \\ I_4 &= \{E_{n'} : y^2z = x^3 + n'z^3 \mid r \in QN_{11}\}. \end{aligned}$$

Achter and Cunningham also give the number of $\mathbb{F}_q$-isomorphism classes of elliptic curves over $\mathbb{F}_q$ in the $\mathbb{F}_q$-isogeny class of a given curve over $\mathbb{F}_q$ as part of a more general result in [1].

One final problem which we have not yet mentioned is the problem of point counting. In all the examples of elliptic curves over finite fields given in this thesis, the orders of the groups of $\mathbb{F}_q$-rational points were very small. While such examples are well-suited to illustrating certain principles and theorems, they are unsuitable for real world applications, since elliptic curve cryptosystems are built on groups which are extremely large (e.g. $q = 2^{155}$ or $q = 2^{160}$). Counting the number of points of an elliptic curve over, say, $\mathbb{F}_{2^{512}}$ is much harder than counting the number of points of a curve over, say, $\mathbb{F}_{11}$ or $\mathbb{F}_{13}$. It is also much more difficult to determine the group structure on these larger, cryptographically interesting curves, since there are many more possibilities.

To conclude, many open problems remain, and elliptic curves continue to present a subject of study that is interesting both from the point of view of mathematics and real world applications.

# Bibliography

[1] J. Achter, C. Cunningham, **Isogeny Classes of Hilbert-Blumenthal Abelian Varieties over Finite Fields**, Journal of Number Theory 92, (2002), 272-303.

[2] M. F. Atiyah, I. G. McDonald, **Introduction to Commutative Algebra**, Addison-Wesley, Reading Menlo Park New York Don Mills Wokingham Amsterdam Bonn Sydney Singapore Tokyo Madrid San Juan Paris Seoul Milan Mexico City Taipei, (1969).

[3] C. Breuil, B. Conrad, F. Diamond, R. Taylor, **On The Modularity of Elliptic Curves Over $\mathbb{Q}$: Wild 3-adic Exercises**, J. Amer. Math. Soc. 14, (2001), no. 4, 843-939.

[4] E. Brieskorn, H. Knörrer, **Plane Algebraic Curves**, Second Edition, Birkhäuser Verlag, Basel, (1986).

[5] J.W.S. Cassels, **Diophantine Equations with Special Reference to Elliptic Curves**, The Journal of the London Mathematical Society, vol. 41, (1966), 193-291.

[6] D. Dummit, R. Foote, **Abstract Algebra**, John Wiley & Sons, Inc., Second Edition, New York, (1999).

[7] A. Enge, **Elliptic Curves and Their Applications to Cryptography, An Introduction**, Kluwer Academic Publishers, Boston, (1999).

[8] G. Frey, **Links Between Stable Elliptic Curves and Certain Diophantine Equations**, Ann. Univ. Sarav. Ser. Math. 1, (1986), no. 1.

[9] W. Fulton, **Algebraic Curves**, Benjamin Cummings, Reading, (1969).

[10] D. J. H. Garling, **A Course in Galois Theory**, Cambridge University Press, Fifth Printing, Cambridge, (1995).

[11] S. Iitaka, **Algebraic Geometry, An Introduction to Birational Geometry of Algebraic Varieties**, Springer-Verlag, New York, (1982).

[12] G. Karpilovsky, **Field Theory: Classical Foundations and Multiplicative Groups**, Marcel Dekker, Inc., New York, (1988).

[13] A. W. Knapp, **Elliptic Curves**, Princeton University Press, Princeton, (1992).

[14] R. A. Mollin, **Fundamental Number Theory with Applications**, CRC Press, Boca Raton, (1998).

[15] R. A. Mollin, **Algebraic Number Theory**, Chapman & Hall/CRC Press, Boca Raton, (1999).

[16] W. K. Nicholson, **Introduction to Abstract Algebra**, PWS Publishing Company, Boston, (1993).

[17] National Institute for Standards and Technology, **FIPS** 186 – 2, **Digital Signatures**, NIST, (2002).

[18] M. and G. Orzech, **Plane Algebraic Curves**, Marcel Dekker, Inc., New York, (1981).

[19] K. A. Ribet, **On Modular Representations of** Gal($\overline{\mathbb{Q}}/\mathbb{Q}$) **Arising from Modular Forms**, Invent. Math. 100, (1990), no. 2, 431-476.

[20] R. Schoof, **Nonsingular Plane Cubic Curves Over Finite Fields**, Journal of Combinatorial Theory Series A, vol. 46, (1987), 183-211.

[21] J.-P. Serre, **On Modular Representations of Degree** 2 **of** Gal($\overline{\mathbb{Q}}, \mathbb{Q}$), Duke Math. J. 54, (1987), no. 1, 179-230.

[22] I. Shafarevich, **Basic Algebraic Geometry**, Springer-Verlag, New York, (1977).

[23] G. Shimura, **Introduction to the Arithmetic Theory of Automorphic Functions**, Princeton University Press, Princeton, (1971).

[24] J. Silverman, **The Arithmetic of Elliptic Curves**, Springer-Verlag, New York, (1986).

[25] J. Tate, **Endomorphisms of Abelian Varieties over Finite Fields**, Inventiones Mathematicae, vol. 2, (1966), 134-144.

[26] R. Taylor, A. Wiles, **Ring-theoretic Properties of Certain Hecke Algebras**, Ann. of Math. (2) 141, (1995), no. 3, 553-572.

[27] R. J. Walker, **Algebraic Curves**, Dover Publications, New York, (1962).

[28] A. Wiles, **Modular Elliptic Curves and Fermat's Last Theorem**, Ann. of Math. (2) 141, (1995), no. 3, 443-551.

# Index of Notation