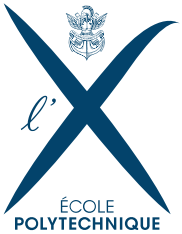

Introduction to Elliptic Curves

Lab Research Project Report
Second Revision

Sirawit Pongnakintr
sirawit.pongnakintr@polytechnique.edu

December 13, 2023

Supervised by
Prof. Diego Izquierdo

Abstract

The lab research project "Introduction to Elliptic Curves" is an individual study on elliptic curves, inspired by its applications on cryptography. The contribution from this project is the clarification on the route of proving the group law on elliptic curves using the Riemann–Roch theorem and a few original examples. This report will be organized as a culmination of basic knowledge required to know about elliptic curves, elliptic curves in general, its group law, and some additional properties of elliptic curves. Extra examples are added to clarify abstract statements, especially about order at a point and viewing projective varities in an affine subspace.

Contents

Acknowledgement

The author greatly thanks his supervisor, Professor Diego Izquierdo, for his kind help on explaining topics that were totally unreachable for a beginner. The author also thanks his friend Pitchayut Saengrungkongka for providing (daily) help on small problems. Without them, it would've been nearly impossible for the author to study the content of this level by himself. The author also thanks his friend Cassidy Kevorkian-Mielly for minor advices on doing a lab research project.

Chapter 1

Introduction

Elliptic curves, in some sense, can be seen as the simplest non-trivial structure in algebraic geometry. An algebraic curve has an interesting particular invariant called *genus*. The curves with genus zero are straight lines and conics, the curves with genus one with some extra properties (i.e. with a specified base point, and without singularities) are elliptic curves.

Elliptic Curves were suggested as a method of cryptography back in 1985, independently by Koblitz [6] and Miller [8]. In order to understand how it works in cryptography, this lab research project will go through a long route from introductory algebraic geometry to the properties of elliptic curves.

This chapter will be (or at least, try to be) complementary topics between the course MAA303: Algebra and Galois Theory [5] (taught in third year of the bachelor program of École Polytechnique) and the beginning of [11].

1.1 Preliminaries

Most of the following in this section is taken and edited from [5]. Some results that will be unused in this report later on, are omitted, to keep it as short as possible. Explanations are provided whenever appropriate.

Definition (Ideal generated by a set)**.** *For a commutative ring R and a subset S of R we denote by $\langle S\rangle$ or (S) for the ideal generated by S, defined as the smallest ideal that contains S.*

Definition (Domain)**.** *A commutative ring R is said to be a domain if for any $a, b \in R$, $ab = 0$ implies $a = 0$ or $b = 0$.*

Definition (Maximal Ideal)**.** *An ideal I of a commutative ring R is said to be maximal if $I \neq R$ and there is no ideal J such that $I \subsetneq J \subsetneq R$.*

Definition (Principal Ideal)**.** *An ideal I of a commutative ring R is said to be principal if there exists $x \in R$ such that $I = (x)$.*

Definition (Prime ideal)**.** *An ideal I of a commutative ring R is said to be prime if $I \neq R$ and for all $a, b \in R$, if $ab \in I$ then $a \in I$ or $b \in I$.*

Example 1. *Let p be a prime number. Then (p) is a prime ideal in $\mathbb{Z}$. To see this, suppose $a, b \in \mathbb{Z}$ with $ab \in (p)$, then ab is divisible by p, and we can apply Euclid's lemma to conclude that p divides a or p divides b, so $a \in (p)$ or $b \in (p)$.*

Definition (Principal Ideal Domain)**.** *A commutative ring R is said to be a PID (principal ideal domain) if it is a domain and every ideal is principal.*

Example 2. *Let K be a field. The polynomial ring $K[x]$ is a PID.*

Proof. Suppose I is an ideal in $K[x]$. If $I = (0)$ then we're done. Suppose otherwise, then there exists a nonzero element of I. Let A be the unique monic polynomial in I with the minimum degree. Now, for any $P \in I$, one can divide P by A and so there exists a unique pair $(Q, R) \in K[x] \times K[x]$ such that $P = AQ + R$ and either R is zero or $\deg R < \deg A$. Since $P, Q \in I$, $R = P - AQ \in I$ also. If R is nonzero then $\deg R < \deg A$, a contradiction, so $R = 0$. This proves that all polynomials in I is divisible by A, hence $I = AK[x] = (A)$ and this completes the proof. □

Theorem 3. *Let R be a commutative ring and I be an ideal of R. R/I is a field if and only if I is maximal.*

Proof. See [5, 3.5.1.(i)]. □

Theorem 4. *Let R be a commutative ring and I be an ideal of R. R/I is a domain if and only if I is prime.*

Proof. See [5, 3.5.1.(ii)]. □

Proposition 5. *If R is a commutative ring, then any maximal ideal is prime.*

Proof. Any maximal ideal $\mathfrak{m}$ of R has $R/\mathfrak{m}$ a field by theorem 3. In particular, it is a domain, so apply the converse of 4 to see that m is prime. □

Definition (Irreducible element)**.** *Given a commutative ring R, an element $x \in R$ is said to be irreducible if $x \notin R^\times$ and whenever x can be written as ab with $a, b \in R$, either a or b is invertible in R.*

Definition (Unique factorization domain)**.** *A commutative ring R is said to be a UFD (unique factorization domain) if it is a domain, and for every element $x \in R \setminus \{0\}$, it can be written in the form*

$$x = up_1 \dots p_r$$

where $u \in R^\times$, $r \in \mathbb{N}$, and $p_1, \dots, p_r$ are irreducible elements of R "uniquely", in a way that if there is another way to write

$$x = vq_1 \dots q_s$$

with $v \in R^\times$, $s \in \mathbb{N}$, and $q_1, \dots, q_s$ are irreducible, then $r = s$, and there exists $u_1, \dots, u_r \in R^\times$ such that $p_i = u_i q_i$ for all $i \in \{1, \dots, r\}$.

Theorem 6. *Let A be a UFD, then so is $A[T]$.*

Proof. See [5, 3.7.12]. □

Example 7. *Let $n \in \mathbb{N}^*$ and let K be a field. Then $K[X_1, \dots, X_n]$ is a UFD.*

Proof. We can do induction since $K[X_1, \dots, X_n] \cong K[X_1, \dots, X_{n-1}][X_n]$, and apply 6. The base case is that K is a UFD, which is true since $K^\times = K \setminus \{0\}$ by definition, so every nonzero element can be "factorized" as itself in the definition of UFD. □

Proposition 8. *If A is a PID, then the following are equivalent.*

(i) The element a is irreducible in A.

(ii) The ideal (a) is prime.

(iii) The ideal (a) is maximal.

Proof. See [5, 3.5.2.]. □

Proposition 9. *If A is a UFD and p is an irreducible element in A, then (p) is prime.*

Proof. See [5, 3.7.7.]. □

Example 10. *Since we've proved that $K[X_1, \dots, X_n]$ is a UFD for all field K and natural n, in the settings of algebraic varieties (later), we may show that an ideal is prime by showing that it is generated by an irreducible polynomial and apply the previous proposition directly.*

Theorem 11 (Eisenstein's criterion)**.** *Let A be a UFD with $K = \mathrm{Frac}(A)$ and let π be an irreducible element in A. Let $P(T) = \sum_{k=0}^{n} a_k T^k$ be a polynomial in $A[T]$. Assume that*

(a) π does not divide a_n;

(b) π divides a_k for each $k \in \{0, \dots, n-1\}$;

(c) π^2 does not divide a_0.

Then P is irreducible in $K[T]$.

Proof. See [5, 3.7.14]. □

Definition (Field extension)**.** *Let K, L be fields. We say L is an extension of K if there is a ring homomorphism from K to L. Such a homomorphism is necessarily injective. We write L/K to say that L is an extension of K. Sometimes we also say K* injects *into L.*

Proof. Let us prove that any ring homomorphism ϕ from K to L is injective. We will prove this by proving that $\ker(\phi) = \{0\}$. Suppose $\ker(\phi) \neq \{0\}$, then there exists a nonzero element $x \in \ker(\phi)$. Then $\phi(1) = \phi(x \cdot x^{-1}) = \underbrace{\phi(x)}_{0} \cdot \phi(x^{-1}) = 0$, which is a contradiction. (Recall that a ring homomorphism sends 1 to 1, not 0!) The rest is obvious. We claim that for all $a \neq 0$, $f(a)^{-1} = f(a^{-1})$. Since we proved that $\ker(\phi) = \{0\}$, $\phi(a) \neq 0$ and so $\phi(a)^{-1}$ is well-defined. Since $1 = f(a)^{-1}f(a)$,

$$f(a^{-1}) = f(a)^{-1}f(a)f(a^{-1}) = f(a)^{-1}f(aa^{-1}) = f(a)^{-1}f(1) = f(a)^{-1}.$$

Now if $\phi(x) = \phi(y) \neq 0$ then $1 = \phi(x)\phi(y)^{-1} = \phi(xy^{-1})$ (by the previous claim). Well $\phi(xy^{-1} - 1) = \phi(xy^{-1}) - \phi(1) = 0$ but we proved that $\ker(\phi) = \{0\}$ so $xy^{-1} - 1$ must be 0, that is $xy^{-1} = 1$, i.e. $x = y$. □

Definition (Algebraic extension)**.** *We say L/K is an algebraic extension if for all $x \in L$, there exists a polynomial $P \in K[x]$ such that $P(x) = 0$.*

Definition (Algebraically closed field)**.** *For a field K, we say that it is algebraically closed if all nonconstant polynomial in $K[x]$ has a root in K.*

Definition (Algebraic closure)**.** *For any field K we denote by the field $\bar{K}$ the algebraic closure of K, defined as the algebraic extension of K such that it is algebraicly closed.*

Theorem 12. *Every field has a unique algebraic closure.*

Proof. See [5, 4.5.4.]. □

Theorem 13. *Let L/K be an algebraic extension and fix an element $\alpha \in L$. Consider the ring homomorphism*

$$\varphi_\alpha \colon \begin{cases} K[x] & \to L \\ P & \mapsto P(x). \end{cases}$$

We have $\ker(\varphi_\alpha) = (P)$ for some $P \in K[x]$ and so $K[x]/(P) \cong K[\alpha] = K(\alpha)$.

Proof. (Taken from [5, 4.3.2.(ii)]) Since α is algebraic, there exists polynomials in $K[x]$ killing α. So $\ker(\varphi_\alpha) \neq \{0\}$ is a nonzero prime[1] ideal in the principal ideal domain $K[x]$, this means that $\ker(\varphi_\alpha) = (P)$ for some irreducible $P \in K[x]$ by proposition 8. If P is not monic, we can divide P by its first coefficient to make it monic and still usable. We call this polynomial the *minimal polynomial* of α in $K[x]$ and denote it by μ_α. Now observe that $\operatorname{im}(\varphi_\alpha) \cong K[\alpha]$. But by proposition 8, (P) is maximal so $K[x]/(P) \cong K[x]/\ker(\varphi_\alpha) \cong \operatorname{im}(\varphi_\alpha)$ (apply the first isomorphism theorem for rings) is a field, so $K[\alpha] = K(\alpha)$. □

Remark. *Usually, we will often use the fact that for all $\alpha \in \bar{K}$, $K[x]/(\mu_\alpha) \cong K(\alpha)$ directly (often without thinking too much, i.e. without recalling this theorem).*

Definition (K-homomorphism)**.** *Let L, M be fields such that L/K and M/K are field extensions. We denote by $\operatorname{Hom}_K(L, M)$ the set of K-homomorphisms, which is the set of ring homomorphisms from L to M fixing K. In other words,*

$$\operatorname{Hom}_K(L, M) := \{\phi \in \operatorname{Hom}(L, M) \colon \phi|_K = \mathrm{id}_K\}.$$

Definition (Normal extension)**.** *Let L/K be an algebraic extension. Then L/K is normal if every irreducible $P \in K[x]$ that has a root in L splits in L. See [5], 5.1.1 and 5.1.2 for examples.*

Definition (Separability)**.** *Let K be a field and $P \in K[x]$. We say P is separable if P has simple roots in $\bar{K}$. Otherwise, we say P is inseparable.*

Let L/K be an extension. An element $x \in L$ is said to be separable over K if it is algebraic and its minimal polynomial in K is separable. We say L/K is separable if every element of L is separable over K.

[1] It is prime because if $PQ \in \ker(\varphi_\alpha)$ then $\varphi_\alpha(PQ) = (PQ)(\alpha) = P(\alpha)Q(\alpha) = 0$ implies $P(\alpha) = 0$ or $Q(\alpha) = 0$ because $P(\alpha)Q(\alpha) \in L$ and L is a field, hence a domain, in particular.

Definition (Perfect field)**.** *A field K is said to be perfect if all algebraic extensions of K are separable.*[2]

Definition (Separable degree)**.** *Let L/K be a finite extension. The separable degree of L/K, denoted by $|L\colon K|_s$, is defined by*

$$|L\colon K|_s := \#\mathrm{Hom}_K(L, \bar{K}).$$

Definition. *Let L/K be a finite extension. The set L_s of elements in L that are separable over K is called the separable closure of K in L. It is a subfield of L containing K. (See [5, 5.2.8])*

Theorem 14 (Primitive Element Theorem)**.** *Let L/K be a finite separable extension. Then there exists $x \in L$ such that $L = K(x)$.*

Proof. See [5, 5.3.1.]. □

Definition. *Let L/K be a field extension. We denote by $\mathrm{Aut}(L/K)$ the group of automorphisms of L fixing K, i.e.*

$$\mathrm{Aut}(L/K) := \mathrm{Hom}_K(L, L).$$

Definition. *An extension L/K is said to be Galois if it is normal and separable. In this case, $\mathrm{Aut}(L/K)$ is denoted by $\mathrm{Gal}(L/K)$ or $G_{L/K}$.*

Theorem 15. *Let L/K be a finite extension. Then*

$$\#\mathrm{Aut}(L/K) \le |L\colon K|_s \le |L\colon K|.$$

with $\#\mathrm{Aut}(L/K) = |L\colon K|_s$ if and only if L/K is normal.

Proof. See [5, 5.4.2.]. □

Definition (Fixed field)**.** *Let L be a field, and $G \le \mathrm{Aut}(L)$. The fixed field of G, denoted by L^G, is the set of elements of L that are fixed by all of G, i.e.*

$$L^G = \{x \in L\colon \sigma(x) = x \text{ for all } \sigma \in G\}.$$

Theorem 16. *Let L/K be a finite Galois extension. Then $L^{\mathrm{Gal}(L/K)} = K$.*

Proof. See [5, 5.5.2]. □

Theorem 17 (Fundamental theorem of (finite) Galois Theory)**.** *Let L/K be a finite Galois extension. The following maps are mutually inverse bijections.*

$$\begin{aligned}\Phi\colon \{M\colon M \text{ is a field and } K \subseteq M \subseteq L\} &\rightleftarrows \{H\colon H \le \mathrm{Gal}(L/K)\}\colon \Psi\\ M &\mapsto \mathrm{Gal}(L/M)\\ L^H &\hookleftarrow H.\end{aligned}$$

Moreover, if H is a subgroup of $\mathrm{Gal}(L/K)$, the extension L^H/K is Galois if and only if H is a normal subgroup of $\mathrm{Gal}(L/K)$. In that case, the Galois group of L^H/K is $Gal(L/K)/H$.

Proof. See [5, 5.5.4.]. □

1.2 Complements On Algebra

This section is a collection of results which are beyond the basics, but are required for the later uses. It is too difficult to derive every result here to make it self-contained, so instead, this section will frequently reference admitted facts proven in the literature. However, relevant propositions are proved here as much as it is appropriate.

Later on, we will frequently consider about $G_{\bar{K}/K}$ for a general perfect field K, so here is a little proposition to check that it is well-defined.

Proposition 18. *Let K be a perfect field. Then $\bar{K}/K$ is a Galois extension.*

Proof. $\bar{K}/K$ is clearly normal. It is also algebraic, so by the assumption that K is perfect, it is separable. □

[2] This definition is not the same as one in [5], but turns out to be equivalent.

Consider another proposition that the separable closure of a perfect field is the algebraic closure.

Proposition 19. *Let K be a perfect field. Let L be the separable closure of K in $\bar{K}$. Then $\bar{K} \cong L$.*

Proof. By definition of perfect field, every algebraic extension of K is separable. Since $\bar{K}/K$ is algebraic, it is separable, then the separable closure of K in $\bar{K}$, by definition, is the set of separable elements of $\bar{K}$ in K, which is of it, in this case, so $L = \bar{K}$ and this completes the proof. □

1.2.1 Transcendence

This subsection utilizes [13, Tag 030D] as the main reference.

Definition (Algebraic independence)**.** *Let K be a field. Let L/K be an extension. Let $\mathscr{F} = \{\alpha_i\}_{i\in I}$ be a family of elements in L. We say that $\mathscr{F}$ is* algebraically independent *over K if the evaluation map*

$$\begin{cases} K[\{X_i\}_{i\in I}] & \to L \\ P & \mapsto P((\alpha_i)_{i\in I}) \end{cases}$$

(evaluating the polynomial P at $(x_i)_{i\in I}$) is injective.

Example 20. *π and π^2 are not algebraically independent over $\mathbb{Q}$ because the polynomial $P(x,y) = x^2$ and the polynomial $Q(x,y) = y$ have the same image π^2 when evaluate at (π, π^2).*

Assuming the well-known fact that π is transcendental, $\{\pi\}$ (the singleton set) is algebraically independent over $\mathbb{Q}$, because if not, then there exists polynomials $P \neq Q \in \mathbb{Q}[x]$ such that $P(\pi) = Q(\pi)$, this means π is a root of $P - Q$, which is a nonzero polynomial in $\mathbb{Q}[x]$, so π is algebraic, which is a contradiction.

As of the date of writing this, no one knows whether π and e are algebraically independent over $\mathbb{Q}$ or not.

Definition (Transcendence basis)**.** *A transcendence basis of L/K is a set $\mathscr{F} = \{\alpha_i\}_{i\in I}$ of elements in L such that $\mathscr{F}$ is algebraically independent over K and $L/K((\alpha_i)_{i\in I})$ is an algebraic extension.*

Definition (Transcendence degree)**.** *Let L/K be a field extension. Then the transcendence degree of L over K, denoted by $\operatorname{trdeg}_K(L)$, is defined by the cardinality of a transcendence basis of L/K. Note that this requires proving that all transcendence bases have the same cardinality, which we refer to [13, Tag 030D], 9.26.3.*

1.2.2 Discrete Valuation

Definition (Discrete valuation ring)**.** *An ring R is said to be a DVR (discrete valuation ring) if it is a PID and it has a unique maximal ideal.*

Definition. *If R is a DVR with its unique maximal ideal $\mathfrak{m}$, then we define the natural*[3] *discrete valuation $\nu\colon R \to \mathbb{N} \cup \{\infty\}$ to be (for all $x \in R$)*

$$\nu(x) = \max\{n \in \mathbb{N} \colon x \in \mathfrak{m}^n\}$$

if the set $\{n \in \mathbb{N} \colon x \in \mathfrak{m}^n\}$ is finite ($\mathfrak{m}^0 = R$, so the set is always nonempty). Otherwise, define $\nu(x) = \infty$.

If R is a DVR with its unique maximal ideal $\mathfrak{m}$, then since R is also a PID, $\mathfrak{m} = (t)$ for some $t \in R$ (we call t a uniformizer of R).

Lemma 21. *For all $a \in R \setminus \{0\}$, for any uniformizer t of R there exists a unique $n \in \mathbb{N}$ and unique $s \in R \setminus \mathfrak{m}$ such that $a = t^n s$.*

Proof. Fix a uniformizer t of R and let $n = \nu(a)$. Then $a \in \mathfrak{m}^n$ and $\mathfrak{m} = (t)$ implies there exists $a_1, \ldots, a_n \in \mathfrak{m} = (t)$ such that $a = \prod_{i=1}^n a_i$. Now write $a_i = ts_i$ for some $s_i \in R$. If $s_i \in \mathfrak{m}$ for some $i \in \{1, \ldots, n\}$ then $a \in \mathfrak{m}^{n+1}$, a contradiction. Therefore, $s_i \notin \mathfrak{m}$ for all $i \in \{1, \ldots, n\}$. Now $a = \prod_{i=1}^n a_i = t^n \prod_{i=1}^n s_i$. But since $\mathfrak{m}$ is prime (by proposition 8), we see that $\prod_{i=1}^n s_i \notin \mathfrak{m}$. Hence one can define $s := \prod_{i=1}^n s_i \in R \setminus \mathfrak{m}$ and conclude that $a = t^n s$. This proves the existence. Now suppose there is $n' \in \mathbb{N}$ such that $a = t^{n'} s'$ for some $s' \in R \setminus \mathfrak{m}$. n' cannot be greater than n because it would imply that $a \in \mathfrak{m}^{n'}$ which contradicts with $n = \nu(a)$. If $n' < n$ then by existence, we have $a = t^n s = t^{n'} s'$, so $t^{n'}(t^{n-n'} s - s') = 0$, and since R is a domain with $t \neq 0$, we have $t^{n-n'} s - s' = 0$, i.e. $s' = t^{n-n'} s \in \mathfrak{m}$, a contradiction. Therefore, $n' = n$ always. Now suppose $a = t^n s_1 = t^n s_2$ then $t^n(s_1 - s_2) = 0$, so $t \neq 0$ gives $s_1 - s_2 = 0$ and the uniqueness is proved. □

[3] This is a nonstandard term.

Proposition 22. *Let R be a DVR with the valuation $\nu\colon R \to \mathbb{N} \cup \{\infty\}$ as defined above. Then,*

(i) For any $a, b \in R$, $\nu(a+b) \geq \min(\nu(a), \nu(b))$;

(ii) For any $a, b \in R$, $\nu(ab) = \nu(a) + \nu(b)$;

(iii) For any $a, b \in R$, if $\nu(a) \neq \nu(b)$ then $\nu(a+b) = \min(\nu(a), \nu(b))$.

(iv) For any $a \in R$, $\nu(a) = \infty$ if and only if $a = 0$.

Proof. Suppose $a, b \in R$. Let $n = \nu(a)$ and $m = \nu(b)$.

(i) Observe that $a, b \in \mathfrak{m}^{\min(n,m)}$, so $a + b \in \mathfrak{m}^{\min(n,m)}$ also, hence $\nu(a+b) \geq \min(\nu(a) + \nu(b))$.

(ii) Pick a uniformizer t of R. By the previous lemma, there exists uniquely $s_a, s_b \in R \setminus \mathfrak{m}$ such that $a = t^{\nu(a)} s_a$ and $b = t^{\nu(b)} s_b$. We have

$$\nu(ab) = \nu(t^{\nu(a)} s_a t^{\nu(b)} s_b) = \nu(t^{\nu(a)+\nu(b)} s_a s_b),$$

and conclude that this value is $\nu(a) + \nu(b)$ by uniqueness from the previous lemma and the fact that $s_a s_b \notin \mathfrak{m}$.

(iii) Pick a uniformizer t of R. Repeat the same argument so that we have $a = t^{\nu(a)} s_a$ and $b = t^{\nu(b)} s_b$ with $s_a, s_b \notin \mathfrak{m}$. Suppose $\nu(a) \neq \nu(b)$. Furthermore, without loss of generality, suppose $\nu(a) < \nu(b)$. Then

$$\nu(a+b) = \nu(t^{\nu(a)} s_a + t^{\nu(b)} s_b) = \nu(t^{\nu(a)}(s_a + t^{\nu(b)-\nu(a)} s_b) = \nu(a) + \nu(s_a + t^{\nu(b)-\nu(a)}).$$

with the last equality follows from *(ii)*. Observe that $s_a + t^{\nu(b)-\nu(a)}$ cannot be in $\mathfrak{m}$ because otherwise, $s_a + t^{\nu(b)-\nu(a)} = t^p q$ with $p = \nu(s_a + t^{\nu(b)-\nu(a)}) > 0$ and a unique $q \in R \setminus \mathfrak{m}$. This means

$$s_a = t(t^{p-1} q - t^{\nu(b)-\nu(a)-1}) \in \mathfrak{m},$$

a contradiction. This proves that $\nu(s_a + t^{\nu(b)-\nu(a)}) = 0$ and so $\nu(a+b) = \nu(b)$.

(iv) This requires some deeper results. The goal is to show that $\bigcap_{n \geq 1} \mathfrak{m}^n = \{0\}$. See [13, Tag 00IP].

This completes the proof. □

We can easily see that $\nu(ab) = \nu(a) + \nu(b)$ for any $a, b \in R$. Hence, let us extend such valuation to the field of fractions of R. Let $\frac{p}{q} \in \mathrm{Frac}(R)$ then $\nu\left(\frac{p}{q}\right) := \nu(p) - \nu(q)$. It is not hard to see that this is well-defined. This gives the extended valuation $\nu\colon \mathrm{Frac}(R) \to \mathbb{Z} \cup \{\infty\}$ on the field $\mathrm{Frac}(R)$.

Example 23 (p-adic valuation)**.** *Consider $\mathbb{Z}$ as the ring of integers. Let p be a prime number. We do a "localization" of $\mathbb{Z}$ at p, defined as*

$$\mathbb{Z}_{(p)} := \left\{ \frac{n}{m} : n, m \in \mathbb{Z} \text{ and } p \nmid m \right\}.$$

We claim that $\mathbb{Z}_{(p)}$ is a DVR.

Proof. Let us first prove that $\mathbb{Z}_{(p)}$ is a domain. Take $\frac{n}{m}, \frac{n'}{m'} \in \mathbb{Z}_{(p)}$ such that $\frac{n}{m}\frac{n'}{m'} = 0$. Then $\frac{nn'}{mm'} = 0 = \frac{0}{1}$, that is, $nn'(1) = 0(mm')$ so $nn' = 0$. Since $\mathbb{Z}$ is a domain, $n = 0$ or $n' = 0$. This implies $\frac{n}{m} = 0$ or $\frac{n'}{m'} = 0$. Now, let us prove that $\mathbb{Z}_{(p)}$ is a PID, by showing that every ideal is principal. Suppose I is an ideal of $\mathbb{Z}_{(p)}$. Then $I \cap \mathbb{Z}$ is an ideal of $\mathbb{Z}$. Since $\mathbb{Z}$ is a PID, $I \cap \mathbb{Z} = k\mathbb{Z}$ for some $k \in \mathbb{Z}$. Now let us show that $I = k\mathbb{Z}_{(p)}$. Take $\frac{m}{n} \in I$ ($p \nmid n$), then $m = n\frac{m}{n} \in I \cap \mathbb{Z} = (k)$. This means $m = kq$ for some $q \in \mathbb{Z}$. So $\frac{m}{n} = k\frac{q}{n} \in k\mathbb{Z}_{(p)}$. Now suppose $k\frac{m}{n} \in k\mathbb{Z}_{(p)}$. Then $km \in k\mathbb{Z} = I \cap \mathbb{Z} \subseteq I$. Since ideals absorb elements, $km \in I$ with $\frac{1}{n} \in \mathbb{Z}_{(p)}$ implies $\frac{km}{n} \in I$. This proves that I is principal, i.e. generated by k in $\mathbb{Z}_{(p)}$. Now we know that $\mathbb{Z}_{(p)}$ is a PID. Let us show that (p) is the unique maximal ideal, i.e. every proper ideal of $\mathbb{Z}_{(p)}$ is contained in (p). Let I be a proper ideal of $\mathbb{Z}_{(p)}$. Since it is principal, suppose $I = (\frac{m}{n})$ for some $\frac{m}{n} \in \mathbb{Z}_{(p)}$. If $p \nmid m$ then $\frac{n}{m} \in \mathbb{Z}_{(p)}$ so $1 = \frac{n}{m}\frac{m}{n} \in I$, i.e. $I = \mathbb{Z}_{(p)}$, a contradiction. Therefore, $p \mid m$ and so $I \subseteq (p)$. □

Now, consider the natural valuation on $\mathbb{Z}_{(p)}$ with the unique maximal ideal (p). This defines the map $\nu\colon \mathbb{Z}_{(p)} \to \mathbb{N} \cup \{\infty\}$. The extension

$$\nu_p\colon \underbrace{\mathrm{Frac}(\mathbb{Z}_{(p)})}_{\mathbb{Q}} \to \mathbb{Z} \cup \{\infty\}$$

is the p-adic valuation function. Note that this is the same as the usual simpler definition of the p-adic valuation function[4]:

$$\nu_p\colon x \in \mathbb{Z} \mapsto \max\{n \in \mathbb{N} \cup \{\infty\}\colon p^n \mid x\}, \qquad \nu_p\colon \frac{r}{s} \in \mathbb{Q} \mapsto \nu_p(r) - \nu_p(s) \in \mathbb{Z} \cup \{\infty\}.$$

Now let us prove a little result which will be useful later.

Proposition 24. *For a DVR R and its maximal ideal $\mathfrak{m}$, we have $R \setminus \mathfrak{m} = R^\times$.*

Proof. First, $R^\times \cap \mathfrak{m} = \emptyset$. To see this, suppose $x \in R^\times \cap \mathfrak{m}$ and see that $x^{-1} \in R^\times$ also, so $1 = xx^{-1} \in \mathfrak{m}$ (absorbed by the ideal $\mathfrak{m}$), this means $\mathfrak{m} = R$, which is a contradiction.

Now let us prove that $R \setminus R^\times \subseteq \mathfrak{m}$. Take $x \in R \setminus R^\times$. If $(x) = \mathfrak{m}$ then this is done. Otherwise, $(x) \subseteq \mathfrak{m}$, and we can keep adding element from $\mathfrak{m}$ into (x) to obtain another ideal that is bigger than (x) but still containing x. The ideal $\mathfrak{m}$ is an upper bound to this process, then we apply Zorn's lemma to conclude that $x \in \mathfrak{m}$.

By contraposition, $R \setminus \mathfrak{m} \subseteq R^\times$. Now pick any $x \in R^\times$ and since $R^\times \cap \mathfrak{m} = \emptyset$, x fails to belong to $\mathfrak{m}$, so $x \in R \setminus \mathfrak{m}$. This completes the proof. □

1.2.3 Projective Geometry

Suppose we're working on a field K with its algebraic closure $\bar{K}$. We denote by $\mathbb{A}^n$ the space $\bar{K}^n$ and call this an *affine space*, and denote by $\mathbb{A}^n(K)$ the space K^n. This is the usual case when we were playing around in the Euclidean space.

Now, let us move to the projective case. We denote by $\mathbb{P}^n$ the structure of points in $\mathbb{A}^{n+1} \setminus \{0\}$ modulo the following equivalence relation defined for all $(x_0, \ldots, x_n), (y_0, \ldots, y_n) \in \mathbb{A}^{n+1}$:

$$(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n)$$

if there exists $\lambda \in \bar{K}^\times$ such that $x_i = \lambda y_i$ for all i. We denote by

$$[x_0, \ldots, x_n]$$

the equivalence class represented by $(x_0, \ldots, x_n)$. We denote by $\mathbb{P}^n(K)$ the set $\{[x_0, \ldots, x_n] \in \mathbb{P}^n\colon x_i \in K \text{ for all } i \in \{0, \ldots, n\}\}$.

Example 25. *Consider the case of $\mathbb{P}^1(K)$ where $K = \mathbb{R}$. We can visualize the space $\mathbb{A}^2$ first and then quotient by $\sim$. Topologically, we see that each equivalence class (colored straight lines)*

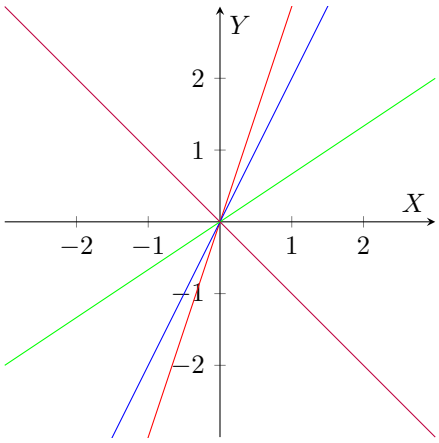

Figure 1.1: The affine space $\mathbb{A}^2$, with equivalent points colored by the same color

has a continuity to the "near" equivalence classes. In fact, $\mathbb{P}^1(\mathbb{R})$ is homeomorphic to S^1 with its antipodal points identified. This can be generalized and viewed from different aspects. See [1, Page 71, (a), (b), (c)].

[4] They're motivated by the same idea anyway; the slight difficulties in localizing $\mathbb{Z}$ is just a tool to fit it in the model of DVR. We will see the same analogy later when localizing something else in the context of algebraic varieties.

Next, let us consider another point of view, which is more important and more relevant in the context of algebraic geometry.

Example 26. *In $\mathbb{P}^n$, define U_i to be*

$$\{[x_0, \dots, x_n] \in \mathbb{P}^n \colon x_i \neq 0\}$$

and observe the bijections $\phi_i \colon \mathbb{A}^n \to U_i$ defined by

$$\phi_i \colon (x_1, \dots, x_n) \mapsto [x_1, \dots, x_i, 1, x_{i+1}, \dots, x_n]$$

and we see that

$$\phi_i^{-1} \colon [x_0, \dots, x_n] \mapsto \left(\frac{x_0}{x_i}, \dots, \frac{x_n}{x_i} \right).$$

Observe that $\bigcup_{i=0}^n U_i = \mathbb{P}^n$. This allows us to work with affine copies $\mathbb{A}^n$, identified to U_i by ϕ_i, and still representing the same object in $\mathbb{P}^n$. We will continue this idea in the subsection about projective varieties.

1.3 Varieties

This section corresponds to the first chapter of [11]. A few examples were added, and a few contents (that might be unused later in this report) were removed. Note that some of the ideas and examples are inspired from [12].

1.3.1 Affine Settings

Definition (Affine algebraic set)**.** *For a polynomial $f \in \bar{K}[X_1, \dots, X_n]$ we denote by $Z(f)$ the set of zeroes of f, i.e.,*

$$Z(f) := \{x \in \mathbb{A}^n \colon f(x) = 0\}.$$

Furthermore, for a set S of polynomials in $\bar{K}[X_1, \dots, X_n]$, we write

$$Z(S) := \{x \in \mathbb{A}^n \colon f(x) = 0 \text{ for all } f \in S\}$$

and call this an affine algebraic set*. Observe that if I is an ideal generated by S, then $Z(I) = Z(S)$. We denote this set by V_I and call it the affine algebraic set generated by ideal I.*

Example 27. *This example is given by [11, I.1.3.1].*

Consider the polynomial $f = X^2 - Y^2 - 1 \in K[X, Y]$ in any field K. We define $V := Z(f)$ as the algebraic set corresponding to the equation. If $K = \mathbb{R}$, we have the following geometric view of the curve (Figure 1.2).

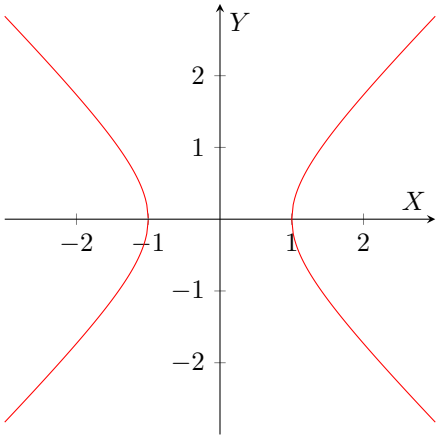

Figure 1.2: The zero locus $V(\mathbb{R})$

One can project the curve by sweeping the lines $X + Y = T$ for all $T \in \mathbb{R} \setminus \{0\}$ as each line would hit the set at exactly one point. By solving that system of equations, we have $X = \frac{T^2+1}{2T}$ and $Y = \frac{T^2-1}{2T}$. This motivates us to parametrize the curve by T. Consider the following map:

$$\begin{cases} \mathbb{A}^1(K) \setminus \{0\} & \to V(K) \\ t & \mapsto \left(\frac{t^2+1}{2t}, \frac{t^2-1}{2t} \right) \end{cases}$$

and observe that it makes a bijection between $\mathbb{R} \setminus \{0\}$ *and* $V(\mathbb{R})$*. Now, generalizing* K *for other cases* ($K \neq \mathbb{R}$)*, we see that if* $\operatorname{char}(K) \neq 2$*, then the map makes sense and is a bijection.*

Definition (Ideal of an algebraic set)**.** *Observe that for any affine algebraic set* V*, the set*

$$\{f \in \bar{K}[X_1, \ldots, X_n] \colon f(x) = 0 \text{ for all } x \in V\}$$

is an ideal in the ring $\bar{K}[X_1, \ldots, X_n]$*. We call this the ideal of* V *and denote by* $I(V)$*. Note that* $I(V_I)$ *may not be equal to* I *in general! If* $I(V)$ *can be generated by polynomials in* $K[X]$*, then we say that* V *is defined over* K*, and write* V/K*. The set of* K*-rational points is defined as the set*

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

Example 28. *Let* $I = (x^2 + 2xy + y^2)$ *be an ideal of* $\bar{K}[x, y]$*. Then* $V_I = Z(I) = \{(x, y) \in \bar{K}^2 \colon x^2 + 2xy + y^2 = 0\}$*. However,* $I(V_I) = (x + y) \neq I$*.*

Proposition 29. *Even though* $I(V_I)$ *might not be equal to* I *in general, we have* $V_{I(V)} = V$ *in general!*

Proof. Let V be an algebraic set over $\bar{K}$, i.e. $V \subseteq \mathbb{A}^n$. Suppose $V = Z(S)$ for some set $S \subseteq \bar{K}[X_1, \ldots, X_n]$. Let $I(V)$ be its ideal. If $f \in S$, then $f(P) = 0$ for all $P \in V$, this means $f \in I(V)$ by definition, i.e. $S \subseteq I(V)$. Now, consider $V_{I(V)} := \{P \in \bar{K}[X_1, \ldots, X_n] \colon f(P) = 0 \text{ for all } f \in I(V)\}$. If $P \in V_{I(V)}$ then $f(P) = 0$ for all $f \in I(V)$. So $f(P) = 0$ for all $f \in S \subseteq I(V)$, in particular. Hence, $V_{I(V)} \subseteq V$. Now if $P \notin V_{I(V)}$ then $f(P) \neq 0$ for some $f \in I(V) = \{g \in \bar{K}[X_1, \ldots, X_n] \colon g(x) = 0 \text{ for all } x \in V\}$. This means $f(P) \neq 0$ meanwhile $f(x) = 0$ for all $x \in V$, so $P \notin V$ for sure. This proves that if $P \notin V_{I(V)}$ then $P \notin V$, so by contraposition, $V \subseteq V_{I(V)}$. □

Corollary 30. *Through the previous proof, we see that* $S \subseteq I(V)$*, i.e. for all ideal* I *of* $\bar{K}[X_1, \ldots, X_n]$*, we have* $I \subseteq I(V_I)$*.*[5]

Definition (Ideal over K)**.** *The previous definition for* $I(V)$ *was for general ideal over* $\bar{K}$*, but we can restrict to those over* K*, defined by*

$$I(V/K) := \{f \in K[X_1, \ldots, X_n] \colon f(P) = 0 \text{ for all } P \in V\} = I(V) \cap K[X_1, \ldots, X_n].$$

Definition. *An affine algebraic set* V *is called an affine variety if* $I(V)$ *is a prime ideal in* $\bar{K}[X_1, \ldots, X_n]$*.*

Example 31. *The algebraic set* $V_1 = Z(\{x^2 + 2xy + y^2\})$ *has* $I(V_1) = (x + y)$ *which is prime because* $x + y$ *is irreducible (see 10), so* V_1 *is an algebraic variety.*

The algebraic set $V_2 = Z(\{x^2 - y^2\})$ *has* $I(V_2) = ((x + y)(x - y))$ *which is not prime (Take* $x + y, x - y \notin I(V_2)$ *but their product is in* $I(V_2)$*). So* V_2 *is not an algebraic variety.*

Definition (Affine coordinate ring)**.** *Let* V/K *be a variety, then the affine coordinate ring of* V/K *is defined by*

$$K[V] := \frac{K[X_1, \ldots, X_n]}{I(V/K)}.$$

By theorem 4, we see that $K[V]$ *is a domain. Its quotient field* $\operatorname{Frac}(K[V])$ *is denoted by* $K(V)$*. Similarly we define,*

$$\bar{K}[V] := K[X]/I(V) \qquad \text{and} \qquad \bar{K}(V) := \operatorname{Frac}(\bar{K}[V]).$$

Example 32. *Consider* $f = y^2 - x^3 - 17 \in \bar{K}[x, y]$*. Let* $V = Z(f)$ *be its algebraic set. Let us look at the ideal* $I(V) = (y^2 - x^3 - 17)$ *and see how it is prime. Let* $A = \bar{K}[x]$ *and see that* A *is a UFD by 6. Now we can see* f *as an element of* $A[y]$*. Let* ω *be a root of* $\omega^3 + 17 = 0$ *in* $\bar{K}$ *and let* $\pi = x + \omega$*. We see that* π *divides* $-x^3 - 17$*, it doesn't divide* 1*, and* π^2 *doesn't divide* $-x^3 - 17$*. Apply 11 to see that* f *is irreducible in* $\operatorname{Frac}(A)[y]$*. This means it is also irreducible in* $\bar{K}[x, y]$*. Apply 10 to see that the ideal* $I(V) = (y^2 - x^3 - 17)$ *is prime, so* V *is an algebraic variety. Consider its affine coordinate ring* $\bar{K}[V]$*. The basic arithmetic inside* $\bar{K}[V]$ *is as usual, but modulo* $I(V)$*, for example,*

$$2y^2 + 34 \equiv 2(y^2 + 17) \equiv 2x^3 \pmod{(y^2 - x^3 - 17)}$$

and we usually write directly that $2y^2 + 34 = 2x^3$ *if it is clear that we're working in* $\bar{K}[V]$*.*[6]

[5] We can actually do better than this. A result called Hilbert's Nullstellensatz [3, I.1.3A] states that $I(V_I) = \sqrt{I}$, where $\sqrt{I}$ is the radical of I, i.e. $\sqrt{I} := \{x \in I \colon x^n \in I \text{ for some } n \in \mathbb{N}^*\}$. We rather mention it here but choose to not go through this result since it is too deep.

[6] This is basically the same as working in a general quotient ring, because, in fact, it's a quotient ring. The example is shown here because it was hard to manipulate things in $\bar{K}[V]$ as a beginner.

Definition (Dimension)**.** *We define* $\dim V := \operatorname{trdeg}_{\bar{K}}(\bar{K}(V))$ *and we call this the dimension of* V*.*

Example 33. *The dimension of* $\mathbb{A}^n$ *is* n*, because* $\bar{K}(\mathbb{A}^n) = \operatorname{Frac}(\bar{K}[\mathbb{A}^n]) = \operatorname{Frac}(\bar{K}[X_1, \ldots, X_n]/(0)) \cong \bar{K}(X_1, \ldots, X_n)$ *which has* $X_1, \ldots, X_n$ *as a transcendence basis over* $\bar{K}$*.*

Proposition 34. *Let* V *be a variety in* $\mathbb{A}^n$*. Then the dimension of* V *is* $n-1$ *if and only if there exists a nonconstant irreducible polynomial* $f \in \bar{K}[X_1, \ldots, X_n]$ *such that* $V = Z(f)$*.*

Proof. See [3, I.1.13]. □

Remark. *[11, I] defined smoothness of a point* P *on a variety* V *by the rank of the Jacobian of generators for* $I(V)$ *at* P*. Instead, to simplify things, we will not take this route and define the smoothness only for the case of curves in the next section.*

1.3.2 Projective Settings

Now let us consider the projective varieties. The following sequence of definitions might look contrived as first, but we will consider examples to see why it works.

Definition. *A polynomial* $f \in \bar{K}[X_0, \ldots, X_n]$ *is said to be* homogeneous *of degree* d *if*

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

An ideal I *of* $\bar{K}[X_0, \ldots, X_n]$ *is said to be homogeneous if it is generated by homogeneous polynomials.*

Definition (Projective algebraic set)**.** *For a homogeneous ideal* I *in* $\bar{K}[X_0, \ldots, X_n]$*, we denote by* V_I *the set*

$$\{P \in \mathbb{P}^n \colon f(P) = 0 \text{ for all homogeneous } f \in I\}.$$

Any set in this form is said to be a projective algebraic set*.*

Definition. *If* V *is a projective algebraic set, then we denote by* $I(V)$ *its homogeneous ideal, is the ideal generated by*

$$\{f \in \bar{K}[X_0, \ldots, X_n] \colon f \text{ is homogeneous and } f(P) = 0 \text{ for all } P \in V\}.$$

If $I(V)$ *can be generated by polynomials in* $K[X_0, \ldots, X_n]$*, we say that* V *is defined over* K *and write* V/K*. If this is the case, the set of* K*-rational points of* V *is*

$$V(K) = V \cap \mathbb{P}^n(K).$$

Remark. *In the projective settings, the reason we only consider homogeneous polynomial is because we want to say that the points*

$$(x_0, \ldots, x_n) \qquad \text{and} \qquad (\lambda x_0, \ldots, \lambda x_n)$$

are actually identical in $\mathbb{P}^n$ *(for any* $\lambda \neq 0$*), if* $f \in \bar{K}[X_0, \ldots, X_n]$ *is a polynomial, we really want* $f(x_0, \ldots, x_n)$ *to be zero if and only if* $f(\lambda x_0, \ldots, \lambda x_n)$ *is zero. Observe that this is achievable in the case of homogeneous polynomials.*

Example 35. *Consider the polynomial* $X^2 + Y^2 - Z^2$ *in* $\bar{K}[X, Y, Z]$*. It is homogeneous of degree* 2*. We can define a projective algebraic set* V *as*

$$\{[X, Y, Z] \in \mathbb{P}^2 \colon X^2 + Y^2 - Z^2 = 0 \text{ for all homogeneous } f \in (X^2 + Y^2 - Z^2)\}.$$

Observe that V *is defined over* K*. We will later see that* $V(K)$ *is "isomorphic"*[7] *to* $\mathbb{P}^1(K)$*. This is achievable by using the machinery from example 26 to see it in* $\mathbb{A}^2$ *and use geometrical intuition in* $\mathbb{R}^2$*.*

Consider that if $X^2+Y^2-Z^2 = 0$ *and we further assume* $Z \neq 0$*, we may write* $\left(\frac{X}{Z}\right)^2 + \left(\frac{Y}{Z}\right)^2 - 1 = 0$*, and, by the map* ϕ_Z^{-1} *from 26, we see that in* $U_Z = \{[X, Y, Z] \in \mathbb{P}^2 \colon Z \neq 0\}$*, we write* $[X, Y, Z]$ *as* $\left(\frac{X}{Z}, \frac{Y}{Z}\right)$ *in* $\mathbb{A}^2$ *and the previous equation becomes*

$$x^2 + y^2 = 1.$$

Which, over $\mathbb{A}^2(\mathbb{R})$*, is the unit circle. Now, we can try to make* $V(K)$ *isomorphic to* $\mathbb{P}^1(K)$ *by projecting the points on the circle onto a line, as follows (see figure 1.3). From the point* $(0, 1)$*,*

[7] It is not defined yet, but we will define this precisely.

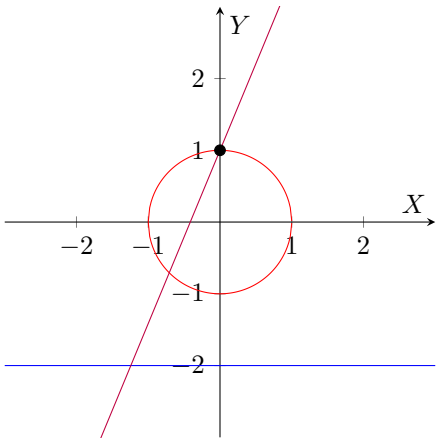

Figure 1.3: Projection from the unit circle onto a line

to any point on the circle (except $(0,1)$), there is a straight line (the figure shows a purple line) between the two points. This line hits the blue line at exactly one point. Our goal is to define this map algebraically. This can be done with basic geometry. Suppose we're considering point (x_P, y_P) on the unit circle, then suppose the line $L\colon Ax + By = C$ passes through $(0,1)$ and (x_P, y_P), then $B = C$ and $Ax_P + By_P = C$, i.e. $Ax_P = B(1 - y_P)$. Well if P is not $(0,1)$ then $y_P \neq 1$ so $B = \frac{Ax_P}{1-y_P}$. This allows us to write $L\colon Ax + \frac{Ax_P}{1-y_P}y = \frac{Ax_P}{1-y_P}$, i.e.

$$L\colon x + \frac{x_P}{1-y_P}y = \frac{x_P}{1-y_P}.$$

To see the coordinate where it hits the blue line (let us name this $Q = (x_Q, y_Q)$), plug in $y_Q = -2$ to see that $x_Q + \frac{x_P}{1-y_P}(-2) = \frac{x_P}{1-y_P}$, i.e. $x_Q = \frac{3x_P}{1-y_P}$. This properly define the map $(x_P, y_P) \mapsto x_Q$, i.e.

$$\phi\colon \begin{cases} \phi^{-1}(V(\mathbb{R}) \cap U_Z) \setminus \{(0,1)\} & \to \mathbb{R} \\ (x_P, y_P) & \mapsto \frac{3x_P}{1-y_P}. \end{cases}$$

to make it easier, we consider the inverse map ϕ^{-1} which sends t to $\left(\frac{6t}{t^2+9}, \frac{t^2-9}{t^2+9}\right)$. We extend ϕ^{-1} to $\mathbb{P}^1(K) \to V(K)$, defined by

$$[s,t] \mapsto \left[6st, t^2 - 9s^2, t^2 + 9s^2\right].$$

Observe that now we can check easily that for any $(s,t) \in K^2 \setminus \{0\}$, $(6st, t^2 - 9s^2, t^2 + 9s^2)$ is a solution to $X^2 + Y^2 = Z^2$. In particular, if $K = \mathbb{Q}$ then the formula $(6st, t^2 - 9s^2, t^2 + 9s^2)$ generates all rational Pythagorean triples! (by varying $[s,t] \in \mathbb{P}^1(\mathbb{Q})$).

Example 36. *([11, Example I.2.5]) The projective algebraic set*

$$V\colon X^2 + Y^2 = 3Z^2$$

is defined over $\mathbb{Q}$. However, $V(\mathbb{Q}) = \emptyset$. To see this, suppose there exists a rational solution $[x,y,z] \in V(\mathbb{Q})$. Since they are fractions of integers, $[x,y,z] = [x',y',z']$ for some $x', y', z' \in \mathbb{Z}$ with $\gcd(x',y',z') = 1$. Then $x'^2 + y'^2 = 3z'^2$, i.e. $x'^2 + y'^2$ is divisible by 3. But $k^2 \not\equiv 2 \pmod 3$ for all $k \in \mathbb{Z}$ so $x'^2 \not\equiv 2$ and $y'^2 \not\equiv 2$, i.e. $x'^2, y'^2 \equiv 0$ or 1. If at least one of them is 1, their sum wouldn't be divisible by 3, a contradiction. Therefore, they are both divisible by 3, i.e. $x' \equiv y' \equiv 0 \pmod 3$. So x'^2 and y'^2 are divisible by 3^2. Hence, by $x'^2 + y'^2 = 3z'^2$ we see that z'^2 is divisible by 3 so z' is also divisible by 3. This is a contradiction because we assumed $\gcd(x',y',z')$ to be 1. Therefore, $[x,y,z] \in V(\mathbb{Q})$ fails to exist.

This example allows us to play the same game generally. To show that $V(\mathbb{Q})$ is empty, it suffices to find a prime p and prove that no integer solution exists in mod p. (or even prime power p^r).

Example 37. *([10, page 205]) The converse to the previous statement is not true in general. Consider the equation*

$$V\colon 3X^3 + 4Y^3 + 5Y^3 = 0.$$

One can check that it has a solution mod p for any prime p, yet $V(\mathbb{Q}) = \emptyset$.

Definition (Projective variety)**.** *A projective algebraic set $V \subseteq \mathbb{P}^n$ is said to be a projective variety if $I(V)$ is prime in $\bar{K}[X_0, \ldots, X_n]$.*

Now let us reconsider a technique from example 26 used in example 35 and generalize it to the general case. Recall the bijection $\phi_i^{-1} \colon U_i \to \mathbb{A}^n$,

$$[x_0, \ldots, x_n] \mapsto \left(\frac{x_0}{x_i}, \ldots, \frac{x_n}{x_i} \right).$$

For a fixed i, later on we will identify $\mathbb{A}^n$ with U_i. So if $V \subseteq \mathbb{P}^n$ is a projective algebraic set, when we say $V \cap \mathbb{A}^n$, this means $\phi_i^{-1}(V \cap U_i)$. Notice that the sets $V \cap U_0, \ldots V \cap U_n$ cover V. If we fix i, one can *dehomogenize* the polynomial $f \in I(V) \subseteq \bar{K}[X_0, \ldots, X_n]$ to the polynomial $(Y_1, \ldots, Y_n) \mapsto f(Y_1, \ldots, Y_{i-1}, 1, Y_i, \ldots, Y_n)$. This is called *dehomogenization* with respect to X_i.

One can reverse the process, i.e., given $f \in \bar{K}[Y_1, \ldots, Y_n]$, define the polynomial $(X_0, \ldots, X_n) \mapsto X_i^d f\left(\frac{X_0}{X_i}, \ldots, \frac{X_{i-1}}{X_i}, \frac{X_{i+1}}{X_i}, \ldots \frac{X_n}{X_i}\right)$ where $d = \deg(f)$ is the smallest integer such that this map becomes a polynomial. We denote this polynomial by f^* and say that f^* is the homogenization of f with respect to X_i.

This gives the following diagram to homogenize/dehomogenize polynomials.

$$\begin{aligned} \bar{K}[X_0, \ldots, X_n] &\rightleftarrows \bar{K}[Y_1, \ldots, Y_n] \\ f(X_0, \ldots, X_n) &\mapsto f(Y_1, \ldots, Y_{i-1}, 1, Y_i, \ldots, Y_n) \\ X_i^d g\left(\frac{X_0}{X_i}, \ldots, \frac{X_{i-1}}{X_i}, \frac{X_{i+1}}{X_i}, \ldots \frac{X_n}{X_i}\right) &\hookleftarrow g(Y_1, \ldots, Y_n) \end{aligned}$$

Definition (Projective closure)**.** *Let $V \subseteq \mathbb{A}^n$ be an affine algebraic set with ideal $I(V)$. Consider*

$$V \hookrightarrow \mathbb{A}^n \xrightarrow{\phi_i} \mathbb{P}^n,$$

so we may say that $V \subseteq \mathbb{P}^n$ by this inclusion. The projective closure of V, denoted by $\bar{V}$, is the projective algebraic set whose $I(\bar{V})$ is generated by

$$\{f^*(X_0, \ldots, X_n) \colon f \in I(V)\}.$$

In practice, we may just define a projective variety just from functions in the affine settings, and then (implicitly) take the projective closure. For an affine variety V, the points in $\bar{V} \setminus V$ is said to be *points at infinity*.

Example 38. *([11, Example I.2.8]) Let V be the projective varity given by*

$$V \colon y^2 = x^3 + 17.$$

This actually means V is a variety in $\mathbb{P}^2$ given by

$$Y^2 Z = X^3 + 17Z^3$$

with the identification being

$$x = \frac{X}{Z}, \qquad y = \frac{Y}{Z}.$$

This variety has one point at infinity $[0, 1, 0]$. In particular,

$$V(\mathbb{Q}) = \{(x, y) \in \mathbb{A}(\mathbb{Q})^2 \colon y^2 = x^3 + 17\} \cup \{[0, 1, 0]\}.$$

Definition. *Let V/K be a projective variety and choose $\mathbb{A}^n \subseteq \mathbb{P}^n$ such that $V \cap \mathbb{A}^n \neq \emptyset$. The dimension of V is the dimension of $V \cap \mathbb{A}^n$. The function field $K(V)$ of V is $K(V \cap \mathbb{A}^n)$. Same for $\bar{K}(V)$, i.e. $\bar{K}(V) := \bar{K}(V \cap \mathbb{A}^n)$. Note that there are many choices to identify $\mathbb{A}^n$ with (i.e. each U_i), but here $K(V)$ and $\bar{K}(V)$ are all isomorphic for any choice of $\mathbb{A}^n$.*

1.3.3 Map Between Varieties

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

$$\phi \colon V_1 \to V_2, \qquad \phi = [f_0, \ldots, f_n]$$

where the functions $f_0, \ldots, f_n \in \bar{K}(V_1)$ have the property that for every point $P \in V_1$ at which $f_0, \ldots, f_n$ are all defined,

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

A rational map may not be defined everywhere in V_1. But we can still evaluate it at some other points. Consider the following example.

Example 39. *Let $V_1 \subseteq \mathbb{P}^2$ be generated by $X^2 + Y^2 = Z^2$. Let V_2 be $\mathbb{P}^1$. Consider the map $\phi = [f_0, f_1]$ where $f_0(X, Y, Z) = X$ and $f_1(X, Y, Z) = (Y - Z)/X$. We check that $\phi(P)$ lands in V_2 for all $P \in V_1$. Suppose $P = [X_P, Y_P, Z_P] \in V_1$ then $\phi(P) = [X_P, (Y_P - Z_P)/X_P]$. Observe that X_P and $(Y_P - Z_P)/X_P$ cannot both be zero at the same time, because $X_P = 0$ would make $(Y_P - Z_P)/X_P$ undefined. Hence $\phi(P)$ lands in $\mathbb{P}^1$ whenever X and $(Y - Z)/X$ are well-defined.*

This map ϕ is a rational map, but is not defined everywhere in V_1. However, we may replace $[f_0, f_1]$ by $[gf_0, gf_1]$ for some appropriate g. In this case, the map is not well-defined when $X_P = 0$, so let $g = \frac{X}{Y-Z}$ and see that $\phi = [gf_0, gf_1] = [\frac{X^2}{Y-Z}, 1] = [\frac{Z^2-Y^2}{Y-Z}, 1] = [-Y - Z, 1]$ is well-defined even when $X = 0$. By the covering of the two cases, ϕ is defined at all point in V_1.

Definition. *A rational map $\phi = [f_0, \ldots, f_n] \colon V_1 \to V_2$ is said to be* regular *or* defined *at point $P \in V_1$ if there is a function $g \in \bar{K}(V_1)$ such that each gf_i is regular at P, and there is some i such that $(gf_i)(P) \neq 0$. If such g exists, we set*

$$\phi(P) := [(gf_0)(P), \ldots, (gf_n)(P)].$$

We may take different g at different points $P \in V_1$. If ϕ is defined at P for all $P \in V_1$, we say ϕ is a morphism.

Definition. *Let V_1 and V_2 be varieties. We say that V_1 and V_2 are isomorphic and write $V_1 \cong V_2$ if there are morphisms $\phi \colon V_1 \to V_2$ and $\psi \colon V_2 \to V_1$ such that $\phi \circ \psi = \mathrm{id}_{V_2}$ and $\psi \circ \phi = \mathrm{id}_{V_1}$. We say that V_1/K and V_2/K are isomorphic over K if ϕ and ψ can be defined over K. Note that both ϕ and ψ have to be morphisms, not just rational maps.*

Example 40. *([11, Example I.3.8]) Consider the varieties*

$$V_1 \colon X^2 + Y^2 = Z^2 \qquad \text{and} \qquad V_2 \colon X^2 + Y^2 = 3Z^2.$$

They are not isomorphic over $\mathbb{Q}$ since $V_2(\mathbb{Q}) = \emptyset$ but $V_1(\mathbb{Q}) \neq \emptyset$. However, they are isomorphic over $\mathbb{Q}(\sqrt{3})$ with an isomorphism given by $\phi \colon V_2 \to V_1, \phi = [X, Y, \sqrt{3}Z]$. In general, they are isomorphic.

We will consider maps between varieties extensively in a more specialized setting of curves, in the next section.

1.4 Curves

This section corresponds to chapter II of [11]. The goal of this section is to introduce the concept of a curve and get to the concept of "genus", since elliptic curves are curves of genus one with a specified base point.

Definition (Curve)**.** *A curve is a projective variety of dimension one.*

Before going to the actual content, let us supply the missing but very important part about "smoothness".

1.4.1 Smoothness

First let us consider the intuition behind smoothness by the following example.

Example 41. *Consider figure 1.4. We want to distinguish the first case of smooth curve from the other two next cases containing a* singular *point at $(0, 0)$. Note that the geometric view here is shown only for intuition only and concerns affine algebraic set over $\mathbb{R}$. In general, we extend this to any variety over any field, not just $\mathbb{R}$.*

Here we used a simplified definition of smoothness at a point, which is only valid for the case of curves.

Definition. *Let C be a curve and let $P \in C$. We say C is* not smooth *or* singular *at P if, by choosing $\mathbb{A}^n \subseteq \mathbb{P}^n$ containing P and writing $C \cap \mathbb{A}^n$ as $Z(f)$ for some irreducible nonconstant $f \in \bar{K}[X_1, \ldots, X_n]$, we have*

$$\partial_{X_1} f(P) = \partial_{X_2} f(P) = \cdots = \partial_{X_n} f(P) = 0$$

and say that C is smooth *or* nonsingular *at P otherwise (i.e. if some of the $\partial_{X_i} f(P)$ is nonzero).*

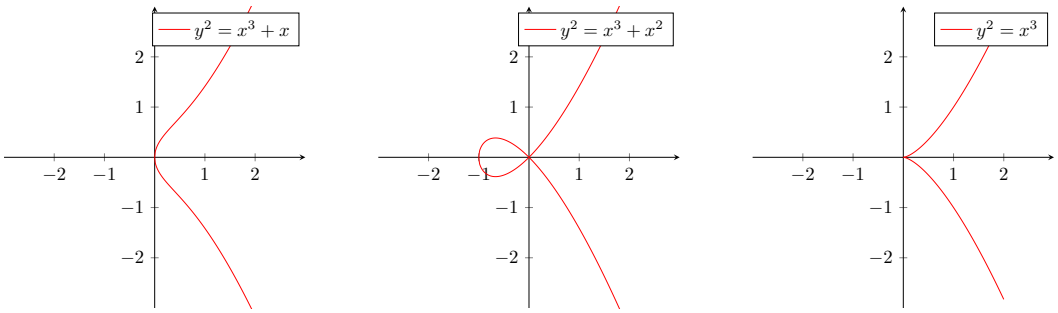

Figure 1.4: A smooth curve, a curve with a node, and a curve with a cusp

This definition makes sense because, considering the example 41, at $(0,0)$, the reason that it is not smooth is that we cannot define the tangent properly at that point. This happens when the partial derivatives $\partial_{X_i} f$ vanish at that point. However, we will consider another, perhaps even more useful, albeit abstract, characterization of smoothness.

Definition (The ideal M_P)**.** *Let V be an affine variety. For each point $P \in V$, define M_P as*

$$\{f \in \bar{K}[V] \colon f(P) = 0\}.$$

M_P is a maximal ideal because

$$\phi \colon \begin{cases} \bar{K}[V]/M_P & \to \bar{K} \\ f & \mapsto f(P) \end{cases}$$

is an isomorphism (this is actually applying the first isomorphism theorem for rings), and we apply theorem 3.

For the projective case, define M_P as $\{f \in \bar{K}[V \cap \mathbb{A}^n] \colon f(P) = 0\}$. Note that one needs to choose a good choice of $\mathbb{A}^n$ so that $P \in \mathbb{A}^n$. Not every choice of $\mathbb{A}^n$ makes sense for this definition.

Proposition 42. *M_P/M_P^2 is a $\bar{K}$-vector space.*

Proof. We use the induced addition in M_P/M_P^2. Now, the multiplication by scalar $\bar{K}$ can be done by the fact that $\bar{K}[V]/M_P \cong \bar{K}$ so $(M_P^2 + aM_P)(M_P + b) = M_P^2 + abM_P \in M_P/M_P^2$ properly, for all $a, b \in \bar{K}[V]$. □

This following proposition is the useful characterization of smoothness.

Proposition 43. *Let C be a curve, and let $V = C \cap \mathbb{A}^n$ be an affine variety. A point P is nonsingular if and only if*

$$\dim_{\bar{K}} M_P/M_P^2 = \dim V.$$

Proof. [3, I.5.1]. Note that here we only define the notion of singularity for curves, but it actually holds for any affine variety V. □

Now we can work with smoothness not only in the concrete gradient form geometrically, but also algebraically in terms of M_P.

1.4.2 Order At A Point

Definition (Local ring)**.** *The local ring of V at P, denoted by $\bar{K}[V]_P$, is the localization of $\bar{K}[V]$ at M_P (compare this with example 23), i.e.*

$$\bar{K}[V]_P := \{F \in \bar{K}(V) \colon F = f/g \text{ for some } f, g \in \bar{K}[V] \text{ with } g(P) \neq 0\}.$$

Notice that the functions in this local ring are regular at P. For the case of curves, we denote by $\bar{K}[C]_P$ the local ring $\bar{K}[C \cap \mathbb{A}^n]_P$ at P.[8]

Now, we play the same game from example 23 with curves, i.e. claim that $\bar{K}[C]_P$ is a DVR, see that M_P is the maximal ideal, define the natural valuation $\operatorname{ord}_P \colon \bar{K}[C]_P \to \mathbb{N} \cup \{\infty\}$, and extend it to $\operatorname{ord}_P \colon \bar{K}(C) \to \mathbb{Z} \cup \{\infty\}$.

Proposition 44. *Let C be a curve and let P be a smooth point on C, then $\bar{K}[C]_P$ is a DVR.*

[8] Same remark as before: one needs to choose $\mathbb{A}^n$ such that $P \in \mathbb{A}^n$, otherwise this won't make sense!

Proof. Apply proposition 43 to see that M_P/M_P^2 is a $\bar{K}$-vector space of dimension one. Now, let us prove that M_P is the unique maximal ideal of $\bar{K}[C]_P$. Suppose I is a proper ideal of $\bar{K}[C]_P$. Let $F \in I$. If $F(P) = 0$ then $F \in M_P$. Now if $F(P) \neq 0$ then by definition of $\bar{K}[C]_P$, $F = f/g$ with $g(P) \neq 0$ so $f(P) \neq 0$ also. Consider $g/f \in \bar{K}[C]_P$ also, hence I absorbs g/f, i.e. $Fg/f \in I$. But $Fg/f = (f/g)(g/f) = 1$ so $I = \bar{K}[C]_P$, contradicting the fact that I is proper. This proves that all proper ideals of $\bar{K}[C]_P$ are contained in M_P, i.e., M_P is the unique maximal ideal of $\bar{K}[C]_P$.

Now we're left with proving that $\bar{K}[C]_P$ is a PID. The fact that it is a domain is already mentioned in the definition of affine coordinate ring. Let us show that every ideal in $\bar{K}[C]_P$ is principal. Suppose I is a nonzero proper ideal of $\bar{K}[C]_P$. Let S be the generating set of I with the minimum cardinality. Let us show that S is a singleton by contradiction. Suppose $s, s' \in S$ are two different element. Then $M_P^2 + s \in M_P/M_P^2$ can be taken as a basis of M_P/M_P^2. Now write $M_P^2 + s' = (M_P^2 + s)(M_P + \lambda)$ for some $\lambda \in \bar{K}[C]_P$, so

$$M_P^2 + s' = M_P^2 + sM_P + s\lambda.$$

This means s' can be written as a multiple of s, hence a contradiction. Therefore, S is a singleton, hence $\bar{K}[C]_P$ is a PID. This completes the proof. □

This also shows that the natural valuation ord_P is defined by

$$\operatorname{ord}_P(f) = \max\{n \in \mathbb{N} \cup \{\infty\} \colon f \in M_P^n\}$$

for all $f \in \bar{K}[C]_P$, and this is extended to $\operatorname{ord}_P \colon \bar{K}(C) \to \mathbb{Z} \cup \{\infty\}$. We call this the *order* of f at P. A uniformizer of P is an element $t \in \bar{K}(C)$ such that $\operatorname{ord}_P(t) = 1$. It need not be unique, but it always exists because $\bar{K}[C]_P \subseteq \bar{K}(C)$ is a PID.

Definition. *For $P \in C$, $f \in \bar{K}(C)$. We say that f has a pole at P if $\operatorname{ord}_P(f) < 0$. We say that f has a zero at P if $\operatorname{ord}_P(f) > 0$. If $\operatorname{ord}_P(f) \geq 0$ then f is regular at P and we can evaluate $f(P)$. Otherwise, $f(P) = \infty$.*

Example 45. *Consider the curve defined by $Y^2 = X^3 + X$. $P = (0, 0)$ is smooth. Now, we see that $X, Y \in M_P$, so M_P is the ideal generated by (X, Y) in $\bar{K}[V]$. Now, we see that M_P^2 is generated by X^2, XY, Y^2. But in M_P, however, $X = Y^2 - X^3 \in M_P$ so M_P/M_P^2 can be generated by Y alone. This also tells us that $Y \in M_P$ but $Y \notin M_P^2$, so $\operatorname{ord}_P(Y) = 1$. Now, since $Y^2 = X^3 + X$, we have*

$$\operatorname{ord}_P(Y^2) = \operatorname{ord}_P(X^3 + X)$$
$$2\operatorname{ord}_P(Y) = \operatorname{ord}_P(X) + \operatorname{ord}_P(X^2 + 1).$$

But $X^2 + 1$ evaluated at P is nonzero and also not a pole, so $\operatorname{ord}_P(X^2 + 1) = 0$. This gives $\operatorname{ord}_P(X) = 2$. Now, $\operatorname{ord}_P(2Y^2 - X) = \operatorname{ord}_P(Y^2 + Y^2 - X) = \operatorname{ord}_P(Y^2 + X^3)$. Since $\operatorname{ord}_P(Y^2) = 2$ but $\operatorname{ord}_P(X^3) = 6$, apply proposition 22 (iii) to see that $\operatorname{ord}_P(2Y^2 - X) = 2$.

Proposition 46. *Let C be a smooth curve and $f \in \bar{K}(C)$ with $f \neq 0$. Then there are only finitely many points of C at which f has a pole or zero. Further, if f has no poles, then $f \in \bar{K}$.*

Proof. See [11, II.1.2]. □

Proposition 47. *Let C/K be a curve, and let $t \in K(C)$ be a uniformizer at some nonsingular point $P \in C(K)$. Then $K(C)/K(t)$ is a finite separable extension.*

Proof. See [11, II.1.4] □

1.4.3 Maps Between Curves

We start with this useful proposition.

Proposition 48. *([11, II.2.1]) Let C be a curve. Let V be a projective variety. Let $P \in C$ be a smooth point. Let $\phi \colon C \to V$ be a rational map. Then ϕ is regular at P. In particular, if C is smooth, then ϕ is a morphism.*

Proof. Suppose $V \subseteq \mathbb{P}^N$ and write $\phi = [f_0, \ldots, f_N]$ with $f_i \in \bar{K}(C)$. Let $t \in \bar{K}(C)$ be a uniformizer at P. Let $n = \min_{0 \leq i \leq N} \operatorname{ord}_P(f_i)$. Then $\operatorname{ord}_P(t^{-n} f_i) \geq 0$ for all i, and $\operatorname{ord}_P(t^{-n} f_j) = 0$ for some j, so the coordinates $[t^{-n} f_0, t^{-n} f_1, \ldots, t^{-n} f_N]$ can be evaluated at P, so $\phi(P)$ is defined, i.e. ϕ is regular at P. □

(This corresponds to [11, Example II.2.2]) Now, if C/K is smooth, anything in $K(C)$ can be identified with a function from C to $\mathbb{P}^1$ as follows. Consider a given function $f \in K(C)$. Define a rational map, which we still denote by the same symbol f, as follows:

$$f\colon \begin{cases} C & \to \mathbb{P} \\ P & \mapsto [f(P), 1] \end{cases}$$

where if $f(P)$ is a pole, then $f(P) = [1, 0]$. By the previous proposition, this map is a morphism.

Conversely, for a given rational map $\phi = [f, g]$ mapping $C \to \mathbb{P}^1$, either $g = 0$ so $\phi(P) = [1, 0]$ for all $P \in C$, or $g \neq 0$ and so $\phi = [f/g, 1]$, where $\frac{f}{g} \in K(C)$. Denoting the former map by ∞, we have a correspondence

$$\begin{aligned} K(C) \cup \{\infty\} &\to \{\text{maps } C \to \mathbb{P}^1 \text{ defined over } K\} \\ f &\mapsto [f, 1] \\ f/g &\leftarrow\!\shortmid [f, g] \end{aligned}$$

Theorem 49. *Let $\phi\colon C_1 \to C_2$ be a morphism of curves, then ϕ is either constant or surjective.*

Proof. See [11, II.2.3]. □

Definition. *Let C_1/K and C_2/K be curves and let $\phi\colon C_1 \to C_2$ be a rational map defined over K. We define*

$$\phi^*\colon \begin{cases} K(C_2) & \to K(C_1) \\ f & \mapsto f \circ \phi \end{cases}$$

then it is not hard to see that ϕ^* is an injection fixing K. This is (implicitly)[9] called the induced injection of function fields of ϕ. Later on we will not talk about this but rather just write a star after any rational map to state this induced injection of function fields.

Theorem 50. *([11, II.2.4]) Let C_1/K and C_2/K be curves.*

(a) Let $\phi\colon C_1 \to C_2$ be a nonconstant map defined over K. Then $K(C_1)/\phi^*(K(C_2))$ is a finite extension.

(b) Let $\iota\colon K(C_2) \to K(C_1)$ be an injection of function fields fixing K. Then there exists a unique nonconstant map $\phi\colon C_1 \to C_2$ such that $\iota = \phi^*$.

(c) Let $\mathbb{K} \subseteq K(C_1)$ be a subfield such that $K(C_1)/\mathbb{K}/K$ is a valid tower of extensions. Then there exists a smooth curve C', unique up to isomorphism, and a nonconstant map $\phi\colon C_1 \to C'$ defined over K such that $\phi^*K(C') = \mathbb{K}$.

Proof. See [11, II.2.4]. □

Definition. *Let $\phi\colon C_1 \to C_2$ be a map of curves defined over K. If ϕ is constant, we define the degree of ϕ to be 0. Otherwise, we say that ϕ is a finite map, and define the degree to be*

$$\deg \phi := |K(C_1)\colon \phi^*K(C_2)|$$

as the degree of field extension. We say that ϕ is separable, inseparable, or purely inseparable if the extension $K(C_1)/\phi^*K(C_2)$ has the corresponding property. We denote the separable and inseparable degree by $\deg_s \phi$ and $\deg_i \phi$, respectively.

Theorem 51. *Let C_1 and C_2 be smooth curves, and let $\phi\colon C_1 \to C_2$ be a map of degree one, then it is an isomorphism of curves.*

Proof. See [11, II.2.4.1]. □

Now we move to the ramification index.

Definition (Ramification index)**.** *Let $\phi\colon C_1 \to C_2$ be a nonconstant map of smooth curves, and let $P \in C_1$. The ramification index of ϕ at P, denoted by $e_\phi(P)$, is $\operatorname{ord}_P(\phi^* t_{\phi(P)})$, where $t_{\phi(P)} \in K(C_2)$ is a uniformizer at $\phi(P)$. Note that $e_\phi(P) \geq 1$. We say that ϕ is unramified at P if $e_\phi(P) = 1$, and ϕ is unramified if it is unramified at every point of C_1.*

[9] This is a non-standard term.

Let us prove that this is well-defined, i.e., we can take any uniformizer $t_{\phi(P)}$ and the ramification index would still be the same.

Proof. Suppose $t_{\phi(P)}$ and $\widetilde{t}_{\phi(P)}$ are uniformizers at $\phi(P)$, then apply 21 and 24 to see that there exists $\lambda \in \bar{K}^\times$ such that $\widetilde{t}_{\phi(P)} = \lambda t_{\phi(P)}$. Now we see that

$$\begin{aligned}\phi^*\widetilde{t}_{\phi(P)} &= \phi^*(\lambda t_{\phi(P)}) \\ &= (\phi^*\lambda)(\phi^* t_{\phi(P)}).\end{aligned}$$

And so $\operatorname{ord}_P(\phi^*\widetilde{t}_{\phi(P)}) = \operatorname{ord}_P(\phi^*\lambda) + \operatorname{ord}_P(\phi^* t_{\phi(P)})$. But $\phi^*\lambda$ is a constant, hence $\operatorname{ord}_P(\phi^*\lambda) = 0$ and this completes the proof. □

Example 52. *(A part of [11, Example II.2.9]) Consider the map*

$$\phi\colon \begin{cases}\mathbb{P}^1 & \to \mathbb{P}^1 \\ [X,Y] & \mapsto [X^3(X-Y)^2, Y^5].\end{cases}$$

Then ϕ is ramified at some points. Let us look at $[0,1]$ and see that $e_\phi([0,1]) = \operatorname{ord}_{[0,1]}(\phi^*(t_{\phi([0,1])}))$. Well $\phi([0,1]) = [0,1]$ so now $\phi^*(t_{\phi([0,1])}) = t_{[0,1]} \circ \phi$. Now choose $t_{[0,1]} = X$ and see that

$$\begin{aligned}\operatorname{ord}_{[0,1]}(\phi^*(t_{\phi([0,1])})) &= \operatorname{ord}_{[0,1]}(t_{[0,1]}([X^3(X-Y)^2, Y^5]) \\ &= \operatorname{ord}_{[0,1]}(X^3(X-Y)^2) \\ &= 3\operatorname{ord}_{[0,1]}(X) + 2\underbrace{\operatorname{ord}_{[0,1]}(X-Y)}_{0} \\ &= 3.\end{aligned}$$

Proposition 53. *Let $\phi\colon C_1 \to C_2$ be a nonconstant map of smooth curves.*

(a) For every $Q \in C_2$,

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

(b) For all but finitely many $Q \in C_2$,

$$\#\phi^{-1}(Q) = \deg_s(\phi).$$

(c) Let $\psi\colon C_2 \to C_3$ be another nonconstant map of smooth curves. Then for all $P \in C_1$,

$$e_{\psi\circ\phi}(P) = e_\phi(P) e_\psi(\phi P).$$

(d) Let $f \in \bar{K}(C_2)^*$, and let $P \in C_1$, then

$$\operatorname{ord}_P(\phi^* f) = e_\phi(P)\operatorname{ord}_{\phi(P)}(f).$$

Proof. See [11, II.2.6] for (a), (b), and (c). (d) is taken from Exercise 2.2. in [11]. Let us prove it here. We assume the result of (c) and consider that f induces a map $C_2 \to \mathbb{P}^1$. Apply (c) to see that

$$\begin{aligned}e_{f\circ\phi}(P) &= e_\phi(P) e_f(\phi(P)) \\ \operatorname{ord}_P((f\circ\phi)^* t_{(f\circ\phi)(P)}) &= e_\phi(P)\operatorname{ord}_{\phi(P)}(f^* t_{(f\circ\phi)(P)}) \\ \operatorname{ord}_P(t_{(f\circ\phi)(P)} \circ f \circ \phi) &= e_\phi(P)\operatorname{ord}_{\phi(P)}(t_{(f\circ\phi)(P)} \circ f).\end{aligned}$$

Now choose $t_{(f\circ\phi)(P)}$ to be just $X \in K[X] \subseteq K[\mathbb{P}^1]$ which induces the identity function, so we have

$$\operatorname{ord}_P(f\circ\phi) = e_\phi(P)\operatorname{ord}_{\phi(P)}(f)$$

which is

$$\operatorname{ord}_P(\phi^* f) = e_\phi(P)\operatorname{ord}_{\phi(P)}(f)$$

as we wished to show. □

Example 54. *We continue from the example 52 and see that $e_\phi([1,1]) = 2$. Also, we see that $\phi^{-1}([0,1]) = \{[0,1],[1,1]\}$ so we have*

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

which satisfies proposition 53.

1.4.4 Divisors

The concept of divisors might looks artificial at first, but turns out to be very useful later on. We define the abelian group of divisors of C as a group of formal sums, i.e. each element can be written as

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

where $n_P \in \mathbb{Z}$ for all $P \in C$ and there exists only a finite number of $P \in C$ such that $n_P \neq 0$. It is a formal sum, meaning that the terms $n_P(P)$ and $n_Q(Q)$ don't interact. Another way to think of this is to see it as a map $D\colon C \mapsto \mathbb{Z}$ such that $C \setminus \ker(D)$ is finite. The set (actually abelian group) of all divisors of C is denoted by $\mathrm{Div}(C)$.

Definition (Degree)**.** *Let $D \in \mathrm{Div}(C)$ and write $D = \sum_{P\in C} n_P(P)$. The degree of D, denoted by $\deg(D)$, is defined as $\sum_{P\in C} n_P$. Note that this is a well-defined integer since the P's with nonzero n_P are finitely many.*

The divisors of D of degree 0 form a subgroup of $\mathrm{Div}(D)$, denoted by $\mathrm{Div}^0(D)$.

Definition (Divisor of a function)**.** *Assume C is smooth, and $f \in \bar{K}(C)^*$, then we define*

$$\mathrm{div}(f) := \sum_{P\in C} \mathrm{ord}_P(f)(P) \in \mathrm{Div}(D).$$

This is well-defined due to 46 and 22(iv), so div *is $\bar{K}(C)^* \to \mathrm{Div}(C)$.*

Example 55. *Consider the curve $C\colon y^2 = x^3 + x$, and let us look at $\mathrm{div}(y^2 - 10)$. By definition, we want to look at the order of f at each point P on C. Now if we evaluate f at $P = (x_P, y_P)$, it is $y_P^2 - 10$. If $y_P^2 - 10 \neq 0$ then $f \notin M_P$, so $\mathrm{ord}_P(y^2 - 10) = 0$. The only interesting points (point with nonzero order) are points where $y_P^2 - 10 = 0$ and points at infinity. The points where $y_P^2 - 1 = 0$ and $y_P^2 = x_P^3 + x_P$ is exactly when $x_P^3 + x_P = 10$. We will not take the geometric path, but rather try to see M_P and M_P^2 algebraically. We see that M_P is generated by $x - x_P$ and $y - y_P$. So M_P^2 is generated by $(x - x_P)^2, (x - x_P)(y - y_P)$, and $(y - y_P)^2$. Now we can see that $y_P^2 = 10$ for any $P \in C$ satisfying $y^2 - 10 = 0$. Since we want to evaluate $\mathrm{ord}_P(y^2 - 10)$, we see that $y^2 - 10 = y^2 - y_P^2 = (y - y_P)(y + y_P) \in M_P$. However, $y^2 - y_P^2 \equiv 2y^2 + 2yy_P \equiv 2y_P(y_P + y) \pmod{M_P^2}$ which is nonzero, so $y^2 - 10 \notin M_P^2$. This tells us that $\mathrm{ord}_P(y^2 - 10) = 1$ for 6 points of P on C (3 different x_P coordinates, each with 2 different y_P). Next, let us consider points at infinity.*

In this case, by taking projective closure, we see that the equation $Y^2Z = X^3 + XZ^2$ has only one point at infinity, namely $P_\infty := [0, 1, 0]$. So we pick $\mathbb{A}^2 := U_Y$ and dehomogenize to $Z/Y = X^3/Y^3 + XZ^2/Y^3$, i.e. $z = x^3 + xz^2$. The point P_∞ is now $(0, 0)$ in the (x, z) coordinate system. Now, M_P is generated by x and z, M_P^2 is generated by x^2, xz, and z^2. But $z^2 = x^6 + 2x^4z^2 + x^2z^4$ is divisible by x^2, and $xz \equiv x(x^3 + xz^2)$ is divisible by x^2 also, so M_P^2 can be generated by only x^2. Now M_P^3 is generated by x^3 and x^2z, but once again, x^2z can be generated by x^3 so $M_P^3 = (x^3)$. Once again, $M_P^4 = (x^4)$. Now, we want to evaluate $\mathrm{ord}_{P_\infty}(y^2 - 10)$, but $y^2 - 10 = \frac{1}{Z^2}(Y^2 - 10Z^2) = \frac{Y^2}{Z^2}(1 - 10\frac{Z^2}{Y^2}) = \frac{1-10z^2}{z^2}$, so let us evaluate $\mathrm{ord}_{P_\infty}(\frac{1-10z^2}{z^2}) = \underbrace{\mathrm{ord}_{P_\infty}(1 - 10z^2)}_{0} - \mathrm{ord}_{P_\infty}(z^2) = -2\,\mathrm{ord}_{P_\infty}(z)$. Now, we see that

$$\begin{aligned}
\mathrm{ord}_{P_\infty}(z) &= \mathrm{ord}_{P_\infty}(x(x^2 + z^2)) \\
&= \mathrm{ord}_{P_\infty}(x(x^2 + x^2(x^2 + z^2)^2)) \\
&= \mathrm{ord}_{P_\infty}(x^3(1 + (x^2 + z^2)^2)) \\
&= \mathrm{ord}_{P_\infty}(x^3) + \underbrace{\mathrm{ord}_{P_\infty}(1 + (x^2 + z^2)^2)}_{0}
\end{aligned}$$

and we can clearly see that $x^3 \in M_P^3$ but $x^3 \notin M_P^4$, so $\mathrm{ord}_{P_\infty}(z)$ must be 3, so $\mathrm{ord}_{P_\infty}(y^2 - 10)$ is actually -6. This shows that

$$\mathrm{div}(y^2 - 10) = (P_1) + (P_2) + (P_3) + (P_4) + (P_5) + (P_6) - 6(P_\infty).$$

where $P_1, \ldots, P_6$ are the six points on $C \cap \mathbb{A}^2$ satisfying $Y^2 - 10 = 0$. Observe that the image of $\deg \circ \mathrm{div}$ is 0 in this case. We will prove this later.

Definition (Principal divisors and linear equivalence)**.** *A divisor $D \in \mathrm{Div}(C)$ is said to be* principal *if it is an image of* div*. Two divisors D_1 and D_2 are* linearly equivalent *if $D_1 - D_2$ is principal. If this is the case, we write $D_1 \sim D_2$. It is easy to see that $\sim$ defines an equivalence relation on $\mathrm{Div}(C)$. The set of principal divisors forms a subgroup*[10]*, and the quotient of $\mathrm{Div}(C)$ by this subgroup is called the* divisor class group *or* Picard group*, written as $\mathrm{Pic}(C)$.*[11]

Definition. *Let C_1 and C_2 be smooth curves. In the same way that $\phi\colon C_1 \to C_2$ induces $\phi^*\colon \bar{K}(C_2) \to \bar{K}(C_1)$, it also induces $\phi^*\colon \mathrm{Div}(C_2) \to \mathrm{Div}(C_1)$, defined (for each point) by*

$$(Q) \mapsto \sum_{P \in \phi^{-1}(Q)} e_\phi(P)(P)$$

and extend this $\mathbb{Z}$-linearly to all of $\mathrm{Div}(C_2)$.

Proposition 56. *Let C be a smooth curve, let $f \in \bar{K}(C)$ be a nonconstant function, then*

$$\mathrm{div}(f) = f^*((0) - (\infty)).$$

Proof. We have

$$\begin{aligned}
\mathrm{div}(f) &= \sum_{P \in C} \mathrm{ord}_P(f)(P) \\
&= \sum_{P \in C, \mathrm{ord}_P(f) > 0} \mathrm{ord}_P(f)(P) + \sum_{P \in C, \mathrm{ord}_P(f) < 0} \mathrm{ord}_P(f)(P) \\
&= \sum_{P \in f^{-1}(0)} \mathrm{ord}_P(f)(P) + \sum_{P \in f^{-1}(\infty)} \mathrm{ord}_P(f)(P) \\
&= \sum_{P \in f^{-1}(0)} \mathrm{ord}_P(f^* t_{f(P)})(P) - \sum_{P \in f^{-1}(\infty)} \mathrm{ord}_P(f^* t_{f(P)})(P) \\
&= \sum_{P \in f^{-1}(0)} e_f(P)(P) - \sum_{P \in f^{-1}(\infty)} e_f(P)(P) \\
&= f^*((0)) - f^*((\infty)) \\
&= f^*((0) - (\infty)),
\end{aligned}$$

where we choose $t_{f(P)}$ to be $X \in \bar{K}(\mathbb{P}^1)$, which is id on $\mathbb{P}^1$ if $P \in f^{-1}(0)$, and note that when $P \in f^{-1}(\infty)$,

$$\mathrm{ord}_P(f) = -\mathrm{ord}_P\left(\frac{1}{f}\right) = -\mathrm{ord}_P(t_{f(P)} \circ f) = -\mathrm{ord}_P(f^* t_{f(P)})$$

where $t_{f(P)}$ is chosen to be $\frac{1}{X} \in \bar{K}(\mathbb{P}^1)$. □

Proposition 57. *Let C be a smooth curve and let $f \in \bar{K}(C)^*$.*

(a) $\mathrm{div}(f) = 0$ *if and only if $f \in \bar{K}^*$.*

(b) $\deg \mathrm{div}(f) = 0$ *for all $f \in \bar{K}(C)^*$.*

Proof. (a) If $\mathrm{div}(f) = 0$ then f has no poles and no zeros so it must be constant. Now if $f \in \bar{K}^*$ then clearly $\mathrm{ord}_P(f) = 0$ everywhere (for each $P \in C$), so $\mathrm{div}(f) = 0$.

(b) Let $f \in \bar{K}(C)^*$. Then (from a middle step of the proof of the previous proposition),

$$\mathrm{div}(f) = \sum_{P \in f^{-1}(0)} e_f(P)(P) - \sum_{P \in f^{-1}(\infty)} e_f(P)(P).$$

So, by applying 53(a), we have

$$\deg \mathrm{div}(f) = \sum_{P \in f^{-1}(0)} e_f(P) - \sum_{P \in f^{-1}(\infty)} e_f(P) = \deg(f) - \deg(f) = 0.$$

This completes the proof. □

[10] Since it's abelian, all subgroups are normal, so the quotient is well-defined.

[11] Note that the set $\mathrm{Pic}(C)$ is equal to $\mathrm{Div}(C)/\sim$, but we define it this way to enable the group structure.

From a given $\phi\colon C_1 \to C_2$, we also define $\phi_*\colon \mathrm{Div}(C_1) \to \mathrm{Div}(C_2)$ as

$$(P) \mapsto (\phi P)$$

and extend $\mathbb{Z}$-linearly to all of $\mathrm{Div}(C_1)$.

The following is a collection of useful identities. We will not be proving the result here but would refer to [11, II.3.6].

Proposition 58. *Let $\phi\colon C_1 \to C_2$ be nonconstant map of smooth curves.*

(a) $\deg(\phi^* D) = (\deg \phi)(\deg D)$ *for all* $D \in \mathrm{Div}(C_2)$.

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

(c) $\deg(\phi_* D) = \deg D$ *for all* $D \in \mathrm{Div}(C_1)$.

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

(e) $\phi_* \circ \phi^*$ *acts as multiplication by* $\deg \phi$ *on* $\mathrm{Div}(C_2)$.

(f) If $\psi\colon C_2 \to C_3$ *is another such map, then*

$$(\psi \circ \phi)^* = \phi^* \circ \psi^* \qquad \text{and} \qquad (\psi \circ \phi)_* = \psi_* \circ \phi_*.$$

Proof. See [11, II.3.6]. □

1.4.5 Differentials

Differential forms on a curve is another important concept. However, we will not make much use here right now. The goal of this subsection is only to properly define the prerequisites for the Riemann–Roch theorem, which will be of more important focus, for now.

Definition. *Let C be a curve. For every $f \in \bar{K}(C)$, we attach a symbol* d *to construct* $\mathrm{d}f$. *This gives the set*

$$\{\mathrm{d}f\colon f \in \bar{K}(C)\}.$$

Now, we quotient out this set by the following rules of equivalence:

(i) $\mathrm{d}(x+y) \sim \mathrm{d}x + \mathrm{d}y$ *for all* $x, y \in \bar{K}(C)$.

(ii) $\mathrm{d}(xy) \sim x\mathrm{d}y + y\mathrm{d}x$ *for all* $x, y \in \bar{K}(C)$.

(iii) $\mathrm{d}a \sim 0$ *for all* $a \in \bar{K}$.

The remaining quotient set is called the space of (meromorphic) differential forms, and is denoted by Ω_C. It is a $\bar{K}(C)$-vector space.

Note that it might look confusing at first. It looks like d can be an operator or some map from $\bar{K}(C)$ to $\bar{K}(C)$. However, from this definition we still don't have any value associated to that, i.e. $\mathrm{d}f$ is just the symbol d attached to f. In [9, II.3] this is denoted by $\mathrm{Diff}_k(K)$, not $\mathrm{Der}_k(K, E)$.

Definition. *Same as before, for a given nonconstant map $\phi\colon C_1 \to C_2$ of curves, we define*

$$\phi^*\colon \begin{cases} \Omega_{C_2} & \to \Omega_{C_1} \\ \sum f_i \mathrm{d}x_i & \mapsto \sum (\phi^* f_i)\mathrm{d}(\phi^* x_i). \end{cases}$$

Proposition 59. *Let C be a curve, then Ω_C is a 1-dimensional $\bar{K}(C)$-vector space.*

Proof. See [11, II.4.2]. (Other results are omitted because they're not used here.) □

Proposition 60. *Let C be a curve, let $P \in C$, and let $t \in \bar{K}(C)$ be a uniformizer at P.*

(a) For every $\omega \in \Omega_C$, there exists a unique function $g \in \bar{K}(C)$ depending on ω and t, satisfying $\omega = g\mathrm{d}t$. We denote g by $\omega/\mathrm{d}t$.

(b) Let $f \in \bar{K}(C)$ be regular at P. Then $\mathrm{d}f/\mathrm{d}t$ is also regular at P.

(c) Let $\omega \in \Omega_C$ with $\omega \neq 0$. The quantity $\mathrm{ord}_P(\omega/\mathrm{d}t)$ depends only on ω and P, independent of the choice of uniformizer t. We call this the order of ω at P and write $\mathrm{ord}_P(\omega)$.

(d) Let $x, f \in \bar{K}(C)$ with $x(P) = 0$, and let $p = \mathrm{char}(K)$. Then

$$\mathrm{ord}_P(f\mathrm{d}x) = \mathrm{ord}_P(f) + \mathrm{ord}_P(x) - 1, \text{if } p = 0 \text{ or } p \nmid \mathrm{ord}_P(x),$$
$$\mathrm{ord}_P(f\mathrm{d}x) \geq \mathrm{ord}_P(f) + \mathrm{ord}_P(x), \text{if } p > 0 \text{ and } p \mid \mathrm{ord}_P(x).$$

(e) Let $\omega \in \Omega_C$, with $\omega \neq 0$. Then $\mathrm{ord}_P(\omega) = 0$ for all but finitely many $P \in C$.

Proof. See [11, II.4.3]. □

Definition. *We define the divisor of a differential in the same way. Let $\omega \in \Omega_C$ with $\omega \neq 0$, then*

$$\mathrm{div}(\omega) := \sum_{P \in C} \mathrm{ord}_P(\omega)(P) \in \mathrm{Div}(C).$$

Note that now $\deg \mathrm{div}(\omega)$ *need not be zero.*

Observe that, for any nonzero differentials $\omega_1, \omega_2 \in \Omega_C$, since the vector space is of dimension one, we can write $\omega_1 = \lambda\omega_2$ for some $\lambda \in \bar{K}(C)$. This gives $\mathrm{div}(\omega_1) = \mathrm{div}(\lambda) + \mathrm{div}(\omega_2)$, i.e. $\mathrm{div}(\omega_1) \sim \mathrm{div}(\omega_2)$. This means the image by div of anything in Ω_C is constant in $\mathrm{Pic}(C)$.

Definition. *We define that image to be* the canonical divisor class *of Ω_C. Any divisor in this class is called a canonical divisor, denoted by $K_C \in \mathrm{Div}(C)$. (When we write K_C without context, we mean that we can take any element from the canonical divisor class as K_C)*

1.4.6 The Riemann–Roch Theorem

In this subsection, we'll present the main tool in the algebraic geometry toolbox, which will be used to prove the group law for elliptic curves. The Riemann–Roch theorem is that powerful tool. It states the relation between the dimension of a divisor and its degree. It also allows us to observe an invariant called "genus" on a curve. For further intuitive information, see [2].

Definition. *We put a partial order on* $\mathrm{Div}(C)$ *defined as: For all $D_1, D_2 \in \mathrm{Div}(C)$ with*

$$D_1 = \sum_{P \in C} n_P(P) \qquad \text{and} \qquad D_2 = \sum_{P \in C} m_P(P),$$

we say $D_1 \geq D_2$ if $n_P \geq m_P$ for all $P \in C$.

Definition. *For a differential $\omega \in \Omega_C$. We say that it is regular (or holomorphic) if* $\mathrm{div}(\omega) \geq 0$, *and we say that it is nonvanishing if* $\mathrm{div}(\omega) \leq 0$.

Definition. *Let $D \in \mathrm{Div}(C)$, then we define*

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

and observe that it is a $\bar{K}$-vector space (recall that $\mathrm{ord}_P(f+g) \geq \min(\mathrm{ord}_P(f), \mathrm{ord}_P(g))$ so it is closed by addition, and scalar multiplication does nothing to the divisor). We denote by $\ell(D)$ its dimension, i.e. $\ell(D) := \dim_{\bar{K}} \mathcal{L}(D)$.

Proposition 61. *Let $D \in \mathrm{Div}(C)$.*

(a) If $\deg D < 0$, then $\mathcal{L}(D) = \{0\}$ and $\ell(D) = 0$.

(b) The vector space $\mathcal{L}(D)$ is finite dimensional.

(c) If $D' \in \mathrm{Div}(C)$ such that $D' \sim D$, then $\mathcal{L}(D') \cong \mathcal{L}(D)$ and $\ell(D') = \ell(D)$.

Proof. See [11, II.5.2]. □

Proposition 62. *([11, II.5.3]) Recall that $K_C = \mathrm{div}(\omega)$ for any $\omega \in \Omega_C$. By definition, $\mathrm{div}(f) \geq -\mathrm{div}(\omega)$ for all $f \in \mathcal{L}(K_C)$, i.e. $\mathrm{div}(f\omega) \geq 0$ for all $f \in \mathcal{L}(K_C)$. In other words, $f\omega$ is holomorphic. Conversely if $f\omega$ is holomorphic then $f \in \mathcal{L}(K_C)$. For every holomorphic $\omega' \in \Omega_C$, there exists a unique $f_{\omega'} \in \bar{K}(C)$ such that $\omega' = f_{\omega'}\omega$, and so this thing is holomorphic, so $f_{\omega'} \in \mathcal{L}(K_C)$. The converse also works the same way, so we obtain an isomorphism of $\bar{K}$-vector spaces*

$$\mathcal{L}(K_C) \cong \{\omega' \in \Omega_C : \omega' \text{ is holomorphic}\}.$$

The dimension $\ell(K_C)$ is an important invariant of the curve C. Now we're ready to state the remarkable result.

Theorem 63 (Riemann–Roch)**.** *Let C be a smooth curve and let K_C be a canonical divisor on C. There exists an integer $g \geq 0$, called the genus of C, such that for every divisor $D \in \operatorname{Div}(C)$,*

$$\ell(D) - \ell(K_C - D) = \deg D - g + 1.$$

Proof. See [7, Chapter 1].[12] □

Corollary 64. *(a) $\ell(K_C) = g$.*

(b) $\deg K_C = 2g - 2$.

(c) If $\deg D > 2g - 2$, then $\ell(D) = \deg D - g + 1$.

Proof. This is actually very straightforward by plugging in different values for D to the Riemann–Roch theorem. □

Theorem 65 (Hurwitz)**.** *Let $\phi\colon C_1 \to C_2$ be a nonconstant separable map of smooth curves of genera g_1 and g_2 respectively. Then*

$$2g_1 - 2 \geq (\deg \phi)(2g_2 - 2) + \sum_{P \in C_1} (e_\phi(P) - 1).$$

Further, equality holds if and only if one of the following is true.

1. $\operatorname{char}(K) = 0$
2. $\operatorname{char}(K) = p > 0$ *and p does not divide $e_\phi(P)$ for all $P \in C_1$.*

Proof. See [11, II.5.9]. □

We end this subsection quite early to devote the big example application of the Riemann–Roch theorem on elliptic curves to the next chapter.

[12] This looks like the most accessible treatment of the Riemann–Roch theorem, though the author haven't gone through the book yet.

Chapter 2

Elliptic Curves

Instead of going through the traditional approach of introducing elliptic curves through Weierstrass equations, we will consider an alternative approach here to show the power of the machinery from the previous chapter.

2.1 Working With Elliptic Curves

Before beginning to work, let us consider some characterizations of $\mathbb{P}^1$ that would help us in the later proofs.

Proposition 66. *([11, Exercise 2.5]) Let C be a smooth curve. Prove that the following are equivalent over $\bar{K}$.*

(i) C is isomorphic to $\mathbb{P}^1$.

(ii) C has genus 0.

(iii) There exists distinct points $P, Q \in C$ satisfying $(P) \sim (Q)$.

Proof. (i) $\Rightarrow$ (ii). Suppose C is isomorphic to $\mathbb{P}^1$, then let $t \in \bar{K}(\mathbb{P}^1)$ be the coordinate function on $\mathbb{P}^1$, then for all $\alpha \in \bar{K}$, $\operatorname{ord}_\alpha(\mathrm{d}t) = \operatorname{ord}_\alpha(\mathrm{d}\underbrace{(t-\alpha)}) = 0$ since $t - \alpha$ is a uniformizer at α. Now for the point at infinity, $\operatorname{ord}_\infty(\mathrm{d}t) = \operatorname{ord}_\infty(-t^2\mathrm{d}\left(\frac{1}{t}\right)) = -2$. Therefore, $\operatorname{div}(\mathrm{d}t) = -2(\infty)$. Now, for any $\omega \in \Omega_{\mathbb{P}^1}$, there exists $g \in \bar{K}(C)$ such that $\omega = g\mathrm{d}t$, so $\operatorname{div}(\omega) = \operatorname{div}(g\mathrm{d}t)$ is still -2. This means all of $\Omega_{\mathbb{P}^1}$ cannot be holomorphic, so $\mathcal{L}(K_C) = \{0\}$ by 62, and $\ell(K_C) = 0$. Apply 64(a) to see that the genus is zero.

(ii) $\Rightarrow$ (iii) Suppose C has genus 0. Take any points $P \neq Q$ in C and consider $D = (P) - (Q)$. Then $\deg D = 0 \geq -1$, so apply 64(c) to see that $\ell(D) = 1$. This mean $\mathcal{L}(D) \setminus \{0\} \neq \emptyset$. Take any $f \in \mathcal{L}(D)$ then $\operatorname{div}(f) \geq -D = (Q) - (P)$. But $\deg \operatorname{div}(f) = 0$, so $\operatorname{ord}_Q(f)$ cannot be strictly greater than one, so it must be one. Now $\operatorname{ord}_P(f)$ also cannot be strictly greater than -1, so it must be -1. This means $\operatorname{div}(f) = (Q) - (P)$, so $(P) \sim (Q)$.

(iii) $\Rightarrow$ (i) Suppose there exists distinct $P, Q \in C$ such that $(P) \sim (Q)$. Then there exists $f \in \bar{K}(C)^*$ such that $\operatorname{div}(f) = (Q) - (P)$. This induces a function $f\colon C \mapsto \mathbb{P}^1$. Since f is nonconstant, it is surjective. Now consider $D = (0)$ and use 58(a) so

$$\deg(f^*((0))) = (\deg f)(\deg(0)).$$

Now $f^*((0)) = \sum_{R \in f^{-1}(0)} e_f(R)(R)$ but the only zero of f is Q, so $f^*((0)) = e_f(Q)(Q)$. It is easy to see that $e_f(Q) = 1$ by definition and by $\operatorname{ord}_Q(f) = 1$. So we conclude that $\deg f = 1$. Apply 51 to see that f is an isomorphism between C and $\mathbb{P}^1$. □

2.1.1 Curves Of Genus One

It would be more precise to say "smooth curves of genus one with a specified base point". We consider such smooth curve C of genus one[1] with the base point $P_0 \in C$ and consider the following.

[1] Curves of genus zero are the conics and straight lines, which are simpler than elliptic curves. This is why sometimes we say that elliptic curves are the simplest non-trivial curves.

Proposition 67. *([11, Exercise 2.6(a)]) For all $P, Q \in C$, there exists a unique $R \in C$ such that*

$$(P) + (Q) \sim (R) + (P_0).$$

We denote this point R by $\sigma(P, Q)$.

Proof. Define $D := (P) + (Q) - (P_0) \in \mathrm{Div}(C)$. By 64 (c), since $\deg D = 1 > 2g - 2 = 0$, we have $\ell(D) = \deg D + g - 1 = 1$. This means $\mathcal{L}(D) \setminus \{0\}$ is nonempty. Pick any $f \in \mathcal{L}(D) \setminus \{0\}$ then $\mathrm{div}(f) \geq -D = (P_0) - (P) - (Q)$. In particular, there are three cases: (i) $\mathrm{div}(f) = (P_0) - (P)$, (ii) $\mathrm{div}(f) = (P_0) - (Q)$, (iii) there exists $R \in C$ such that $\mathrm{div}(f) = (P_0) + (R) - (P) - (Q)$. For the first two cases, this means $(P_0) \sim (P)$ and $(P_0) \sim (Q)$ respectively, so one can take R to be Q and P respectively. And for the third case, this precisely means $(P) + (Q) \sim (R) + (P_0)$. Hence the existence is proved.

Now, let us prove the uniqueness. Suppose R_1 and R_2 satisfy $(P) + (Q) \sim (R_1) + (P_0) \sim (R_2) + (P_0)$. So $(R_1) \sim (R_2)$. If they're different, then we can apply 66 and arrive at the contradiction that C has genus 0. Hence $R_1 = R_2$. □

Proposition 68. *([11, Exercise 2.6(b)]) The set C with the map $\sigma \colon C \times C \to C$ makes an abelian group with identity element P_0.*

Proof. For associativity, we want to show that for all $P, Q, R \in C$, $\sigma(P, \sigma(Q, R)) = \sigma(\sigma(P, Q), R)$. Let $S = \sigma(Q, R)$, let $T = \sigma(P, S)$, let $U = \sigma(P, Q)$, and let $V = \sigma(U, R)$. We have

$$\begin{aligned}(Q) + (R) &\sim (S) + (P_0)\\ (P) + (S) &\sim (T) + (P_0)\\ (P) + (Q) &\sim (U) + (P_0)\\ (U) + (R) &\sim (V) + (P_0).\end{aligned}$$

This gives $(P) + (Q) + (R) \sim (T) + 2(P_0)$ and $(P) + (Q) + (R) \sim (V) + 2(P_0)$, i.e. $(T) \sim (V)$. Apply 66 to see that if $T \neq V$ then the genus must be 0, a contradiction, so $T = V$.

Now the commutativity and identity is obvious. Let us prove the inverse. Let us show that for all $P \in C$, there exists $Q \in C$ such that $\sigma(P, Q) = P_0$. Consider another structure $\sigma_P \colon C \times C \to C$ with the same definition but the base point is now P. Then let $Q := \sigma_P(P_0, P_0)$ so that $(P_0) + (P_0) \sim (Q) + (P)$. This means $\sigma(P, Q) = P_0$, by uniqueness of $\sigma(P, Q)$. Hence completes the proof. □

Proposition 69. *The abelian group made by σ is isomorphic to $\mathrm{Pic}^0(C)$.*

Proof. Define $\kappa \colon C \to \mathrm{Pic}^0(C)$ as $P \mapsto [(P) - (P_0)]_\sim$. Let us show that κ is a group isomorphism from (C, σ) to $(\mathrm{Pic}^0(C), +)$.

First, κ is injective because if $[(Q) - (P_0)]_\sim = [(P) - (P_0)]_\sim$ then $(Q) \sim (P)$ and apply 66 to see that it can't be different. Now, suppose $[D]_\sim \in \mathrm{Pic}^0(C)$ with $D \in \mathrm{Div}^0(C)$. Write $D = \sum_{Q \in C} n_Q(Q)$ with $\sum_Q n_Q = 0$. Consider $D' = D + (P_0)$ so $\deg D' = 1$. Apply 64(c) to see that $\ell(D') = 1$. Now pick any $f \in \mathcal{L}(C) \setminus \{0\}$ and observe that $\mathrm{div}(f) \geq -D' = -D - (P_0)$. Since $\deg \mathrm{div}(f) = 0$, $\mathrm{div}(f)$ must be $-D - (P_0) + (P)$ for some $P \in C$. So $[(P) - (P_0)]_\sim = [D]_\sim$, i.e. $\kappa(P) = [D]_\sim$. This proves the bijectivity.

Now κ is a homomorphism because

$$\kappa(\sigma(P, Q)) = [\sigma(P, Q) - (P_0)]_\sim = [(P) + (Q) - 2(P_0)]_\sim = \kappa(P) + \kappa(Q).$$

This completes the proof. □

The previous results proves the group law of an elliptic curve, assuming Riemann–Roch theorem. If the curve C is defined over K and $P_0 \in K$, we say that the elliptic curve is defined over K and write C/K.[2]

Now a very useful aspect of elliptic curves is that it can be viewed through Weierstrass equations, i.e., every elliptic curve (E, O) defined over K is isomorphic to a curve $C/K \subseteq \mathbb{P}^2$ with $P_0 \in C(K)$

Proposition 70. *Let E/K be an elliptic curve with base point $O \in E(K)$. Then, there exists functions $x, y \in K(E)$ such that the map*

$$\phi \colon \begin{cases} E & \to \mathbb{P}^2 \\ \phi & = [x, y, 1] \end{cases}$$

[2] Actually, by convention, we will use the letter E instead of C for elliptic curves and it will be clear by context that we're referring to elliptic curves rather than general curves.

gives an isomorphism between E/K onto a curve C given by a Weierstrass equation

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

with coefficients $a_1, a_2, a_3, a_4, a_6 \in K$ and $\phi(O) = [0, 1, 0]$. The functions x and y are called Weierstrass coordinates for the elliptic curve E.

Proof. See [11, III.3.1]. □

2.1.2 Weierstrass Equations

Since every elliptic curve can be written in the homogeneous form

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

with the base point $O = [0, 1, 0]$, we can devote some of our time to study the particular curves in this form. Note that curves defined in the Weierstrass equation might not be elliptic curves if some point is singular.

Definition. *We often rewrite the Weierstrass equation in the non-homogeneous form*

$$E\colon y^2 + a_1xy + a_3y = x^3a_2x^2 + a_4x + a_6,$$

since we've already known that there is only single undefined point at infinity, and it can be dealt with easily.

Now, we define the following quantities.

b_2	$a_1^2 + 4a_2$
b_4	$2a_4 + a_1a_3$
b_6	$a_3^2 + 4a_6$
b_8	$a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$
c_4	$b_2^2 - 24b_4$
c_6	$-b_2^3 + 36b_2b_4 - 216b_6$
Δ	$-b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$
j	c_4^3/Δ
ω	$\frac{\mathrm{d}x}{2y+a_1x+a_3} = \frac{\mathrm{d}y}{3x^2+2a_2x+a_4-a_1y}$

If $\mathrm{char}(K) \neq 2$, the substitution $y \mapsto \frac{1}{2}(y - a_1x - a_3)$ in E gives the equation of the form

$$E\colon y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6.$$

One can verify that $4b_8 = b_2b_6 - b_4^2$ and $1728\Delta = c_4^3 - c_6^2$.

Furthermore, if $\mathrm{char}(K) \neq 2, 3$, then the substitution $(x, y) \mapsto \left(\frac{x-3b^2}{36}, \frac{y}{108}\right)$ gives an even simpler equation

$$E\colon y^2 = x^3 - 27c_4x - 54c_6.$$

Proposition 71. *(a) The curve given by a Weierstrass equation satisfies:*

(i) It is nonsingular if and only if $\Delta \neq 0$.

(ii) It has a node if and only if $\Delta = 0$ and $c_4 \neq 0$.

(iii) It has a cusp if and only if $\Delta = c_4 = 0$.

In cases (ii) and (iii), there is only one singular point.

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

(c) Let $j_0 \in \bar{K}$, then there exists an elliptic curve defined over $K(j_0)$ whose j-invariant is equal to j_0.

Proof. See [11, III.1.4]. The details are mostly tedious calculations. □

Now, the next result tells us that singular and nonsingular curves given by Weierstrass equation behave very differently.

Proposition 72. *If E is singular then $E \cong \mathbb{P}^1$. Note that we cannot apply 51 because E is not smooth.*

Proof. See [11, III.1.6]. □

2.1.3 Geometric Group Law

The group law of an elliptic curve can also be given geometrically. We use Bézout's theorem [3, I.7.8] to see that a straight line intersects an elliptic curve at exactly three points (counted with multiplicity). If P and Q is given, we draw a line L passing through P and Q, such that it hits another point R on the elliptic curve. Now we draw another line between R and O (the base point), so that it hits another point S. We define $P+Q$ to be S. Consider figure 2.1.

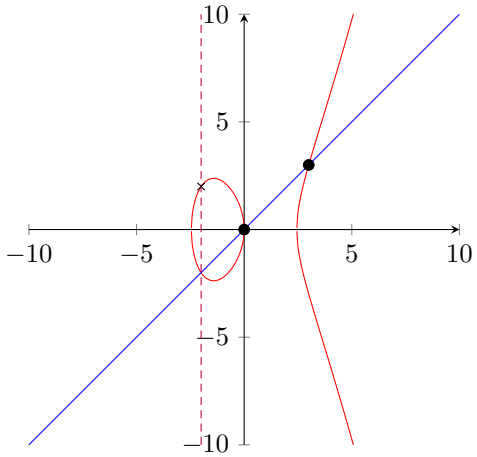

Figure 2.1: An elliptic curve with two specified points an a line passing through them, where O is the point at infinity. The sum of the two black dots is denoted by $\times$ at $(-2,2)$.

The geometric view is viewed in the classical $\mathbb{R}^2$, but the algebraic terms can be lifted to $\mathbb{P}^2$ in general. It turns out that the geometric group law and the algebraic group law give the same output [11, III.3.4e]. The summary of the elementary algebraic terms defined from geometric group law can be seen in [11, III.2.3]. We're not writing it here because it is too long.

2.2 Isogenies

Definition. *Let E_1 and E_2 be elliptic curves with base points O_1 and O_2 respectively. A morphism $\phi\colon E_1 \to E_2$ is said to be an isogeny if $\phi(O_1) = O_2$. Since every morphism on smooth curves are either constaint or surjective, ϕ satisfies either $\phi(E_1) = \{O_2\}$ or $\phi(E_1) = E_2$. The only case that $\phi(E_1) = \{O_2\}$ is the zero map (mapping everything to O_2). Hence other isogenies are nonconstant and surjective. We, once again, obtain the usual induced injection*

$$\phi^*\colon \bar{K}(E_2) \to \bar{K}(E_1),$$

with the same old definition of degree, separable degree, inseparable degree, separable map, inseparable map, purely inseparable map. By convention, we set the degree of the zero map to be zero: $\deg[0] = 0$. *Hence,*

$$\deg(\psi \circ \phi) = \deg(\psi)\deg(\phi) \text{ for all chains of isogenies } E_1 \xrightarrow{\phi} E_2 \xrightarrow{\psi} E_3.$$

Now, isogenies form groups. We denote by $\mathrm{Hom}(E_1, E_2)$ the group of isogenies from E_1 to E_2. In particular, $\mathrm{End}(E) := \mathrm{Hom}(E, E)$ and we introduce multiplication by composition. This forms a ring $\mathrm{End}(E)$. Refer to [11, III.4.8] for a proof of the distributive law. The invertible elements of $\mathrm{End}(E)$ forms the automorphism group, denoted by $\mathrm{Aut}(E)$. We use the usual subscript $(\cdot)_K$ to talk about the set of isogenies defined over K.

2.3 The m-torsion subgroup of E

Consider the multiplication-by-m map on an elliptic curve E, defined as follows (for $m \in \mathbb{N}^*$):

$$[m]\colon \begin{cases} E & \to E \\ P & \mapsto \underbrace{P + P + \cdots + P}_{m} \end{cases}$$

and extend this to the case of negative integers and zero.

We see that $[m]$ is nonconstant ([11, III.4.2a]) whenever $m \neq 0$. Next is a relatively trivial result but wasn't mentioned in [11].

Proposition 73. *Let $[m]$ be the multiplication-by-m map with $m \neq 0$. Let $\phi \in \mathrm{End}(E)$, then*

$$[m] \circ \phi = \phi \circ [m].$$

Proof. Since ϕ is a group homomorphism, we see that

$$\phi(\underbrace{P + P + P + \cdots + P}_{m}) = \underbrace{\phi(P) + \phi(P) + \cdots + \phi(P)}_{m},$$

so $\phi([m]P) = [m]\phi(P)$. One easily extend this to the case of negative integers. This completes the proof. □

Definition (m-torsion subgroup)**.** *Let $m \in \mathbb{N}^*$ and define the m-torsion subgroup as*

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

The torsion subgroup is the group of points of finite order

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

Example 74. *([4, Exercise 3]) Let k be an algebraically closed field with characteristic different from 2. Let E be an elliptic curve over k with Weierstrass equation $Y^2Z = X^3 + aXZ^2 + bZ^3$ with neutral element $O = [0, 1, 0]$. We shall see that the group $E[2]$ has cardinality 4, and is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. One way to get the direct result is to apply [11, III.6.4b] directly. However, let us go through this example without using the heavy machinery from the invariant differential and the dual isogeny.*

Consider $f \colon [X, Y, Z] \mapsto Y^2Z - X^3 - aXZ^2 - bZ^3$. We consider the geometric group law and see that $[2]P = O$ if and only if the tangent at P doesn't intersect the curve at other points than infinity. Since the point at infinity is $[0, 1, 0]$, we seek for P such that the tangent line at P is vertical, i.e., $\partial_Y f = 2YZ = 0$. This is the case if $Y = 0$ or $Z = 0$. If $Z = 0$, it's the point $O = [0, 1, 0]$ at infinity. Now if $Y = 0$, then we're left with solving $f([X, 0, Z]) = -X^3 - aXZ^2 - bZ^3 = 0$. Let $x = \frac{X}{Z}$ and this would be $x^3 + ax + b = 0$, an ordinary cubic equation. Since k is algebraically closed, we have three roots for x. Observe that $(x^3 + ax + b)' = 3x^2 + a$ so the roots are simple. Now we're able to deduce that the cardinality of $E[2]$ is 4, consisting of a point at infinity and three points as the set of solutions to this equation. Now observe that $E[2]$ is abelian, so it must be isomorphic to either $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. The former is not possible since the order of points are at most 2, so the generator of the group doesn't exist. Therefore, $E[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

By the result of [11, III.6.4b], we have that if either $\mathrm{char}(K) = 0$ or ($\mathrm{char}(K) = p > 0$ and $p \nmid m$), then

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

This can be proven through the tools of invariant differentials and dual isogeny. However, we will not walk through that path here since this piece of writing is already too long. Instead, let us present a few interesting properties (without proof) to conclude about what we can say about elliptic curves in general.

Before moving on, let us consider an important result here.

Theorem 75. *Let E be an elliptic curve and let $D = \sum n_P(P) \in \mathrm{Div}(E)$. Then D is a principal divisor if and only if*

$$\sum_{P \in E} n_P = 0 \qquad \text{and} \qquad \sum_{P \in E} [n_P]P = 0.$$

Proof. See [11, III.3.5]. □

2.4 Further Properties

This section is outside the goal. It is presented here to show some structures that can be studied within the context of elliptic curves in general.

2.4.1 The Weil Pairing

Assume m is coprime to p, as $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, the goal of this subsection is to define a determinant on $E[m]$. An initial guess would be to fix a basis $\{T_1, T_2\}$ and define

$$\det\colon \begin{cases} E[m] \times E[m] & \to \mathbb{Z}/m\mathbb{Z} \\ (aT_1 + bT_2, cT_1 + dT_2) & \mapsto ad - bc. \end{cases}$$

There are two problems with this approach.

- The value of the determinant depends on the choice of basis.
- (More serious) It is not Galois-invariant, i.e., with $\sigma \in G_{\bar{K}/K}$, $\det(P^\sigma, Q^\sigma)$ and $\det(P, Q)^\sigma$ might not be the same.

Instead, we can define the Weil pairing as follows.

Definition. *Let $T \in E[m]$, then take $T' \in E$ such that $[m]T' = T$. By 75, there is a function $g \in \bar{K}(E)$ satisfying*

$$\operatorname{div}(g) = [m]^*(T) - [m]^*(O)$$

However, even if we translate $g(X)$ to $g(X+S)$, its divisor is still the same, so $\frac{g(X+S)}{g(X)}$ is a constant. We observe that this quantity does not depend on X. Therefore, observe that, if we set $X_i \leftarrow X + [i]S$ then

$$\left(\frac{g(X+S)}{g(X)}\right)^m = \prod_{i=0}^{m-1} \frac{g(X_i+S)}{g(X_i)} = \frac{g(X+[m]S)}{g(X)} = 1,$$

so $\frac{g(X+S)}{g(X)}$ is a root of unity. This allows us to define

$$e_m\colon \begin{cases} E[m] \times E[m] & \to \boldsymbol{\mu}_m \\ (S, T) & \mapsto \frac{g(X+S)}{g(X)}, \end{cases}$$

which we call this by the Weil pairing.

2.4.2 The Endomorphism Ring

Let E be an elliptic curve, then $\operatorname{End}(E)$ turns out to fall into few categories. The main result of this subsection is the following.

Theorem 76. *([11, III.9.4]) For E/K, $\operatorname{End}(E)$ is either*

- *$\mathbb{Z}$,*
- *an order in an imaginary quadratic field,*
- *an order in a quaternion algebra.*

If $\operatorname{char}(K) = 0$, then only the first two are possible.

Proof. See [11, III.9.4]. □

2.4.3 The Automorphism Group

The main result of this subsection, given by [11, III.10], is that the automorphism group $\operatorname{Aut}(E)$ can be classified by order as follows.

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

Proof. See [11, III.10.1]. □

Bibliography

[1] M. A. Armstrong. *Basic Topology*. Springer New York, 1983.

[2] Rok Gregoric. Baby's first riemann–roch, 2020.

[3] Robin Hartshorne. *Algebraic Geometry*. Springer New York, 1977.

[4] Diego Izquierdo. MAT 562 - Feuille d'exercices 5.

[5] Diego Izquierdo. *MAA303: Algebra and arithmetic*. 2022.

[6] Neal Koblitz. Elliptic curve cryptosystems. *Mathematics of Computation*, 48(177):203–209, 1987.

[7] Serge Lang. *Introduction to Algebraic and Abelian Functions*. Springer New York, 1982.

[8] Victor S. Miller. Use of elliptic curves in cryptography. In Hugh C. Williams, editor, *Advances in Cryptology — CRYPTO '85 Proceedings*, pages 417–426, Berlin, Heidelberg, 1986. Springer Berlin Heidelberg.

[9] Alain Robert. *Elliptic Curves*. Springer Berlin Heidelberg, 1973.

[10] Ernst S. Selmer. The Diophantine equation $ax^3 + by^3 + cz^3 = 0$. *Acta Mathematica*, 85(none):203 – 362, 1951.

[11] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Springer New York, 2009.

[12] Joseph H. Silverman and John T. Tate. *Rational Points on Elliptic Curves*. Springer International Publishing, 2015.

[13] The Stacks project authors. The stacks project. https://stacks.math.columbia.edu, 2023.