Algebraic Geometry of Curves

Andrew Kobin

Fall 2016
## Contents

0 Introduction

0.1 Geometry and Number Theory ............................................. 2
0.2 Rational Curves ......................................................... 4
0.3 The \( p \)-adic Numbers .................................................. 6

1 Algebraic Geometry ....................................................... 9

1.1 Affine and Projective Space ............................................. 9
1.2 Morphisms of Affine Varieties ....................................... 15
1.3 Morphisms of Projective Varieties ................................... 19
1.4 Products of Varieties .................................................... 21
1.5 Blowing Up ............................................................... 22
1.6 Dimension of Varieties .................................................. 24
1.7 Complete Varieties ...................................................... 26
1.8 Tangent Space ............................................................ 27
1.9 Local Parameters ......................................................... 32

2 Curves ............................................................................. 33

2.1 Divisors ......................................................................... 34
2.2 Morphisms Between Curves ............................................. 36
2.3 Linear Equivalence ......................................................... 38
2.4 Differentials ................................................................. 40
2.5 The Riemann-Hurwitz Formula ....................................... 42
2.6 The Riemann-Roch Theorem ......................................... 43
2.7 The Canonical Map ....................................................... 45
2.8 Bézout’s Theorem .......................................................... 45
2.9 Rational Points of Conics ................................................ 47

3 Elliptic Curves .................................................................... 52

3.1 Weierstrass Equations .................................................... 53
3.2 Moduli Spaces .............................................................. 55
3.3 The Group Law .............................................................. 56
3.4 The Jacobian ................................................................. 58

4 Rational Points on Elliptic Curves ...................................... 61

4.1 Isogenies ........................................................................ 62
4.2 The Dual Isogeny ........................................................... 65
4.3 The Weil Conjectures ..................................................... 67
4.4 Elliptic Curves over Local Fields ................................... 69
4.5 Jacobians of Hyperelliptic Curves ................................... 75

5 The Mordell-Weil Theorem .................................................. 77

5.1 Some Galois Cohomology ................................................ 77
5.2 Selmer and Tate-Shafarevich Groups ............................... 80
5.3 Twists, Covers and Principal Homogeneous Spaces ............ 84
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.4 Descent</td>
<td>89</td>
</tr>
<tr>
<td>5.5 Heights</td>
<td>97</td>
</tr>
<tr>
<td>6 Elliptic Curves and Complex Analysis</td>
<td>99</td>
</tr>
<tr>
<td>6.1 Elliptic Functions</td>
<td>99</td>
</tr>
<tr>
<td>6.2 Elliptic Curves</td>
<td>105</td>
</tr>
<tr>
<td>6.3 The Classical Jacobian</td>
<td>110</td>
</tr>
<tr>
<td>6.4 Jacobians of Higher Genus Curves</td>
<td>115</td>
</tr>
<tr>
<td>7 Complex Multiplication</td>
<td>117</td>
</tr>
<tr>
<td>7.1 Classical Complex Multiplication</td>
<td>117</td>
</tr>
<tr>
<td>7.2 Torsion and Rational Points</td>
<td>120</td>
</tr>
<tr>
<td>7.3 Class Field Theory with Elliptic Curves</td>
<td>123</td>
</tr>
</tbody>
</table>
0 Introduction

These notes come from a course in algebraic geometry and elliptic curves taught by Dr. Lloyd West at the University of Virginia in Fall 2016. The first part of the notes are a survey of the main concepts in algebraic geometry, with an emphasis on curves (i.e. varieties of dimension 1). Key topics include:

- Affine and projective varieties
- Dimension
- Singular and nonsingular points and tangent spaces
- Morphisms between varieties
- Intersection theory
- Divisors
- Genus
- The Riemann-Hurwitz theorem and Riemann-Roch theorem
- Jacobian of a curve

The main algebraic geometry reference used is Shafarevich’s *Basic Algebraic Geometry 1*.

The second part of the course covers the basic results in the arithmetic geometry of elliptic curves, including:

- Abelian varieties and isogenies
- Models over local and global fields
- Moduli
- Reduction mod $p$
- Zeta functions
- Statement of the Weil conjectures for curves
- Heights
- Descent (à la Fermat)
- Hasse’s local-global principle
- Torsors and Galois actions
- Galois cohomology in degrees 0, 1 and 2
- Selmer and Tate-Shafarevich groups

Additional topics include the application of elliptic curves to cryptography, higher genus curves and $L$-functions. The main text used is Silverman’s *Arithmetic of Elliptic Curves*.  

---

1
0.1 Geometry and Number Theory

Consider the following questions:

**Question 1.** Describe the set of all right triangles with integer sides.

**Question 2.** A rational number \( n \) is said to be congruent if there exists a rational right triangle with area \( n \). Which rational numbers \( n \) are congruent?

We will see that Question 1 is easy to answer, while Question 2 is still unsolved. The fundamental difference lies in the geometry of each situation.

**Definition.** We say \((a, b, c) \in \mathbb{Z}^3\) is a **pythagorean triple** if \( a^2 + b^2 = c^2\).

For example, \((3, 4, 5)\) and \((5, 12, 13)\) are pythagorean triples. Notice that multiplying any pythagorean triple by an integer \( n \in \mathbb{Z} \) yields another pythagorean triple (in particular, there are infinitely many pythagorean triples), so we may assume \( a, b, c \) are coprime. Such a triple is called a **primitive pythagorean triple**.

**Theorem 0.1.1.** Denote the set of all primitive pythagorean triples by \( \Pi \). Then there is a bijection \( \Pi \leftrightarrow \{(x, y) \in \mathbb{Q}^2 \mid x^2 + y^2 = 1\} \).

**Proof.** It is easy to check that the assignments
\[
(a, b, c) \mapsto \left(\frac{a}{c}, \frac{b}{c}\right)
\]
\[
(a, b, c) \mapsto (x, y) = \left(\frac{a}{c}, \frac{b}{c}\right) \quad \text{with } a, b, c \text{ coprime}
\]

exhibit the desired bijection.

Thus the problem of rational triangles and pythagorean triples reduces to studying the rational points of the unit circle in the \(xy\)-plane.

**Definition.** Let \( k \) be a field and fix a polynomial \( f \in k[x, y] \) which is irreducible over the algebraic closure \( \bar{k} \). Then the **curve associated to** \( f \) is a functor \( C = C_f \) given by
\[
C: \text{Fields}_k \to \text{Sets}
\]
\[
K/k \mapsto C_k(K) := \{(x, y) \in K^2 \mid f(x, y) = 0\}.
\]

For a field extension \( K/k \), the set \( C(K) \) is called the \( K \)-**rational points** of the curve \( C \).

In this language, Question 1 reads, “What is \( \#C_f(\mathbb{Q}) \) when \( f = x^2 + y^2 - 1\)?

**Example 0.1.2.** Let \( f = x^2 + y^2 - 1 \) and consider the geometric objects defined by \( C(K) = C_f(K) \) for \( K = \mathbb{R} \) and \( K = \mathbb{Q} \).

\[
C(\mathbb{R}) = S^1 \subseteq \mathbb{R}^2.
\]
\[
C(\mathbb{C}), \text{ the Riemann sphere in } \mathbb{C}^2
\]
Also note that since $f \in \mathbb{Q}[x, y]$, we can view $f$ as a polynomial with coefficients in any finite field $\mathbb{F}_q$, and consequently the $\mathbb{F}_q$-rational points $C(\mathbb{F}_q)$ are defined.

Next, fix the point $(-1, 0)$ on $C(K)$ for any field $K$ and consider the line $L : x = 0$.

\[ \begin{array}{c}
\text{slope} = t \\
(-1, 0) \\
L
\end{array} \]

**Theorem 0.1.3.** Let $k$ be any field and $C = C_f$ the curve defined by $f = x^2 + y^2 - 1$. Then there is a bijection

\[
C(k) \setminus \{(-1, 0)\} \longrightarrow L(k) \\
(x, y) \longrightarrow (0, \chi(x, y)) \\
(\psi(t), \phi(t)) \longmapsto t
\]

where $\chi, \psi$ and $\phi$ are rational functions, i.e. $\chi \in k(x, y)$ and $\psi, \phi \in k(t)$.

**Proof.** The rational functions

\[
\chi(x, y) = \frac{y}{x + 1}, \quad \psi(t) = \frac{1 - t^2}{1 + t^2} \quad \text{and} \quad \phi(t) = \frac{2t}{1 + t^2}
\]

exhibit the bijection. \qed

Theorems 0.1.1 and 0.1.3 answer Question 1: the set of all primitive pythagorean triples is completely described by the line $L$ given by $x = 0$, and this description holds over any field $k$.

For Question 2, we must understand the set of congruent numbers over a field $k$. For $n \in \mathbb{Q}$, define the set

\[
C_n(k) = \{(a, b, c) \in k^3 : a^2 + b^2 = c^2 \text{ and } \frac{1}{2}ab = n\}.
\]

**Definition.** We say $n$ is congruent over $k$ if $C_n(k)$ is nonempty.

In particular, Question 2 reduces to deciding when $C_n(\mathbb{Q})$ is nonempty. Notice that we may assume $n$ is a squarefree integer. Above, we parametrized the circle $S^1$ by a line $L$.

Here, we parametrize $C_n(k)$ with a zero set of a different polynomial. Define a bijection

\[
C_n(k) \longrightarrow E_n(k) := \{(x, y) \in k^2 : y^2 = x^3 - nx, y \neq 0\} \\
(a, b, c) \longmapsto \left(\frac{nb}{c - a}, \frac{2n^2}{c - a}\right) \\
\left(\frac{x^2 - n^2}{y}, \frac{2nx}{y}, \frac{x^2 + n^2}{y}\right) \longmapsto (x, y).
\]

The set $E_n(k)$ is called an elliptic curve over $k$. 

3
Example 0.1.4. The elliptic curve defined by \( y^2 = x^3 - 25x \) over \( \mathbb{R} \) is shown below, with some points of \( E_n(\mathbb{Q}) \) highlighted.

0.2 Rational Curves

Let \( C \) be a plane curve defined by an irreducible polynomial \( f \in k[x, y] \).

**Definition.** We say \( C \) is unirational over \( k \) if there exist nonconstant rational functions \( \psi, \phi \in k(t) \) such that \( f(\psi(t), \phi(t)) = 0 \) for all \( t \).

**Definition.** We say \( C \) is rational over \( k \) if it is unirational and there exists a rational function \( \chi \in k(x, y) \) such that \( \psi(\chi(x, y)) = x \) and \( \phi(\chi(x, y)) = y \) for all \( x, y \in k \), with the possible exception of finitely many points.

Example 0.2.1. By Theorem 0.1.3, the circle \( S^1 = C_f \) for \( f = x^2 + y^2 - 1 \) is rational over \( \mathbb{Q} \). This example illustrates the idea that a curve is rational if it has a ‘rational parametrization’ by a line.

In general, the notions of unirationality and rationality are equivalent for curves (this is not true for higher dimensional varieties):

**Theorem 0.2.2** (Lüroth). A curve \( C \) over \( k \) is unirational if and only if it is rational.

To prove Lüroth’s theorem, we formulate the statement in terms of field theory.

**Definition.** Let \( f \in k[x, y] \) be an irreducible polynomial over \( \overline{k} \) and let \( C = C_f \) be the associated plane curve. Then a **rational function** on \( C \) is an equivalence class of functions \( u(x, y) \in k(x, y) \), with \( u = \frac{p}{q}, p, q \in k[x, y] \) and \( f \nmid q \) over \( \overline{k} \), where we say \( u_1 = \frac{p_1}{q_1} \) and \( u_2 = \frac{p_2}{q_2} \) are equivalent if \( f \) divides \( p_1q_2 - p_2q_1 \).
Example 0.2.3. On the circle $S^1 = C_f$, $f = x^2 + y^2 - 1$, the functions

$$u_1(x, y) = \frac{y}{1 + x} \quad \text{and} \quad u_2 = \frac{1 - x}{y}$$

are equivalent, so they define a common rational function on $C$.

**Definition.** The set of rational functions on $C$ with coefficients in $k$ is called the **function field** of $C$, denoted $k(C)$.

**Lemma 0.2.4.** $k(C)$ is a field.

**Proof.** Routine. \qed

**Proposition 0.2.5.** A curve $C$ is unirational over $k$ if and only if $k(C) \subseteq k(t)$.

**Proof.** ($\Rightarrow$) is clear.

($\Leftarrow$) $k(C) \subseteq k(t)$ implies that the functions $x, y \in k(t)$, so $x = \psi(t)$ and $y = \phi(t)$ for some rational functions $\psi, \phi \in k(t)$. Since $f(x, y) = 0$, we have $f(\psi, \phi) \equiv 0$ so $C$ is unirational by definition. \qed

**Proposition 0.2.6.** A curve $C$ is rational over $k$ if and only if $k(C) = k(t)$.

**Proof.** Similar to Lemma 0.2.5. \qed

Then Lüroth’s theorem is proven using the fact that $\text{tr deg}_k k(C) = 1$ when $C$ is a curve, which means $k(C) \subseteq k(t)$ if and only if $k(C) = k(t)$.

The situation for $S^1$, i.e. that existence of rational points is determined by rational parametrization by a line, in fact holds for all curves defined by a degree 2 polynomial. (Such a curve is called a quadratic curve or conic.)

**Proposition 0.2.7.** Let $f \in k[x, y]$ be an irreducible quadratic polynomial. Then the curve $C = C_f$ is rational over $k$ if and only if $C(k)$ is nonempty.

**Proof.** (Sketch) Fix a point $(x_0, y_0) \in C(k)$ and construct the line $\ell$ of slope $t$ through $(x_0, y_0)$ in the plane $k^2$, calling the intersection with $C(k) \setminus \{(x_0, y_0)\}$ $(x, y)$. Then $f(x, t(x - x_0) + y_0)$ is the quadratic polynomial defining $x$ coordinates of $\ell \cap C$, and the polynomial

$$\psi(t) = \frac{f(x, t(x - x_0) + y_0)}{x - x_0}$$

is linear with coefficients in $k$. A similar parametrization of $y$ coordinates gives a rational function $\phi(t)$ which, together with $\psi(t)$, shows that $C$ is unirational over $k$. Hence by Lüroth’s theorem, $C$ is rational over $k$. \qed

Thus the theory of conics reduces to the problem of finding if a conic curve has a rational point over a given field.

**Example 0.2.8.** For the quadratic polynomial $f = x^2 + y^2 + 1$, $C_f(\mathbb{R})$ is empty and so of course $C_f(\mathbb{Q})$ is empty. Thus by Proposition 0.2.7, $f$ is not rational over $\mathbb{Q}$. 

5
Example 0.2.9. Consider the quadratic polynomial $f = x^2 + y^2 - 3$ and its associated conic $C = C_f$. We will show $C(\mathbb{Q}) = \emptyset$. Suppose there exist $a, b \in \mathbb{Q}$ such that $f(a, b) = 0$. Write $a = \frac{x}{z}$ and $b = \frac{y}{z}$ for $x, y, z \in \mathbb{Z}$ coprime, $z \neq 0$ (this step is called homogenization of the quadratic polynomial, corresponding to viewing $C$ inside its projective closure). This gives us an equation

$$3z^2 = x^2 + y^2.$$  

We study roots of this equation by reducing modulo different primes. In the finite field $\mathbb{F}_3$, the only squares are $x^2, y^2, z^2 \equiv 0$ or $1 \pmod{3}$, so the only possible solutions are $(0, 0, z)$. Since $z \neq 0$, we must have $z^2 \equiv 1 \pmod{3}$. Next, in $\mathbb{Z}/9\mathbb{Z}$ we have $3z^2 \equiv 1 \pmod{9}$ since $z \equiv 1 \pmod{3}$. However, the only squares mod 9 are $x^2, y^2 \equiv 1, 4, 7 \pmod{9}$ so we see that there are no solutions to $(*)$ mod 9, and thus no solutions to $(*)$ in integers. Hence $x^2 + y^2 - 3$ is not rational over $\mathbb{Q}$.

The strategy of studying roots mod primes $p$ to understand the structure of solutions in $\mathbb{Z}$ illustrates Hasse’s so-called ‘local-global principle’. Part of this theory is formalized in the next section.

### 0.3 The $p$-adic Numbers

In this section we make the formal the notion of studying solutions modulo $p^n$ for primes $p$ and exponents $n \geq 1$. This leads to the introduction of a new ring $\mathbb{Z}_p$, the ring of $p$-adic integers, and its field of fractions $\mathbb{Q}_p$. We will see that

**Theorem 0.3.1.** For an irreducible quadratic polynomial $f \in \mathbb{Q}[x, y]$, if $C_f(\mathbb{Q}_p) \neq \emptyset$ for all primes $p$ and $C_f(\mathbb{R}) \neq \emptyset$, then $C_f(\mathbb{Q}) \neq \emptyset$.

**Definition.** Let $p$ be a prime. The ring of $p$-adic integers are the inverse limit of the sequence $\mathbb{Z}/p\mathbb{Z} \leftarrow \mathbb{Z}/p^2\mathbb{Z} \leftarrow \mathbb{Z}/p^3\mathbb{Z} \leftarrow \cdots$, that is,

$$\mathbb{Z}_p := \lim_{\leftarrow} \mathbb{Z}/p^n\mathbb{Z} = \left\{ (\alpha_0, \alpha_1, \alpha_2, \ldots) \in \prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z} : \alpha_n \equiv \alpha_{n-1} \pmod{p^n} \right\}.$$  

A useful way to view an element $\alpha = (\alpha_0, \alpha_1, \alpha_2, \ldots)$ in $\mathbb{Z}_p$ is as a “power series” in $p$:

$$\alpha = \alpha_0 + \alpha_1 p + \alpha_2 p^2 + \ldots$$

**Remarks.** Let $p$ be a prime number. The following facts are standard in a commutative algebra course.

- There is a natural embedding $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ given by $x \mapsto (x, x, x, \ldots)$.
- $\mathbb{Z}_p$ is a local ring with maximal ideal $m = \{ (0, \alpha_1, \alpha_2, \ldots) \in \mathbb{Z}_p \}$.
- Define the $p$-adic valuation $v_p: \mathbb{Z}_p \to \mathbb{N}_0$ by setting $v_p(0) = \infty$ and for $\alpha \neq 0$,

$$v_p(\alpha) = \text{ord}_p(\alpha) = \inf \{ n \in \mathbb{N}_0 \mid \alpha \not\in m^n \} = \inf \{ n \in \mathbb{N}_0 \mid \alpha_n \neq 0 \}.$$
If $k = p^n m$ where $p \nmid m$ then $v_p(k) = n$. For example, $v_3(9) = v_3(3^2) = 2$. Then $\mathbb{Z}_p$ is a discrete valuation ring (DVR) with
\[ m = \{ \alpha \in \mathbb{Z}_p \mid v_p(\alpha) > 0 \} \]
and \[ \mathbb{Z}_p^\times = \{ \alpha \in \mathbb{Z}_p \mid v_p(\alpha) = 0 \} = \mathbb{Z}_p \setminus m. \]

- The $p$-adic valuation determines an absolute value function $| \cdot |_p$ on $\mathbb{Z}_p$, called the (normalized) $p$-adic absolute value:
\[ |\alpha|_p := p^{-v_p(\alpha)}. \]
This has the following important properties: For all $\alpha, \beta \in \mathbb{Z}_p$,

(i) $|\alpha \beta|_p = |\alpha|_p |\beta|_p$

(ii) $|\alpha + \beta|_p \leq \max \{ |\alpha|_p, |\beta|_p \}$

- Define the $p$-adic rational field $\mathbb{Q}_p$ to be the field of fractions of the domain $\mathbb{Z}_p$. Elements in $\mathbb{Q}_p$ can be viewed as Laurent series in powers of $p$:
\[ \alpha = \alpha_n p^{-n} + \ldots + \alpha_0 + \alpha_1 p + \alpha_2 p^2 + \ldots \]
where $n < \infty$. Note that since $\mathbb{Q} = \text{Frac}(\mathbb{Z})$ and $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$, we get an embedding $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$.

- The $p$-adic valuation extends to a valuation on $\mathbb{Q}_p$, also denoted $v_p$, given by
\[ v_p \left( \frac{\alpha}{\beta} \right) = v_p(\alpha) - v_p(\beta). \]

The following results are standard.

**Theorem 0.3.2.** For each prime $p$, $(\mathbb{Q}_p, | \cdot |_p)$ is a complete metric space.

**Theorem 0.3.3** (Ostrowski). If $K$ is a completion of $\mathbb{Q}$ then $K = \mathbb{Q}_p$ for some prime $p$ or $K = \mathbb{R}$.

A famous result of Hensel establishes a connection between approximate solutions to polynomial equations in a complete DVR and exact solutions. The more common form of Hensel’s Lemma follows as a corollary.

**Theorem 0.3.4** (Hensel’s Lemma). Let $R$ be a complete DVR with valuation $v$ and fix a polynomial $f \in R[t]$. Suppose $\alpha_0 \in R$ such that $v(f(\alpha_0)) > 2v(f'(\alpha_0))$, where $f'$ is the formal derivative of $f$. Then there exists $\alpha \in R$ such that $f(\alpha) = 0$ and $v(\alpha - \alpha_0) > v(f(\alpha_0))/f'(\alpha_0)^2$.

**Proof.** (Sketch) One uses Newton’s method to prove the existence of a solution $\alpha$ in the following way. Given $\alpha_0$, define the sequence $\alpha_{n+1} = \alpha_n - \frac{f(\alpha_n)}{f'(\alpha_n)}$ and show that it is Cauchy with respect to $v$. Since $R$ is complete, there exists a limit $\alpha \in R$ of this sequence. Then one checks that $f(\alpha) = 0$, using the fact that polynomials are continuous with respect to the topology on $R$ induced by $v$, and $v(\alpha - \alpha_0) > v(f(\alpha_0))/f'(\alpha_0)^2$. \qed
Corollary 0.3.5. If $f$ is a polynomial with roots in $\mathbb{Z}$ with a simple root mod $p$, then it lifts to a root in $\mathbb{Z}_p$.

Corollary 0.3.6. Let $\beta \in \mathbb{Z}_p^\times$. Then $x^2 = \beta$ has a solution in $\mathbb{Z}_p$ if and only if $x^2 \equiv \beta \mod p^\varepsilon$ has a solution, where $\varepsilon = 3$ when $p = 2$ and $\varepsilon = 1$ otherwise.

Proof. Let $f(x) = x^2 - \beta \in \mathbb{Z}[x]$ so that $f'(x) = 2x$. Suppose $\alpha_0 \in \mathbb{Z}_p$ is a solution to $f(x) \equiv 0 \mod p^\varepsilon$, i.e. $v(f(\alpha_0)) \geq \varepsilon$. Then $\alpha_0^2 \equiv \beta \not\equiv 0 \mod p$ so since $\mathbb{Z}_p$ is a DVR, $\alpha_0$ must be a unit, i.e. $v(\alpha_0) = 0$. Now we have

$$2v_p(f'(\alpha_0)) = 2v_p(2a_0) = 2(v_p(a_0) + v_p(2))$$

$$= 2v_p(2) = \begin{cases} 2, & p = 2 \\ 0, & p \neq 2 \end{cases}$$

$$< v(f(\alpha_0)) \text{ in all cases.}$$

Therefore Hensel’s Lemma applies. \qed
1 Algebraic Geometry

1.1 Affine and Projective Space

Let $k$ be a field and let $\bar{k}$ denote its algebraic closure.

**Definition.** For each $n \in \mathbb{N}$, we define **affine** $n$-space over $k$ to be

$$\mathbb{A}^n = \mathbb{A}^n_k = \{(x_1, \ldots, x_n) | x_i \in k\}.$$  

As sets, $\mathbb{A}^n = k^n$, but the new notation carries with it the implication that $\mathbb{A}^n$ is viewed geometrically.

**Remark.** Alternatively, for any field $k \subseteq K \subseteq \bar{k}$, one can define $\mathbb{A}^n_k(K)$ to be the fixed points of $\mathbb{A}^n_k$ under the action of the Galois group $\text{Gal}(\bar{k}/K)$. In particular, $\mathbb{A}^n_k = \mathbb{A}^n_k(k) = (\bar{k}^n)^{G_k}$ where $G_k = \text{Gal}(\bar{k}/k)$ is the absolute Galois group of the field $k$.

We will let $A$ denote the polynomial ring $k[t_1, \ldots, t_n]$.

**Definition.** For a polynomial $f \in A$, define its **zero set** (or **zero locus**) to be

$$Z(f) = \{P \in \mathbb{A}^n | f(P) = 0\}.$$  

We extend the definition of zero set to sets of polynomials $f_1, \ldots, f_r \in A$ by

$$Z(f_1, \ldots, f_r) = \bigcap_{i=1}^r Z(f_i).$$

The definition of zero set can be extended to arbitrary subsets $\mathcal{F} \subseteq A$ by

$$Z(\mathcal{F}) = \bigcap_{f \in \mathcal{F}} Z(f).$$

Notice that if $I = (\mathcal{F})$ is the ideal of $A$ generated by $\mathcal{F}$, then $Z(\mathcal{F}) = Z(I)$. By Hilbert’s basis theorem, there exists a finite subset $\{f_1, \ldots, f_r\} \subseteq \mathcal{F}$ such that $Z(\mathcal{F}) = Z(f_1, \ldots, f_r)$.

**Definition.** A subset $X \subseteq \mathbb{A}^n$ is called an **algebraic set** if $X = Z(\mathcal{F})$ for a set $\mathcal{F} \subseteq A$, that is, $X$ is algebraic if it is the zero set of some collection of polynomials in $k[t_1, \ldots, t_n]$.

By the remark, it is equivalent to say $X$ is a zero set if $X = Z(I)$ for some ideal $I \subseteq A$. Thus the operation $Z(\cdot)$ takes a subset of a ring and assigns to it a geometric space. There is a dual notion:

**Definition.** For any subset $X \subseteq \mathbb{A}^n$, we define the **vanishing ideal** of $X$ to be

$$J(X) = \{f \in A | f(P) = 0 \text{ for all } P \in X\}.$$  

**Lemma 1.1.1.** For all $X \subseteq \mathbb{A}^n$, $J(X)$ is a radical ideal of $A$. 

9
Proof. Take \( f, g \in J(X) \) and \( r \in A \). Then for any \( P \in X \), \((f - g)(P) = f(P) - g(P) = 0 \) and \((rf)(P) = r(P)f(P) = 0 \) so \( f + g, rf \in J(X) \) and thus \( J(X) \) is an ideal. Moreover, for any \( m \in \mathbb{N}, f^m(P) = 0 \) if and only if \( f(P) = 0 \) so we see that \( r(J(X)) = J(X) \). \( \square \)

Examples.

1. \( \emptyset = Z(A) \) and \( \mathbb{A}^n = Z(0) \) are both algebraic sets.

2. If \( U \subseteq \mathbb{A}^n \) is an affine subspace, i.e. \( U = P_0 + V \) for a point \( P_0 \in \mathbb{A}^n \) and a linear subspace \( V \subseteq k^n \), then \( U = Z(L_1, \ldots, L_{n-d}) \) where \( d = \dim_k V \) and \( L_1, \ldots, L_{n-d} \) are linear polynomials in \( A \).

3. For any point \( P = (a_1, \ldots, a_n) \in \mathbb{A}^n \), \( \{P\} = Z(t_1 - a_1, \ldots, t_n - a_n) \). Consider the maximal ideal \( \mathfrak{m}_P = (t_1 - a_1, \ldots, t_n - a_n) \subset A \). Then \( \{P\} = Z(\mathfrak{m}_P) \). When \( k \) is algebraically closed, points of \( \mathbb{A}^n_k \) are in one-to-one correspondence with the maximal ideals of \( A \) via the association \( P \leftrightarrow \mathfrak{m}_P \).

4. In \( \mathbb{A}^2 \), an example of an algebraic curve is \( C = \{(T^2 - 1, T(T^2 - 1))\} = Z(x^2 + x^3 - y^2) \):

![Diagram of C]

5. The algebraic set \( Z(y, y - x^2) = Z(x, y) \) consists of just the point \((0,0)\) in \( \mathbb{A}^2_k \):

![Diagram of Z(y, y - x^2)]

Definition. If \( X = Z(S) \subseteq \mathbb{A}^n_k(\overline{k}) \) is an algebraic set and \( K \) is a field such that \( k \subseteq K \subseteq \overline{k} \), define the \( K \)-points of \( X \) by \( X(K) := X \cap \mathbb{A}_k^n(K) = X^{G_K} \), where \( G_K = \text{Gal}(\overline{k}/K) \). Moreover, we say \( X \) is defined over \( K \) if \( J(X) \) has a generating set consisting of elements of \( K[t_1, \ldots, t_n] \).
Lemma 1.1.2. Let \( X, Y \subseteq \mathbb{A}^n \) be sets and \( I, I_1, I_2 \) and \( I_\ell \subset A \) be ideals, with \( \ell \in L \) some indexing set. Then

(a) If \( Y \subseteq X \) then \( J(Y) \supseteq J(X) \).

(b) If \( I_2 \subseteq I_1 \) then \( Z(I_2) \supseteq Z(I_1) \).

(c) \( Z(J(X)) \supseteq X \).

(d) \( Z(J(I)) \supseteq I \).

(e) \( Z(J(Z(I))) = Z(I) \).

(f) \( J(Z(J(X))) = J(X) \).

(g) \( Z(I_1) \cup Z(I_2) = Z(I_1 \cap I_2) = Z(I_1I_2) \).

(h) \( \bigcap_{\ell \in L} Z(I_\ell) = Z \left( \bigcup_{\ell \in L} I_\ell \right) = Z \left( \sum_{\ell \in L} I_\ell \right) \).

Proof. (a) – (d) are obvious from the definitions of \( Z \) and \( J \).

(e) By (c), \( Z(I) \subseteq Z(J(Z(I))) \) so it remains to prove the reverse containment. However, we have that \( I \subseteq J(Z(I)) \) by (d) so then applying \( Z \) gives \( Z(I) \supseteq Z(J(Z(I))) \) by (b).

(f) is similar to (e). Here, (d) gives us \( J(X) \subseteq J(Z(J(X))) \). On the other hand, we have \( X \subseteq Z(J(X)) \) by (c), so applying \( J \) yields \( J(X) \supseteq J(Z(J(X))) \) by (a).

(g) We get \( Z(I_1) \cup Z(I_2) \subseteq Z(I_1 \cap I_2) \subseteq Z(I_1I_2) \) immediately from the containments \( I_1 \supseteq I_1 \cap I_2 \supseteq I_1I_2 \) and \( I_2 \supseteq I_1 \cap I_2 \supseteq I_1I_2 \), using (b). Suppose \( P \in Z(I_1I_2) \) and \( P \notin Z(I_1) \). Then there is some \( f \in I_1 \) such that \( f(P) \neq 0 \), but for any \( g \in I_2 \), we have \( (fg)(P) = f(P)g(P) = 0 \). Since \( A = k[t_1, \ldots, t_n] \) is a domain and \( f(P) \neq 0 \), we must have \( g(P) = 0 \). This shows \( P \in Z(I_2) \). Hence \( Z(I_1) \cup Z(I_2) \supseteq Z(I_1I_2) \) so we have established all three equalities.

(h) The containments \( I_\ell \subseteq \bigcup_{\ell \in L} I_\ell \subseteq \sum_{\ell \in L} I_\ell \) give us \( Z(I_\ell) \supseteq Z \left( \bigcup_{\ell \in L} I_\ell \right) \supseteq Z \left( \sum_{\ell \in L} I_\ell \right) \) for each \( \ell \in L \), by (b), and therefore \( \bigcap_{\ell \in L} Z(I_\ell) \supseteq Z \left( \bigcup_{\ell \in L} I_\ell \right) \supseteq Z \left( \sum_{\ell \in L} I_\ell \right) \). Suppose \( P \in \bigcap_{\ell \in L} Z(I_\ell) \). Then for every \( f_\ell \in I_\ell, f_\ell(P) = 0 \). In particular, for any \( f = \sum_{\ell \in L} f_\ell \in \bigcup_{\ell \in L} I_\ell, f(P) = 0 \) for each \( \ell \) so \( f(P) = 0 \). Thus \( P \in Z \left( \bigcup_{\ell \in L} I_\ell \right) \). This shows \( \bigcap_{\ell \in L} Z(I_\ell) \subseteq Z \left( \bigcup_{\ell \in L} I_\ell \right) \), so we have all three equalities.

In particular, these properties demonstrate that the algebraic subsets of \( \mathbb{A}^n \) form the closed sets of a topology on \( \mathbb{A}^n \).

Definition. The topology on \( \mathbb{A}^n \) having as its closed sets all algebraic subsets of \( \mathbb{A}^n \) is called the Zariski topology on \( \mathbb{A}^n \).

In (c) and (d), we see that \( Z \) and \( J \) are not quite inverse operations.

Lemma 1.1.3. If \( X \subseteq \mathbb{A}^n \) is any subset and \( \overline{X} \) is the Zariski-closure of \( X \) in \( \mathbb{A}^n \), then

(a) \( J(X) = J(\overline{X}) \).

(b) \( Z(J(X)) = \overline{X} \).

11
Example 1.1.6. The point $G$.

So $z$.

Now by (a), Theorem 1.1.4 (Hilbert’s Nullstellensatz) bijective, between the ideals of $A$ in $Q$. Definition. For a point $P$ for every ideal $I$ such that $P(I) = \mathbb{Q}$. Now by (a), $Z(J(X)) = Z(J(I)) = Z(J(Z(I)))$ which by Lemma 1.1.2(e) equals $Z(I) = \overline{X}$. So $Z(J(X)) = \overline{X}$ as required. \qed

The key development so far is that $J$ and $Z$ establish a correspondence, though not always bijective, between the ideals of $A$ and the closed subsets of $A^n$. Hilbert’s Nullstellensatz says that when $k$ is algebraically closed, there is a bijective correspondence between algebraic sets in $A^n_k$ and radical ideals of $A = k[t_1, \ldots, t_n]$.

Theorem 1.1.4 (Hilbert’s Nullstellensatz). If $k$ is algebraically closed, then $J(Z(I)) = r(I)$ for every ideal $I \subset A$.

Next, we introduce projective space and projective algebraic sets in a manner parallel to the presentation of affine algebraic sets.

Definition. For $n \in \mathbb{N}$, we define projective $n$-space over $k$ to be the quotient space $\mathbb{P}^n = \mathbb{P}^n_k = \mathbb{P}^{n+1}_k \setminus \{0\} / \sim$ where $(a_0, \ldots, a_n) \sim (b_0, \ldots, b_n)$ if and only if there is some $\lambda \in k^*$ such that $(b_0, \ldots, b_n) = (\lambda a_0, \ldots, \lambda a_n)$. The coordinates of $\mathbb{P}^n$ are written $[a_0, \ldots, a_n]$, called homogeneous coordinates.

As in the affine case, for $k \subseteq K \subseteq \overline{k}$ we can define $\mathbb{P}^n_k(K) = \{[a_0, \ldots, a_n] : a_i \in K\}$.

Lemma 1.1.5. For any $k \subseteq K \subseteq \overline{k}$, $\mathbb{P}^n_k(K) = (\mathbb{P}^n_k(\overline{k}) )^{G_k}$, where $G_K = \text{Gal}(\overline{k}/K)$.

Proof. Apply Hilbert’s Theorem 90. \qed

Definition. For a point $P = [a_0, \ldots, a_n] \in \mathbb{P}^n_k(\overline{k})$, the minimal field of definition for $P$ over $k$ is the field $k(P) = k\left(\frac{a_0}{a_i}, \ldots, \frac{a_n}{a_i}\right)$ where $a_i \neq 0$. Alternatively, $k(P) = \overline{k}^{G(P)}$ where $G(P) = \{\sigma \in G_k \mid \sigma(P) = P\} \leq G_k$.

Example 1.1.6. The point $P = (\sqrt{2}, \sqrt{2}, \sqrt{2}) \in \mathbb{P}^3_\mathbb{Q}(\mathbb{Q})$ has minimal field of definition $\mathbb{Q}(P) = \mathbb{Q}$ since scaling by $\frac{1}{\sqrt{2}}$ gives $(1, 1, 1) \in \mathbb{A}^3_\mathbb{Q}$.

Let $S = k[t_0, \ldots, t_n]$ be the polynomial ring in $n + 1$ indeterminates. Recall that $S$ is a graded ring with graded pieces given by total degree:

$$S = \bigoplus_{d=0}^{\infty} S_d \quad \text{where} \quad S_d = \{f \in S \mid \deg f = d\}.$$  

An arbitrary polynomial in $S$ does not have a well-defined vanishing set in $\mathbb{P}^n$. However, homogeneous polynomials do have vanishing sets:

Definition. For $f \in S_d$, define the zero set of $f$ to be $Z(f) = \{P \in \mathbb{P}^n \mid f(P) = 0\}$,

where $f(P) = f(p_0, \ldots, p_n)$ if $P = [p_0, \ldots, p_n]$. This set is well-defined, since $f \in S_d$ implies $f(\lambda a_0, \ldots, \lambda a_n) = \lambda^d f(a_0, \ldots, a_n)$ for all $\lambda \in k^*$.  

12
Set $S^h = \bigcup_{d=0}^{\infty} S_d$. For a collection of homogeneous polynomials $\mathcal{F} \subseteq S^h$, define the zero set of this collection by $Z(\mathcal{F}) = \bigcap_{f \in \mathcal{F}} Z(f)$.

**Definition.** Let $S = k[t_0, \ldots, t_n]$ and suppose $I \subset S$ is an ideal. Then $S$ is **homogeneous** if $I = \bigoplus_{d=0}^{\infty} I_d$ where $I_d = I \cap S_d$ for each $d \in \mathbb{N}_0$.

**Definition.** Let $X \subseteq \mathbb{P}^n$ be any subset. The **(homogeneous) vanishing ideal** of $X$ is defined to be

$$J(X) = \{ f \in S^h \mid f(P) = 0 \text{ for all } P \in X \}.$$ 

$X$ is called a **(projective) algebraic subset** if $X = Z(I)$ for some homogeneous ideal $I \subset S$.

**Lemma 1.1.7.** Let $I$ be an ideal of $S$ and $X \subseteq \mathbb{P}^n$ a subset. Then

(a) If $I = (f_1, \ldots, f_m)$ then $Z(I) = \bigcap_{i=1}^{m} Z(f_i)$.

(b) $J(X)$ is a homogeneous, radical ideal of $S$.

**Proof.** Similar to the proof of Lemma 1.1.1. □

As in the affine case, the sets $Z(I)$ form the closed sets in the Zariski topology on $\mathbb{P}^n$.

**Theorem 1.1.8** (Hilbert’s Nullstellensatz, Projective Version). Let $k$ be an algebraically closed field and set $S = k[t_0, \ldots, t_n]$. Then for any homogeneous ideal $I \subset S$,

(a) $J(Z(I)) = \mathfrak{r}(I)$ if $Z(I) \neq \emptyset$.

(b) $Z(I) = \emptyset$ if and only if $I = S$ or $\mathfrak{r}(I) = (t_0, \ldots, t_n)$.

**Definition.** A nonempty topological space $X$ is said to be **irreducible** if for any two closed subsets $X_1, X_2 \subseteq X$ such that $X_1 \cup X_2 = X$, we have $X = X_1$ or $X = X_2$.

**Definition.** An **affine algebraic variety** over $k$ is an irreducible algebraic subset of $\mathbb{A}^n$. A **quasi-affine variety** is a nonempty, open subset of an affine variety.

**Definition.** A **projective variety** is an irreducible closed subset of $\mathbb{P}^n$. A **quasi-projective variety** is a nonempty, open subset of a projective variety. A **quasi-projective variety** is a nonempty, open subset of a projective variety.

**Definition.** If $X$ is an irreducible algebraic set in $\mathbb{A}^n_k(\bar{k})$ or $\mathbb{P}^n_k(\bar{k})$, then $X$ is called **geometrically irreducible**.

**Lemma 1.1.9.** Let $Y$ be a subspace of a topological space $X$. Then $Y$ is irreducible if and only if for any closed sets $X_1, X_2 \subseteq X$ such that $Y \subseteq X_1 \cup X_2$, we have $Y \subseteq X_1$ or $Y \subseteq X_2$.

**Proof.** Obvious. □

**Lemma 1.1.10.** A set $X \subseteq \mathbb{A}^n$ is irreducible if and only if $J(X)$ is a prime ideal of $A$. 

13
Proof. (\(\implies\)) Assume \(f, g \in A\) such that \(fg \in J(X)\). Then \(X \subseteq X(fg) = Z(f) \cup Z(g)\) by Lemma 1.1.2(g), so we can write \(X = (Z(f) \cap X) \cup (Z(g) \cap X)\) – note that each of these sets is closed in \(X\). If \(X\) is irreducible, then we must have \(X = Z(f) \cap X\) or \(X = Z(g) \cap X\). In particular, \(X \subseteq Z(f)\) or \(X \subseteq Z(g)\), so \(f \in J(X)\) or \(g \in J(X)\). Hence \(J(X)\) is prime.

(\(\impliedby\)) Given that \(J(X)\) is prime, suppose \(X \subseteq X_1 \cup X_2\) for two closed sets \(X_1, X_2 \subseteq A^n\). Then there exist ideals \(I_1, I_2 \subseteq A\) such that \(Z(I_1) = X_1\) and \(Z(I_2) = X_2\). By Lemma 1.1.2(g), \(X \subseteq Z(I_1) \cup Z(I_2) = Z(I_1I_2)\) so applying \(J\), we get \(J(X) \supseteq J(Z(I_1I_2)) \supseteq I_1I_2\) by Lemma 1.1.2(a) and (d). Since \(J(X)\) is prime, we must have \(J(X) \supseteq I_1\) or \(J(X) \supseteq I_2\), but then \(X \subseteq Z(J(X)) \subseteq Z(I_1) = X_1\) or \(X \subseteq Z(J(X)) \subseteq Z(I_2) = X_2\). By Lemma 1.1.9 we are done. \(\square\)

**Definition.** A subset \(Y\) of a noetherian space \(X\) is called an irreducible component of \(X\) if \(Y\) is a maximal irreducible subspace of \(X\).

**Example 1.1.11.** Consider the affine plane \(A^2\). Take \(f = xy\) in \(k[x, y]\). Then \(V(f)\) is the union of the \(x\) and \(y\) axes, each of which is an irreducible subspace of \(A^2\):

\[
\begin{array}{c}
| & | \\
\downarrow & \downarrow \\
Y & A^2 \\
\downarrow & \downarrow \\
x & \\
\end{array}
\]

**Example 1.1.12.** Take an irreducible polynomial \(f \in k[x, y]\). Since \(k[x, y]\) is a UFD, \((f)\) is a prime ideal so \(C := Z(f)\) is irreducible by Lemma 1.1.10. \(C\) is called the (affine) algebraic curve defined by \(f\), sometimes written \((f(x, y) = 0)\). In general, an irreducible polynomial in \(k[x_1, \ldots, x_n]\) corresponds to an affine variety \(Y = Z(f) \subseteq A^n\), called an (affine) algebraic hypersurface.

**Proposition 1.1.13.** If \(X\) is a nonempty algebraic set, then it has finitely many irreducible components \(X_1, \ldots, X_m\) such that \(X = \bigcup_{i=1}^{m} X_i\).

**Definition.** Given a polynomial \(f \in k[t_1, \ldots, t_n]\) of degree \(d\), we obtain a homogeneous form \(f_h \in k[t_0, \ldots, t_n]\) by defining

\[
f_h(x_0, \ldots, x_n) = x_0^d f \left( \frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0} \right),
\]

called the homogenization of \(f\).

Conversely, a homogeneous polynomial \(F \in k[t_0, \ldots, t_n]\) determines a polynomial \(F_{(i)} \in k[t_1, \ldots, t_n]\) for each \(0 \leq i \leq n\) given by

\[
F_{(i)}(x_1, \ldots, x_n) = F(x_1, \ldots, x_{i-1}, 1, x_i, \ldots, x_n),
\]

called the \(i\)th dehomogenization of \(F\).
Definition. For an ideal \( I \subseteq k[t_1, \ldots, t_n] \), define the homogenization of \( I \) by
\[
I_h = \{ f_h \mid f \in I \} \subseteq k[t_0, \ldots, t_n].
\]
Likewise, for an ideal \( J \subseteq k[t_0, \ldots, t_n] \), the \( i \)th dehomogenization of \( J \) is
\[
J_{(i)} = \{ F_{(i)} \mid F \in J \} \subseteq k[t_1, \ldots, t_n].
\]

Define the \( i \)th projective hyperplane by \( H_i = Z(t_i) \subseteq \mathbb{P}^n \) for \( 0 \leq i \leq n \). Set \( U_i = \mathbb{P}^n \setminus H_i \), an open set in \( \mathbb{P}^n \). Then \( \mathbb{P}^n = \bigcup_{i=0}^n U_i \), that is, the complements of the coordinate hyperplanes are an open cover of \( \mathbb{P}^n \).

Proposition 1.1.14. Each \( U_i \) is homeomorphic to \( \mathbb{A}^n \). That is, \( \mathbb{P}^n \) is locally affine.

Proof. Define \( \varphi_i : U_i \to \mathbb{A}^n \) by \( \varphi_i(a_0, \ldots, a_n) = \left( \frac{a_0}{a_1}, \ldots, \frac{a_{i-1}}{a_i}, \frac{a_{i+1}}{a_i}, \ldots, \frac{a_n}{a_i} \right) \). This is Zariski-continuous and has a continuous inverse given by \( \psi_i(b_1, \ldots, b_n) = [b_1, \ldots, b_i, 1, b_{i+1}, \ldots, b_n] \).

Therefore \( \varphi_i \) is a Zariski-homeomorphism for each \( 0 \leq i \leq n \).

\( \square \)

Corollary 1.1.15. If \( Y \subseteq \mathbb{P}^n \) is a projective variety, then \( Y = \bigcup_{i=0}^n (Y \cap U_i) \). In particular, every projective variety may be covered by open sets which are homeomorphic to affine varieties in \( \mathbb{A}^n \).

For a projective algebraic set \( Y \subseteq \mathbb{P}^n_k \), where \( Y = Z(J) \) for an ideal \( J \subseteq k[t_0, \ldots, t_n] \), we get \( n + 1 \) affine algebraic sets \( Y_i = \varphi_i^{-1}(Y \cap U_i) = Z(J_{(i)}) \). These are called the dehomogenizations of \( Y \). Conversely, for an affine algebraic set \( X \subseteq \mathbb{A}^n_k \), with \( X = Z(I) \), the projective closure of \( X \) in \( \mathbb{P}^n_k \) is the Zariski closure in \( \mathbb{P}^n_k \) of \( \varphi_0(X) \), denoted \( \overline{X} \). Note that \( \overline{X} = Z(I(\varphi_0(X))) = Z(I_h) \).

Lemma 1.1.16. The map \( \varphi_0|_X : X \to \overline{X} \cap \varphi_0(X) \) is a homeomorphism.

1.2 Morphisms of Affine Varieties

Definition. We call a topological space \( X \) a ringed space (over a field \( k \)) if it possesses a sheaf of \( k \)-valued functions, that is, an assignment \( U \mapsto \mathcal{O}_X(U) \) to each open set \( U \subseteq X \) a \( k \)-algebra \( \mathcal{O}_X(U) \) of functions \( U \to k \), such that

(a) If \( U = \bigcup_{\alpha} U_{\alpha} \) for open sets \( U_{\alpha} \subseteq X \), then \( f \in \mathcal{O}_X(U) \) if and only if \( f \in \mathcal{O}_X(U_{\alpha}) \) for every \( U_{\alpha} \).

(b) If \( f \in \mathcal{O}_X(U) \), the set \( D(f) = \{ P \in U \mid f(P) \neq 0 \} \) is an open set in \( U \) and \( \frac{1}{f} \in \mathcal{O}_X(D(f)) \).

Definition. A morphism between ringed spaces is a map \( \varphi : X \to Y \) such that for any open set \( V \subseteq Y \) and regular function \( f \in \mathcal{O}_Y(V) \), the pullback
\[
\varphi^* f : x \mapsto f \circ \varphi(x)
\]
is a regular function on \( \varphi^{-1}(V) \), i.e. \( \varphi^* f \in \mathcal{O}_X(\varphi^{-1}(V)) \).
A morphism \( \varphi : X \to Y \) determines a \( k \)-algebra homomorphism \( \varphi^* : \mathcal{O}_Y(V) \to \mathcal{O}_X(\varphi^{-1}(V)) \) for every open set \( V \subseteq Y \).

**Definition.** An isomorphism of ringed spaces is an invertible morphism \( \varphi : X \to Y \) such that \( \varphi^{-1} \) is also a morphism.

**Example 1.2.1.** Consider the varieties \( X \) and \( Y \) defined by \( X = \mathbb{A}^1_k \) (the affine line) and \( Y = Z(y^2 - x^3) \subseteq \mathbb{A}^2_k \). Then the map
\[
\varphi : X \to Y \\
t \mapsto (t^2, t^3)
\]
is both invertible and a morphism, but its inverse is not a morphism so \( \varphi \) is not an isomorphism of ringed spaces.

**Definition.** For an algebraic set \( X \subseteq \mathbb{A}^n_k \), we define the coordinate ring of \( X \) to be the quotient ring \( k[X] := k[t_1, \ldots, t_n]/J(X) \). For any intermediate field \( k \subseteq K \subseteq \bar{k} \), if \( X \) is defined over \( K \) we also set \( K[X] = K[t_1, \ldots, t_n]/J_K(X) \). The coordinate ring is defined similarly for \( X \subseteq \mathbb{P}^n_k \).

**Proposition 1.2.2.** Suppose \( k \) is algebraically closed and \( X \) is an affine variety over \( k \). Then
\[
\begin{align*}
(a) & \quad \mathcal{O}_X(X) = k[X], \text{ that is, the coordinate ring of } X \text{ consists of regular } k \text{-valued functions } X \to k. \\
(b) & \quad \text{For any } f \in k[X] \setminus \{0\}, \mathcal{O}_X(D(f)) = k[X]_f, \text{ the localization of } k[X] \text{ at the element } f.
\end{align*}
\]

Notice that by Lemma 1.1.10, \( X \subseteq \mathbb{A}^n_k \) is a variety if and only if \( k[X] \) is an integral domain.

**Definition.** For an affine algebraic variety \( X \subseteq \mathbb{A}^n_k \), the function field of \( X \) over \( k \) is the fraction field \( k(X) := \text{Frac} k[X] \). An element of \( k(X) \) is called a rational function on \( X \). If \( X \) is defined over some \( k \subseteq K \subseteq \bar{k} \), then the field \( K(X) := \text{Frac} K[X] \) is called the field of \( K \)-rational functions on \( X \).

**Lemma 1.2.3.** For any tower \( k \subseteq K \subseteq \bar{k} \) over which \( X \) is defined, \( K[X] = \bar{k}[X]^{G_K} \) and \( K(X) = \bar{k}(X)^{G_K} \).

**Remark.** Let \( X \) be an algebraic variety. By Hilbert’s Nullstellensatz, there are one-to-one correspondences
\[
\begin{align*}
\{ \text{closed subvarieties} \} & \quad \longleftrightarrow \quad \text{Spec } \bar{k}[X] \\
Y & \quad \longleftrightarrow \quad I(Y) \\
Z(p) & \quad \longleftrightarrow \quad p \\
\{ \text{points } P \in X \} & \quad \longleftrightarrow \quad \text{MaxSpec } \bar{k}[X] \\
P & \quad \longleftrightarrow \quad m_P := \{ f \in \bar{k}[X] \mid f(P) = 0 \}.
\end{align*}
\]

For any field \( k \) we call elements of \( \text{MaxSpec } k[X] \) the closed points of \( X \) over \( k \).
Theorem 1.2.4. The closed points of $X$ over a field $k$ are in bijective correspondence with the orbits of $G_k$ on $\text{MaxSpec} \, \bar{k}[X]$.

Example 1.2.5. Let $X \subseteq \mathbb{A}_Q^1$ be the algebraic variety defined by the irreducible polynomial $f = x^{3701} - 2$. Then $\mathbb{Q}[X] = \mathbb{Q}[x]/(x^{3701} - 2) \cong \mathbb{Q}(\sqrt[3701]{2})$ is a field, so $\text{MaxSpec} \, \mathbb{Q}[X]$ consists of a single point. On the other hand, $\text{MaxSpec} \, \mathbb{Q}[X]$ contains $3701$ points.

Fix a variety $X$ over $k$. The embedding $i : k[X] \hookrightarrow \bar{k}[X]$ induces a map on maximal ideals

$$i^* : \text{MaxSpec} \, \bar{k}[X] \longrightarrow \text{MaxSpec} \, k[X]$$

with the following properties:

- For every maximal ideal $\mathfrak{m} \in \text{MaxSpec} \, k[X]$, the fibre $\alpha(\mathfrak{m}) := (i^*)^{-1}(\mathfrak{m})$ is finite and nonempty.
- The absolute Galois group $G_k$ acts transitively on each fibre $\alpha(\mathfrak{m})$, and $\text{MaxSpec} \, k[X] = (\text{MaxSpec} \, \bar{k}[X])/G_k$.
- In other words, we can view $i^*$ as a covering space.
- If $k$ is a perfect field, $\#\alpha(\mathfrak{m}) = [k(P) : k]$ for any point $P \in \alpha(\mathfrak{m})$.
- The $k$-points of $X$ are in correspondence with the orbits of size one of this action.

Let $X/\bar{k}$ be an affine algebraic set. Then $X$ is a ringed space whose structure sheaf $\mathcal{O}_X : U \mapsto \mathcal{O}_X(U)$ is defined on open sets $U \subseteq X$ by

$$\mathcal{O}_X(U) = \left\{ f : U \to \bar{k} \mid \text{there exists a cover } U = \bigcup U_\alpha \text{ such that } f|_{U_\alpha} = \frac{g_\alpha}{h_\alpha} \text{ for } g_\alpha, h_\alpha \in \bar{k}[X] \text{ with } h_\alpha(P) \neq 0 \text{ for all } P \in U_\alpha \right\}$$

Proposition 1.2.6. Let $X$ be an affine algebraic set defined over $\bar{k}$. Then

(a) $\mathcal{O}_X(X) = \bar{k}[X]$.

(b) For any $f \in \bar{k}[X]$, $\mathcal{O}_X(D(f)) = \bar{k}[X]_f = \bar{k}[X]\left[\frac{1}{f}\right]$, the localization of $\bar{k}[X]$ at powers of $f$.

(c) For any prime ideal $\mathfrak{p} \subseteq \bar{k}[X]$, $\mathcal{O}_X(X \setminus Z(\mathfrak{p})) = \bar{k}[X]_\mathfrak{p}$.

Definition. For a point $P \in X$, the local ring of $X$ at $P$ is

$$\mathcal{O}_{X,P} = \left\{ \frac{f}{g} : f, g \in \bar{k}[x], g(P) \neq 0 \right\}.$$
1.2 Morphisms of Affine Varieties

Remark. For any \( P \in X \), the local ring at \( P \) can alternatively be characterized by a localization or a direct limit:
\[
\mathcal{O}_{X,P} = \bar{k}[X]_{m_P} = \lim_{\to} \mathcal{O}_X(U).
\]
Then indeed \( \mathcal{O}_{X,P} \) is a local ring with maximal ideal \( m_P \bar{k}[X] \); by abuse of notation, we will also denote this maximal ideal by \( m_P \). Also note that the residue field \( \kappa(P) := \mathcal{O}_{X,P}/m_P \) is isomorphic to \( \bar{k} \). We will prove that when \( X \) is a curve,
\[
\bar{k}[X] = \bigcap_{P \in X} \mathcal{O}_{X,P}.
\]
We can now define morphisms between affine varieties.

Definition. A morphism of affine varieties is a map \( \varphi : X \to Y \) that is a morphism of ringed spaces, that is, for any open set \( V \subseteq Y \) and regular function \( f \in \mathcal{O}_Y(V) \), the pullback \( \varphi^*f \) is a regular function in \( \mathcal{O}_X(\varphi^{-1}(V)) \). Such a map is also sometimes called regular.

There is a more useful equivalent definition that we introduce now. Suppose \( X \subseteq \mathbb{A}^n \) with \( k[X] = k[t_1, \ldots, t_n]/J(X) \) and \( Y \subseteq \mathbb{A}^m \) with \( k[Y] = k[t_1, \ldots, t_m]/J(Y) \). Then a morphism of varieties \( \varphi : X \to Y \) induces a \( k \)-algebra homomorphism
\[
\varphi^* : k[Y] \to k[X].
\]
For each \( 1 \leq j \leq m \), we get \( \varphi_j := \varphi^*(t_j) \in k[t_1, \ldots, t_n]/J(X) \) so we can view \( \varphi_j \) as a polynomial in \( t_1, \ldots, t_n \).

Lemma 1.2.7. A morphism \( \varphi : X \to Y \) is given by polynomials
\[
\varphi(P) = (\varphi_1(P), \ldots, \varphi_m(P)) \quad \text{for } P \in X,
\]
where \( \varphi_1, \ldots, \varphi_m \in k[t_1, \ldots, t_n] \) such that \( f(\varphi_1, \ldots, \varphi_m) \equiv 0 \) for any \( f \in J(Y) \).

Remark. Suppose \( k \subseteq K \subseteq \bar{k} \) and \( X \) and \( Y \) are defined over \( K \). If \( \varphi = (\varphi_1, \ldots, \varphi_m) : X \to Y \) is a morphism such that each \( \varphi_i \in K[t_1, \ldots, t_n] \), we say the morphism is defined over \( K \). In particular, any \( \varphi : X \to Y \) induces a morphism of \( K \)-rational points, \( \varphi_K : X(K) \to Y(K) \), that is defined over \( K \).

Theorem 1.2.8. For any affine varieties \( X \) and \( Y \), there is an isomorphism
\[
\text{Hom}_{\text{Aff}_k}(X, Y) \cong \text{Hom}_{k-\text{alg}}(\bar{k}[Y], \bar{k}[X]).
\]
In particular, there is an equivalence of categories between \( \text{Aff}_k \), the affine varieties over \( k \) together with variety morphisms, and \( (k-\text{alg})^{\text{op}} \), the opposite category of finitely generated \( k \)-algebras together with \( k \)-algebra homomorphisms.

Definition. A rational map between affine varieties over a field \( k \) is a partial morphism \( \varphi : X \dashrightarrow Y \) consisting of a pair of open sets \( U \subseteq X \) and \( V \subseteq Y \) and a morphism of quasi-affine varieties \( U \to Y \).
1.3 Morphisms of Projective Varieties

By Lemma 1.2.7, a rational map \( \varphi : X \rightarrow Y \) is given by polynomials \( \varphi = (\varphi_1, \ldots, \varphi_m) : \mathbb{A}^n \rightarrow \mathbb{A}^m \) such that \( \varphi_i \in \mathcal{O}_X(U) \) for each \( 1 \leq i \leq m \). A rational map \( \varphi \) defines a homomorphism of \( k \)-algebras

\[
\varphi^* : k[Y] \rightarrow k(X)
\]

\[
f \mapsto f \circ \varphi.
\]

Note that if \( \varphi(U) \) is dense in \( Y \), the induced homomorphism extends to an inclusion of function fields:

\[
\varphi^* : k(Y) \hookrightarrow k(X)
\]

\[
f \mapsto \varphi^*(f) \quad \frac{f}{g} \mapsto \frac{\varphi^*(f)}{\varphi^*(g)}.
\]

This property is so important that such morphisms are given a name.

**Definition.** A morphism \( \varphi : X \rightarrow Y \) is said to be **dominant** if \( \varphi(X) \) is dense in \( Y \).

**Definition.** Let \( X \) and \( Y \) be affine varieties over \( k \). If there exists a rational \( \varphi : X \rightarrow Y \) which has a rational inverse, that is a rational map \( \psi : Y \rightarrow X \) such that \( \varphi \circ \psi \) and \( \psi \circ \varphi \) are equal to the identity where they are defined, then \( X \) and \( Y \) are said to be **birationally equivalent** over \( k \).

**Lemma 1.2.9.** \( X \) and \( Y \) are birationally equivalent over \( k \) if and only if \( k(X) \cong k(Y) \) as \( k \)-algebras.

A major area of interest in algebraic geometry is the classification of varieties up to birational equivalence. For curves, there is a canonical invariant called the **genus** which completely classifies curves up to birational equivalence over the algebraic closure \( \overline{k} \) of a field \( k \).

**Definition.** A **rational variety** is a variety \( X \) over \( k \) which is birationally equivalent to \( \mathbb{A}^n \) for some \( n \).

## 1.3 Morphisms of Projective Varieties

Using the affine patches \( U_i \) as charts on \( \mathbb{P}^n \), we can define regular functions and morphisms on projective varieties as follows. Let \( U_i \) be the \( i \)th affine patch of projective \( n \)-space, as defined at the end of Section 1.1.

**Definition.** A function on \( X \subseteq \mathbb{P}^n_k \) is **regular** if it pulls back along \( U_i \hookrightarrow \mathbb{P}^n_k \) (i.e. restricts) to a regular function on each affine patch \( X_i = U_i \cap X \).

**Definition.** Let \( X \subseteq \mathbb{P}^n_k \) be a projective variety. A **rational function** on \( X \) is an equivalence class of quotients of homogeneous forms of the same degree,

\[
f = \frac{F(x_0, \ldots, x_n)}{G(x_0, \ldots, x_n)}
\]

for \( F, G \in k[t_0, \ldots, t_n], \ G \not\in J(X), \) where we say \( f = \frac{F_1}{G_1} \) and \( g = \frac{F_2}{G_2} \) are equivalent if \( F_1G_2 - F_2G_1 \in J(X) \).
Definition. The function field of $X \subseteq \mathbb{P}_k^n$ is the set of rational functions on $X$, denoted $k(X)$.

Lemma 1.3.1. For each affine patch $X_i = X \cap U_i$, $k(X) \cong k(X_i)$ as $k$-algebras.

In particular, if $Y \subseteq \mathbb{A}_k^n$ is an affine variety, then $k(Y) \cong k(\overline{Y})$, where $\overline{Y}$ is the projective closure of $Y$.

Definition. A function $f \in k(X)$ is regular at a point $P \in X$ if $f$ can be written $f = \frac{F}{G}$ for homogeneous forms $F, G \in k[t_0, \ldots, t_n]$ such that $G(P) \neq 0$.

Proposition 1.3.2. A projective variety $X \subseteq \mathbb{P}_k^n$ is a ringed space with structure sheaf $\mathcal{O}_X : U \mapsto \mathcal{O}_X(U)$ defined on open sets $U \subseteq X$ by

$$\mathcal{O}_X(U) = \{ f \in k(X) \mid f \text{ is regular at } P \text{ for all } P \in U \}.$$ 

We can now define morphisms between projective varieties using this ringed space structure.

Definition. A morphism of (quasi-)projective varieties is a map $\varphi : X \to Y$ that is a morphism of the ringed spaces.

The definition of rational maps between affine varieties extends to projective varieties in the following way.

Definition. For projective varieties $X \subseteq \mathbb{P}_k^n$ and $Y \subseteq \mathbb{P}_k^m$, a rational map $\varphi : X \dashrightarrow Y$ is a pair of open sets $U \subseteq X$ and $V \subseteq Y$ and a morphism $\varphi = (\varphi_0, \ldots, \varphi_m) : U \to V$, such that each $\varphi_i \in k[t_0, \ldots, t_m]$ is a homogeneous polynomial, $\varphi(P) \in Y$ for each $P \in X$ and some $\varphi_i \notin J(X)$.

Definition. A map $\varphi : X \to Y$ is regular at a point $P \in X$ if at least one $\varphi_i(P) \neq 0$. We say $\varphi$ is a regular map if it is regular at every $P \in X$.

Lemma 1.3.3. A map $\varphi : X \to Y$ is regular if and only if it is a morphism of varieties.

Note that a quasi-projective set with the Zariski topology is not Hausdorff in general. Indeed, if $X$ is irreducible, then any nonempty open set is dense. Thus we need a notion to replace the Hausdorff condition for algebraic sets.

Proposition 1.3.4. A quasi-projective set is T1.

Proof. If $P = [\alpha_0, \ldots, \alpha_n] \in X$ is a point then $P = Z((\alpha_i t_j - \alpha_j t_i)_{i,j}) = Z(m_P)$. Thus points are closed in the Zariski topology. \qed

Corollary 1.3.5. If $U \subseteq X$ is open, $P, Q \in X$ and $f(P) = f(Q)$ for all $f \in \mathcal{O}_X(U)$, then $P = Q$.

Corollary 1.3.6. Let $X$ and $Y$ be quasi-projective sets and $\varphi, \psi : X \to Y$ two morphisms. Then if the set $U_{\varphi, \psi} := \{ P \in X \mid \varphi(P) = \psi(P) \}$ contains an open dense set, we have $\varphi = \psi$.

Definition. For a function $f \in k[X]$, define the principal open subset of $f$ by $D(f) := \{ P \in X \mid f(P) \neq 0 \}$.

Lemma 1.3.7. If $X$ is a quasi-projective variety, then the collection $\{ D(f) \mid f \in k[X] \}$ is a basis for the Zariski topology on $X$. 

20
1.4 Products of Varieties

Consider two ringed spaces $X$ and $Y$. We may take their set-theoretic product $X \times Y$ and, if each space is a topological space, endow $X \times Y$ with the product topology. Unfortunately, in the category of algebraic varieties, this operation does not preserve the structure of two varieties $X$ and $Y$; that is, the product topology arising from the spaces’ Zariski topologies does not suffice to do algebraic geometry.

Instead, consider the projections $\pi_X : X \times Y \to X$ and $\pi_Y : X \times Y \to Y$. For any ringed space $Z$, we must have a bijection

$$\text{Hom}(Z, X \times Y) \leftrightarrow \text{Hom}(Z, X) \times \text{Hom}(Z, Y)$$

$$\varphi \mapsto (\varphi \circ \pi_X, \varphi \circ \pi_Y).$$

We thus make $X \times Y$ into a ringed space with $O_{X \times Y}(U \times V)$ defined for all open sets $U \subseteq X, V \subseteq Y$ by stipulating that anything of the form

$$f = \sum (\pi_X^* g_i)(\pi_Y^* h_i), \quad \text{for } g_i \in O_X(U) \text{ and } h_i \in O_Y(V),$$

is regular on $U \times V$. If $g \in O_X(U)$, we must have $\pi_X^* g \in O_{X \times Y}(U \times V)$ and likewise, if $h \in O_Y(V)$, then $\pi_Y^* h \in O_{X \times Y}(U \times V)$. Thus for such an $f$ as above, $D(f)$ is an open subset of $X \times Y$ that would not be open in the usual product topology.

**Example 1.4.1.** Under the above description of products of affine varieties, $A^n \times A^m \cong A^{n+m}$ for any $n, m \in \mathbb{N}$. Note that even for $n = m = 1$, the Zariski topology on $A^2$ is not equivalent to the product topology on $A^1 \times A^1$.

**Lemma 1.4.2.** If $X$ and $Y$ are affine varieties, then

(a) $X \times Y$ is an affine variety.

(b) $k[X \times Y] = k[X] \otimes_k k[Y]$.

To define products of projective varieties requires a little more care.

**Proposition 1.4.3 (Segre Embedding).** For any $n, m \in \mathbb{N}$, there is an embedding

$$\sigma_{n,m} : \mathbb{P}^n \times \mathbb{P}^m \to \mathbb{P}^{(n+1)(m+1)-1}$$

$$([x_0, \ldots, x_n], [y_0, \ldots, y_m]) \mapsto [x_i y_j]_{i,j}$$

such that the image $\Sigma_{n,m} := \sigma_{n,m}(\mathbb{P}^n \times \mathbb{P}^m)$ has the structure of an algebraic subset that coincides with the Zariski topology of the product $\mathbb{P}^n \times \mathbb{P}^m$.

**Proof.** (Sketch) Viewing $\mathbb{P}^{(n+1)(m+1)-1}$ as a space of $(n+1) \times (m+1)$ matrices, we have that

$$\Sigma_{n,m} = \{[z_{ij}]_{i,j} \mid \text{all } 2 \times 2 \text{ minors of } (z_{ij}) \text{ vanish}\}.$$

Then clearly $\Sigma_{n,m} = Z((z_{ij}z_{kl} - z_{kj}z_{il})_{i,j,k,l})$, so $\Sigma_{n,m}$ is an algebraic set. The fact that $\sigma_{n,m}$ is a bijection is obvious. One can now verify that the induced topology corresponds to the topology on $\mathbb{P}^n \times \mathbb{P}^m$. \qed
Then this explains why we can write \( B \) called a quadric surface \( z \) and the embedded image \( \Sigma \)

**Example 1.4.7.** Consider the Segre embedding \( \mathbb{P}^k \times \mathbb{P}^k \to \mathbb{P}^3 \) and set \( Q = \Sigma_{1,1} = Z(z_0z_1 - z_0z_1) \). The polynomial \( z_0z_1 - z_0z_1 \) is called a quadric and the embedded image \( Q \) is called a quadric surface. For each \( \alpha, \beta \in \mathbb{P}^1 \), one gets lines on the quadric surface realized by \( \{\alpha\} \times \mathbb{P}^1 \to Q \) and \( \mathbb{P}^1 \times \{\beta\} \to Q \). Note that lines of these forms cover \( Q \), for which reason \( Q \) is called a ruled surface.

**1.5 Blowing Up**

We now have a working notion of products of varieties, so consider the space \( \mathbb{A}^n \times \mathbb{P}^{n-1} \). Coordinates in this space are \( (P, [\ell]) \), where \( P \in \mathbb{A}^n \) is a point and \( [\ell] \in \mathbb{P}^{n-1} \) is the class of some line through the origin \( \ell \) in \( \mathbb{A}^n \). Consider the set \( B \subseteq \mathbb{A}^n \times \mathbb{P}^{n-1} \) defined by

\[
B = \{(P, [\ell]) \mid P \in \ell\}.
\]

Then \( B \) is an algebraic subset: \( B = Z((x_iy_j - x_jy_i)_{i,j}) \) if \( \mathbb{A}^n = \{(x_1, \ldots, x_n)\} \) and \( \mathbb{P}^{n-1} = \{[Y_1, \ldots, Y_n]\} \).

In dimension \( n = 2 \), notice that for any point \( P = (u, v) \) and line \( [\ell] = [\alpha, \beta] \), we have

\[
P \in \ell \iff \frac{u}{v} = \frac{\alpha}{\beta} \iff u\beta - v\alpha = 0.
\]

This explains why we can write \( B = Z(x_1Y_2 - x_2Y_1) \subseteq \mathbb{A}^2 \times \mathbb{P}^1 \).
Now let \( \pi : \mathbb{A}^n \times \mathbb{P}^{n-1} \to \mathbb{A}^n \) be the canonical projection. If \( P \neq 0 \) in \( \mathbb{A}^n \), then \( \pi^{-1}(P) = (P, [\ell_P]) \) is defined, where \( \ell_P \) is the unique line through the origin containing \( P \). Therefore \( \pi \) is an isomorphism on an open subset of \( B \):
\[
\pi : B \setminus \{(P, [\ell]) \mid P = 0) \to \mathbb{A}^n \setminus \{0\}.
\]

On the other hand, if \( P = 0 \), the set \( \pi^{-1}(0) = \{(0, [\ell]) \in \mathbb{A}^n \times \mathbb{P}^{n-1} \} \) is isomorphic to \( \mathbb{P}^{n-1} \).

In the dimension 2 case, \( B \) is covered by the following affine patches:
\[
U_1 = \{((x, y), [Y_1, Y_2]) \mid Y_1 \neq 0\} \cap B \quad \text{and} \quad U_2 = \{((x, y), [Y_1, Y_2]) \mid Y_2 \neq 0\} \cap B
\]

On \( U_1 \), set \( t = \frac{Y_2}{Y_1} \) so that in local coordinates \((x, y, t)\), \( U_1 = Z(xt - y) \cong \mathbb{A}^2 \). Likewise, for \( U_2 \), set \( s = \frac{Y_1}{Y_2} \) so that in the coordinates \((x, y, s)\), \( U_2 = Z(x - ys) \cong \mathbb{A}^2 \). Thus we see that each affine patch \( U_i \) is a quadric surface. Effectively, we have replace a point \((0, 0)\) in \( \mathbb{A}^2 \) with a copy of \( \mathbb{P}^1 \) so that every line through the origin in \( \mathbb{A}^2 \), all of which are indistinguishable in \( \mathbb{P}^1 \) to begin with, now corresponds to a unique line on one of the affine quadric surfaces.

**Definition.** The set \( B \) is called the **blowup** of \( \mathbb{A}^n \) at the point \( 0 \), denoted \( B = \text{Bl}_0 \mathbb{A}^n \). The set \( E_0 \mathbb{A}^n := \pi^{-1}(0) \cong \mathbb{P}^{n-1} \) is called the **exceptional divisor** of the blowup.

**Definition.** Let \( X \subseteq \mathbb{A}^n \) be an affine variety and \( \pi : \mathbb{A}^n \times \mathbb{P}^{n-1} \to \mathbb{A}^n \) the canonical projection. The pullback \( \pi^{-1}(X) \) is called the **total transform** of \( X \), while the **proper** (or **strict**) transform of \( X \) is defined as
\[
\text{Bl}_0 X := \pi^{-1}(X \setminus \{0\}).
\]

As the notation suggests, this set is also called the **blowup** of \( X \) at \( 0 \). The set
\[
E_0 X := \text{Bl}_0 X \cap E_0 \mathbb{A}^n
\]
is called the **exceptional divisor** of the blowup of \( X \).

**Remark.** More generally, for any subvariety \( Z \subseteq X \), one can define the **blowup of \( X \) along \( Z \)**, a variety \( \text{Bl}_Z X \) that is birationally equivalent to \( X \), such that \( Z \) is a codimension 1 subvariety of \( \text{Bl}_Z X \).

**Example 1.5.1.** Consider the plane curve \( X = Z(y^2 - x^2(x + 1)) \subseteq \mathbb{A}^2 \).
Note that this variety has a singularity at the point \((0,0)\). Using the blowup of \(\mathbb{A}^2\) defined above, \(\text{Bl}_0\mathbb{A}^2\), we can blowup \(X\) to ‘remove the singularity’ at 0. Let \(U_1\) be the first affine patch and \(\varphi : U_1 \to \mathbb{A}^2\) the standard isomorphism. We make the substitution \(y = xt\), so that \(\varphi(\pi^{-1}(X)) = Z(x^2(t^2 - x - 1))\). The \(x^2\) factor of this polynomial corresponds to the exceptional divisor \(E_0X\) under this blowup, so the proper transform of \(X\) at 0 looks like

\[
\varphi(\text{Bl}_0(X)) = Z(t^2 - x - 1)
\]
on the affine patch \(U_1\). Note also that

\[
E_0X = \text{Bl}_0 X \cap E_0\mathbb{A}^2 = Z(t^2 - x - 1) \cap Z(x) = Z(t^2 - 1) = \{\pm 1\},
\]
so the exceptional set of \(X\) consists of two points.

**Lemma 1.5.2.** The projection \(\pi : \text{Bl}_0 X \dashrightarrow X\) is a birational equivalence.

Blowing up allows us to replace singular curves (or more generally, varieties) with non-singular curves by a sequence of blowups, such that in each step the birational equivalence class of the curve is preserved. The problem of finding such a nonsingular blowup is known as resolution of singularities. Much progress has been made on this problem (e.g. Hironaka’s theorem says that nonsingular blowups exist for any finite dimensional variety over a field of characteristic zero), but there is still much to be done (e.g. in finite characteristic cases).

### 1.6 Dimension of Varieties

In this section we explore various notions of dimension in commutative algebra and geometry and see how they coincide for algebraic varieties.

**Definition.** If \(X\) is a topological space, the **dimension** of \(X\) is defined by

\[
\dim X = \sup \left\{ \ell \in \mathbb{N}_0 \left| \begin{array}{l}
\text{there exists a chain of closed, irreducible subsets} \\
Y_0 \subsetneq Y_1 \subsetneq \cdots \subsetneq Y_\ell \text{ with } Y_\ell \subseteq X
\end{array} \right. \right\}.
\]

On the algebraic side, we have a similar notion of dimension due to Krull.

**Definition.** If \(A\) is a ring and \(p \subseteq A\) is prime, the **height** of \(p\) is defined as

\[
\text{ht}(p) = \sup \{ \ell \geq 0 \left| \begin{array}{l}
\text{there is a chain of prime ideals} \\
p_0 \subsetneq p_1 \subsetneq \cdots \subsetneq p_\ell \subsetneq p
\end{array} \right. \right\}.
\]

The **Krull dimension** of \(A\) is then defined by

\[
\dim A = \sup \{ \text{ht}(p) \left| p \subseteq A \text{ is prime} \right. \}.
\]

**Proposition 1.6.1.** Let \(X \subseteq \mathbb{A}^n_k\) be an affine variety. Then

(a) \(\dim X \leq \dim k[X]\).

(b) If \(k\) is algebraically closed, then \(\dim X = \dim k[X]\).
Proof. (a) If \( Y_0 \subsetneq Y_1 \subsetneq \cdots \subsetneq Y_\ell \) is a chain of closed, irreducible subsets of \( X \), then \( J(X_0) \supseteq J(Y_1) \supseteq \cdots \supseteq J(Y_\ell) \) is a chain of prime ideals in \( k[X] \), by Lemma 1.1.10. (The inclusions are strict since \( Z(J(Y_i)) = Y_i \) for each \( 0 \leq i \leq \ell \), by Lemma 1.1.3(b).) Thus \( \dim X \leq \dim k[X] \).

(b) Assume \( k \) is algebraically closed and let \( p_0 \subsetneq p_1 \subsetneq \cdots \subsetneq p_m \) be a strictly ascending chain of prime ideals in \( k[X] \). For each \( i \), \( p_i = p'_i/J(X) \) for some prime ideal \( p'_i \subset A = k[t_1, \ldots, t_n] \) containing \( J(X) \). Thus by Hilbert’s Nullstellensatz, \( J(Z(p'_i)) = p'_i \) for each \( i \), which gives us

\[
Z(p'_0) \supseteq Z(p'_1) \supseteq \cdots \supseteq Z(p'_m),
\]

a strictly descending chain of affine subsets of \( \mathbb{A}^n \). Since each \( p'_i \) contains \( J(X) \), this is a chain of closed, irreducible subsets of \( X \). Hence \( \dim k[X] \leq \dim X \) so we have equality.  

Corollary 1.6.2. Suppose \( k \) is algebraically closed and \( X \subseteq \mathbb{A}^n \) is an affine variety. Then \( \dim X = \text{tr deg}_k k(X) \), the transcendence degree of the function field of \( X \).

Proof. It is well known from commutative algebra that \( \dim k[X] = \text{tr deg}_k k(X) \). Apply Proposition 1.6.1.

Proposition 1.6.3. For an affine variety \( X \) with projective closure \( \overline{X} \), \( k(\overline{X}) = k(X) \).

We extend the notion of dimension to projective and quasi-projective varieties by using the transcendence degree definition. Proposition 1.6.3 says that this definition agrees with the topological definition of dimension.

Definition. For any quasi-projective variety \( X \), the dimension of \( X \) is defined by

\[
\dim X := \text{tr deg}_k k(X).
\]

The following is a classic result due to Krull, which is proven by an algebraic statement about height of prime ideals in \( k[t_1, \ldots, t_n] \).

Theorem 1.6.4 (Krull’s Hauptidealsatz). Suppose \( k \) is algebraically closed. Then

(a) If \( I = (f_1, \ldots, f_s) \) is an ideal of \( A = k[t_1, \ldots, t_n] \), then \( \dim Z(I) \geq n - s \).

(b) If \( X \subseteq \mathbb{A}^n \) is any algebraic subset with irreducible components \( X_1, \ldots, X_m \subseteq X \), then \( \dim X_i = n - 1 \) for all \( 1 \leq i \leq m \) if and only if there exists an \( f \in A \setminus k \) with \( X = Z(f) \).

Corollary 1.6.5. A variety \( X \subseteq \mathbb{A}^n_k \) has codimension 1 if and only if \( X = Z(f) \) for a nonconstant, irreducible polynomial \( f \in k[t_1, \ldots, t_n] \).

Example 1.6.6. For affine space, \( \dim \mathbb{A}^n_k = \dim k[t_1, \ldots, t_n] = n \).

Example 1.6.7. If \( f \in k[x, y] \) is an irreducible polynomial, then Corollary 1.6.5 says \( \dim Z(f) = 1 \). This gives meaning to the name curve for zero sets of irreducible polynomials in \( \mathbb{A}^2 \): they are the codimension 1 subvarieties, as we would like.

Corollary 1.6.8. If \( X \) is an affine variety with dimension \( n \) and \( r \leq n \), then any polynomials \( f_1, \ldots, f_r \in k[X] \) have a common zero.

Corollary 1.6.9. In \( \mathbb{P}^2 \), for any forms \( F \) and \( G \) defining curves \( C_1 = Z(F) \) and \( C_2 = Z(G) \), we have \( C_1 \cap C_2 \neq \emptyset \).
1.7 Complete Varieties

Definition. A variety $X$ is complete if for any variety $Y$, the projection map $X \times Y \to Y, (x, y) \mapsto y$, is a closed map.

Proposition 1.7.1. Let $X$ be a complete variety. Then

1. Any closed subvariety of $X$ is complete.
2. If $Y$ is complete then $X \times Y$ is also complete.
3. For every morphism $\varphi : X \to Y$, $\varphi(X)$ is closed in $Y$ and complete.
4. If $X \subseteq Y$ as a subvariety, then $X$ is closed.

Proof. (1) Let $X' \subseteq X$ be a closed subvariety and $Y$ any variety, and consider $\pi' : X' \times Y \to Y$. Suppose $Z \subseteq X' \times Y$ is a closed subset. In general $\{x\} \times Y$ is closed in $X \times Y$ so the diagram

$$
\begin{array}{ccc}
Z \subseteq X' \times Y & \xrightarrow{i} & X \times Y \\
\downarrow{\pi} & & \downarrow{\pi} \\
Y & & Y
\end{array}
$$

commutes and thus the image of $Z$ is closed.

(2) Assume $Y$ is complete and let $Z$ be an arbitrary variety. We can factor the map $X \times Y \times Z \to Z$ as

$$
X \times Y \times Z \to Y \times Z \to Z
$$

but both of these maps are closed since $X$ and $Y$ are each complete. The composition of closed maps is closed, so $X \times Y$ is complete.

(3) Let $\Gamma = \{(x, \varphi(x)) | x \in X \} \subseteq X \times Y$ be the graph of $\varphi$. Then $\Gamma$ is closed, so $\varphi(X)$ is the projection of $\Gamma = X \times \varphi(X)$ onto $Y$, and since $X$ is complete, $\varphi(X)$ is closed. For completeness, use (1).

(4) follows from applying (3) to the inclusion $i : X \to Y$.

Theorem 1.7.2. Every projective variety is complete.

Proof. We proved that every closed subvariety of a complete variety is complete, so it suffices to prove $\mathbb{P}^n$ is complete for all $n \geq 1$. In other words we will show that if $\pi : \mathbb{P}^n \times Y \to Y$ is the projection map and $C \subseteq \mathbb{P}^n \times Y$ is closed then $\pi(C) \subseteq Y$ is closed. Set $A = k[Y]$ and $B = A[T_0, T_1, \ldots, T_n]$. Then $B$ is a ring of $k$-valued functions on $k^{n+1} \times Y$. For every proper homogeneous ideal $I \subset B$, define

$$
Z^*(I) = \{(x^*, y) | f(x, y) = 0 \text{ for all } f \in I\} \subseteq \mathbb{P}^n \times Y.
$$

Then the $Z^*(I)$ are the closed subsets of $\mathbb{P}^n \times Y$ so it suffices to prove $\pi(Z^*(I))$ is closed for all proper homogeneous ideals $I \subset B$. We may assume $Z^*(I)$ is irreducible, i.e. $I$ is prime.
1.8 Tangent Space

We may also assume \( \pi|_{Z^*(I)} \) is dominant (changing the target to \( \pi(Z^*(I)) \) if necessary). Then we must show for every \( y \in Y \), there exists \( x^* \in \mathbb{P}^n \) so that \((x^*, y) \in Z^*(I)\), since then we will have \( \pi(Z^*(I)) = \pi(Z^*(I)) \).

Take \( M \subset A \) to be the maximal ideal that vanishes at \( y \). Then \( J = MB + I \) is a homogeneous ideal so \( Z^*(J) \) is defined, and if we show \( Z^*(J) \) is nonempty, we’ll be done. Assume to the contrary that \( Z^*(J) = \emptyset \). Then there is a \( k > 0 \) such that \( T_i^k \in J \) for each \( T_i \).

Equivalently, there is an \( m > 0 \) so that \( B_m \), the set of all degree \( m \) homogeneous polynomials in \( B \), is contained in \( J \). Set \( N = B_m/(B_m \cap I) \). This is a finitely generated \( A \)-module in the obvious way. Moreover, notice that \( MN = N \). Then by Nakayama’s Lemma, this implies \( N = 0 \). But then \( B_m = B_m \cap I \) so it follows that \( Z^*(I) = \emptyset \), which is impossible for a proper ideal \( I \subset B \). Hence \( Z^*(J) \neq \emptyset \) so the theorem is proved.

Example 1.7.3. Consider the variety \( X = Z(xy - 1) \subseteq \mathbb{A}^2 \). Then under the projection \( \mathbb{A}^2 \to \mathbb{A}^1 \), the image of \( X \) is \( \mathbb{A}^1 \setminus \{0\} \) which is not a closed set, so \( X \) is not complete. We will see below that affine varieties are not complete in general.

Corollary 1.7.4. Let \( X \) be a connected complete variety. Then \( \mathcal{O}_X(X) = k \). That is, every regular \( k \)-valued function on \( X \) is constant.

Proof. Take \( f \in \mathcal{O}_X(X) \). Then \( f \) is a map \( f : X \to k = \mathbb{A}^1 \). Extend this to a map

\[
g : X \to \mathbb{A}^1 \hookrightarrow \mathbb{P}^1,
\]

so \( g \) is not surjective onto \( \mathbb{P}^1 \). By completeness of \( X \), \( g(X) \) is closed in \( \mathbb{P}^1 \), but the only proper closed subsets of \( \mathbb{P}^1 \) are point-sets. Since \( X \) is connected, we must have \( g(X) = \{x_0\} \), or in other words, \( g \) is constant. This implies \( f \) is constant. \( \square \)

This fact is analoguous to the theorem in complex analysis that every holomorphic function on a connected compact domain is constant.

Corollary 1.7.5. Let \( X \) be a projective variety. Then any morphism \( X \to Y \) into an irreducible, projective curve \( Y \) is either surjective or constant.

Corollary 1.7.6. Nontrivial affine varieties are not projective.

Proof. Let \( X \) be an affine variety of dimension at least 1. View \( X \) as a proper subset of affine \( n \)-space \( \mathbb{A}^n \), which has coordinate algebra \( k[T_1, \ldots, T_n] \). Then some coordinate function \( T_i \) does not vanish on \( X \), so \( T_i \in \mathcal{O}_X(X) \) is a nonconstant regular function on \( X \). \( \square \)

1.8 Tangent Space

Suppose \( k \) is algebraically closed and \( X \subseteq \mathbb{A}^N \) is an affine variety over \( k \). For a point \( P = (\alpha_1, \ldots, \alpha_N) \in X \), take a line through \( P \), \( L_\alpha = \{\alpha t + P \mid t \in k\} \) for some \( \alpha \in k^N \setminus \{0\} \). Then if \( J(X) = (f_1, \ldots, f_m) \), we see that \( X \cap L_\alpha = Z(g_1, \ldots, g_m) \), where \( g_i(t) = f_i(\alpha t) \in k[t] \).

For \( L_\alpha \) to be tangent to \( X \) at \( P \), we need these \( g_i \) to vanish ‘to a higher multiplicity’, as in complex analysis.
Definition. If \( L \) is a line and \( P \in X \cap L \), the multiplicity of \( X \cap L \) at \( P \) is defined to be the multiplicity of \( t = 0 \) as a root of the polynomial
\[
f_\alpha(t) := \gcd(f_1(\alpha t), \ldots, f_m(\alpha t)).
\]
(Formally, we say that the multiplicity of any \( t \) as a root of the zero polynomial is \( \infty \).) Then \( L \) is tangent to \( X \) at \( P \) if the multiplicity of \( X \cap L \) at \( P \) is at least 2.

Definition. The tangent space to \( X \) at \( P \) is a linear subspace \( T_P X \) of \( \mathbb{A}^N \) consisting of all lines through the origin \( L_\alpha = \{ \alpha t \mid t \in k \} \) such that the affine line \( L_\alpha^P = \{ \alpha t + P \mid t \in k \} \) is tangent to \( X \) at \( P \).

Proposition 1.8.1. For any \( P \in X \), \( T_P X \) is a well-defined vector subspace of \( \mathbb{A}^N \).

Proof. If \( J(X) = (f_1, \ldots, f_m) \), write
\[
f_i = \sum_{\ell=1}^{\infty} f_i^{(\ell)}
\]
where \( f_i^{(\ell)} \) is the homogeneous part of \( f_i \) of degree \( \ell \). If \( P \in X \), then \( f_i^{(0)}(P) = 0 \). Thus \( f_i(\alpha t) = t f_i^{(1)}(\alpha) + t^2 f_i^{(2)}(\alpha) + \ldots \). This shows that \( L_\alpha \subseteq T_P X \) if and only if \( f_i^{(1)}(\alpha) \) which is a linear condition. Thus \( T_P X \) is a linear subspace of \( \mathbb{A}^N \) as claimed.

Examples.

1. For any \( P \in \mathbb{A}^N \), \( T_P \mathbb{A}^N = \mathbb{A}^N \).

2. If \( X = Z(f) \subseteq \mathbb{A}^N \) is a hypersurface defined by an irreducible polynomial \( f \in k[t_1, \ldots, t_N] \), then for any \( P \in X \), \( T_P X = Z(f^{(1)}) \). Notice that
\[
f^{(1)}(t_1, \ldots, t_N) = \sum_{i=1}^{N} \frac{\partial f}{\partial t_i}(t_i - \alpha_i)
\]
so it is immediate that \( T_P X \) is equal to the kernel of the \( 1 \times N \) matrix \( \left( \frac{\partial f}{\partial t_j} \right)_{1 \leq j \leq N} \). We see once again that \( T_P X \) is a vector space since it is the kernel of a linear map. In particular, \( \dim T_P X = N - \text{rank} \left( \frac{\partial f}{\partial t_j} \right) \).
3. More generally, if \( J(X) = (f_1, \ldots, f_m) \), then \( \left( \frac{\partial f_i}{\partial t_j} \right) \) is an \( m \times N \) matrix and
\[
T_P X = \ker \left( \frac{\partial f_i}{\partial t_j} \right).
\]

This shows that \( \dim T_P X = N - \text{rank} \left( \frac{\partial f_i}{\partial t_j} \right) \).

We can use this notion of tangency to formalize the property of “singularity” at a point of a variety.

**Definition.** For an affine variety \( X \), write \( s_X = \min \{ \dim T_P X \mid P \in X \} \). Then a point \( P \in X \) is nonsingular (or, \( X \) is nonsingular at \( P \)) if \( \dim T_P X = s_X \). Otherwise, \( P \) is said to be singular.

**Proposition 1.8.2.** The subset \( \text{Sing } X = \{ P \in X \mid P \text{ is singular} \} \) is a proper, Zariski-closed subset of \( X \). In particular, \( X \) has a dense, open subset of nonsingular points.

**Proof.** The condition that \( \dim T_P X = \ell \) is equivalent to the nonvanishing of the \( (N - \ell) \times (N - \ell) \) minors of the matrix \( \left( \frac{\partial f_i}{\partial x_j} \right) \). These minors are polynomials over \( k \), so their zero locus, \( \text{Sing } X \), is closed. \( \square \)

The next theorem connects the dimension of the tangent space to the topological dimension of the space \( X \). By Proposition 1.6.1, this also relates the dimension of the tangent space to the Krull dimension of the coordinate ring of \( X \).

**Theorem 1.8.3.** If \( P \in X \) is a nonsingular point of an affine variety \( X \), then \( \dim T_P X = \dim X \).

**Proof.** Let \( \varphi : X \to Y \) be an isomorphism of varieties. This determines an isomorphism of vector spaces \( T_P X \to T_{\varphi(P)} Y \). By the proof of Proposition 1.8.2, \( \dim T_P X = \ell \) is an open condition, so it suffices to consider any variety that is birationally equivalent to \( X \). It is a general fact that any affine variety is birationally equivalent to a hypersurface; thus we may assume \( X \subseteq \mathbb{A}^N \) is a hypersurface, with \( J(X) = (f) \) for some irreducible polynomial \( f \in k[t_1, \ldots, t_N] \).

We need to show that \( s_X = \dim X = N - 1 \). Note that
\[
T_P X = Z \left( \sum_{i=1}^N \frac{\partial f}{\partial x_i}(P)(x_i - \alpha_i) \right).
\]

Since \( X \) is a hypersurface, \( \dim T_P X \geq N - 1 \). However, the only way for us to have \( \dim T_P X = N \) is if each partial derivative \( \frac{\partial f}{\partial x_i} \) is identically zero on \( X \). If \( \text{char } k = 0 \), this is only true for \( f = 0 \) so we are done. If \( \text{char } k = p > 0 \), the above condition holds if and only if \( f = g(x_1^p, \ldots, x_N^p) = [g(x_1), \ldots, x_N]^p \) for some \( g \in k[t_1, \ldots, t_N] \). But \( J(X) \) is radical, which implies \( g \in J(X) \), so \( (f) \neq J(X) \). This a contradiction of course, so in all cases, \( \dim T_P X = N - 1 \) as required. \( \square \)
Definition. Let \( f \in k[t_1, \ldots, t_N] \) and \( P = (\alpha_1, \ldots, \alpha_N) \in \mathbb{A}^N \). The linear term in the homogeneous expansion of \( f \) at \( P \),

\[
d_P f := \sum_{i=1}^{N} \frac{\partial f}{\partial x_i}(P)(x_i - \alpha_i),
\]
is called the differential of \( f \) at \( P \).

**Lemma 1.8.4.** For any \( P \in \mathbb{A}^N \), the differential \( d_P \) is a derivation:

(a) \( d_P(f + g) = d_P f + d_P g \).

(b) \( d_P(fg) = (d_P f)g + f(d_P g) \).

**Corollary 1.8.5.** If \( X \subseteq \mathbb{A}^N \) is a variety with \( J(X) = (f_1, \ldots, f_m) \) and \( P \in X \), then

\[
T_P X = Z(d_P f_1, \ldots, d_P f_m).
\]

**Remark.** For \( g \in k[X] \), we can represent \( g \) by a form \( G \in k[t_1, \ldots, t_N] \), so that \( g = G + J(X) \). Set \( d_P g := d_P G \). This is only well-defined up to elements of the form \( d_P f \) for \( f \in J(X) \). Thus, if \( G' = G + f \) for \( f \in J(X) \), then \( d_P G' = d_P G + d_P f \) but since \( T_P X = Z(f_1, \ldots, f_m) \) and \( f \in (f_1, \ldots, f_m) \), the differential of \( f \) disappears. Thus we can define \( d_P g \) by

\[
d_P g = d_P G|_{T_P X}
\]

for any lift \( G \in k[t_1, \ldots, t_N] \) such that \( g = G + J(X) \).

The differential \( d_P \) induces a map into the dual of the tangent space:

\[
k[X] \longrightarrow (T_P X)^* \quad g \longmapsto d_P G \quad \text{where} \quad g = G + J(X).
\]

**Theorem 1.8.6.** Let \( X \subseteq \mathbb{A}^N \) be an affine variety and \( P \in X \). Then the differential \( d_P \) induces an isomorphism \( m_P / m_P^2 \rightarrow (T_P X)^* \).

**Proof.** Restricting \( d_P \) to \( m_P \) gives a map \( d_P : m_P \rightarrow (T_P X)^* \), which is linear since \( d_P \) is a derivation. Now any linear form \( \lambda \) on \( T_P X \) is induced by a linear function \( \ell \) on \( \mathbb{A}^N \) with \( \ell(P) = 0 \). Then \( d_P \ell = \lambda \), so \( d_P \) is surjective.

Next, suppose \( g \in m_P \) with \( d_P g = 0 \) and take a lift \( G \in k[t_1, \ldots, t_N] \) with \( G|_X = g \). Then \( 0 = d_P g = d_P G|_{T_P X} \), so if \( g = \sum_{i=1}^{m} a_i f_i \) then \( d_P G = \sum_{i=1}^{m} a_i d_P f_i \). Then

\[
G' := G - \sum_{i=1}^{m} a_i f_i
\]

has no linear term by construction and thus \( G' \in (t_1 - \alpha_1, \ldots, t_N - \alpha_N) \). On the other hand, \( G'|_X = G|_X = g \) so if \( G' \in (t_1 - \alpha_1, \ldots, t_N - \alpha_N)^2 \) then we must have \( g \in m_P^2 \). This shows that \( \ker d_P \subseteq m_P^2 \). The reverse inclusion is shown similarly, so by the first isomorphism theorem, \( m_P / m_P^2 \cong (T_P X)^* \). \( \square \)
Corollary 1.8.7. For any affine variety $X$ over an algebraically closed field $k$, $\dim X = \dim_k \mathfrak{m}_P/\mathfrak{m}_P^2$ for any nonsingular point $P \in X$.

Proof. Apply Theorems 1.8.3 and 1.8.6. \qed

Definition. The vector space $\mathfrak{m}_P/\mathfrak{m}_P^2$ is called the cotangent space to $X$ at $P$. It is the dual of the tangent space by Theorem 1.8.6.

Definition. If $\varphi : X \to Y$ is a morphism of varieties, the induced map $\varphi^* : k[Y] \to k[X]$ determines a linear map $\mathfrak{m}_{\varphi(P)}/\mathfrak{m}_{\varphi(P)}^2 \to \mathfrak{m}_P/\mathfrak{m}_P^2$. The dual of this map,

$$d_P \varphi : T_P X \to T_{\varphi(P)} Y,$$

is called the differential of $\varphi$ at $P \in X$.

Theorem 1.8.8. If $\varphi : X \to Y$ is an isomorphism of varieties, then the differential $d_P \varphi : T_P X \to T_{\varphi(P)} Y$ is a linear isomorphism for all $P \in X$.

Remark. The above description shows that $T_P X$ is an ‘intrinsic object’ to $X$; that is, it only depends on the isomorphism class of $X$. The next result says that the tangent space is also a local object.

Theorem 1.8.9. For any $P \in X$, $(T_P X)^* \cong \mathfrak{m}_P \mathcal{O}_{X,P}/(\mathfrak{m}_P \mathcal{O}_{X,P})^2$.

Proof. We can extend $d_P : k[X] \to (T_P X)^*$ to a map $d_P : \mathcal{O}_{X,P} \to (T_P X)^*$ by:

$$d_P \left( \frac{f}{g} \right) = \frac{gd_P f - f d_P g}{g^2}.$$

Then the proof of Theorem 1.8.6 goes through with appropriate modifications. \qed

Definition. For any quasi-projective variety $X$ and point $P \in X$, we define the tangent space to $X$ at $P$ by

$$T_P X = (\mathfrak{m}_P \mathcal{O}_{X,P}/(\mathfrak{m}_P \mathcal{O}_{X,P})^2)^*.$$

By Theorem 1.8.9, this description agrees with $T_P (X \cap U_i)$ for any affine patch $U_i$ (i.e. the tangent spaces are isomorphic).

Definition. For a projective variety $X \subseteq \mathbb{P}^N$ such that $J(X) = (F_1, \ldots, F_m)$, and a point $P \in X \cap U_i$, we define the projective tangent space to $X$ at $P$ to be

$$T_P X = \overline{T_{\varphi^{-1}(P)}(\varphi^{-1}(X \cap U_i))}.$$

Lemma 1.8.10. $T_P X$ is a linear subvariety of $\mathbb{P}^N$.

Proof. This follows from the fact that

$$T_P X \cong Z \left( \left\{ \sum_{i=0}^{N} \frac{\partial F_i}{\partial X_i} : 1 \leq j \leq m \right\} \right).$$

\qed
1.9 Local Parameters

As with affine tangent spaces, we have
\[
\dim T_P X = \dim \overline{T_P X} = N - \text{rank} \left( \frac{\partial F_i}{\partial X_j}(P) \right).
\]

**Definition.** A quasi-projective variety \( X \) is **nonsingular** at a point \( P \in X \) if
\[
\dim X = N - \text{rank} \left( \frac{\partial F_i}{\partial X_j}(P) \right).
\]

**Example 1.8.11.** A hypersurface \( X = Z(F) \) is nonsingular at \( P \) if and only if \( \frac{\partial F}{\partial x_i}(P) \neq 0 \) for some \( 1 \leq i \leq N \).

1.9 Local Parameters

**Definition.** Let \( X \) be a nonsingular variety of dimension \( n \). We say \( t_1, \ldots, t_n \in \mathcal{O}_{X, P} \) are local parameters at \( P \) if

1. \( t_i(P) = 0 \) for each \( i \); that is, \( t_i \in \mathfrak{m}_P \).

2. \( \bar{t}_1, \ldots, \bar{t}_n \) form a basis of the vector space \( \mathfrak{m}_P / \mathfrak{m}_P^2 \).

**Proposition 1.9.1.** Local parameters generate the maximal ideal at \( P \).

**Proof.** This follows from Nakayama’s Lemma. \( \square \)

**Definition.** Let \( A \) be a local ring with maximal ideal \( \mathfrak{m} \) and residue field \( k = A/\mathfrak{m} \). Then \( A \) is said to be a **regular ring** if \( \dim A = \dim_k \mathfrak{m}/\mathfrak{m}^2 \).

Proposition 1.9.1 shows that \( P \in X \) is nonsingular if and only if the local ring \( \mathcal{O}_{X, P} \) is a regular ring.

**Remark.** For a nonsingular point \( P \in X \), the topological completion of \( \mathcal{O}_{X, P} \) at \( \mathfrak{m}_P \), denoted \( \hat{\mathcal{O}}_{X, P} \), is isomorphic to the power series ring \( k[[t_1, \ldots, t_n]] \), where \( t_1, \ldots, t_n \) are local parameters at \( P \). This can be used, for example, to show that \( \mathcal{O}_{X, P} \) is a UFD, since power series rings are UFDs in general. In the next chapter, we will prove directly that the local rings of \( X \) are UFDs when \( X \) is a curve.
2 Curves

In this chapter we further study the geometry of algebraic varieties of dimension 1.

**Definition.** An irreducible, projective algebraic variety $X$ of dimension $\dim X = 1$ is called an algebraic curve.

For the rest of the chapter, $X$ will denote an algebraic curve. The first important result is that the local rings $\mathcal{O}_{X,P}$ of a nonsingular curve are discrete valuation rings.

**Theorem 2.0.1.** Let $X$ be an algebraic curve and $P \in X$ a nonsingular point. Then $\mathcal{O}_{X,P}$ is a DVR.

**Proof.** Fix $P \in X$ and let $\mathcal{O}_P = \mathcal{O}_{X,P}$ be the local ring at $P$, with maximal ideal $m_P$ and residue field $\kappa(P) = \mathcal{O}_P/m_P$. Then by Proposition 1.9.1, $\mathcal{O}_P$ is a regular local ring. Thus Corollary 1.8.7 gives us $\dim_{\kappa(P)}(m_P/m_P^2) = \dim X = 1$. Let $t \in m_P$ such that $d_P t \neq 0$; that is, $t$ is a local parameter at $P$. Then for $f \in \bar{k}(X)$ with $f(P) = 0$, we have $f = t^ru$ in $\mathcal{O}_P$, for some $u \in \mathcal{O}_P^\times$. Define a map

$$\text{ord}_P : \mathcal{O}_P \to \mathbb{Z}$$

$$f \mapsto \text{ord}_P(f) = \max\{d \in \mathbb{Z} \mid f \in m_P^d\}.$$ 

Explicitly, if $f = t^ru$ where $u$ is a unit, then $\text{ord}_P(f) = r$. Formally, we also set $\text{ord}_P(f) = 0$ if $f(P) \neq 0$, to get a map on all of $\bar{k}(X)$. One then shows that $\text{ord}_P$ is a discrete valuation with $\mathcal{O}_P$ as its valuation ring. \hfill $\square$

**Corollary 2.0.2.** For any nonsingular point $P \in X$, $\mathcal{O}_P$ is a PID and therefore a UFD.

**Proof.** By the above, every ideal of $\mathcal{O}_P$ is of the form $(t^r)$ where $t \in m_P$ is a local parameter. \hfill $\square$

**Definition.** A local parameter $t \in m_P$ is called a uniformizer at $P$.

**Definition.** Fix a rational function $f \in \bar{k}(X)$ and an integer $r > 0$. We say $f$ has a pole of order $r$ at $P$ if $\text{ord}_P(f) = -r$, and a zero of order $r$ at $P$ if $\text{ord}_P(f) = r$.

**Remark.** A rational function $f \in \bar{k}(X)$ is regular at $P$ if and only if $\text{ord}_P(f) \geq 0$.

**Proposition 2.0.3.** Every nonconstant, rational function $f \in \bar{k}(X)$ has at least one pole.

**Proof.** A rational function $f \in \bar{k}(X)$ with no poles is regular everywhere on $X$, and therefore constant by Corollary 1.7.4, since $X$ is projective. \hfill $\square$

**Remark.** Each $f \in \bar{k}(X)$ has only finitely many zeroes and poles, or none at all.
2.1 Divisors

Definition. Let $X$ be a variety. An irreducible divisor on $X$ is a closed, irreducible $k$-subvariety $x$ of $X$ of codimension 1.

When $X$ is a curve over $k$, an irreducible divisor is a closed point of MaxSpec $k[X \cap U]$ for some affine patch $U_i$, or alternatively, a $G_k$-orbit of points in $X(\overline{k})$.

Definition. The degree of an irreducible divisor $x$ on $X$ is the size of the $G_k$-orbit in $X(\overline{k})$ corresponding to $x$, i.e. $\deg(x) = [k(P) : k]$ for any $P \in x$.

Example 2.1.1. Let $X = \mathbb{P}^1$. On an affine patch $\mathbb{A}^1 \hookrightarrow U \subseteq \mathbb{P}^1$, the irreducible divisors correspond to irreducible polynomials in $k[\mathbb{A}^1] = k[t]$.

Definition. Let $X$ be a curve over $k$. The divisor group on $X$, $\text{Div}(X)$, is the free abelian group on the set of irreducible divisors on $X$:

$$\text{Div}(X) = \left\{ D = \sum_{x \in X} n_x x : n_x \in \mathbb{Z}, n_x \neq 0 \text{ for finitely many } x \right\}.$$

The elements of $\text{Div}(X)$ are called divisors on $X$. For a divisor $D = \sum_{x \in X} n_x x \in \text{Div}(X)$, the degree of $D$ is $\deg(D) = \sum_{x \in X} n_x \deg(x)$.

Example 2.1.2. If $k$ is algebraically closed, then the irreducible divisors are the points of $X$, so each $D \in \text{Div}(X)$ is a weighted sum of points of $X$: $D = \sum_{x \in X} n_x x$. The degree of such a divisor is just the sum of the weights: $\deg(D) = \sum_{x \in X} n_x$.

Now assume $X$ is a nonsingular curve. For $f \in k(X)^*$, we can define a divisor $D(f) = \sum_{x \in X} \text{ord}_x(f)x$, called the principal divisor of $f$. This defines a map

$$D : k(X)^* \rightarrow \text{Div}(X)$$

whose image is denoted $\text{PDiv}(X)$, the group of principal divisors on $X$.

Definition. The Picard group, or divisor class group, of $X$ is the quotient group

$$\text{Pic}(X) = \text{Div}(X)/\text{PDiv}(X).$$

This defines an equivalence relation on divisors: $D_1 \sim D_2$ if $D_1 = D_2 + D(f)$ for some $f \in k(X)^*$.

Example 2.1.3. Consider the variety $E = Z(y^2 - x^3 - 3x^2 - 2x)$. This is the elliptic curve defined by $y^2 = f(x)$ where $f = x^3 + 3x^2 + 2x = x(x+1)(x+2)$. The projective closure of $E$ is $\overline{E} = Z(f_h)$, where

$$f_h = ZY^2 - X^3 - 3X^2Z - 2XZ^2.$$

Setting $y = \frac{Y}{Z}$, we can compute its divisor on $E$:

$$D(y) = \sum_{P \in X} \text{ord}_P(y)P.$$

On the affine part, there are only zeroes of $y$, and they occur precisely at $P = (-2, 0), (-1, 0)$ and $(0, 0)$.
Note that $t \in \mathcal{O}_{E,P}$ is a uniformizer whenever $d_P t \neq 0$. Viewing $t \in k[x,y]$, i.e. as a lift of $[t] \in \mathcal{O}_{E,P}$, we have that

- $t = x$ is a uniformizer as long as $d_P x = x|_{T_pE} \neq 0$, which is equivalent to $\frac{\partial f}{\partial y}(P) \neq 0$.

- $t = y$ is a uniformizer as long as $d_P y = y|_{T_pE} \neq 0$, that is, $\frac{\partial f}{\partial x}(P) \neq 0$.

In particular, we can always find a uniformizer! For $P = (-2,0), (-1,0)$ and $(0,0)$, $t = y$ is a uniformizer. It follows that $\text{ord}_P(y) = 1$ at each of these points, and $\text{ord}_Q(y) = 0$ for any other point $Q \in E$. Thus the divisor for $y$ is

$$(y) = (-2,0) + (-1,0) + (0,0) + \text{ord}_\infty(y)\infty.$$  

The point at infinity is where $Z = 0$, so by the defining equation for $E$, $X = 0$ and, in projective space, $Y = 1$. Set $P = \infty = [0,1,0]$. On a different affine patch containing $P$, we have coordinates $\zeta = \frac{Z}{Y}$ and $\xi = \frac{X}{Y}$. Then $y = \frac{1}{\zeta}$ so $\text{ord}_P(Y) = \text{ord}_P\left(\frac{1}{\zeta}\right) = -\text{ord}_P(\zeta)$. In these coordinates, the defining equation for $E$ becomes

$$g = \zeta - (\xi^3 + 3\xi^2\zeta + 2\xi\zeta^2).$$

Notice that $\frac{\partial g}{\partial \zeta}(0,0) = 1$, so $\xi$ is a uniformizer on this patch. Now

$$\text{ord}_P(\zeta) = \text{ord}_P(\xi^3 + 3\xi^2\zeta + 2\xi\zeta^2) \geq \min\{\text{ord}_P(\xi^3), \text{ord}_P(3\xi^2\zeta), \text{ord}_P(2\xi\zeta^2)\}.$$
We have \( \text{ord}_P(\xi^3) = 3 \) and \( \text{ord}_P(3\xi^2\zeta), \text{ord}_P(2\xi^2) \geq 3 \). If all three orders are equal to 3, then by the ultrametric inequality \( \text{ord}_P(\zeta) \) must be strictly greater than the minimum, which is 3 in this case. But then \( \text{ord}_P(3\xi^2\zeta) = \text{ord}_P(\xi^2) + \text{ord}_P(\zeta) > 2 + 3 > 3 \), so in fact we cannot have all three orders equal to 3. Hence \( \text{ord}_P(\zeta) = 3 \). We have thus calculated the divisor of \( y \) on the elliptic curve \( E \):

\[
(y) = (-2, 0) + (-1, 0) + (0, 0) - 3\infty.
\]

## 2.2 Morphisms Between Curves

**Proposition 2.2.1.** Let \( C \) be an algebraic curve and \( X \) a projective variety, and suppose \( \varphi : C \rightarrow X \) is a rational map. If \( P \in C \) is a nonsingular point then \( \varphi \) is regular at \( P \).

**Proof.** A more general result is that if \( Y \) is a normal variety, i.e. the local rings \( O_{Y,P} \) are normal rings, then the locus of nondeterminacy of such a rational map \( \varphi : Y \rightarrow X \) is a subvariety of codimension at least 2. For \( Y = C \) a curve, this means there are no points where \( \varphi \) fails to be regular. \( \square \)

A nonconstant rational map \( \varphi : C_1 \rightarrow C_2 \) between curves induces a field extension \( k(C_2) \hookrightarrow k(C_1) \). Since both function fields have transcendence degree 1, this is in fact a finite field extension.

**Definition.** For curves \( C_1 \) and \( C_2 \) and a rational map \( \varphi : C_1 \rightarrow C_2 \), define the **degree** of \( \varphi \) by \( \text{deg} \varphi = [k(C_1) : k(C_2)] \); the **separable degree** of \( \varphi \) by \( \text{deg}_s \varphi = [k(C_1) : k(C_2)]_s \); and the **inseparable degree** of \( \varphi \) by \( \text{deg}_i \varphi = [k(C_1) : k(C_2)]_i \). We say \( \varphi \) is **separable** if \( k(C_1) \supseteq k(C_2) \) is a separable extension.

**Definition.** Any finitely generated field extension of \( k \) with transcendence degree 1 over \( k \) is called a **function field** of degree 1 over \( k \).

**Proposition 2.2.2.** There is an equivalence of categories

\[
\left\{ \begin{array}{c}
\text{nonsingular curves over } k \\
\text{with nonconstant, rational maps}
\end{array} \right\} \leftrightarrow \left\{ \begin{array}{c}
\text{function fields of deg. 1 over } k \\
\text{with } k\text{-homomorphisms}
\end{array} \right\}.
\]

**Proof.** (Sketch) The assignment \( X \mapsto k(X) \) determines one direction: we have seen that \( k(X) \) is indeed a function field over \( k \). Conversely, for a function field \( K/k \), we associate an abstract algebraic curve \( X_K \) to \( K \) by putting a Zariski topology on the maximal ideals of the valuation rings \( O \subset K \). The structure sheaf is given by \( O_{X_K}(U) = \bigcap_{P \in U} O_P \) where \( U \subseteq X_K \) is open and \( O_P \) is the valuation ring corresponding to \( P \). This determines the reverse assignment \( K \mapsto X_K \). One now checks that these assignments are inverse and preserve categorical structure. \( \square \)

Now fix nonsingular curves \( X \) and \( Y \) over \( k \) and a morphism \( \varphi : X \rightarrow Y \) defined over \( k \). Then an irreducible divisor \( y \in \text{Div}(Y) \) corresponds to a maximal ideal \( m_Y \) (on some affine patch) with uniformizer \( t_y \in k(Y) \).
Definition. The **pullback** of \( \varphi \) is a map \( \varphi^* : \text{Div}(Y) \to \text{Div}(X) \) defined on irreducible divisors by
\[
\varphi^* y = \sum_{x \in X} \text{ord}_X (\varphi^* t_y) x,
\]
where \( t_y \) is a uniformizer at \( y \), and extended linearly.

**Example 2.2.3.** Let \( X \) be the plane curve defined by \( y^2 - x \) and \( Y = \mathbb{P}^1 \) the projective line, and let \( \varphi : X \to Y \) be the \( x \)-coordinate projection.

\[
\begin{align*}
\varphi^* y_0 &= 2x_0 + \text{ord}_\infty (\varphi^* t_{y_0}) \infty \\
\varphi^* y_1 &= x_1 + x_2 + \text{ord}_\infty (\varphi^* t_{y_1}) \infty.
\end{align*}
\]

**Definition.** Let \( \varphi : X \to Y \) be a morphism, \( x \in X \) and \( y = \varphi(x) \in Y \). The number \( e_\varphi(x) = \text{ord}_x (\varphi^* t_y) \) is called the **ramification index** of \( \varphi \) at \( x \). If \( e_\varphi(x) = 1 \) and the residue field extension \( \kappa(x)/\kappa(y) \) is separable, we say \( \varphi \) is **unramified** at \( x \). Otherwise, we say \( \varphi \) is **ramified** at \( x \), and \( y \) is called a **branch point** of \( \varphi \).

**Proposition 2.2.4.** Fix a morphism \( \varphi : X \to Y \), \( x \in X \) and \( y = \varphi(x) \in Y \). Then

1. \( e_\varphi(x) \) does not depend on the choice of uniformizer \( t_y \).
2. For any \( Q \in Y \), \( \sum_{P \in \varphi^{-1}(Q)} e_\varphi(P) = \deg \varphi \).
3. All but finitely many \( Q \in Y \) have \( \# \varphi^{-1}(Q) = \deg_\varphi \).
4. If \( \psi : Y \to Z \) is a morphism then \( e_{\varphi \psi}(x) = e_\varphi(x) e_\psi(y) \).

**Definition.** Given a morphism \( \varphi : X \to Y \), the **pushforward** of \( \varphi \) is a map \( \varphi_* : \text{Div}(X) \to \text{Div}(Y) \) defined on irreducible divisors \( x \in X \) by
\[
\varphi_* x = [\kappa(x) : \kappa(\varphi(x))] \varphi(x)
\]
and extended linearly.
Proposition 2.2.5. Let \( \varphi : X \to Y \) be a morphism and \( D \in \text{Div}(Y) \) and \( D' \in \text{Div}(X) \) divisors. Then

1. \( \deg(\varphi^*D) = (\deg \varphi)(\deg D) \).
2. \( \varphi^*(f) = (\varphi^*f) \) for any function \( f \in k(Y) \).
3. \( \deg(\varphi_* D') = \deg(D') \).
4. \( \varphi_* \varphi^* D = (\deg \varphi)D \).

Corollary 2.2.6. For any function \( f \in k(X) \) on a curve \( X \), \( \deg(f) = 0 \).

Proof. View \( f \) as a function \( X \to \mathbb{P}^1 \). Then \( \deg(f) = \deg(\varphi^*(0) - \varphi^*(\infty)) = 0 \).

Let \( \text{Div}^0(X) \) be the subgroup of \( \text{Div}(X) \) consisting of divisors of degree zero. Then Corollary 2.2.6 shows that \( \text{PDiv}(X) \subseteq \text{Div}^0(X) \). Set

\[ \text{Pic}^0(X) := \text{Div}^0(X)/\text{PDiv}(X). \]

Then the degree map determines an exact sequence

\[ 0 \to k^\times \to k(X)^\times \xrightarrow{D} \text{Div}^0(X) \to \text{Pic}^0(X) \to 0. \]

If \( X \) is defined over the algebraic closure \( \bar{k} \), write \( \text{Pic}(X/\bar{k}) \) for \( \text{Pic}(X(\bar{k})) \). Consider \( \text{Div}(X/\bar{k})^G_k \). Then we have an embedding

\[ \text{Pic}^0(X/k) \hookrightarrow \text{Pic}^0(X/\bar{k})^G_k. \]

Unfortunately, this map is not surjective in general.

2.3 Linear Equivalence

Definition. The classes \([D] = \{D + (f) : f \in k(X)^\times\}\) in the Picard group of \( X \) determines a linear equivalence: \( D \sim D' \) if there exists an \( f \in k(X)^\times \) such that \( D + (f) = D' \).

Lemma 2.3.1. For two divisors \( D, D' \in \text{Div}(X) \), \( D \sim D' \) if and only if \( \deg(D) = \deg(D') \). Therefore the degree map descends to a map on the Picard group,

\[ \deg : \text{Pic}(X) \longrightarrow \mathbb{Z}. \]

Definition. A divisor \( D = \sum n_x x \) on \( X \) is called effective if \( n_x \geq 0 \) for all \( x \in X \). In this case we will write \( D \geq 0 \). Also, if \( D_1, D_2 \in \text{Div}(X) \) and \( D_1 - D_2 \) is an effective divisor, we write \( D_1 \geq D_2 \). This defines an ordering on \( \text{Div}(X) \).

Definition. Let \( D \) be an effective divisor on \( X \). Then the Riemann-Roch space associated to \( D \) is the \( k \)-vector space

\[ \mathcal{L}(D) = \{ f \in k(X)^\times \mid D + (f) \geq 0 \} \cup \{0\}. \]

We denote its dimension by \( \ell(D) = \dim_k \mathcal{L}(D) \).
The condition that $D + (f) \geq 0$ can be restated as $(f) \geq -D$, or if $D = \sum n_x x$ then $\text{ord}_x f \geq -n_x$ for all $x \in X$.

**Example 2.3.2.** Let $x \in X$ and $n > 0$. For the divisor $D = nx$, the space $\mathcal{L}(D)$ consists of all $f \in k(X)^\times$ with no poles except possibly at $x$ of order at most $n$.

**Definition.** Fix a divisor $D \in \text{Div}(X)$. The projective space

$$\mathcal{L}(D) := \{D' \in \text{Div}(X) : [D'] = [D] \text{ and } D' \geq 0\} \cong \mathbb{P}(\mathcal{L}(D))$$

is called the **complete linear system** of $D$ on $X$. Any projective subspace of $\mathcal{L}(D)$ is called a **linear system** of $D$ on $X$.

Note that $D$ is linearly equivalent to an effective divisor if and only if $\mathcal{L}(D) \neq 0$.

**Theorem 2.3.3.** For any $D \in \text{Div}(X)$, $\mathcal{L}(D)$ is finite dimensional.

**Lemma 2.3.4.** If $D_1, D_2 \in \text{Div}(X)$ are linearly equivalent, say $D_1 - D_2 = (g)$ for some $g \in k(X)^\times$, then there is an isomorphism

$$\mathcal{L}(D_1) \longrightarrow \mathcal{L}(D_2)$$

$$f \mapsto gf.$$ 

In particular, $\ell(D)$ is a well-defined invariant of each class $[D] \in \text{Pic}(X)$.

**Remark.** If $X$ is defined over an extension $k \subseteq K \subseteq \bar{k}$, write $\mathcal{L}_K(D)$ and $\ell_K(D)$ for the Riemann-Roch space of $D$ on $X(K)$ and its dimension. Then $\mathcal{L}_K(D)$ has a basis consisting of functions $f \in k(X)^\times$, so $\ell_K(D) = \ell_k(D)$. Thus we are justified in writing $\ell(D)$ for any of these.

**Proposition 2.3.5.** Let $D, D_1, D_2 \in \text{Div}(X)$. Then

1. $\ell(D) \leq \deg(D) + 1$ if $D \geq 0$.
2. If $D_1 \leq D_2$ then $\mathcal{L}(D_1) \subseteq \mathcal{L}(D_2)$.

**Example 2.3.6.** For $X = \mathbb{P}^1$, any divisor $D$ is linearly equivalent to $d\infty$ for some $d \in \mathbb{Z}$. Then $\mathcal{L}(D) \cong \mathcal{L}(d\infty) = \{f \in k[t] : \deg f \leq d\}$ which has dimension exactly $d + 1$. Thus the equality $\ell(D) = \deg(D) + 1$ holds for any divisor on $\mathbb{P}^1$.

**Example 2.3.7.** If $X \neq \mathbb{P}^1$ and $D$ is an effective divisor, then $\ell(D) \leq \deg(D)$. In particular, if $\deg(D) \leq 0$ then $\ell(D) = 0$.

Next, we explore how much less than $\deg(D) + 1$ the dimension $\ell(D)$ can be. This culminates with the Riemann-Roch theorem in Section 2.6. Set $\gamma(D) = \deg(D) + 1 - \ell(D)$.

**Theorem 2.3.8 (Riemann Inequality).** For an nonsingular algebraic curve $X$, there is a bound $\gamma_X$ such that $\gamma(D) \leq \gamma_X$ and $1 + \deg(D) - \gamma_X < \ell(D)$ for all divisors $D \in \text{Div}(X)$. 


The Riemann-Roch spaces are useful for constructing maps \( X \to \mathbb{P}^N \) and in particular embeddings into projective space. Given a rational map \( \varphi = (\varphi_0, \ldots, \varphi_N) : X \to \mathbb{P}^N \) with \( \varphi_i \in k(X) \), define the divisor of \( \varphi \) to be
\[
D_\varphi = \gcd\{(\varphi_0), \ldots, (\varphi_N)\}.
\]
Then for each \( \varphi_i, (\varphi_i) - D_\varphi \geq 0 \) so \( \varphi_i \in \mathcal{L}(-D_\varphi) \). Set \( D = D_\varphi \). Let \( M \) be the subspace of \( \mathcal{L}(-D) \) spanned by \( (\varphi_0), \ldots, (\varphi_N) \). We may assume that these \( (\varphi_i) \) are linearly independent, lowering \( N \) if necessary. Then \( \dim M = N + 1 \). Next, \( \delta = \{(g) - D \mid g \in M\} \) is a linear system of dimension \( N \), i.e. a subspace of \( | - D| \). Thus every rational map \( X \to \mathbb{P}^N \) determines a linear system of \( D \), and it turns out the converse is also true.

Given \( \delta \subseteq |D| \) a linear subspace of \( |D| \subseteq \mathbb{P}^N \) of dimension \( N \), define the base locus of \( \delta \) by
\[
B(\delta) = \left\{ P \in X : n_P \neq 0 \text{ for all } D' = \sum n_{P'} P' \in \delta \right\}.
\]
Choose a basis \( f_0, \ldots, f_N \) of functions for \( \mathcal{L}(D) \) corresponding to \( \delta \). Then \( \varphi_\delta = (f_0, \ldots, f_N) : X \to \mathbb{P}^N \) is a rational map that restricts to a morphism on \( X \smallsetminus B(\delta) \). This is in fact unique up to automorphism of \( \mathbb{P}^N \) – corresponding to a choice of basis.

**Definition.** A linear system \( \delta \subseteq |D| \) is called **basepoint-free** if \( B(\delta) = \emptyset \).

A basepoint-free linear system \( \delta \) determines a regular map \( \varphi_\delta : X \to \mathbb{P}^N \).

**Definition.** If the complete linear system \( |D| \) is basepoint-free and the morphism \( \varphi_{|D|} : X \to \mathbb{P}^N \) is an embedding, we say \( |D| \) is **very ample**. If for some \( m > 0 \), the complete linear system \( |mD| \) is very ample, then we say \( |D| \) is **ample**.

**Theorem 2.3.9.** Let \( X \) be a curve and \( D = \sum n_x x \) an effective divisor on \( X \). Then
1. \( D \) is basepoint-free if and only if for all \( x \in X \) such that \( n_x \neq 0 \), \( \ell(D - x) < \ell(D) \).
2. \( |D| \) is very ample if and only if \( \ell(D - P - Q) < \ell(D - P) < \ell(D) \) for all \( P, Q \in X \).

### 2.4 Differentials

**Definition.** For a curve \( X \), the space of **meromorphic differentials** on \( X \) is the \( k(X) \)-vector space \( \Omega_X \) consisting of formal differentials \( df \) for each \( f \in k(X)^\times \) satisfying
- \( d(f + g) = df + dg \),
- \( d\alpha = 0 \) if \( \alpha \in k \),
- \( d(fg) = f \, dg + g \, df \).

If \( \varphi : X \to Y \) is a morphism of curves, we get a map of fields \( \varphi^* : k(Y) \to k(Y) \). Define the induced map on meromorphic differentials by
\[
\varphi^* : \Omega_Y \longrightarrow \Omega_X \quad \varphi^* \left( \sum f_i \, dt_i \right) \longmapsto \sum \varphi^* f_i \, d(\varphi^* t_i).
\]
Lemma 2.4.1. For any algebraic curve $X$, $\dim_{k(X)} \Omega_X = \dim X = 1$.

Proposition 2.4.2. For any $f \in k(X)$, the following are equivalent:

(i) $df \neq 0$.

(ii) $df$ is a basis for $\Omega_X$.

(iii) $k(X)/k(f)$ is finite and separable.

(iv) $f \not\in k$ if $\text{char } k = 0$, or $f \not\in k(X)^p$ if $\text{char } k = p > 0$.

Lemma 2.4.3. A nonconstant morphism $\varphi : X \to Y$ is separable if and only if the induced map $\varphi^* : \Omega_Y \to \Omega_X$ is nonzero.

For a point $P \in X$, choose a uniformizer $t = t_P$ in $O_{X,P}$. Then $\Omega_X$ is generated by $dt$.

Hence for any $\omega \in \Omega_X$, there exists $g \in k(X)$ such that $\omega = gdt$.

Definition. Define the order of $\omega$ at $P \in X$ to be $\text{ord}_P(\omega) = \text{ord}_P(g)$, where $\omega = gdt$. The principal divisor associated to $\omega$ is then defined to be

$$(\omega) = \sum_{P \in X} \text{ord}_P(\omega)P.$$  

Proposition 2.4.4. Let $X$ be a curve, $P \in X$, $f \in k(X)$ and $\omega \in \Omega_X$. Then

(1) If $f$ is regular at $P$ then $df = f dt$ for $t = t_P$ a local uniformizer.

(2) For any $s \in k(X)$ such that $s(P) = 0$, $\text{ord}_P(f ds) = \text{ord}_P(f) + \text{ord}_P(s) - 1$ if $p \nmid \text{ord}_P(s)$, and $\text{ord}_P(f ds) \geq \text{ord}_P(f) + \text{ord}_P(s)$ if $p \mid \text{ord}_P(s)$.

(3) $\text{ord}_P(\omega) = 0$ for all but finitely many $P \in X$.

Definition. The canonical class on a curve $X$ is the class $K_X = [(\omega)]$ in $\text{Pic}(X)$ for any nonzero differential $\omega \in \Omega_X$.

Lemma 2.4.5. The canonical class is well-defined, i.e. does not depend on the choice of $\omega \in \Omega_X$.

Proof. For nonzero $\omega_1, \omega_2 \in \Omega_X$, write $\omega_1 = f \omega_2$ for some $f \in k(X)^\times$. Then $(\omega_1) = (f \omega_2) = (f) + (\omega_2)$. Thus $[(\omega_1)] = [(\omega_2)]$. \qed

Definition. We say $\omega \in \Omega_X$ is a holomorphic (or regular) differential on $X$ if $\text{ord}_P(\omega) \geq 0$ for all $P \in X$. We denote the space of holomorphic differentials on $X$ by $\Omega[X]$.

Note that $\Omega[X]$ is a $k$-vector space but need not be a $k(X)$-vector space.

Definition. The geometric genus of $X$ is defined as $g(X) := \ell(K_X)$, the dimension of the Riemann-Roch space $L(K_X)$ of the canonical class.

Lemma 2.4.6. There is an isomorphism $L(K_X) \to \Omega[X]$. 
Proof. The map is \( f \mapsto f \omega \) for any fixed \( \omega \in \Omega[X] \) defining the canonical class. \( \square \)

Corollary 2.4.7. For any curve \( X \), \( g(X) = \dim_k \Omega[X] \).

Remark. For any divisor \( D \in \text{Div}(X) \), \( \ell_k(D) = \ell_k(\overline{D}) \) implies \( g(X(\overline{k})) = g(X(k)) \), so the geometric genus is unchanged when passing to the algebraic closure \( \overline{k} \). Moreover, \( g(X) \) is a birational invariant of \( X \).

Example 2.4.8. Let \( X = \mathbb{P}^1 \) and let \( t \) be a coordinate function on some affine patch \( U \) of \( \mathbb{P}^1 \). We claim that \( (dt) = -2\infty \). Indeed, for any \( \alpha \in U \cong \mathbb{A}^1 \), \( t - \alpha \) is a local uniformizer at \( \alpha \). Thus \( \text{ord}_\alpha(dt) = \text{ord}_\alpha(d(t - \alpha)) = 0 \). At infinity, \( \frac{1}{t} \) is a local uniformizer so we can write \( dt = -t^2d\left(\frac{1}{t}\right) \). Hence

\[
\text{ord}_\infty(dt) = \text{ord}_\infty(-t^2d\left(\frac{1}{t}\right)) = \text{ord}_\infty(-\frac{1}{t^2}) + \text{ord}_\infty(d\left(\frac{1}{t}\right)) = -2 + 0 = -2.
\]

So \( (dt) = -2\infty \) as claimed. Now for any \( \omega \in \Omega_{\mathbb{P}^1} \), \( \deg(\omega) = -2 \) so we see that \( \ell(K_{\mathbb{P}^1}) = \ell(-2\infty) = 0 \). Hence the genus of the projective line is \( g(\mathbb{P}^1) = 0 \).

Corollary 2.4.9. There are no holomorphic differentials on \( \mathbb{P}^1 \).

Proof. By Corollary 2.4.7, \( g(\mathbb{P}^1) = \dim_k \Omega[\mathbb{P}^1] \) but by the calculations above, the genus of \( \mathbb{P}^1 \) is zero. \( \square \)

2.5 The Riemann-Hurwitz Formula

Let \( \varphi : X \to Y \) be a nonconstant morphism of curves and fix \( P \in X \). Then \( e_\varphi(P) = \text{ord}_P(\varphi^*t_\varphi(P)) \) where \( t_\varphi(P) \) is a local uniformizer. We would like to see what happens to the canonical class \( K_X \) under a morphism. Take \( t \) to be a uniformizer at \( Q = \varphi(P) \) and set \( e_\varphi(P) = e \). Then \( \varphi^*(dt) = d(\varphi^*t) \). Moreover, if \( s \) is a uniformizer on \( X \) at \( P \), then \( \varphi^*t = us^e \) for some unit \( u \in \mathcal{O}_P^* \). Now \( d(\varphi^*t) = d(us^e) = s^e du + ues^{e-1} ds \). Write \( du = g ds \) for a regular function \( g \in \mathcal{O}_P \); this is possible by (1) of Proposition 2.4.4. Then

\[
d(\varphi^*t) = s^e g ds + ues^{e-1} ds \quad \implies \quad \text{ord}_P(d(\varphi^*t)) = \text{ord}_P(s^e g + ues^{e-1}) = \min\{\text{ord}_P(s^e g), \text{ord}_P(ues^{e-1})\}.
\]

If \( \text{char } k \nmid e \), then this minimum is \( e - 1 \); otherwise, when \( \text{char } k \mid e \) the minimum is at least \( e \).

Definition. If \( \varphi \) is ramified and \( \text{char } k \nmid e_\varphi(P) \) for all \( P \in X \), we say \( \varphi \) is tamely ramified. Otherwise \( \varphi \) is wildly ramified.

Remark. If \( \varphi \) is tamely ramified, then \( \text{ord}_P(d(\varphi^*t)) = e_\varphi(P) - 1 \) for each \( P \). If \( \varphi \) is wildly ramified at \( P \), then \( \text{ord}_P(d(\varphi^*t)) \geq e_\varphi(P) \).

Definition. For a morphism \( \varphi : X \to Y \), define the ramification divisor

\[
R_\varphi = \sum_{P \in X} \text{ord}_P(d(\varphi^*t))P.
\]
Now for $\omega \in \Omega_Y$, the canonical classes on $X$ and $Y$ can be defined by $K_Y = [(\omega)]$ and $K_X = [(\varphi^*\omega)]$. On the other hand, the pullback defines a divisor $\varphi^*K_Y \in \operatorname{Div}(X)$. We want to determine the relation between these three divisors.

**Lemma 2.5.1.** If $\varphi : X \to Y$ is a morphism of curves, then $K_X = \varphi^*K_Y + [R_\varphi]$, where $R_\varphi$ is the ramification divisor of $\varphi$.

**Proof.** If $\omega = f\, dt \in \Omega_Y$, then

$$\text{ord}_P(\varphi^*\omega) = \text{ord}_P(\varphi^*f\, d(\varphi^*t)) = \text{ord}_P(\varphi^*f) + \text{ord}_P(d(\varphi^*t)),$$

so we see that $\text{ord}_P(\varphi^*\omega)$ gives the coefficient in $K_X$, $\text{ord}_P(\varphi^*f)$ gives the coefficient in $\varphi^*K_Y$ and $\text{ord}_P(d(\varphi^*t))$ gives the coefficient in $R_\varphi$. Summing over $P \in X$ gives the desired equality. \qed

Taking $\varphi$ to be tamely ramified, $R_\varphi = \sum_{P \in X} (e_\varphi(P) - 1)P$ so the degree function applied to the equation in Lemma 2.5.1 gives

$$\deg(K_X) = \deg(\varphi^*K_Y) + \sum_{P \in X} (e_\varphi(P) - 1).$$

We will show in Section 2.6 that $\deg(K_X) = 2g(X) - 2$. This proves:

**Theorem 2.5.2 (Riemann-Hurwitz Formula).** For any morphism $\varphi : X \to Y$,

$$2g(X) - 2 = (\deg \varphi)(2g(Y) - 2) + \sum_{P \in X} (e_\varphi(P) - 1).$$

**Corollary 2.5.3.** For any morphism $\varphi : X \to Y$, $g(X) \geq g(Y)$.

### 2.6 The Riemann-Roch Theorem

Recall from Theorem 2.3.8 that $\ell(D) \geq 1 + \deg(D) - \gamma_X$. The classic Riemann-Roch theorem gives a precise value for $\gamma_X$ in terms of the dimensions of the Riemann-Roch spaces of $X$ and the genus.

**Theorem 2.6.1 (Riemann-Roch).** For an algebraic curve $X$ with genus $g = g(X)$, $\gamma_X = g$ satisfies the Riemann Inequality. Moreover,

$$\ell(D) - \ell(K - D) = 1 - g + \deg(D),$$

where $K = K_X$ is the canonical divisor of $X$.

**Remark.** One typically proves the Riemann-Roch theorem using sheaf cohomology – the vector spaces $\mathcal{L}(D)$ form a sheaf on $X$ – as well as Serre duality. See Hartshorne for details.

**Corollary 2.6.2.** If $K_X$ is the canonical divisor on $X$, then $\deg(K_X) = 2g - 2$. 

43
2.6 The Riemann-Roch Theorem

Proof. Set $D = K = K_X$. Then the Riemann-Roch theorem says that
\[ \ell(K) - \ell(0) = \deg(K) + 1 - g \]
but $\ell(K) = g$ by definition and $\ell(0) = 1$. Solving for $\deg(K)$ we get $\deg(K) = 2g - 2$. \qed

Corollary 2.6.3. Suppose $\deg(D) > 2g - 2$ for some divisor $D \in \text{Div}(X)$. Then $\ell(D) = \deg(D) + 1 - g$.

The genus is a discrete invariant of nonsingular curves. There are two natural questions that arise:

1. What are the curves with genus $g$ for a particular $g \in \mathbb{N}_0$?

2. How do we describe the structure of the collection of all genus $g$ curves?

We will see that one can put the structure of a variety on the collection of genus $g$ curves.

Lemma 2.6.4. Let $X$ be an algebraic curve. Then $X \cong \mathbb{P}^1$ if and only if there is some divisor $D \in \text{Div}(X)$ such that $\deg(D) = 1$ and $\ell(D) \geq 2$.

Proof. ($\Rightarrow$) If $X \cong \mathbb{P}^1$ then $g(X) = g(\mathbb{P}^1) = 0$ by Example 2.4.8. Take a point $P \in X$ and set $D = P \in \text{Div}(X)$; of course $\deg(D) = 1$. Then by the Riemann-Roch theorem,
\[ \ell(D) = 1 - g + \deg(D) + \ell(K - D) = 1 - 0 + 1 + \ell(K - D) = 2 + \ell(K - D) \geq 2. \]

($\Leftarrow$) Since $\ell(D) \geq 2$, there exists a nonconstant function $g \in \mathcal{L}(D)$. Then $D \sim D + (g) \geq 0$ so we may assume $D$ is effective. The only way for $\deg(D) = 1$ is for $D = P$ for some point $P \in X(k)$. Now $g$ determines a map $g : X \to \mathbb{P}^1$, under which $g^*\infty = \text{ord}_\infty(g) = P$, so we must have $\deg(g) = 1$. Hence $g$ is an isomorphism of curves. \qed

Proposition 2.6.5. For an algebraic curve $X$ with genus $g = g(X)$, the following are equivalent:

1. $X \cong \mathbb{P}^1$.

2. $g = 0$ and there exists a divisor $D \in \text{Div}(X)$ with $\deg(D) = 1$.

3. $g = 0$ and $X(k) \neq \emptyset$.

Proof. (1) $\implies$ (2) follows immediately from Lemma 2.6.4.

(2) $\implies$ (1) Since the genus is 0, $\deg(D) > 2g - 2 = -2$ is certainly true. By Corollary 2.6.3, $\ell(D) = \deg(D) + 1 - g = 1 + 1 - 0 = 2$, so Lemma 2.6.4 once again applies.

(2) $\implies$ (3) follows from the proof of Lemma 2.6.4.

(3) $\implies$ (2) Any rational point $P \in X(k)$ is a divisor on $X$ of degree 1. \qed

This shows that the main interest for curves of genus 0 is in finding rational points $P \in X(k)$. Moreover, when $g(X) = 0$, the complete linear system $|K_X|$ is very ample by Theorem 2.3.9 and the Riemann-Roch theorem, and the embedding $\varphi|_{K_X} : X \hookrightarrow \mathbb{P}^2$ realizes $X$ as a plane conic.

Remark. If $\varphi : \mathbb{P}^1 \to X$ is a morphism, Corollary 2.5.3 says that $g(X) = 0$. Further, when $k$ is algebraically closed or we consider the $k$-points $X(\bar{k})$, one has $X \cong \mathbb{P}^1$. Notice that this gives another proof of Lüroth’s theorem (0.2.2).
2.7 The Canonical Map

We saw in the last section that the theory of genus 0 curves for the most part reduces to studying whether $X$ has rational points and describing the embedding $\varphi|_{K_X} : K \hookrightarrow \mathbb{P}^2$. What about higher genus curves?

**Proposition 2.7.1.** Let $X$ be a nonsingular algebraic curve over $k$ of genus $g \geq 1$. If $K_X$ is the canonical divisor of $X$ then the complete linear system $|K_X|$ is basepoint-free.

*Proof.* This follows from the Riemann-Roch theorem and Theorem 2.3.9, taking $D = K_X$. \qed

Thus $|K_X|$ determines a regular map into projective space.

**Definition.** The **canonical map** of a genus $g \geq 1$ curve $X$ is the map $\varphi|_{K_X} : X \to \mathbb{P}^{g-1}$.

**Definition.** A **hyperelliptic curve** is a smooth curve $X$ together with a separable, degree 2 map $X \to \mathbb{P}^1$.

**Example 2.7.2.** When $\text{char } k \neq 2$, a hyperelliptic curve is of the form $X = Z(y^2 - f(x))$ for a polynomial $f \in k[x]$. More generally, the minimal degree of a nonconstant morphism $X \to \mathbb{P}^1$ is called the **gonality** of $X$. Thus, a hyperelliptic curve is a curve of gonality 2.

**Proposition 2.7.3.** If $X$ is not hyperelliptic and $g \geq 2$, the canonical map $\varphi|_{K_X} : X \to \mathbb{P}^{g-1}$ is an embedding.

**Proposition 2.7.4.** If $X$ is a nonsingular algebraic curve of genus $g$ and $D \in \text{Div}(X)$, then

1. If $\deg(D) \geq 2g$ then $|D|$ is basepoint-free.
2. If $\deg(D) \geq 2g + 1$ then $|D|$ is very ample.

**Corollary 2.7.5.** If $g \geq 2$ then $\varphi|_{3K_X} : X \to \mathbb{P}^{5g-6}$ is an embedding.

**Definition.** The map $\varphi|_{3K_X}$ is called the **tricanonical map** of a curve $X$.

**Theorem 2.7.6 (Faltings).** If $X$ is a curve of genus $g \geq 2$ then $\#X(\mathbb{Q})$ is finite.

We have for the most part dealt completely with the cases of curves of genus $g = 0$ and $g \geq 2$, so the most interesting work remains to be done for curves of genus $g = 1$.

2.8 Bézout’s Theorem

For this section let $k$ be algebraically closed, fix $X \subseteq \mathbb{P}^N$ a projective curve and $Y \subseteq \mathbb{P}^N$ a hypersurface defined by $Y = Z(F)$ for some $F \in k[X_0, \ldots, X_N]$. Further suppose that $X \not\subseteq Y$, i.e. that $F \not\in J(X)$. Then by counting codimensions, $X \cap Y$ must be some dimension 0 variety in $\mathbb{P}^N$, i.e. $X$ and $Y$ intersect in some discrete set of points. We want to count these points, including some notion of multiplicity, in a rigorous way.
Definition. The intersection multiplicity of $X$ and $Y = \mathbb{Z}(F)$ at a point $P \in X \cap Y$, denoted $(X \cdot F)_P$, is defined as follows. Let $G \in k[X_0, \ldots, X_N]$ be any form of the same degree as $F$ such that $G(P) \neq 0$. Then $F/G \in k(X)$ so the intersection multiplicity at $P$ is defined: $(X \cdot F)_P := \text{ord}_P(F/G)$. Further, the intersection divisor of $F$ on $X$ is

$$
\text{div}_X(F) = \sum_{P \in X \cap Y} (X \cdot F)_P P,
$$

and its order $(X \cdot F) := \sum_{P \in X \cap Y} (X \cdot F)_P$ is called the intersection number of $X$ and $Y$.

If $L$ is the linear form representing the line in the figure, then $(X \cdot L)_P = 1$, $(X \cdot L)_Q = 2$ and the intersection number is $(X \cdot L) = 1 + 2 = 3$.

Proposition 2.8.1. If $F_1 \in k[X_0, \ldots, X_N] \setminus J(X)$ is another form with $\deg F_1 = \deg F$, then $(X \cdot F) = (X \cdot F_1)$.

Proof. Set $f = F/F_1 \in k(X)$. Then $\text{div}_X(F) \sim \text{div}_X(F_1)$, so $\deg(\text{div}_X(F)) = \deg(\text{div}_X(F_1))$, and thus the intersection number is well-defined. □

Corollary 2.8.2. If $\deg F = m$ and $L$ is any linear form such that $L \not\in J(X)$, then $(X \cdot F) = m(X \cdot L)$.

Proof. Since intersection multiplicity at a point is multiplicative, this formula is clear. □

Lemma 2.8.3. For any form $F \not\in J(X)$ and any point $P \in X \cap Z(F)$, $(X \cdot F)_P = 1$ if and only if $F(P) = 0$ and $T_P X \not\subset T_P Z(F)$.

Stated another way, Lemma 2.8.3 says that the intersection multiplicity at $P$ is 1 if and only if $X$ and $Z(F)$ meet transversely.

Lemma 2.8.4. For any smooth curve $X$, there exists a linear form $L$ such that $(X \cdot L)_P \leq 1$ for all $P \in X \cap Z(L)$.

Definition. The degree of a projective curve $X \subseteq \mathbb{P}^N$ is defined to be

$$
\deg_{\mathbb{P}^N} X := \max\{\#(X \cap H) : H \text{ is a hyperplane and } X \not\subset H\}.
$$

Corollary 2.8.5. Let $X$ be a projective curve in $\mathbb{P}^N$. Then $\deg_{\mathbb{P}^N} X = (X \cdot L)$ for any linear form $L$.

Theorem 2.8.6 (Bézout). Let $X \subset \mathbb{P}^N$ be a projective curve and $F \in k[X_0, \ldots, X_N]$ a form such that $F \not\in J(X)$. Then $(X \cdot F) = (\deg_{\mathbb{P}^N} X)(\deg F)$.

Example 2.8.7. If $X \subset \mathbb{P}^2$ is a planar curve given by a form $G = 0$, then $\deg_{\mathbb{P}^2} X = \deg G$ so we can count intersection multiplicities in the plane by:

$$(X \cdot F) = (\deg G)(\deg F)$$

for any $F \in k[X_0, X_1, X_2] \setminus J(X)$.
2.9 Rational Points of Conics

Given a plane conic $C$ over a field of characteristic $\text{char } k \neq 2$, say

$$ C : ax^2 + 2bxy + 2cx + dy^2 + 2ey + f = 0 $$

in $A^2_k$, we can homogenize to get a curve in $P^2_k$:

$$ \overline{C} : F(X,Y,Z) = aX^2 + 2bXY + 2cXZ + dY^2 + 2cYZ + fZ^2 = 0. $$

Then $F$ is a quadratic form on the vector space $V = k^3$.

**Definition.** For a $k$-vector space $V$, a function $q : V \to k$ is a **quadratic form** if

(a) $q(\lambda v) = \lambda^2 v$ for all $\lambda \in k$ and $v \in V$.

(b) The pairing $b_q(v,w) = \frac{1}{2}(q(v+w) - q(v) - q(w))$ is symmetric and $k$-bilinear.

A quadratic form $q$ is said to be **nondegenerate** if $b_q$ induces an isomorphism $V \cong V^*$. Otherwise $q$ is **degenerate**.

If $F(X,Y,Z)$ is a quadratic form on $V = k^3$, then there is a matrix

$$ M_F = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} $$

such that $F(X,Y,Z) = (X\ Y\ Z)M_F(X\ Y\ Z)^t$. The determinant $\text{deg } M_F$ is called the **discriminant** of $F$.

**Lemma 2.9.1.** A quadratic form $F(X,Y,Z)$ is nondegenerate if and only if $\text{deg } M_F \neq 0$.

Since $M_F$ is symmetric when $F$ is quadratic, we may transform it by some invertible matrix $T \in GL_3(k)$ to a diagonal form $D_F = T^t M_F T$. In these coordinates of $k^3$, we have

$$ F = \sum_{i=1}^3 a_i X_i^2. $$

Further, if $k = \mathbb{Q}$, we may assume the $a_i \in \mathbb{Z}$ are squarefree and relatively prime.

**Definition.** A quadratic form $F$ represented by a diagonal matrix $M$ with squarefree, coprime integer entries is called a **primitive quadratic form**.

The crucial Hasse-Minkowski theorem says that a plane conic having a $\mathbb{Q}$-rational point is equivalent to the conic having a rational point over every completion of $\mathbb{Q}$.

**Theorem 2.9.2 (Hasse-Minkowski).** Let $F \in \mathbb{Q}[X_0, \ldots, X_n]$ be a primitive quadratic form and let $X = Z(F) \subseteq \mathbb{P}_\mathbb{Q}^n$. Then $X(\mathbb{Q}) \neq \emptyset$ if and only if $X(\mathbb{Q}_v) \neq \emptyset$ for all places $v$ of $\mathbb{Q}$. 

47
This theorem is the classic example of Hasse’s “local-to-global principle”: points over the local fields $\mathbb{Q}_v$ determine points over $\mathbb{Q}$. Note that the Hasse-Minkowski theorem does not hold for general varieties $X$, nor for general fields $k$.

**Example 2.9.3.** For a conic $X$, $X(\mathbb{R}) \neq \emptyset$ if and only if there is a change of sign among the coefficients $a_i$ in the form $F$ defining $X$. This condition is easily checked as long as one can diagonalize $M_F$.

Thus to find rational points of a conic, we need only ask if there is an algorithm for checking whether $X$ has points over each $p$-adic field $\mathbb{Q}_p$.

**Example 2.9.4.** Let $X = \mathbb{P}^n$. Then $\mathbb{P}^n(\mathbb{Q}) = \mathbb{P}^n(\mathbb{Z})$ and for any prime $p$, $\mathbb{P}^n(\mathbb{Q}_p) = \mathbb{P}^n(\mathbb{Z}_p)$, so it’s enough to look for integer solutions. If $P = [\alpha_0, \ldots, \alpha_n] \in \mathbb{P}^n(\mathbb{Q}_p)$, then we can clear denominators so that $\bar{P} = [\beta_0, \ldots, \beta_n] \in \mathbb{P}^n(\mathbb{F}_p)$.

It turns out that quadratic forms always have points over finite fields. To prove this, we will need the following counting lemma.

**Lemma 2.9.5.** For a sum $s = \sum_{\alpha \in \mathbb{F}_q^n} \alpha_1^{k_1} \cdots \alpha_n^{k_n}$, where $\alpha = (\alpha_1, \ldots, \alpha_n)$ and $k_i \in \mathbb{Z}_{\geq 0}$, if at least one $k_i$ is not a positive integer multiple of $q - 1$, then $s = 0$.

**Proof.** Write

$$s = \sum_{\alpha \in \mathbb{F}_q^n} \alpha_1^{k_1} \cdots \alpha_n^{k_n} = \prod_{i=1}^n \left( \sum_{a \in \mathbb{F}_q} a^{k_i} \right).$$

If any $k_i = 0$ then $\sum_{a \in \mathbb{F}_q} a^{k_i} = \sum_{a \in \mathbb{F}_q} 1 = q \equiv 0 \pmod{p}$ so we may assume all $k_i \neq 0$. Let $\phi$ be a generator of the cyclic group $\mathbb{F}_q^\times$ and write $\psi = \phi^{k_i}$. If $k_i$ is not a positive multiple of $q - 1$, then $\psi \neq 1$. Now we have

$$\sum_{a \in \mathbb{F}_q} a^{k_i} = \sum_{a \in \mathbb{F}_q} \psi^m = \sum_{m=0}^{q-2} (\phi^m)^{k_i} = \sum_{m=0}^{q-2} \psi^m = \frac{1 - \psi^{q-1}}{1 - \psi} \equiv \frac{1 - 1}{1 - \psi} = 0.$$

Therefore $s = 0$. \hfill $\square$

**Theorem 2.9.6** (Chevalley-Warning). Let $\mathbb{F}_q$ be a finite field of characteristic $p$ and let $f_0, \ldots, f_r \in \mathbb{F}_q[X_1, \ldots, X_n]$ be polynomials satisfying $n > \sum_{j=1}^r \deg f_j$. Set $X = Z(f_0, \ldots, f_r) \subseteq \mathbb{A}_\mathbb{F}_q^n$. Then

(a) $\#X(\mathbb{F}_q) \equiv 0 \pmod{p}$.

(b) If $(0, \ldots, 0) \in X(\mathbb{F}_q)$ is a point on the curve then $\#X(\mathbb{F}_q) \geq p$.  

48
Proof. Define the indicator function for $X(\mathbb{F}_q)$:

$$P(X_1, \ldots, X_n) = \prod_{i=1}^{r} (1 - f_j(X_1, \ldots, X_n)^q - 1).$$

Notice that $P(\alpha) = 1$ if $\alpha \in X(\mathbb{F}_q)$ and 0 otherwise. Then

$$\#X(\mathbb{F}_q) = \sum_{\alpha \in \mathbb{F}_q} P(\alpha) \mod p.$$ 

Now we have

$$\deg P = \sum_{i=1}^{r} \deg f_i(q - 1) < \sum_{i=1}^{n} n(q - 1)$$

by hypothesis. So for each monomial term $X_1^{k_1} \cdots X_n^{k_n}$ in $P(X_1, \ldots, X_n)$, $k_1 + \cdots + k_n < n(q - 1)$, so at least one $k_i$ must be less than $q - 1$. Hence by Lemma 2.9.5,

$$\#X(\mathbb{F}_q) = \sum_{\alpha \in \mathbb{F}_q} P(\alpha) = 0 \mod p.$$ 

This proves (a), and (b) follows trivially.

Corollary 2.9.7. Every quadratic form in at least three variables has a point over each finite field.

The theory of Hasse-Minkowski extends more generally to number fields $K/\mathbb{Q}$, with similar local-global principles at work.

We next determine when solutions to quadratic equations $F = 0$ over finite fields lift to solutions in $\mathbb{Z}_p$, similar to Hensel’s Lemma. To do so, we introduce the notion of an integral model for a variety over $\mathbb{Q}$.

Definition. For a projective variety $X \subseteq \mathbb{P}^N_{\mathbb{Q}}$, an integral model for $X$ is a choice of homogenous forms $F_1, \ldots, F_m \in \mathbb{Z}[X_0, \ldots, X_n]$ such that $X = Z(F_1, \ldots, F_m)$. Denote these forms $\{F_1, \ldots, F_m\}$ by $\mathcal{X}$.

Note that we may assume the set of all coefficients of an integral model $\mathcal{X} = \{F_1, \ldots, F_m\}$ is coprime.

Definition. Let $\mathcal{X} = \{F_1, \ldots, F_m\}$ be an integral model of $X$ over $\mathbb{Q}$. For a prime $p$, the reduction of $\mathcal{X}$ mod $p$ is the variety

$$\mathcal{X}_F = Z(\overline{F}_1, \ldots, \overline{F}_m) \subseteq \mathbb{P}^N_{\mathbb{F}_p},$$

where $\overline{F}_i = F_i \mod p$. We say $\mathcal{X}_F$ is geometrically reduced if the ideal $(\overline{F}_1, \ldots, \overline{F}_m)$ is radical in $\mathbb{F}_p[X_0, \ldots, X_N]$.

Notice that $\mathcal{X}_F$ depends on the integral model $\mathcal{X}$ chosen for $X$. 

49
Definition. We say an integral model $X$ has **good reduction** mod $p$ if $X_{\mathbb{Z}_p}$ is geometrically reduced and nonsingular, and **bad reduction** mod $p$ otherwise.

**Lemma 2.9.8.** An integral model $X = \{F_1, \ldots, F_m\}$ has good reduction mod $p$ if and only if $\mathbb{Z}[X_0, \ldots, X_N]/(F_1, \ldots, F_m) \otimes \mathbb{F}_p$ is a regular ring.

**Example 2.9.9.** If $X \subseteq \mathbb{P}^2$ is a plane conic and $X$ is an integral model of $X$ over $\mathbb{Q}$ given by a primitive quadratic form $F \in \mathbb{Z}[X_0, X_1, X_2]$, then $X$ has bad reduction at a prime $p$ if and only if $p$ divides the discriminant $\Delta(F)$.

**Corollary 2.9.10.** A primitive quadratic form $F \in \mathbb{Z}[X_0, X_1, X_2]$ has bad reduction at only finitely many primes.

The following is a stronger version of Hensel’s Lemma (Theorem 0.3.4) that we will need for lifting solutions of quadratic forms.

**Theorem 2.9.11.** Let $(R, v)$ be a complete DVR, $f \in R[x_1, \ldots, x_N]$ and suppose $(a_1, \ldots, a_N) \in R^N$ such that

$$v(f(a_1, \ldots, a_N)) > 2v\left(\frac{\partial f}{\partial x_i}(a_1, \ldots, a_N)\right)$$

for some $1 \leq i \leq N$. Then $f$ has a root in $R^N$.

**Corollary 2.9.12.** If $X = Z(F)$ is an integral model over $\mathbb{Z}_p$ and $P$ is a smooth point of $X(\mathbb{F}_p)$, then $P$ lifts to a point of $X(\mathbb{Z}_p)$.

This leaves the question of lifting singular points.

**Theorem 2.9.13.** Let $F = \sum_{i=0}^{n} a_i X_i^2$ be a primitive quadratic form over $\mathbb{Z}_p$ and set $X = Z(F) \subseteq \mathbb{P}^2_{\mathbb{Z}_p}$. Suppose $\beta_0, \ldots, \beta_n \in \mathbb{Z}_p$ such that $\text{ord}_p(\beta_j) = 0$ for some $0 \leq j \leq n$, with $F(\beta_0, \ldots, \beta_n) = 0 \mod p^{\varepsilon + 1}$, where

$$\varepsilon = \begin{cases} 
1, & p \neq 2 \\
3, & p = 2. 
\end{cases}$$

Then there exists a nontrivial root of $F$ in $\mathbb{Z}_p$, that is, $\alpha = (\alpha_0, \ldots, \alpha_n) \in \mathbb{Z}_p^n$, with $\alpha_\ell \neq 0$ for some $0 \leq \ell \leq n$, and $F(\alpha_0, \ldots, \alpha_n) = 0$.

**Proof.** Since $F$ is primitive, $a_i, \beta_j \in \mathbb{Z}_p^\times$ for some $0 \leq i, j \leq n$. If $i = j$, then the point $P = (\beta_0, \ldots, \beta_n)$ is a smooth point of $X_{\mathbb{Z}_p}$. By Theorem 2.9.11, $P$ lifts to a solution in $\mathbb{Z}_p$. On the other hand, assume without loss of generality that $\beta_0 \in \mathbb{Z}_p^\times$ and $a_0 \notin \mathbb{Z}_p^\times$. Then $a_0 = pa'_0$ for some $a'_0 \in \mathbb{Z}_p^\times$. Set $c = a_1 \beta_1^2 + \ldots + a_n \beta_n^2$. Then $pa'_0c^2 + c \equiv 0 \mod p^{\varepsilon + 1}$ so $p \mid c$; write $c = pc'$. Then $pa'_0c^2 + c' \equiv 0 \mod p^{\varepsilon}$. This implies $c' \in \mathbb{Z}_p^\times$—in fact, $c' \in 1 + p^{\varepsilon}\mathcal{O}_p$ so $\frac{c'}{a'_0} \in \mathbb{Z}_p^\times$. In particular, $-\frac{c'}{a'_0}$ is a square in $\mathbb{Z}_p$ by Corollary 0.3.6. Write $-\frac{c'}{a'_0} = \theta^2$ for $\theta \in \mathbb{Z}_p$. Then $\alpha = (\theta, \beta_1, \ldots, \beta_n)$ is a solution to $F(\alpha) = 0$ over $\mathbb{Z}_p$ as required.

We have proven the following theorem characterizing rational points of quadratic forms (conics) over $\mathbb{Q}$. 

50
Theorem 2.9.14. Let $F$ be a nondegenerate, primitive quadratic form over $\mathbb{Z}$ and let $X = Z(F)$ be the corresponding conic over $\mathbb{Q}$. Then $X(\mathbb{Q}) \neq \emptyset$ if and only if

(1) There is a sign change in the coefficients – i.e. $X(\mathbb{R}) \neq \emptyset$.

(2) $F = 0$ has a primitive solution mod 16 – i.e. $X(\mathbb{Q}_2) \neq \emptyset$.

(3) $F = 0$ has a primitive solution mod $p^2$ for all primes $p > 2$ – i.e. $X(\mathbb{Q}_p) \neq \emptyset$.

In practice, one need only check (2) and (3) for primes at which $X$ has bad reduction, and by Corollary 2.9.10 there are only finitely many of these.
3 Elliptic Curves

If $X$ is a nonsingular algebraic curve of genus $g = 1$, then the canonical divisor $K = K_X$ has degree 0 by Corollary 2.6.2, so there is no good canonical map of $X$ into projective space. However, we have:

**Proposition 3.0.1.** Suppose $X$ is a curve with $g(X) = 1$ and there exists a rational point $O \in X(k)$. Then the complete linear system $|3O|$ gives an embedding $\varphi|_{3O} : X \to \mathbb{P}^2$.

**Proof.** Set $D = 3O$. Then $\deg(D) = 3$ so by the Riemann-Roch theorem, $\ell(D) = 3$. Choose a basis $\{1, \alpha\}$ for $L(2O)$. Then since $L(2O) \subseteq L(3O)$, this extends to a basis $\{1, \alpha, \beta\}$ of $L(D)$. The map $\varphi = \varphi|_{D}$ is given by $\varphi : P \mapsto [\alpha(P), \beta(P), 1]$. Notice that $1, \alpha, \beta, \alpha^2$ all have different orders at $O$, we must have $A \neq 0$ and $D \neq 0$. Replace $\alpha$ with $AD\alpha$, $\beta$ with $AD^3\beta$ and divide by $A^3D^4$ to obtain:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$  

This defines a curve $E \subset \mathbb{P}^2$, and under the map $\varphi$, we get $X \cong E$. \qed

**Definition.** A curve of genus 1 with a choice of rational point $O \in X(k)$ is called an **elliptic curve** over $k$. An equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$  

defining $X$ in $\mathbb{P}^2$ is called a **Weierstrass equation** of $X$.

Choosing different $\alpha', \beta' \in L(3O)$ gives an alternate Weierstrass equation:

$$(y')^2 + a'_1x'y' + a'_3y' = (x')^3 + a'_2(x')^2 + a'_4x' + a'_6.$$  

Moreover, since $\text{Span}\{1, \alpha\} = \text{Span}\{1, \alpha'\} = L(2O)$, we must have $\alpha = u_1\alpha' + r$ for some $u_1 \in k^\times$ and $r \in k$. Similarly, $\beta = u_2\beta' + s_2\alpha' + t$ for $u_2 \in k^\times$ and $s_2, t \in k$. Substituting these into the original Weierstrass equation in $x, y$ gives the relation $u_2^2 = u_1^3$. Set $u = \frac{u_1}{u_2}$ and $s = \frac{s_2}{u_2^2}$. Then the transformation of coordinates between the two Weierstrass equations has the form

$$x = u^2x' + r, \quad y = u^3y' + su^2x' + t.$$  

Since every elliptic curve has a Weierstrass equation, the above can be taken as the general form of an isomorphism between elliptic curves.
3.1 Weierstrass Equations

Let \( y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \) be the Weierstrass equation of an elliptic curve \( E \) over \( k \). If \( \text{char } k \neq 2 \), one can complete the square on the left side of the equation by substituting \( y \mapsto \frac{1}{2}(y - a_1 x - a_3) \) to get a simpler expression

\[
    y^2 = 4x^3 + b_2 x^2 + 2b_4 x + b_6
\]

where \( b_2, b_4, b_6 \in \mathbb{Z}[a_i] \). Moreover, if \( \text{char } k \neq 3 \) as well, the substitution \((x, y) \mapsto (x - \frac{3b_2}{36}, \frac{y}{108})\) gives

\[
    y^2 = x^3 - 27c_4 x - 54c_6
\]

for \( c_4, c_6 \in \mathbb{Z}[b_i] \). Typically we set \( A = -27c_4 \) and \( B = -54c_6 \) to get an equation

\[
    y^2 = x^3 + Ax + B.
\]

**Definition.** An equation of the form \( y^2 = x^3 + Ax + B \) is called a short Weierstrass form for \( E \).

The transformations preserving a short Weierstrass form are of the form

\[
    x = u^2 x' \quad \text{and} \quad y = u^3 y' \quad \text{for } u \in k^\times.
\]

Under such a transformation, \( c_4 = u^4 c'_4 \) and \( c_6 = u^6 c'_6 \) so we immediately see that \( \frac{c_4^2}{c_6} = \left(\frac{c'_4}{c'_6}\right)^2 \).

Thus this ratio is an isomorphism invariant of \( E \).

Conversely, we may ask the question, ‘When does a Weierstrass equation define an elliptic curve over \( k \)?’

**Definition.** Let \( y^2 = x^3 + Ax + B \) be a short Weierstrass form. Then the number \( \Delta = -16(4A^3 + 27B^2) \) is called the discriminant of the Weierstrass equation.

Note that if two Weierstrass forms describe the same curve, then their discriminants are related by \( \Delta = u^{12} \Delta' \) for some \( u \in k^\times \).

**Proposition 3.1.1.** The curve defined by a Weierstrass equation is nonsingular if and only if \( \Delta \neq 0 \).

**Proof.** To study nonsingularity, we compute the Jacobian criteria for the curve \( X \) defined by \( y^2 = x^3 + Ax + B \):

- The point at infinity is always a nonsingular point of such an equation.
- On an affine patch, \( X \) is defined by the vanishing of \( f(x, y) = y^2 - x^3 - Ax - B \). Thus \( \frac{\partial f}{\partial x} = -3x^2 - A \) and \( \frac{\partial f}{\partial y} = 2y \).

Then \( X \) is singular at \( P \in \mathbb{A}_k^2 \) if and only if \( f(P) = \frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0 \), but these conditions are equivalent to

\[
    \begin{cases} 
        -x^3 - Ax - B = 0, \\
        -3x^2 - A = 0.
    \end{cases}
\]

That is, \( X \) is singular at \( P \) if and only if the cubic \( -x^3 - Ax - B \) and its derivative vanish, but this is governed by the discriminant of the cubic, \( D(-x^3 - Ax - B) = -4A^3 - 27B^2 \). Thus \( f \) being nonsingular at \( P \) is equivalent to \( \Delta = 16D(-x^3 - Ax - B) \neq 0 \).
Proposition 3.1.2. A Weierstrass equation defines

(1) A nonsingular curve if $\Delta \neq 0$;

(2) A nodal curve if $\Delta = 0$ and $c_4 \neq 0$;

(3) A cuspidal curve if $\Delta = 0$ and $c_4 = 0$.

Definition. The invariant differential of a Weierstrass equation $y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$ is the meromorphic differential $\omega = \frac{dx}{2y + a_1 x + a_3}$.

Proposition 3.1.3. The invariant differential $\omega$ of a Weierstrass equation for an elliptic curve $E$ is regular and nonvanishing. In particular, $\deg(\omega) = 0$.

Example 3.1.4. Let $X$ be a curve over $k$ of genus $g = 1$ and let $D \in \text{Div}(X)$ be a divisor of minimal degree. In many cases this minimal degree determines important properties of the curve:

- If $\deg(D) = 1$, $D$ is linearly equivalent to a point $O \in X(k)$ and therefore $X$ is an elliptic curve defined over $k$. As we saw in Proposition 3.0.1, $|3O|$ determines an embedding $X \hookrightarrow \mathbb{P}^2$ as a Weierstrass equation.

- If $\deg(D) = 2$, $\ell(D) = 2$ by Riemann-Roch (Corollary 2.6.3), so we get a map $\varphi = \varphi|_D : X \to \mathbb{P}^1$. By the Riemann-Hurwitz formula (Theorem 2.5.2), $\varphi$ is branched at exactly 4 points. It is known that such a curve is of the form $Y^2 Z = U(X, Z)$ for a quartic $U$. When one of the branch points is rational, dehomogenizing gives a Weierstrass equation $y^2 = u(x)$ where $u$ is a cubic in $x$.

- If $\deg(D) = 3$, $\ell(D) = 3$ by Corollary 2.6.3, so $\varphi = \varphi|_D$ is an embedding $X \hookrightarrow \mathbb{P}^2$. The image of $X$ is defined by $U(X, Y, Z) = 0$ for some ternary cubic $U$. In this case, $U(X, Y, Z) = 0$ is a Weierstrass equation if and only if there is only one point at infinity, which in turn means $D = 3P$ for some point $P \in X(k)$.

- When $\deg(D) = 4$, Riemann-Roch gives $\ell(D) = 4$ and the canonical map is an embedding $\varphi : X \hookrightarrow \mathbb{P}^3$. In this case, the elements of $\mathcal{L}(2D)/\mathcal{L}(D)$ are quadratic forms on $\mathbb{P}^3$. The space of all quadratic forms on $\mathbb{P}^3$ has dimension 6, while $\ell(2D) = 8$ by Riemann-Roch, so $\dim \mathcal{L}(2D)/\mathcal{L}(D) = 4$. Thus there are two linearly independent quadratic forms on $\mathbb{P}^3$ that vanish on $X$, and in fact these forms define $\varphi(X)$ as an algebraic subset of $\mathbb{P}^3$. 

54
3.2 Moduli Spaces

Recall that if \( E_1 \) and \( E_2 \) are isomorphic elliptic curves defined by Weierstrass equations 
\[
y^2 = x^3 - 27c_4(E_j)x - 54c_6(E_j), \quad j = 1, 2,
\]
then the ratio \( \frac{c_4(E_j)}{c_6(E_j)} \) is the same for \( j = 1, 2 \).

**Definition.** The \( j \)-invariant of an elliptic curve defined by the Weierstrass equation 
\[
y^2 = x^3 - 27c_4x - 54c_6
\]
is the number 
\[
j(E) = \frac{c_4^3}{\Delta} = \frac{-1728(4A)^3}{\Delta},
\]
where \( \Delta = 4A^3 - 27B^2 \).

**Proposition 3.2.1.** Let \( E_1 \) and \( E_2 \) be elliptic curves over \( k \). If \( E_1 \) is isomorphic to \( E_2 \) then 
\( j(E_1) = j(E_2) \). Conversely, if \( E_1 \) and \( E_2 \) are defined over \( \bar{k} \) then \( j(E_1) = j(E_2) \) implies \( E_1 \) and \( E_2 \) are isomorphic over \( \bar{k} \).

**Proof.** The first statement follows from the definition of the \( j \)-invariant, together with the fact that the ratio \( \frac{c_4}{c_6} \) is an isomorphism invariant. On the other hand, let \( E_1 \) and \( E_2 \) be defined by short Weierstrass equations 
\[
E_1: y^2 = x^3 + Ax + B \quad \text{and} \quad E_2: y^2 = x^3 + A'x + B'.
\]
Then \( j(E_1) = j(E_2) \) implies 
\[
\frac{(4A)^3}{4A^3 - 27B^2} = \frac{(4A')^3}{4(A')^3 - 27(B')^2} \implies A^3(B')^2 = (A')^3B^2.
\]
If \( AB \neq 0 \), i.e. \( j(E) \neq 0, 1728 \), then set \( u = \left( \frac{A}{A'} \right)^{1/4} = \left( \frac{B}{B'} \right)^{1/6} \in \bar{k} \). Then \( u \) is the transformation of \( \mathbb{P}^2 \) realizing the isomorphism \( E_1 \to E_2 \). The cases \( j(E) = 0 \) and \( 1728 \) are similar. \( \square \)

The \( j \)-invariant gives a map 
\[
\left\{ \text{isomorphism classes of elliptic curves over } \bar{k} \right\} \xrightarrow{j} \mathbb{A}^1(\bar{k}).
\]
Moduli spaces allow us to understand when this mapping is a bijection.

**Proposition 3.2.2.** Let \( j \in \mathbb{A}^1(\bar{k}) \) and let \( E_j \) be the curve in \( \mathbb{P}^2(\bar{k}) \) defined by 
\[
\begin{cases}
y^2 + xy = x^3 - \frac{36}{j-1728}x - \frac{1}{j-1728}, & j \neq 0, 1728 \\
y^2 + y = x^3, & j = 0 \\
y^2 = x^3 + x, & j = 1728.
\end{cases}
\]
Then \( E_j \) is an elliptic curve with \( j \)-invariant equal to \( j \).
Corollary 3.2.3. The $j$-invariant is a bijection between isomorphism classes of elliptic curves over $\overline{k}$ and $\mathbb{A}^1(\overline{k})$.

This bijection does not hold in general with classes of elliptic curves over a non-algebraically closed field. However, Proposition 3.2.2 shows that $j$ is a surjection in general; that is, it is possible to construct an elliptic curve of any prescribed $j$-invariant.

Example 3.2.4. If $E$ is given by the short Weierstrass form $y^2 = x^3 + Ax + B$, then for any $d \in k^\times/(k^\times)^2$, the twist $E_d : dy^2 = x^3 + Ax + B$ is not isomorphic to $E$. Further, when $j \neq 0, 1728$ we will see that $\text{Aut}(E) = \mathbb{Z}/2\mathbb{Z}$. One can then construct these twists of $E$ using cocycles in the Galois cohomology group $H^1(k, \text{Aut}(E))$.

Definition. Let $\mathcal{C}$ be a collection of objects in a category. If there is a space $M$ such that the isomorphism classes of objects in $\mathcal{C}$ are in bijection with the points of $M$, then $M$ is called a moduli space for $\mathcal{C}$.

Example 3.2.5. The projective space $\mathbb{P}^n_k$ is a moduli space for the collection of lines through the origin in $k^{n+1}$. Likewise, the Grassmannian $Gr(k,n)$ is a moduli space for the $k$-dimensional subspaces of a vector space $V$.

Corollary 3.2.3 says that $M_1(\overline{k}) = \mathbb{A}^1(\overline{k})$ is a moduli space for the collection of elliptic curves $E$ defined over the algebraic closure $\overline{k}$. There are more complicated moduli spaces $M_g(\overline{k})$ that parametrize the curves of genus $g$ up to isomorphism, for $g \geq 2$.

3.3 The Group Law

By studying the arc length of an ellipse and related shapes, giving rise to elliptic functions, mathematicians such as Abel, Jacobi and Weierstrass discovered that the points on an elliptic curve can be “added” in a certain way so as to define a group structure. Geometrically, this group structure may be realized as the so-called “chord-and-tangent method”.

Let $E$ be an elliptic curve over $k$, let $O \in E(k)$ be the point at infinity and fix two points $P, Q \in E(k)$. In the plane $\mathbb{P}^2$, there is a unique line containing $P$ and $Q$; call it $L$. (If $P = Q$, then take $L = TP_E$.) Then by Bézout’s theorem (2.8.6), $E \cap L = \{P, Q, R\}$ for some third point $R \in E(k)$, which may not be distinct from $P$ and $Q$ if multiplicity is counted. Let $L'$ be the line through $R$ and $O$ and call its third point $R'$.
Definition. Addition of two points \( P, Q \in E(k) \) is defined by \( P + Q = R' \), where \( R' \) is the unique point lying on the line through \( R \) and \( O \). If \( R = O \), we set \( R' = O \).

**Proposition 3.3.1.** Let \( E \) be an elliptic curve with \( O \in E(k) \). Then

(a) If \( L \) is a line in \( \mathbb{P}^2 \) such that \( E \cap L = \{ P, Q, R \} \), then \( (P + Q) + R = O \).

(b) For all \( P \in E(k) \), \( P + O = P \).

(c) For all \( P, Q \in E(k) \), \( P + Q = Q + P \).

(d) For all \( P \in E(k) \), there exists a point \( -P \in E(k) \) satisfying \( P + (-P) = O \).

(e) For all \( P, Q, R \in E(k) \), \( (P + Q) + R = P + (Q + R) \).

Together, (b) – (e) say that chord-and-tangent addition of points defines an associative, commutative group law on \( E(k) \). The proofs of (a) – (d) are rather routine using the definition of this addition law, whereas verifying associativity is notoriously difficult. We will obtain all of these facts as a consequence of the relation between \( E(k) \) and \( \text{Pic}^0(X) \) in Section 3.4.

**Proposition 3.3.2.** Suppose \( E \) is an elliptic curve given by Weierstrass equation

\[
y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6.
\]

Let \( P = (x, y) \) and \( P_i = (x_i, y_i), i = 1, 2, 3, \) be points in \( E(k) \) such that \( P_1 + P_2 = P_3 \). Then

(a) \( -P = (x, -(y + a_1 x + a_3)) \).

(b) If \( x_1 = x_2 \) and \( y_1 + y_2 + a_1 x + a_3 = 0 \), then \( P_1 + P_2 = O \).

(c) If \( x_1 = x_2 \) and \( y_1 + y_2 + a_1 x + a_3 \neq 0 \), then

\[
x_3 = \left( \frac{3x_1^2 + 2a_2 x_1 + a_4 - a_1 y_1}{2y_1 + a_1 x_1 + a_3} \right)^2 + a_1 \frac{3x_1^2 + 2a_2 x_1 + a_4 - a_1 y_1}{2y_1 + a_1 x_1 + a_3} - a_2 - 2x_1
\]

and

\[
y_3 = -\left( \frac{3x_1^2 + 2a_2 x_1 + a_4 - a_1 y_1}{2y_1 + a_1 x_1 + a_3} + a_1 \right)x_3 - \frac{-x_3^3 + a_4 x_1 + 2a_6 - a_3 y_1}{2y_1 + a_1 x_1 + a_3} - a_3.
\]

(d) Otherwise, if \( x_1 \neq x_2 \), then

\[
x_3 = \left( \frac{y_2 - y_1}{x_2 - x_1} \right)^2 + a_1 \frac{y_2 - y_1}{x_2 - x_1} - a_2 - x_1 - x_2
\]

and

\[
y_3 = -\left( \frac{y_2 - y_1}{x_2 - x_1} + a_1 \right)x_3 - \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1} - a_3.
\]
3.4 The Jacobian

For a smooth algebraic curve $X$ over $k$ of genus $g$, the quotient $\text{Pic}^0(X) = \text{Div}^0(X) / \text{PDiv}(X)$ has the structure of a group. Remarkably, we can also give this object the structure of an algebraic variety in a way that is compatible with the group structure, such that its dimension as a variety is $g$.

**Definition.** An algebraic group over a field $k$ is a variety $G$ over $k$ together with morphisms $\mu : G \times G \to G$ and $i : G \to G$ such that $\mu(a, b) = ab$ and $i(a) = a^{-1}$ define a group structure on $G$, with identity element $e \in G(k)$.

**Remark.** For any extension $K \supset k$, the variety $G(K)$ is also an algebraic group. The terminology from Chapter 1 carries over to algebraic groups with appropriate modifications, e.g. an algebraic group is defined over $k$ if it is defined over $k$ as a variety and the multiplication and inversion morphisms are defined over $k$.

**Example 3.4.1.** For any field $k$, the additive group $\mathbb{G}_a = \mathbb{A}^1_k$ is an algebraic group under addition $\mu(a, b) = a + b$. The multiplicative group $\mathbb{G}_m = \mathbb{A}^1_k \setminus \{0\}$ is also an algebraic group under multiplication $\mu(a, b) = ab$.

We will prove that the $k$-rational points on an elliptic curve form an algebraic group. One can show that these are essentially all of the dimension 1 algebraic groups:

**Theorem 3.4.2.** Any connected algebraic group of dimension 1 is isomorphic over $\bar{k}$ to $\mathbb{G}_a, \mathbb{G}_m$ or an elliptic curve $E$.

**Definition.** An abelian variety is an irreducible, projective algebraic group.

**Example 3.4.3.** For any $n \geq 1$, $GL_n(k)$ is an algebraic group defined as a variety by the nonvanishing of the polynomial $\det(x_{ij})$. Thus $GL_n(k)$ is an affine – not a projective – variety.

**Theorem 3.4.4.** Every abelian variety is a commutative group.

An important construction in algebraic geometry is that of the Jacobian of a variety $X$, which is an abelian variety into which $X$ embeds. A special case of this for curves is given by the following theorem, which we prove later in the section.

**Theorem 3.4.5.** Let $X$ be a nonsingular algebraic curve of genus $g$ which is geometrically connected. Then there exists an abelian variety $J(X)$ defined over $k$ of dimension $g$ with compatible group isomorphisms $J_K(X) \cong \text{Pic}^0(X/K)$ for any field extension $K \supset k$ for which $X(K) \neq \emptyset$. In particular, $J(X) \cong \text{Pic}^0(X)$.

**Definition.** The abelian variety $J(X)$ is called the Jacobian of $X$.

When $E$ is an elliptic curve, we will prove that $J(E) \cong E$ as curves. To do this, we first construct a bijection $\text{Pic}^0(E) \leftrightarrow E(k)$ to get a group structure on $E(k)$. We then show that this determines the structure of an abelian variety on $E$. 
Lemma 3.4.6. Suppose $X$ is a curve of genus $g = 1$. Then for any $P, Q \in X(k)$, $[P] \sim [Q]$ if and only if $P = Q$.

Proof. $(\Leftarrow)$ is trivial. For $(\Rightarrow)$, suppose $f \in X(k)$ and $f$ is surjective. Then $f \in L(Q)$ but since $L(Q) = 1$ by Riemann-Roch and $L(Q)$ contains the constants, $f$ itself must be constant. Therefore $0 = (f) = P - Q$ so $P = Q$. □

Lemma 3.4.7. Let $E$ be an elliptic curve with fixed point $O \in E(k)$. For all $D \in \text{Div}^0(E)$, there exists a unique point $P \in E$ such that $D \sim P - O$. Moreover, the map

$$\xi_O := \text{Div}^0(E) \longrightarrow E(k)$$

$$D \longmapsto P$$

is surjective, and if $D_1, D_2 \in \text{Div}^0(E)$, then $\xi_O(D_1) = \xi_O(D_2)$ if and only if $D_1 \sim D_2$.

Proof. For $D \in \text{Div}^0(E)$, we have $\ell(D + O) = 1$ by Riemann-Roch, so take $f \in L(D + O)$ with $f \neq 0$ and $(f) + D + O \geq 0$. Since $\deg(f) = 0$, $(f) = (-D - O) + P$ for some point $P \in E(k)$. Thus $D \sim P - O$. To see that $P$ is unique, suppose $D \sim P' - O$ for another point $P \in E(k)$. Then $P \sim D - O \sim P'$, or $P \sim P'$ by transitivity, so $P = P'$ by Lemma 3.4.6.

This defines the map $\xi_O : D \mapsto P$ on the divisors of degree 0. It is clear that $\xi_O$ is surjective: if $P \in E(k)$, $D = P - O$ is a degree 0 divisor and $\xi_O(P - O) = P$. Finally, set $\xi_O(D_1) = P_1$ and $\xi_O(D_2) = P_2$. Then if $D_1 \sim P_1 - O$ and $D_2 \sim P_2 - O$ then $D_1 - D_2 \sim P_1 - P_2$. So

$$\xi_O(D_1) = \xi_O(D_2) \iff P_1 = P_2$$

$$\iff P_1 - P_2 \sim O \text{ by Lemma 3.4.6}$$

$$\iff D_1 - D_2 \sim O$$

$$\iff D_1 \sim D_2.$$ □

Theorem 3.4.8. There is a bijection $\text{Pic}^0(E) \cong E(k)$ given by

$$\text{Pic}^0(E) \longleftrightarrow E(k)$$

$$D \mapsto P \text{ where } D \sim P - O$$

$$[P - O] \mapsto P.$$  

Definition. The inverse of $\xi_O$ is the map $\kappa : E(k) \rightarrow \text{Pic}^0(E), P \mapsto [P - O]$, called the Abel-Jacobi map.

For points $P, Q \in E(k)$, the Abel-Jacobi map defines an abelian group law by $P + Q := \xi_O(\kappa(P) + \kappa(Q))$, with $\kappa(P) + \kappa(Q)$ taking place in $\text{Pic}^0(E)$. We now show that this group law matches the chord-and-tangent operation from Section 3.3.

Lemma 3.4.9. The chord-and-tangent and Abel-Jacobi operations on $E(k)$ are the same.
Proof. Fix the points $P, Q, R, R' \in E(k)$ and lines $L, L'$ be as in Section 3.3. Then $L$ is a line given by some linear form $f(X_1, X_2, X_3) = \alpha X_1 + \beta X_2 + \gamma X_3$. Note that $\frac{f}{X_3}$ defines a rational function on $E$, and $\text{div}_E(f) = \left(\frac{f}{X_3}\right) = P + Q + R - 3O$ – we can deduce that $\text{ord}_O(f) = 3$ since the divisor $\left(\frac{f}{X_3}\right)$ must have degree 0. On the other hand, $L'$ is given by some other linear form $f'(X_1, X_2, X_3)$, for which we have $\text{div}_E(f') = \left(\frac{f'}{X_3}\right) = R + O + R' - 3O$. Subtracting these equations gives:

$$R' - P - Q + O = \text{div}_E(f) - \text{div}_E(f') = \left(\frac{f}{f'}\right) \sim 0.$$  

Adding and subtracting $O$, we get

$$(R - O') - ((P - O) + (Q - O)) \sim O \implies \kappa(R') - (\kappa(P) + \kappa(Q)) = 0 \quad \text{in Pic}^0(E) \implies \kappa(R') = \kappa(P) + \kappa(Q).$$

Finally, since $\xi_O$ is a bijection, $\xi_O(\kappa(P) + \kappa(Q)) = R' = P + Q$ as required. 

Corollary 3.4.10. The chord-and-tangent law is an associative group law on $E(k)$.

Theorem 3.4.11. The operation $\mu : (P, Q) \mapsto P + Q$ is a morphism on $E(k)$.

Proof. Suppose $E$ is given by a short Weierstrass form $y^2 = x^3 + Ax + B$ and fix points $P = (x_1, y_1), Q = (x_2, y_2) \in E(k)$. Then $-P = (x_1, -y_1).$ The line $L$ through $P$ and $Q$ is explicitly given by the linear form

$$f : y - y_1 = \lambda(x - x_1) \quad \text{where} \quad \lambda = \frac{y_2 - y_1}{x_2 - x_1}.$$  

Substituting this into the Weierstrass equation, we get

$$(y_1 + \lambda(x - x_1))^2 = x^3 + Ax + B \implies 0 = x^3 - \lambda^2 x^2 + (2\lambda y_1 - A)x + (y_1^2 - 2\lambda y_1 x_1 - 2\lambda x_1 + \lambda^2 x_1^2 - B).$$

This cubic equation has three solutions, two of which are known already: $x_1$ and $x_2$. Further, if $P + Q + R = 0$ for $R = (x_3, y_3)$, then the trace of the cubic polynomial is given by $\lambda^2 = x_1 + x_2 + x_3$ when $P$ and $Q$ are distinct. Therefore we get the following formula for $R$:

$$R = (x_3, y_3) = (\lambda^2 - x_1 - x_2, \lambda(x_3 - x_1) + y_1).$$

(Compare this to the formulas in Proposition 3.3.2.) Similarly, for $P = Q$ we get

$$R = (x_3, y_3) = \left(\frac{3x_1 + A^2}{2y_1}\right)^2 - 2x_1, -\left(\frac{3x_1 + A}{2y_1}\right)x_3 - \frac{-x_1^3 + Ax_1 + 2B}{2y_1}.$$  

In both cases, the map $(P, Q) \mapsto -R = P + Q$ is given by rational functions on the affine patch of $E(k)$ away from the point at $\infty$, and the argument at $\infty$ is similar. 

Corollary 3.4.12. $E(k)$ is an abelian variety, and therefore so is the Jacobian $J(E)$

Remark. In cryptography, it is vital to be able to compute $nP$ quickly, say over a finite field $\mathbb{F}_q$. To do this efficiently, one writes $n$ as a binary sequence and employs a fast adding-and-doubling formula for the coordinates of a point. For example, $10P = 2(2(2P) + P)$ can be computed in a small number of steps. An alternative is to use different coordinates for an elliptic curve, such as the Jacobian-Edwards coordinates.
4 Rational Points on Elliptic Curves

Let $E$ be an elliptic curve defined over a field $k$ with point $O \in E(k)$. We saw in Chapter 3 that the rational points $E(k)$ form an abelian group, and in fact an abelian variety over $k$. In this chapter we will describe the structure of this group.

Definition. The $n$-torsion points of $E(k)$ form a subset

$$E_n(k) = \{ P \in E(k) \mid nP = O \}$$

of $E(k)$. The torsion subgroup of $E(k)$ is the union of all of these subgroups:

$$E_{\text{tors}}(k) = \bigcup_{n=0}^{\infty} E_n(k).$$

Lemma 4.0.1. For each $n \geq 0$, $E_n(k)$ is a subgroup of $E(k)$.

Proof. A consequence of Theorem 3.4.11 is that for any $n$, the map $[n] : E \to E, P \mapsto nP$ is regular. Clearly the kernel of this map is $E_n(k)$. \hfill \Box

We will prove:

Theorem 4.0.2. Let $[n] : E \to E$ be the multiplication by $n$ map, $P \mapsto nP$, suppose $\text{char } k = 0$. Then

1. $[n]$ is unramified at $O$.
2. $\deg[n] = n^2$ and for every $d \mid n$, the set of $d$-torsion points of $E_n(k)$ has size $\#E_n(k)[d] = d^2$.
3. $E_n(k) \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Ultimately, our goal is to characterize $\mathbb{Q}$-rational points of an elliptic curve. The classic result in this direction is the Mordell-Weil theorem:

Theorem 4.0.3 (Mordell-Weil). For any elliptic curve $E$, $E(\mathbb{Q})$ is finitely generated.

As a consequence, we can write $E(\mathbb{Q}) = E_{\text{tors}}(\mathbb{Q}) \oplus \mathbb{Z}^r$ where $r$ is called the rank of $E$. Then Theorem 4.0.2 and its analogues in characteristic $p$ give a characterization of the torsion part of $E(k)$. It turns out that $E_{\text{tors}}(\mathbb{Q})$ can be effectively computed from the Weierstrass equation for $E$. There are countless other interesting results about this group of rational points, such as Mazur’s surprising theorem:

Theorem 4.0.4 (Mazur). For any elliptic curve $E$, $\#E_{\text{tors}}(\mathbb{Q}) \leq 16$.

Thus the mystery lies in the rank of $E$. There is a method for finding the generators of the free part of $E(k)$, known as descent. To understand this here and in Chapter 5, we will study isogenies, height functions and the Selmer and Tate-Shafarevich groups.
4.1 Isogenies

The class of elliptic curves $E$ over $k$ with specified point $O \in E(k)$ form a category, and the morphisms in this category are called isogenies.

**Definition.** An *isogeny* between two elliptic curves $(E_1, O_1)$ and $(E_2, O_2)$ is a nonconstant morphism $\varphi : E_1 \to E_2$ such that $\varphi(O_1) = O_2$.

**Example 4.1.1.** For the purpose of studying the group $E(k)$, an important isogeny is the multiplication map $[n] : E \to E, P \mapsto nP$. This is regular by Theorem 3.4.11.

**Proposition 4.1.2.** An isogeny is a morphism of algebraic groups.

*Proof.* The pushforward map $\varphi_* : \text{Div}(E_1) \to \text{Div}(E_2)$ descends to the Picard group, inducing a commutative diagram

$$
\begin{array}{ccc}
\text{Pic}^0(E_1) & \xrightarrow{\varphi_*} & \text{Pic}^0(E_2) \\
\kappa \downarrow & & \downarrow \kappa \\
E_1 & \xrightarrow{\varphi} & E_2
\end{array}
$$

Here, the vertical arrows are the Abel-Jacobi maps, which are isomorphisms by Theorem 3.4.8. Assuming $\varphi(O_1) = O_2$, the diagram shows $\varphi(P + Q) = \varphi(P) + \varphi(Q)$ so the group structure is preserved. \qed

**Remark.** Let $P \in E$ be a point on an elliptic curve and define a morphism $\tau_P : E \to E$ by $Q \mapsto Q + P$. Then for any regular map $\alpha : E_1 \to E_2$, the composition $\tau_{\alpha(O_1)} \circ \alpha$ is an isogeny. That is, every regular map is an isogeny up to translation.

**Definition.** For two elliptic curves $E_1, E_2$ over $k$, define the *$k$-morphisms*

$$
\text{Hom}_k(E_1, E_2) = \{\text{isogenies } E_1 \to E_2 \text{ defined over } k\} \cup \{[0]\}.
$$

For any elliptic curve $E$ over $k$, we also define the *endomorphisms* and *automorphisms* of $E$ by:

$$
\text{End}_k(E) = \text{Hom}_k(E, E) \quad \text{and} \quad \text{Aut}(E) = \text{End}_k(E)^\times.
$$

**Lemma 4.1.3.** $\text{Hom}_k(E_1, E_2)$ is an abelian group under pointwise addition: $(\varphi + \psi)(P) = \varphi(P) + \psi(P)$. Further, $\text{End}_k(E)$ is a ring under function composition.

*Proof.* Obvious. \qed

**Proposition 4.1.4.** (a) For any elliptic curve $E$, the multiplication map $[m] : E \to E$ is an isogeny for all nonzero $m \in \mathbb{Z}$.

(b) $\text{Hom}_k(E_1, E_2)$ is torsion-free.

(c) $\text{End}_k(E)$ is an integral domain of characteristic 0.
Example 4.1.5. Consider the elliptic curve $E : y^2 = x^3 - x$. Then $\mathbb{Z}[i] \hookrightarrow \text{End}_k(E)$ by mapping $i \mapsto [i]$, where $[i]$ is the isogeny $(x, y) \mapsto (-x, iy)$.

We have seen that $[m] : P \mapsto mP$ are an important family of isogenies on an elliptic curve. We can come up with many more isogenies by recalling that morphisms of curves correspond bijectively to embeddings of function fields (Proposition 2.2.2). For an elliptic curve $E$, the field $k(E)$ is sometimes referred to as the “field of elliptic functions” defined by $E$. This terminology has roots in the study of elliptic functions over Riemann surfaces, which was the original motivation for understanding elliptic curves.

Example 4.1.6. If $k = \mathbb{C}$, elliptic curves are canonically identified with complex tori $E \cong \mathbb{C}/\Lambda$. Therefore if $E_1 = \mathbb{C}/\Lambda_1$ and $E_2 = \mathbb{C}/\Lambda_2$ are complex tori, then $\text{Hom}_\mathbb{C}(E_1, E_2) = \{\alpha \in \mathbb{C} : \alpha \Lambda_1 \subset \Lambda_2\}$. The field of elliptic functions $\mathbb{C}(E)$ is generated as a function field over $\mathbb{C}$ by special functions $\wp(z)$ and $\wp'(z)$, where $\wp(z)$ is called the Weierstrass $\wp$-function.

Theorem 4.1.7. Let $\varphi : E_1 \to E_2$ be an isogeny over the algebraic closure $\overline{k}$. Then

1. $\# \varphi^{-1}(Q) = \deg_s \varphi$ for all $Q \in E_2$. Therefore $e_{\varphi}(Q) = \deg_s \varphi$.
2. The map

$$\ker \varphi \longrightarrow \text{Aut}(k(E_1)/\varphi^*k(E_2))$$

$$P \mapsto \tau_P$$

is an isomorphism.

Proof. (1) $\deg_s \varphi = \# \varphi^{-1}(Q)$ for all but finitely many $Q \in E_2$. Fix such a $Q$ and let $Q' \in E_2$ and $R \in E_1$ such that $\varphi(R) = Q' - Q$. Then $\tau_R : \varphi^{-1}(Q) \to \varphi^{-1}(Q')$ is a bijection, so all points in $E_2$ have the same number of preimages.

It is clear that $\tau_P^* \varphi k(E_1)$ so we need only check it fixes $\varphi^* k(E_2)$. For $P \in \ker \varphi$, $\varphi \circ \tau_P = \varphi$ since $\varphi(P) = O$. Thus for $f \in k(E_2)$,

$$\tau_P^* (\varphi^* f) = (\tau_P \circ \varphi)^* f = \varphi^* f$$

so $\varphi^* k(E_2)$ is fixed. Also, it is clear that $P \mapsto \tau_P^*$ is a group homomorphism by definition of the $\tau_P$. From (1), we know that $\# \ker \varphi = \deg_s \varphi$, but

$$\# \text{Aut}(k(E_1)/\varphi^* k(E_2)) \leq \deg_s \varphi.$$
4.1 Isogenies

If \( k \) is not algebraically closed, then each \( P \in \ker \varphi \) may not be defined over \( k \). However, if this condition is satisfied, we would still have \( \ker \varphi \cong \text{Aut}(k(E_1)/\varphi^*k(E_2)) \).

**Remark.** In the language of Grothendieck’s algebraic geometry, (1) says that “separable isogenies are étale covers”, while (2) says that “separable isogenies are Galois covers”. Thus we see the connections between Galois theory, covering space theory and isogenies between elliptic curves begin to emerge.

**Corollary 4.1.8.** Suppose \( \varphi : E_1 \to E_2 \) and \( \psi : E_1 \to E_3 \) are isogenies, where \( \varphi \) is separable and \( \ker \varphi \subseteq \ker \psi \). Then there is a unique isogeny \( \lambda \) making the following diagram commute:

\[
\begin{array}{ccc}
E_1 & \xrightarrow{\varphi} & E_2 \\
\downarrow{\psi} & & \downarrow{\lambda} \\
E_3 & & \\
\end{array}
\]

**Proof.** Set \( G = \text{Gal}(k(E_1)/\varphi^*k(E_2)) \); we may use this notation since by hypothesis the field extension is Galois. Then \( G \cong \ker \varphi \subseteq \psi \cong \text{Aut}(k(E_1)/\psi^*k(E_3)) \), so in particular \( G \) fixes \( \psi^*k(E_3) \). Since \( k(E_1)/\varphi^*k(E_2) \) is Galois, we have inclusions of fields \( \psi^*k(E_3) \subseteq \varphi^*k(E_2) \subseteq k(E_1) \), so by Proposition 2.2.2, we get a regular map \( \lambda : E_2 \to E_3 \). (Finish: show \( \lambda \) is an isogeny and is unique.)

**Proposition 4.1.9.** Let \( \Phi \subset E \) be a finite, \( G_k \)-invariant subgroup of \( E \). Then there exists a unique choice of elliptic curve \( E' \) and isogeny \( \varphi : E \to E' \) such that \( \ker \varphi = \Phi \).

**Proof.** (Sketch) There is an embedding \( \Phi \hookrightarrow \text{Aut}(k(E)/k) \) given by \( P \mapsto \tau_P^\# \). This induces an action of \( \Phi \) on \( k(E) \), so consider the subfield \( k(E)\Phi \subseteq k(E) \). By Proposition 2.2.2, there is a curve \( E'/k \) with \( k(E') = k(E)\Phi \) and an isogeny \( \varphi : E \to E' \) corresponding to the field embedding \( k(E') \hookrightarrow k(E) \). Using the Riemann-Hurwitz formula (Theorem 2.5.2), one now shows that \( \varphi \) is unramified and \( E' \) is an elliptic curve.

In particular, quotients of elliptic curves by kernels of isogenies again give elliptic curves.

**Remark.** Suppose \( E_1 \) and \( E_2 \) are elliptic curves in short Weierstrass form. Then for any isogeny \( \varphi : E_1 \to E_2 \) over \( k \), we can write

\[
\varphi(x,y) = \left( \frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y \right) \quad \text{for } u, v, s, t \in k[x].
\]

In this case \( \deg \varphi = \max\{\deg u, \deg v\} \), and \( \varphi \) is inseparable if and only if \( u = f(x^p) \) and \( v = g(x^p) \) for \( f, g \in k[x] \), where \( p = \text{char } k \).

Differentials (Section 2.4) are useful for characterizing separability of isogenies.

**Theorem 4.1.10.** An isogeny \( \varphi : E_1 \to E_2 \) is separable if and only if the induced map \( \varphi^* : \Omega_{E_2} \to \Omega_{E_1} \) is nonzero.
Recall that the invariant differential of an elliptic curve in Weierstrass form is the meromorphic differential \( \omega = \frac{dx}{2y + a_1x + a_3} \in \Omega_E \). By Lemma 2.4.1, \( \dim_{k(E)} \Omega_E = 1 \) so \( \omega \) is a generator. The following proposition explains the name of the invariant differential.

**Proposition 4.1.11.** For every point \( P \in E \), \( \tau_P^* \omega = \omega \).

**Theorem 4.1.12.** If \( \varphi, \psi : E_1 \to E_2 \) are isogenies and \( \omega \in \Omega_{E_2} \) is the invariant differential on \( E_2 \), then \( (\varphi + \psi)^* \omega = \varphi^* \omega + \psi^* \omega \).

**Corollary 4.1.13.** Let \( E \) be an elliptic curve, \( \omega \in \Omega_E \) the invariant differential on \( E \), and for \( m \in \mathbb{Z} \), let \([m] : E \to E \) be the multiplication by \( m \) map. Then \([m]^* \omega = m \omega \). Therefore \([m] \) is separable if and only if \( \text{char} \ k \nmid m \).

**Proof.** The first property is clear for \( m = 0, 1 \). Now induct on \( m \), using Theorem 4.1.12 on \([m + 1]^* \omega = [m]^* \omega + \omega \).

**Corollary 4.1.14.** If \( k = \mathbb{F}_q \) is a finite field, \( E \) is an elliptic curve over \( k \) and \( \pi_q : E \to E \) is the \( q \)th power Frobenius map, then the map \([n] + [m] \pi_q : E \to E \) is separable if and only if \( q \nmid n \).

**Example 4.1.15.** An important application is that the map \([1] - \pi \) is always separable. Notice that \([1] - \pi : E(\mathbb{F}_q) \to E(\overline{\mathbb{F}}_q) \) has kernel \( E(\mathbb{F}_q) \).

### 4.2 The Dual Isogeny

In this section we introduce the notion of a dual isogeny, which is vital for calculating degrees of isogenies.

**Theorem 4.2.1** (Dual Isogeny). Let \( \varphi : E_1 \to E_2 \) be an isogeny. Then there exists a unique isogeny \( \widehat{\varphi} : E_2 \to E_1 \) satisfying \( \widehat{\varphi} \circ \varphi = [\deg \varphi] \in \text{End}_k(E_1) \).

**Proof.** For the construction, recall the Abel-Jacobi map and its inverse from Theorem 3.4.8:

\[
\kappa : E_2 \longrightarrow \text{Div}^0(E_2) \quad \text{and} \quad \xi_{O_1} : \text{Div}^0(E_1) \longrightarrow E_1 \quad P \mapsto P - O_2 \quad \sum n_QQ \mapsto \sum [n_Q]Q.
\]

Then the dual isogeny may be defined as the following composition:

\[
\widehat{\varphi} : E_2 \xrightarrow{\kappa} \text{Div}^0(E_2) \xrightarrow{\varphi^*} \text{Div}^0(E_1) \xrightarrow{\xi_{O_1}} E_1.
\]

(See Silverman for the rest of the details.)

**Proposition 4.2.2.** The dual isogeny satisfies the following properties:

1. If \( \varphi : E_1 \to E_2 \) is separable, then the dual isogeny \( \widehat{\varphi} \) is also separable.
2. \( \widehat{\varphi} \circ \psi = \widehat{\psi} \circ \widehat{\varphi} \) for any isogenies \( E_1 \xrightarrow{\varphi} E_2 \xrightarrow{\psi} E_3 \).
4.2 The Dual Isogeny

4 Rational Points on Elliptic Curves

(3) \( \hat{\varphi + \psi} = \hat{\varphi} + \hat{\psi} \) for any \( \varphi, \psi : E_1 \to E_2 \).

(4) For \( m \in \mathbb{Z} \) and the isogeny \([m] : E \to E, [m] = [m]. \) In particular, \( \deg[m] = m^2 \) when \( \text{char } k \nmid m \).

(5) \( \deg \hat{\varphi} = \deg \varphi \).

(6) \( \hat{\hat{\varphi}} = \varphi \).

**Proposition 4.2.3.** For any pair of elliptic curves \( E_1, E_2 \), degree map \( \deg : \text{Hom}(E_1, E_2) \to \mathbb{Z} \) is a positive definite quadratic form, meaning for all \( \varphi, \psi \in \text{Hom}(E_1, E_2) \),

(1) \( \deg(-\varphi) = \deg(\varphi) \);

(2) \( \deg \varphi \geq 0 \) and \( \deg \varphi = 0 \) if and only if \( \varphi = 0 \).

(3) The pairing \( \langle \varphi, \psi \rangle = \deg(\varphi + \psi) - \deg \varphi - \deg \psi \) is bilinear.

**Definition.** The **trace** of an endomorphism \( \psi \in \text{End}_k(E) \) is the endomorphism \( \text{tr } \psi = \psi + \hat{\psi} \).

**Lemma 4.2.4.** For any endomorphism \( \psi \in \text{End}_k(E) \), the trace is equal to

\[
\text{tr } \psi = 1 + [\deg \psi] - [\deg(1 - \psi)].
\]

**Proof.** Using Proposition 4.2.3, we have

\[
[\deg(1 - \psi)] = (1 - \hat{\psi}) \circ (1 - \psi) = (1 - \hat{\psi}) \circ (1 - \psi) = 1 - \psi - \hat{\psi} + \hat{\psi} \circ \psi = 1 - \text{tr } \psi + [\deg \psi].
\]

Rearranging gives the desired expression for \( \text{tr } \psi \). \( \square \)

**Definition.** The **characteristic polynomial** of an endomorphism \( \psi \in \text{End}_k(E) \) is \( c_\psi(x) = x^2 - (\text{tr } \psi)x + \deg \psi \).

**Remark.** As with linear endomorphisms and the Cayley-Hamilton theorem in linear algebra, an endomorphism \( \psi : E \to E \) satisfies its own characteristic polynomial:

\[
c_\psi(\psi) = \psi \circ \psi - (\text{tr } \psi) \circ \psi + [\deg \psi] = 1 - \psi - \hat{\psi} + \hat{\psi} \circ \psi = 1 - \text{tr } \psi + [\deg \psi].
\]

**Theorem 4.2.5** (Cauchy-Hasse). For all endomorphisms \( \psi \in \text{End}_k(E) \) and \( r \in \mathbb{Q} \), \( c_\psi(r) \geq 0 \). Therefore \( |\text{tr } \psi| \leq 2\sqrt{\deg \psi} \).

**Proof.** Let \( r = \frac{m}{n} \in \mathbb{Q} \) with \( m, n \in \mathbb{Z} \) and \( n \neq 0 \). Then

\[
n^2 c_\psi(r) = m^2 + mn(\text{tr } \psi) + n^2(\deg \psi) = (m + n\psi) \circ (m + n\hat{\psi}) = (m + n\psi) \circ (\hat{m} + n\psi) = \deg(m + n\psi) \geq 0.
\]

Since \( n^2 \geq 0 \), we get \( c_\psi(r) \geq 0 \). In particular, the discriminant of \( c_\psi(x) \) is nonpositive, but \( \text{disc}(c_\psi) = (\text{tr } \psi)^2 - 4 \deg \psi \geq 0 \) so this implies the second statement. \( \square \)
Corollary 4.2.6 (Hasse Bound). Let $E$ be an elliptic curve over a finite field $\mathbb{F}_q$ and $\pi_q : E \to E$ the $q$th power Frobenius map. Then $\#E(\mathbb{F}_q) = q+1 - \text{tr} \pi_q$. Moreover, $|\text{tr} \pi_q| \leq 2\sqrt{q}$.

Proof. The map $\pi_q : E \to E$ is given by $(x,y) \mapsto (x^q, y^q)$ on the affine piece of $E$. Then $(x,y) \in E(\mathbb{F}_q)$ if and only if $\pi_q(x,y) = (x,y)$. Thus

$$
\#E(\mathbb{F}_q) = \#\{\text{fixed points of } \pi_q\} = \#\ker(1 - \pi_q)
= \deg_s(1 - \pi_q) \quad \text{by Example 4.1.15}
= \deg(1 - \pi_q) \quad \text{since } 1 - \pi_q \text{ is separable by Corollary 4.1.14}
= (1 - \pi_q) \circ (1 - \pi_q)
= (1 - \widehat\pi_q) \circ (1 - \pi_q)
= 1 - (\pi_q + \widehat\pi_q) + \widehat\pi_q \circ \pi_q
= 1 - \text{tr} \pi_q + \deg \pi_q = q + 1 - \text{tr} \pi_q.
$$

The inequality $|\text{tr} \pi_q| \leq 2\sqrt{q}$ now follows from the Cauchy-Hasse theorem. \qed

Proposition 4.2.7. Let $E$ be an elliptic curve over $k$ and $m \in \mathbb{Z}$. Then

1. If $\text{char } k \nmid m$ then $E_m(k) = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.
2. If $\text{char } k = p > 0$, then for any $e \geq 1$, either $E_{p^e}(k) = 0$ or $E_{p^e}(k) = \mathbb{Z}/p^e\mathbb{Z}$.

Proof. (1) follows from (4) of Proposition 4.2.3.

(2) For any $e \geq 1$, let $\pi : E \to E$ be the $p$th power Frobenius map, which is inseparable by Corollary 4.1.14. Then

$$
\#E_{p^e}(k) = \deg_s[p^e] \quad \text{by (1) of Theorem 4.1.7}
= \deg_s((\widehat{\pi} \circ \pi)^e)
= \deg_s(\widehat{\pi}^e \circ \pi^e)
= \deg_s(\widehat{\pi}^e) \deg_s(\pi^e)
= \deg_s(\widehat{\pi}^e)
$$

since $\pi$ is inseparable. Now $\deg_s(\widehat{\pi}^e) = 1$ when $\widehat{\pi}$ is inseparable and $p^e$ when $\widehat{\pi}$ is separable, so the two cases follow. \qed

Definition. An elliptic curve $E$ over a field $k$ of characteristic $p > 0$ is called supersingular if $E_{p^e}(k) = 0$ for any $e \geq 1$. Otherwise if $E_{p^e}(k) = \mathbb{Z}/p^e\mathbb{Z}$ for all $e \geq 1$, $E$ is said to be ordinary.

By the proof of Proposition 4.2.7, $E$ is supersingular exactly when $\widehat{\pi}$ is inseparable, where $\pi : E \to E$ is the Frobenius map.

4.3 The Weil Conjectures

Suppose $X$ is a smooth projective variety over a finite field $\mathbb{F}_q$. 
Definition. The **zeta function** of $X$ over $\mathbb{F}_q$ is the formal power series
\[
Z(X/\mathbb{F}_q, t) = \exp \left( \sum_{r=1}^{\infty} N_r \frac{t^r}{r} \right)
\]
where $N_r = \#X(\mathbb{F}_{q^r})$ for each $r \geq 1$.

The zeta functions of curves have many parallels to Dedekind zeta functions of number fields in algebraic number theory.

**Example 4.3.1.** For $X = \mathbb{P}^1$, the projective line, we have $N_r = q^r + 1$ for every $r$. In particular, one can show that
\[
Z(\mathbb{P}^1/\mathbb{F}_q, t) = \frac{1}{(1-t)(1-qt)}.
\]
In particular, $Z(\mathbb{P}^1, t)$ is a rational function!

The following statements were conjectured by Weil and proven in the 20th century by Weil (for curves), Artin, Grothendieck and Deligne.

**Theorem 4.3.2** (Weil Conjectures). Let $X$ be a smooth projective variety over $\mathbb{F}_q$ of dimension $n$. Then

(a) (Rationality) The zeta function $Z(X/\mathbb{F}_q; t)$ is rational.

(b) (Functional Equation) There is an integer $e = e(X)$, called the Euler characteristic of $X$, for which the zeta function satisfies
\[
Z(X/\mathbb{F}_q, 1/q^n t) = \pm q^{ne/2} t^e Z(X/\mathbb{F}_q, t).
\]

(c) (Riemann Hypothesis) The zeta function may be written
\[
Z(X/\mathbb{F}_q, t) = \frac{p_1(t)p_3(t)\cdots p_{2n-1}(t)}{p_0(t)p_2(t)\cdots p_{2n}(t)}
\]
with $p_0(t) = 1 - t$, $p_{2n}(t) = 1 - q^n t$ and for each $0 \leq i \leq 2n$, $p_i(t) = \prod_{j=1}^{k_i} (1 - \alpha_{ij} t)$ for $\alpha_{ij} \in \mathbb{C}$ satisfying $|\alpha_{ij}| = q^{1/2}$.

Recall that $N_r$ is the number of fixed points of $\pi^r$, where $\pi = \pi_q : X \to X$ is the $q$th power Frobenius map. In topology, one studies fixed points using Lefschetz’s fixed point theorem, which requires knowing the trace of maps on cohomology groups. In algebraic geometry, topological (singular) cohomology theory does not suffice to give such a description. However, Artin, Grothendieck and others were able to devise a cohomology theory called **étale cohomology** for which the following fixed point property holds:

\[
\#\{\text{fixed points of } \pi^r\} = \sum_{i=0}^{\infty} (-1)^i \text{tr}(\pi^r)^* : H^i(X, \mathbb{Q}_\ell) \to H^i(X, \mathbb{Q}_\ell),
\]

where $H^i(X, \mathbb{Q}_\ell)$ is the $\ell$th étale cohomology group of $X$. As a sidenote, the étale cohomology groups satisfy $H^i(X, \mathbb{Q}_\ell) \otimes \mathbb{C} \cong H^i(X(\mathbb{C}); \mathbb{C})$, where the latter is the topological (singular) cohomology of $X$ with coefficients in $\mathbb{C}$. 68
Remark. Setting \( t = q^{-s} \), the zeta function of a variety \( X/\mathbb{F}_q \) can be written
\[
\zeta_{X/\mathbb{F}_q}(s) := Z(X/\mathbb{F}_q, q^{-s}).
\]
Then the functional equation has a nice form: \( \zeta_{X/\mathbb{F}_q}(1 - s) = \zeta_{X/\mathbb{F}_q}(s) \), as with Dedekind zeta functions. Also, the Riemann hypothesis says that \( \zeta_{X/\mathbb{F}_q}(s) = 0 \) for \( s \in \mathbb{C} \) satisfying \( |q^s| = \sqrt{q} \), i.e. \( \text{Re}(s) = \frac{1}{2} \).

Example 4.3.3. For an elliptic curve \( E/\mathbb{F}_q \), one can prove that
\[
Z(E/\mathbb{F}_q, t) = (1 - \alpha t)(1 - \beta t)(1 - t)(1 - qt)^2.
\]
Then by the Hasse bound (Corollary 4.2.6), \( (\text{tr} \pi)^2 - 4q \geq 0 \), so the roots \( t = \frac{1}{\alpha} \) and \( \frac{1}{\beta} \) are complex conjugates. Thus \( |\alpha| = |\beta| \), but since \( \alpha \beta = q \), we get \( |\alpha| = q^{1/2} \). Thus the Riemann hypothesis holds for elliptic curves.

4.4 Elliptic Curves over Local Fields

Let \( K \) be a local field (e.g. \( K = \mathbb{Q}_p \)) with valuation ring \( R \), valuation ideal \( m \subset R \), residue field \( k = R/m \) and valuation \( v \). Our goal is to understand when an elliptic curve has points over \( K \). To do this, we introduce the notion of minimal models, imitating the use of integral models for conics over \( \mathbb{Q} \) in Section 2.9.

Definition. For an elliptic curve \( E \) over \( K \), a model for \( E \) over \( R \) is a polynomial \( f = y^2 - x^3 - Ax - B \), where \( A, B \in R \), such that \( E(K) = Z(f) \).

Given a Weierstrass equation for \( E \) over \( K \), we may always change coordinates by \( A = u^4A' \) and \( B = u^6B' \) so that the Weierstrass equation becomes a model for \( E \) over \( R \). Such a change in coordinates changes the discriminant of the Weierstrass equation by \( \Delta = u^{12}\Delta' \).

Definition. A minimal model for \( E \) over \( R \) is a model such that \( v(\Delta) \) is minimal among the discriminants of all models for \( E \) over \( R \).

Example 4.4.1. When \( \text{char } k \neq 2, 3 \), a model is minimal if and only if \( v(\Delta) < 12 \), or equivalently, \( v(c_4) < 4 \) where \( c_4 \) is the coefficient in the long Weierstrass equation. There is a more sophisticated algorithm to determine minimal models, due to Tate, in the case \( \text{char } k = 2, 3 \).

Suppose \( f = y^2 - x^3 - Ax - B \) is a minimal model for \( E \) over \( R \). Denote the reduction of \( E \) over \( k = R/m \) by
\[
\widetilde{E} = Z(y^2 - x^3 - Ax - B) \subseteq \mathbb{A}_k^2.
\]
Then \( \widetilde{E} \) is a curve over \( k \).

Lemma 4.4.2. A minimal (long) Weierstrass equation is unique up to a change of coordinates of the form
\[
x = u^2x' + r \quad y = u^3y' + u^2sx' + t
\]
for \( u \in R^\times \) and \( r, s, t \in R \).
Corollary 4.4.3. The reduction $\tilde{E}$ is unique up to a change of Weierstrass equation over $k$.

In particular, the isomorphism class of $\tilde{E}$ over $k$ is well-defined. By clearing denominators, $\mathbb{P}^2_k(R) = \mathbb{P}^2_K(K)$, so one can write the reduction of a point $P = [\alpha_0, \alpha_1, \alpha_2] \in \mathbb{P}^2_K$ as $\tilde{P} = [\bar{\alpha}_0, \bar{\alpha}_1, \bar{\alpha}_2] \in \mathbb{P}^2_k$, where $\bar{\alpha}_i = \alpha_i + m \in k = R/m$.

Definition. Let $E$ be an elliptic curve over a local field $K$, with reduction $\tilde{E}$ over $k$, and define the following sets:

$\tilde{E}^{\text{ns}} = \{P \in \tilde{E} : P \text{ is nonsingular}\}$

$E^{(0)}(K) = \{P \in E(K) : \tilde{P} \in \tilde{E}^{\text{ns}}(k)\}$

$E^{(1)}(K) = \{P \in E(K) : \tilde{P} = \tilde{O}\}$.

Then $\tilde{E}^{\text{ns}}$ is called the nonsingular locus of the reduction; $E^{(0)}(K)$ the points of nonsingular reduction; and $E^{(1)}(K)$ the kernel of reduction.

Notice that $E^{(1)}(K) \subseteq E^{(0)}(K)$.

Proposition 4.4.4. Let $E$ be an elliptic curve over a local field $K$ with reduction $\tilde{E}$. Then

(a) $\tilde{E}$ is a curve over $k$ with at most one singular point.

(b) $\tilde{E}^{\text{ns}}$ is a connected algebraic group.

(c) If $\tilde{\Delta} \neq 0$, then $\tilde{E}$ is nonsingular, and hence an elliptic curve over $k$.

(d) If $\tilde{\Delta} = 0$ and $\tilde{A} \neq 0$, then $\tilde{E}$ has a nodal singular point. Moreover, if $y = \alpha_1 x + \beta_1$ and $y = \alpha_2 x + \beta_2$ are the equations of the two tangent lines at the nodal point of $\tilde{E}$, then there is an isomorphism of algebraic groups

$$\tilde{E}^{\text{ns}} \longrightarrow \mathbb{G}_m = \mathbb{A}_k^1 \setminus \{0\}$$

$$(x, y) \longmapsto \frac{y - \alpha_1 x - \beta_1}{y - \alpha_2 x - \beta_2}.$$ 

(e) If $\tilde{\Delta} = 0$ and $\tilde{A} = 0$, then $\tilde{E}$ has a cuspidal singular point. Moreover, if $y = \alpha x + \beta$ is the tangent line at this cusp $(x_0, y_0)$, then there is an isomorphism of algebraic groups

$$\tilde{E}^{\text{ns}} \longrightarrow \mathbb{G}_a = \mathbb{A}_k^1$$

$$(x, y) \longmapsto \frac{x - x_0}{y - \alpha x - \beta}.$$ 

Definition. The reduction scenarios in (c) – (e) are given names:

- If $\tilde{\Delta} \neq 0$, $E$ is said to have good reduction. Otherwise, $E$ has bad reduction.
- If $\tilde{\Delta} = 0$ and $\tilde{A} \neq 0$, then $E$ is said to have multiplicative reduction.
- If $\tilde{\Delta} = 0$ and $\tilde{A} = 0$, then $E$ is said to have additive reduction.
Proposition 4.4.5. There is a short exact sequence of groups

\[ 0 \to E^{(1)}(K) \to E^{(0)}(K) \to \tilde{E}^{\text{ns}}(k) \to 0. \]

This gives us the beginning of a filtration of \( \tilde{E}^{\text{ns}}(k) \).

Lemma 4.4.6. Suppose \( P = [X, Y, Z] \in E(K) \). Then \( P \in E^{(0)}(K) \) if and only if for some \( N \geq 1 \), \( v(X) = 2N \), \( v(Y) = 0 \) and \( v(Z) = 3N \).

Definition. For a point \( P = [X,Y,Z] \in E(K) \), the \( N \) satisfying Lemma 4.4.6 is called the level of \( P \). We formally define the level of \( O \) to be \( \infty \). For each \( N \geq 1 \), define \( E^{(N)}(K) = \{ P \in E^{(0)}(K) : \text{the level of } P \text{ is } N \} \).

Theorem 4.4.7. Let \( E \) be an elliptic curve over \( K \). Then

1. For each \( N \geq 1 \), \( E^{(N)}(K) \) is a subgroup of \( E(K) \).
2. \( E^{(0)}(K)/E^{(1)}(K) \cong \tilde{E}^{\text{ns}}(k) \).
3. For each \( N \geq 1 \), \( E^{(N)}(K)/E^{(N+1)}(K) \cong \mathbb{G}_a(k) \).

Proof. (1) easy.

(2) in Silverman.

(3) Assume \( K = \mathbb{Q}_p \) and put \( X_N = p^{2N}X, Y_N = Y \) and \( Z_N = p^{3N}Z \) for \( N \geq 1 \). Then if \( E \) is given by the homogeneous form

\[ E : Y^2Z = X^3 + AXZ^2 + BZ^3 \]

over \( K \), then the curve \( E_N \) defined by

\[ E_N : Y_N^2Z_N = X_N^3 + p^{4N}AX_NZ_N^2 + p^{6N}BZ_N^3 \]

is also a curve over \( K \). Moreover, the reduction \( \tilde{E}_N \) is given by \( Y_N^2Z_N = X_N^3 \) which is a cuspidal curve, so \( \tilde{E}_N \) has additive reduction. Also observe that \( E^{(N)}(K) = E^{(0)}_N(K) \) and \( E^{(N+1)}(K) = E^{(1)}_N(K) \) for any \( N \geq 1 \). Applying the short exact sequence from Proposition 4.4.5 to these groups gives isomorphisms

\[ E^{(N)}(K)/E^{(N+1)}(K) = E^{(0)}_N(K)/E^{(1)}_N(K) \cong \tilde{E}^{\text{ns}}(k) \cong \mathbb{G}_a(k) \]

by Proposition 4.4.4(e). Hence each intermediate quotient is \( \mathbb{G}_a(k) \) as claimed.

This gives us important information about torsion points over local fields. We will leverage this to embed certain torsion parts of \( E(K) \) into the reduction \( \tilde{E}(k) \).

Corollary 4.4.8. Suppose the residue field \( k \) has characteristic \( p > 0 \). If \( P \in E^{(1)}(K) \) is a torsion point then its order is \( p^r \) for some \( r \geq 1 \).
4.4 Elliptic Curves over Local Fields

Theorem 4.4.10. Assume $E$ has a minimal model in short Weierstrass form. Then $E^{(1)}(K)$ is torsion-free.

Proof. Without loss of generality we may assume $|u(P_1)| \geq |u(P_2)|$. Let $N$ be the level of $P_1$, and set $X_N = p^{2N}X, Y_N = Y$ and $Z_N = p^{3N}Z$, defining the curve $E_N$ as in the proof of Theorem 4.4.7. Then $E_N$ has additive reduction with singular point $(0,0)$. Further, since $P_1, P_2 \in E^{(1)}(K) \subseteq E^{(0)}(K)$, neither of these reduces to the singular point. Now the line between $\tilde{P}_1$ and $\tilde{P}_2$ does not pass through $(0,0)$, so before reduction, the line between $P_1$ and $P_2$ has the form

$$Z_N = \ell X_N + mY_N \quad \text{for} \ l, m \in \mathbb{Z}, |\ell| \leq 1, |m| \leq 1.$$
The third point of intersection between this line and $E_N$ is calculated by:

\[
0 = -Y_N(\ell X_N + mY_N) + X_N^3 + p^{4N}AX_N(\ell X_N + mY_N)^2 + p^{6N}B(\ell X_N + mY_N)^3 \\
= c_3X_N^3 + c_2X_N^2Y_N + c_1X_NY_N^2 + c_0Y_N^3.
\]

(*)

Rearranging, we get the following relations:

\[
c_3 = 1 + p^{4N}A\ell^3 + p^{6N}B\ell^3 \quad (1)
\]

\[
c_2 = 2p^{4N}A\ell m + 3p^{6N}Bm\ell^2. \quad (2)
\]

Then (1) implies $|c_3| = 1$, while (2) implies $|c_2| \leq p^{-4N}$. On the other hand, dehomogenizing (*), we find that the roots of the equation are $p^{-N}u(P_1), p^{-N}u(P_2)$ and $p^{-N}u(P_1 + P_2)$. The sum of the roots must be $\frac{-c_2}{c_3}$, so combining all of this information gives us

\[
|u(P_1 + P_2) - u(P_1) - u(P_2)| \leq \max\{|u(P_1)|^5, |u(P_2)|^5\}.
\]

\[\square\]

**Lemma 4.4.12.** For all $P \in E^{(1)}(\mathbb{Q}_p)$ and $m \in \mathbb{Z}$, $|u([m]P)| = |m| |u(P)|$.

**Proof.** This is trivial when $m = 0$. For $m > 0$, Lemma 4.4.11 implies $|u(mP) - mu(P)| \leq |u(P)|^5$. When $p \nmid m$, $|u(mP)| = p^{-N}$ and $|mu(P)| = p^{-L}$ for some $N \geq L > 1$. If $L \neq N$, then $|u(mP) - mu(P)| = p^{-L} > |u(P)|^5$ by the ultrametric inequality, but this contradicts Lemma 4.4.11. Thus $L = N$, so $|u(mP)| = |m| |u(P)|$. A similar proof works for the case $p = m$. Finally, if $p \mid m$, the equality is verified by induction on the power of $p$ dividing $m$. \[\square\]

We now give the proof of Theorem 4.4.10.

**Proof.** If $P \in E^{(1)}(\mathbb{Q}_p)$ is a nontrivial torsion point, then $[m]P = O$ for some $m \in \mathbb{Z}$. However, by Lemma 4.4.12, $0 = |u(O)| = |u([m]P)| = |m| |u(P)| \neq 0$, a contradiction. Hence $E^{(1)}(\mathbb{Q}_p)$ has no nontrivial torsion. \[\square\]

**Remark.** If $E$ is not in short Weierstrass form, e.g. if $p = 2$, the theorem may be false. However, in that case the same proof shows that $E^{(2)}(\mathbb{Q}_p)$ is torsion-free.

**Corollary 4.4.13.** If $E$ is an elliptic curve with good reduction over $K$, then there is an embedding $E_{\text{tors}}(K) \hookrightarrow \tilde{E}(k)$.

**Proof.** By Proposition 4.4.5, there is a short exact sequence

\[
0 \rightarrow E^{(1)}(K) \rightarrow E^{(0)}(K) \rightarrow \tilde{E}^{\text{ns}}(k) \rightarrow 0.
\]

Then $E^{(1)}(K)$ is torsion-free by Theorem 4.4.10, and by hypothesis $\tilde{E}^{\text{ns}}(k) = \tilde{E}(k)$ and therefore $E^{(0)}(K) = E(K)$. Hence $E_{\text{tors}}(K) \hookrightarrow \tilde{E}(k)$ is an embedding. \[\square\]

**Corollary 4.4.14.** If $E$ is an elliptic curve with good reduction over $K$, then $E_{\text{tors}}(K)$ is a finite group.
Suppose $E$ is an elliptic curve over $\mathbb{Q}$ with good reduction mod $p$. Then there are embeddings $E_{\text{tors}}(\mathbb{Q}) \hookrightarrow E_{\text{tors}}(\mathbb{Q}_p) \hookrightarrow \tilde{E}(\mathbb{F}_p).$ This proves:

**Corollary 4.4.15.** For any elliptic curve $E/\mathbb{Q}$, $E_{\text{tors}}(\mathbb{Q})$ is finite.

**Example 4.4.16.** Consider the elliptic curve

$$E : y^2 + y = x^3 - x + 1.$$ 

Then $\Delta_E = -611 = -13 \cdot 47$ so $E$ has good reduction mod 2. One can see that $\tilde{E}(\mathbb{F}_2) = \{O\}$, so it follows that $E(\mathbb{Q})$ is torsion-free.

**Example 4.4.17.** Consider the elliptic curve

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

Here $\Delta_E = -3888 = -2^4 \cdot 3^5$, so $E$ has good reduction mod $p$ for all primes $p \geq 5$. Using the methods described, one can check that $\#\tilde{E}(\mathbb{F}_5) = 6$, while $\#\tilde{E}(\mathbb{F}_7) = 13$, so it follows that $E(\mathbb{Q})$ has no torsion. Notice that $(1, 2) \in E(\mathbb{Q})$ is a rational point. Then $(1, 2)$ has infinite order, a completely nontrivial fact.

**Example 4.4.18.** Let $E$ be the elliptic curve given by

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

Then its discriminant is $\Delta_E = -64$. One checks that $(0, 0)$ is a point of order 2 in $E(\mathbb{Q})$, and that $\#\tilde{E}(\mathbb{F}_3) = 4$, $\#\tilde{E}(\mathbb{F}_5) = 4$ and $\#\tilde{E}(\mathbb{F}_7) = 8$. So the trick in the previous two examples will not work here. However, one can further show that

$$\tilde{E}(\mathbb{F}_3) = \{O, (0, 0), (2, 1), (2, 2)\} \cong \mathbb{Z}/4\mathbb{Z},$$

while

$$\tilde{E}(\mathbb{F}_5) = \{O, (0, 0), (2, 0), (3, 0)\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$ 

So $E_{\text{tors}}(\mathbb{Q})$ can only consist of $\{O, (0, 0)\}$.

**Theorem 4.4.19.** Let $(K, R)$ be an arbitrary local field whose residue field $k$ has characteristic $p > 0$. Consider an elliptic curve $E$ over $K$ and a point $P = (x, y) \in E(K)$. Then

1. If $P \in E(K)[m]$ for $p \nmid m$, then $x, y \in R$.

2. If $P \in E(K)[p^n]$ for $n \geq 1$, then $\pi^{2r} x, \pi^{3r} y \in R$ where $r = \left\lfloor \frac{v(p)}{p^{n-1}(p-1)} \right\rfloor$.

**Theorem 4.4.20** (Lutz-Nagell). Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve with integral coefficients and take $P = (x, y) \in E_{\text{tors}}(\mathbb{Q})$. Then $x, y \in \mathbb{Z}$, and either $y = 0$, in which case $2P = O$, or $y^2 \mid 4A^3 + 27B^2$.
Proof. For any prime $p$ at which $E$ has good reduction, there is an embedding $E_{\text{tors}}(\mathbb{Q}) \hookrightarrow E_{\text{tors}}(\mathbb{Q}_p)$, but we know by Theorem 4.4.10 that $x, y \in \mathbb{Z}_p$. Since $\mathbb{Z}_p \cap \mathbb{Q} = \mathbb{Z}$, it follows that $x, y \in \mathbb{Z}$.

Next, it is clear that $[2]P = O$ if and only if $y = 0$, so suppose $[2]P = (x_2, y_2)$. Since $P$ is torsion, $[2]P$ is also torsion, so $x_2, y_2 \in \mathbb{Z}$ by the first paragraph. From the addition formula (Proposition 3.3.2), we see that

$$x_2 = \left(\frac{3x^2 + A}{2y}\right)^2 + 2x,$$

but since $x_2, 2x \in \mathbb{Z}$, we must have $y^2 \mid (3x^2 + A)^2$. On the other hand,

$$(3x^2 + 4A)(3x^2 + A)^2 \equiv 4A^3 + 27B^2 \pmod{x^3 + Ax + B}$$

and $y^2 = x^3 + Ax + B$, so we see that $4A^3 + 27B^2 \equiv 0 \pmod{y^2}$. This proves the result. 

**Theorem 4.4.21.** A point $P \in E(\mathbb{Q})$ is non-torsion if and only if there exists some $n \in \mathbb{Z}$ such that $[n]P$ has non-integral coordinates.

This statement is proven by Siegel’s result that an elliptic curve over $\mathbb{Q}$ has at most finitely many integral points.

### 4.5 Jacobians of Hyperelliptic Curves

Take a curve $C$ of genus 1, perhaps with no $k$-rational points. That is, $C$ is a hyperelliptic curve. Then $E = J(C)$ is an elliptic curve and there is an isomorphism $C \to E$ defined over $\bar{k}$; that is, $E$ is a twist of $C$ (see Section 5.3). Taking a divisor $D \in \text{Div}(C)$ of degree $\deg(D) = n$, we get a map

$$\alpha_D : C \to E = J(C)$$

$$P \mapsto [n]P - D.$$

This endows $C$ with the structure of an $[n]$-cover of $E$ (again, see Section 5.3). For example, a divisor $D \in \text{Div}(C)$ of degree $n = 2$ determines a map $\varphi_D : C \to \mathbb{P}^1$ whose image is a variety given by the equation $Y^2Z^2 = U(X, Z)$, where $U$ is a quartic in $X, Z$. There is an $SL_2(k)$ action on the set of all quartic forms:

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \cdot U(X, Z) = U(\alpha X + \beta Z, \gamma X + \delta Z).$$

In particular, $SL_2(k)$ acts on $k[a_1, \ldots, a_5]$, and it turns out that the invariant subring is of the form $k[a_1, \ldots, a_5]^{SL_2(k)} \cong k[I, J]$ for two invariant generators $I, J$. If $V$ is the space of all quartic forms, these define maps $I, J : V \to k$ which are equivariant:

$$I(U^g) = I(U)^g \quad \text{and} \quad J(U^g) = J(U)^g \quad \text{for all} \quad g \in SL_2(k).$$

This shows that $V$ is a 5-dimensional representation of $SL_2(k)$. 

75
There are particular forms \( g(X, Z) \) and \( h(X, Z) \) such that the \( SL_2(k) \)-covariance of \( V \) is given by

\[
\text{Cov}(V) \cong k[U, I, J, g, h] / (h^2 - (4g^3 - Ig^2 - JU^3)).
\]

Further, one can show that the embedding \( C \hookrightarrow E = J(C) \) is given by

\[
[X, Y, Z] \mapsto \left( \frac{g(X, Z)}{Y^2 Z^2}, \frac{h(X, Z)}{Y^3 Z^3} \right).
\]

Under this embedding, \( E \) is an elliptic curve given by the Weierstrass form

\[
E : y^2 = 4x^3 - Ix - J,
\]

with \( j \)-invariant \( j(E) = \frac{J^2}{I^3} \).
5 The Mordell-Weil Theorem

Now that we understand $E_{\text{tors}}(\mathbb{Q})$, our goal is to prove Mordell’s theorem that $E(\mathbb{Q})$ is finitely generated. Our strategy is as follows, and will take the entirety of Chapter 5 to describe.

1. (Weak Mordell-Weil Theorem) Show that $E(\mathbb{Q})/mE(\mathbb{Q})$ is finitely generated for $m > 1$. This is achieved by constructing a certain short exact sequence

$$0 \to E(\mathbb{Q})/mE(\mathbb{Q}) \to \text{Sel}^{(m)}(E/\mathbb{Q}) \to \text{III}(E/\mathbb{Q})[m] \to 0,$$

where $\text{Sel}^{(m)}(E/\mathbb{Q})$ is a finite group called the Selmer group and $\text{III}(E/\mathbb{Q})$ is the Tate-Shafarevich group.

2. Use height functions to construct a function $\hat{h} : E(\mathbb{Q}) \to \mathbb{R}_{\geq 0}$ which satisfies

   (i) For all $B > 0$, the set $\{P \in E(\mathbb{Q}) : \hat{h}(P) < B\}$ is finite.
   (ii) $\hat{h}([m]P) = m^2 \hat{h}(P)$ for all $m \in \mathbb{Z}$.
   (iii) $\hat{h}$ is a quadratic form, and thus there is a pairing

$$\langle P, Q \rangle = \frac{1}{2}(\hat{h}(P + Q) - \hat{h}(P) - \hat{h}(Q))$$

which is symmetric and bilinear.

3. Combining the weak Mordell-Weil theorem and height functions gives a proof that $E(\mathbb{Q})$ is finitely generated.

5.1 Some Galois Cohomology

To introduce the Selmer and Tate-Shafarevich groups, we first need to review some basic results in Galois cohomology. Let $G$ be a profinite group, i.e. an inverse limit $G = \lim \leftarrow G_i$ of some inverse system $\{G_i\}$ of finite groups. For example, the $p$-adic integers are profinite group: $\mathbb{Z}_p = \lim \leftarrow \mathbb{Z}/p^n\mathbb{Z}$ (see Section 0.3). The primary example we will be interested in is the absolute Galois group of a field $k$, defined as

$$G_k = \text{Gal}(\bar{k}/k) : = \lim \leftarrow \text{Gal}(L/k)$$

where the inverse limit is over all finite extensions $L/k$. Let $A$ be an abelian group with the discrete topology and suppose $G$ acts on $A$ continuously. Specifically, for each $\sigma \in G$ there is a map $A \to A, a \mapsto a^\sigma$, which satisfies

- (i) $a^1 = a$ for all $a \in A$.
- (ii) $(a + b)^\sigma = a^\sigma + b^\sigma$ for all $a, b \in A$.
- (iii) If $\sigma, \tau \in G$ then $(a^\sigma)^\tau = a^{\sigma \tau}$.

77
(iv) For each $a \in A$, $\text{Stab}_G(a) = \{ \sigma \in G : a^\sigma = a \}$ is a subgroup of finite index in $G$.

Notice that (i) – (iii) are the axioms for a right group action of $G$ on $A$, while (iv) says that the action is continuous.

**Definition.** For a continuous action of $G$ on $A$, the set of $G$-invariants of $A$ is

$$A^G := \{ a \in A : a^\sigma = a \text{ for all } \sigma \in G \}.$$  

**Example 5.1.1.** The key situation for our purposes is when $G = G_k$ is the absolute Galois group of a field $k$ and $A = \mathcal{E}(\bar{k})$ is the points of an elliptic curve over the algebraic closure, with the continuous action described in Section 1.1 (for any variety). In particular, for any $P \in \mathcal{E}(\bar{k})$, $\text{Stab}_G(P) = \text{Gal}(\bar{k}/k(P))$ is a finite index subgroup, where $k(P)$ is the field of definition of $P$. In this situation, the fixed points of the Galois action are just the $k$-rational points of $E$: $\mathcal{E}(\bar{k})^G = \mathcal{E}(k)$.

In general, the assignment $A \mapsto A^G$ is a functor from the category of $G$-modules to the category of abelian groups, called the invariant functor.

**Lemma 5.1.2.** $A \mapsto A^G$ is a left exact functor, meaning for every short exact sequence of $G$-modules $0 \to A \to B \to C \to 0$, there is an exact sequence $0 \to A^G \to B^G \to C^G$.

**Example 5.1.3.** Consider the short exact sequence $0 \to E[m] \to E \overset{[m]}{\to} E \to 0$. Then applying the invariant functor $(-)^G$, where $G = G_k$, fails to preserve exactness on the right.

**Definition.** The $i$th group cohomology of $G$ with coefficients in a $G$-module $A$ is the $i$th right derived functor of the invariant functor:

$$H^i(G, A) := R^i(-)^G(A).$$

**Theorem 5.1.4.** Let $G$ be a profinite group. Then

1. $H^0(G, A) = A^G$ for any $G$-module $A$.

2. For any short exact sequence of $G$-modules $0 \to A' \to A \to A'' \to 0$, there is a long exact sequence in cohomology

$$0 \to H^0(G, A') \to H^0(G, A) \to H^0(G, A'') \to H^1(G, A') \to H^1(G, A) \to H^1(G, A'') \to \cdots$$

which is functorial in each of $A', A, A''$.

**Definition.** When $G = G_k = \text{Gal}(\bar{k}/k)$, the group cohomology functors are called Galois cohomology, written

$$H^i(k, A) := H^i(\text{Gal}(\bar{k}/k), A).$$

**Example 5.1.5.** If a profinite group $G$ acts trivially on $A$, then $H^0(G, A) = A$ and $H^1(G, A) = \text{Hom}_{cts}(G, A)$, the group of continuous homomorphisms $G \to A$. 

78
Group cohomology can also be constructed as the homology of a certain cochain complex:

\[ H^i(G, A) = Z^i(G, A)/B^i(G, A), \]

where \( Z^i(G, A) \) are the \( i \)-cocycles, or maps \( G \times \cdots \times G \to A \) satisfying a certain combinatorial condition (e.g. for \( \xi : G \to A \), the cocycle condition is that \( \xi_{\sigma \tau} = (\xi_\sigma)^\tau + \xi_\tau \) for any \( \sigma, \tau \in G \)), and \( B^i(G, A) \) are the \( i \)-coboundaries, i.e. the cocycles of the form \( \xi : \sigma \mapsto a^\sigma - a \) for some \( a \in A \).

For a closed subgroup \( H \leq G \), any \( G \)-module \( A \) is also an \( H \)-module by restricting the \( G \)-action to \( H \). This determines a map called restriction:

\[ \text{Res} : H^i(G, A) \to H^i(H, A). \]

On 0th cohomology, this is just given by \( A^G \to A^H \). On the other hand, for a normal, finite-index subgroup \( H \leq G \), the quotient \( G/H \) is a finite group and \( A^H \) has the structure of a \( G/H \)-module. This allows one to define an induced map called inflation:

\[ \text{Inf} : H^i(G/H, A^H) \to H^i(G, A). \]

**Theorem 5.1.6 (Inflation-Restriction Sequence).** For a profinite group \( G \), a normal finite-index subgroup \( H \) and a \( G \)-module \( A \), there is an exact sequence

\[ 0 \to H^1(G/H, A^H) \xrightarrow{\text{Inf}} H^1(G, A) \xrightarrow{\text{Res}} H^1(H, A). \]

**Example 5.1.7.** If \( K \) is a number field, \( v \) is a place on \( K \) and \( K_v \) is the completion of \( K \) at \( v \), then the Galois group \( G_v := \text{Gal}(K_v/K) \) is a subgroup of \( G = \text{Gal}(\overline{K}/K) \). In this case, there is a local restriction sequence at \( v \):

\[ \text{Res}_v : H^1(K, A) \xrightarrow{\text{Res}} H^1(K_v, A) \to H^1(K_v, A(K_v)). \]

(for any Galois module \( A \)).

**Proposition 5.1.8.** For any field \( K \), \( H^1(K, \mathbb{G}_a) = 0 \) and \( H^1(K, \mathbb{G}_m) = 1 \). Further, if \( \text{char } K = 0 \) or \( \text{char } K \nmid m \), then there is an isomorphism \( H^1(K, \mu_m) \cong K^\times/(K^\times)^m \), where \( \mu_m \) is the group of \( m \)th roots of unity lying in \( K \).

**Proof.** The first statement is Hilbert’s Theorem 90. For the second statement, consider the short exact sequence

\[ 1 \to \mu_m \to \mathbb{G}_m \xrightarrow{[m]} \mathbb{G}_m \to 0. \]

Applying Galois cohomology gives a sequence

\[ 1 \to \mu_m(K) \to K^\times \xrightarrow{m} K^\times \to H^1(K, \mu_m) \to H^1(K, \mathbb{G}_m) = 0. \]

Taking the quotient gives the result.
5.2 Selmer and Tate-Shafarevich Groups

In this section we introduce the Selmer and Tate-Shafarevich groups of an isogeny between elliptic curves. Let $\phi: A \to B$ be such an isogeny over a field $K$. Set $A[\phi] = \ker \phi$, we have a short exact sequence in the category of elliptic curves:

$$0 \to A[\phi] \to A \xrightarrow{\phi} B \to 0.$$ 

Applying Galois cohomology gives a long exact sequence

$$0 \to A[\phi](K) \to A(K) \xrightarrow{\phi^*} B(K) \xrightarrow{\delta} H^1(K, A[\phi]) \to H^1(K, A) \xrightarrow{\phi} H^1(K, B) \to \cdots$$

We isolate part of this sequence as a short exact sequence:

$$0 \to B(K)/\phi A(K) \xrightarrow{\delta} H^1(K, A[\phi]) \to H^1(K, A)[\phi] \to 0.$$ 

We will construct the Selmer group as a subgroup of $H^1(K, A[\phi])$, avoiding the obstacles of working with the infinite group $H^1(K, A[\phi])$. Notice that when $A = B = E$ and $\phi = [m]$, the first term in this sequence is $E(K)/mE(K)$, sometimes called the weak Mordell-Weil group.

**Example 5.2.1.** In the case $A = B = E$, suppose $\phi = [m]$ where $E[m] \subseteq E(K)$. Then by Proposition 4.2.7 and Proposition 5.1.8,

$$H^1(K, E[m]) = \text{Hom}_{cts}(G_K, E[m]) = \text{Hom}_{cts}(G_K, \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}) \cong K^x/(K^x)^m \times K^x/(K^x)^m.$$ 

**Lemma 5.2.2.** Let $K$ be a number field and $v$ a place of $K$. Then for any isogeny of elliptic curves $\phi: A \to B$ over $K$, there is a commutative diagram

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & B(K)/\phi A(K) & \longrightarrow & H^1(K, A[\phi]) & \longrightarrow & H^1(K, A)[\phi] & \longrightarrow & 0 \\
& & \downarrow \text{Res}_v & & \downarrow \text{Res}_v & & \downarrow \text{Res}_v & & \\
0 & \longrightarrow & B(K_v)/\phi A(K_v) & \longrightarrow & H^1(K_v, A[\phi]) & \longrightarrow & H^1(K_v, A)[\phi] & \longrightarrow & 0
\end{array}
$$

Since we have such a diagram for every place of $K$, we can take the product over all places of $K$ to obtain a commutative diagram

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & \prod_v B(K)/\phi A(K_v) & \longrightarrow & \prod_v H^1(K, A[\phi]) & \longrightarrow & \prod_v H^1(K, A)[\phi] & \longrightarrow & 0 \\
& & \downarrow \alpha & & \downarrow \alpha & & \downarrow \alpha & & \\
0 & \longrightarrow & \prod_v B(K_v)/\phi A(K_v) & \longrightarrow & \prod_v H^1(K_v, A[\phi]) & \longrightarrow & \prod_v H^1(K_v, A)[\phi] & \longrightarrow & 0
\end{array}
$$
Here the vertical arrow in the middle is given by a product of local restrictions: \( \xi \mapsto (\xi_v)_v \). Let \( \xi \in \delta(B(K)) \). Then \( \xi_v \) must lie in \( \delta(B(K_v)) \) for each place \( v \). This puts a condition on the cocycles in the image of \( \delta \); define

\[
L_v := \{ \xi \in H^1(K, A[\varphi]) : \xi_v \in \delta(B(K_v)) \}
\]

and set \( H^1_L(K, A[\varphi]) = \bigcap_v L_v \). Then we see that \( \delta(B(K_v)) \subseteq H^1_L(K, A[\alpha]) \).

**Definition.** The **Selmer group** of \( \varphi : A \to B \) is the group

\[
\text{Sel}^{(\varphi)}(A/K) := H^1_L(K, A[\varphi]) = \ker \alpha,
\]

where \( \alpha : H^1(K, A[\alpha]) \to \prod_v H^1(K_v, A)[\varphi] \) is the product of the local restriction maps.

The key observation is that \( \text{im} \delta \subseteq \text{Sel}^{(\varphi)}(A/K) \), so in order to prove the weak Mordell-Weil theorem, it will be enough to show that the Selmer group is finite. The cokernel of the map \( \delta : B(K)/\varphi A(K) \to \text{Sel}^{(\varphi)}(A/K) \) has an important role as well.

**Definition.** The **Tate-Shafarevich group** of \( \varphi : A \to B \) is the group

\[
\text{III}(A/K) := \ker \left( \text{Res} : H^1(K, A) \to \prod_v H^1(K_v, A) \right).
\]

**Proposition 5.2.3.** For any isogeny \( \varphi : A \to B \), there is a short exact sequence

\[
0 \to B(K)/\varphi A(K) \to \text{Sel}^{(\varphi)}(A/K) \to \text{III}(A/K)[\varphi] \to 0.
\]

**Proof.** Consider the diagram

\[
\begin{array}{ccccccc}
B(K)/\varphi A(K) & \to & \text{Sel}^{(\varphi)}(A/K) & \to & \text{III}(A/K)[\varphi] & \to & 0 \\
\downarrow & & \downarrow & & \downarrow & & \\
0 & \to & B(K)/\varphi A(K) & \to & H^1(K, A[\varphi]) & \to & H^1(K, A)[\varphi] & \to & 0 \\
\downarrow & & \downarrow & & \downarrow \alpha & & \\
0 & \to & 0 & \to & \prod_v H^1(K_v, A)[\varphi] & \cong & \prod_v H^1(K_v, A) & \to & 0
\end{array}
\]

Applying the Snake Lemma gives the desired short exact sequence. \( \Box \)

Fix a place \( v \) of \( K \) and let \( K_v^{ur} \) be the maximal unramified extension of the completion \( K_v \), so that \( \text{Gal}(K_v/K_v^{ur}) = I_v \), the inertia group of \( K_v \). Set \( G_v = \text{Gal}(K_v/K_v) \). For any \( G_v \)-module \( A \), we have a map

\[
H^1(K_v, A) \xrightarrow{\text{Res}_v} H^1(K_v^{ur}, A) \cong H^1(I_v, A).
\]

Denote by \( H^1_{ur}(K_v, A) \) the kernel of this map. Elements of \( H^1_{ur}(K_v, A) \) are called **unramified cocycles**; for an element \( \xi \in H^1(K, A) \), we say \( \xi \) is unramified at \( v \) if \( \xi_v \in H^1_{ur}(K_v, A) \).
5.2 Selmer and Tate-Shafarevich Groups

Definition. For a finite set of places $S$ on $K$, we define

$$H^1_S(K, A) = \{ \xi \in H^1(K, A) \mid \xi \text{ is unramified at all places } v \notin S \}.$$ 

Proposition 5.2.4. Let $K$ be a number field, $A$ an elliptic curve over $K$ and $\varphi : A \to B$ an isogeny defined over $K$. Let $S$ the finite set consisting of all archimedean places of $K$, places at which $A$ has bad reduction and places dividing $m = \deg \varphi$. Then $\text{Sel}^{(\varphi)}(A/K)$ is a subset of $H^1_S(K, A[\varphi])$.

Proof. Let $\xi \in \text{Sel}^{(\varphi)}(A/K)$ and fix a place $v \notin S$. By definition of the Selmer group, $\xi_v = 1$ in $H^1(K_v, A)[\varphi]$, so by the exact sequence in Lemma 5.2.2, $\xi_v = \delta(P)$ for some point $P \in B(K_v)$. Explicitly, $\delta(P) = \xi$, where $\xi : \sigma \mapsto Q^\sigma - Q$ for some $Q \in A(K_v)$ with $\varphi(Q) = P$. Since $v \notin S$, $A$ has good reduction at $v$, so in the residue field $k_v = \mathcal{O}_v/m_v$, the reduction of $\xi_v = Q^\sigma - Q$ for any $\sigma \in I_v$ is give by

$$\xi_v = Q^\sigma - Q = \bar{Q}^\sigma - \bar{Q} = (\bar{Q})^\sigma - \bar{Q} = \bar{Q} - \bar{Q} = 0$$

since $\sigma \in I_v$ acts trivially on $k_v$. This shows that $\xi_v \in A^{(1)}(K_v)[\varphi] \subseteq A^{(1)}(K_v)[m]$, where $\deg \varphi = m$. Further, since $A$ has good reduction at $v$ and $v \nmid m$, then by Theorem 4.4.9, $A(K_v)[m] \hookrightarrow \tilde{A}(k_v)$ is an injection. Hence $\xi_v = 0$ in $\tilde{A}(k_v)$ implies $\xi_v = 0$ in $A(K_v)$. Thus we have shown $\xi_v$ is trivial for all $\sigma \in I_v$, i.e. $\xi$ is unramified at every $v \notin S$. Hence $\text{Sel}^{(\varphi)}(A/K) \subseteq H^1_S(K, A[\varphi])$. $\square$

Proposition 5.2.5. Let $S$ be a finite set of places of $K$ and let $M$ be any finite abelian $G_K$-module. Then $H^1_S(K, M)$ is finite.

Proof. Since $M$ is finite and $G_K$ acts continuously on $m$, there exists an open subgroup of finite index in $G_K$ that fixes every element of $M$. Such a subgroup corresponds, by infinite Galois theory, to an extension $K'/K$. For this extension, we have an inflation-restriction sequence (Theorem 5.1.6):

$$0 \to H^1_S(K', M^{G_{K'}}) \to H^1_S(K, M) \to H^1_S(K', M).$$

Since $M$ is finite, $H^1_S(K', M^{G_{K'}})$ is finite, so it’s enough to show $H^1_S(K', M)$ is finite to imply that $H^1_S(K, M)$ is finite.

By definition, $K'$ is the extension of $K$ for which $G_{K'}$ acts trivially on $M$, so after replacing $K$ with $K'$, we may assume $M$ is in fact a trivial $G_K$-module. Also assume $\mu_n \subseteq K$ for some $n$. Since $G_K$ acts trivially on $M$, we have that $H^1_S(K, M) = \text{Hom}^S_{\text{cts}}(G_K, M)$. However, such homomorphisms are in correspondence with abelian extensions of $K$ of exponent $m$ which are unramified outside $S$. By Lemma 5.2.6 below, there are finitely many of these, so $H^1_S(K, M)$ is finite. $\square$

Lemma 5.2.6. Let $K$ be a number field and $M$ a finite abelian $G_K$-module. If $m$ is the exponent of $M$ (i.e. the smallest integer such that $mx = 0$ for all $x \in M$), and $L/K$ is the maximal abelian extension of exponent $m$ which is unramified outside $S$, then $[L : K]$ is finite.
Proof. Assume $\mu_n \subseteq K$. By Kummer theory, the short exact sequence $1 \to \mu_n \to K^\times \xrightarrow{n} K^\times \to 0$ induces a long exact sequence

$$0 \to \mu_n \to K^\times \xrightarrow{n} K^\times \to H^1(K, \mu_n) \to H^1(K, K^\times) = 0$$

(the last term is 0 by Hilbert’s Theorem 90). Thus there is an isomorphism

$$\delta : K^\times/(K^\times)^n \to H^1(K, \mu_n)$$

$$\alpha \mapsto \left( \xi : \sigma \mapsto \frac{\sigma(\beta)}{\beta} \right)$$

where $\beta^n = \alpha$.

In particular, this exhibits a Galois correspondence

$$\begin{cases}
\text{cyclic subgroups of} & \text{cyclic extensions of } L/K \\
K^\times/(K^\times)^n & \text{with } \text{Gal}(L/K) = \mathbb{Z}/n\mathbb{Z}
\end{cases}$$

$$\langle \alpha \rangle \mapsto K(\sqrt[n]{\alpha})/K.$$

Let $\mathcal{O}_S$ be the ring of $S$-integers in $K$, i.e.

$$\mathcal{O}_S = \{ x \in K : |x|_v \leq 1 \text{ for all } v \notin S \}.$$

By algebraic number theory, there are finitely many degree $d$ extensions $L/K$ unramified outside $S$ for any given $d > 0$. Further, by Dirichlet’s $S$-unit theorem, $\mathcal{O}_S^x$ is a finitely generated abelian group of rank $r(S) = r + s - 1 + \# \mathfrak{a}$, where $r$ and $s$ are, respectively, the numbers of real and complex embeddings of $\mathbb{Q}$ in $K$. By class field theory, the class group $C(\mathcal{O}_S)$ is finite and generated by some fractional ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$. Adding all the primes dividing the $\mathfrak{a}_j$ to $S$, we get a finite set of places $S'$ for which $C(\mathcal{O}_{S'}) = 1$. Therefore we may assume from the start that $\mathcal{O}_S$ is a PID.

With these reductions, we will now prove $L/K$ is finite. In fact, we will show

1. $L = K(\alpha^{1/m} \mid \alpha \in \mathcal{O}_S^x)$
2. $\text{Gal}(L/K) \cong (\mathbb{Z}/m\mathbb{Z})^{r(S)+1}$.

By Kummer theory, the maximal abelian extension of $K$ with exponent $m$ is $K(\alpha^{1/m} \mid \alpha \in K^\times)$. Thus $L \subseteq K(\alpha^{1/m} \mid \alpha \in K^\times)$. Let $L' = K(\alpha^{1/m} \mid \alpha \in \mathcal{O}_S^x)$. We want to show $L' = L$. First, for any $\alpha \in K^\times$ and place $v$ for which $v(m) = 0$, we claim $v$ is unramified in $K(\alpha^{1/m})$ if and only if $\text{ord}_v(\alpha) \equiv 0 \mod m$. Indeed, if $\text{ord}_v(\alpha) \equiv 0 \mod m$, then $\alpha = u\pi_v^{rm}$ for some $u \in \mathcal{O}_v^x$ and $r \in \mathbb{Z}$. Then $K_v(\alpha^{1/m}) = K_v(u^{1/m})$ so $u^{1/m}$ satisfies $x^m - u = 0$. This polynomial has discriminant $\Delta = m^m u^{m-1}$, so in particular $v(\Delta) = 0$ and thus $v$ is unramified in $K(\alpha^{1/m})$. Conversely, if $v$ is unramified in $K(\alpha^{1/m})$ then $v(K(\alpha^{1/m})^x) = v(K^x) = \mathbb{Z}$. So if $\alpha = u\pi_v^{r}$ then $m \mid r$ and hence $\text{ord}_v(\alpha) = r \equiv 0 \mod m$. Thus the claim holds.

The paragraph above shows that $L$ is the compositum of all $K(\alpha^{1/m})$ for $\alpha \in K^\times$ with $\text{ord}_v(\alpha) \equiv 0 \mod m$ for all $v \notin S$. That is, for all $v \notin S$, $\text{ord}_v(\alpha) = r_v m$ for some $r_v \in \mathbb{Z}$. Take such an $\alpha \in K^\times$ and $v \notin S$ and let $p_v$ be the corresponding prime of $\mathcal{O}_S$. By our reductions, $\mathcal{O}_S$ is a PID, so

$$\prod_{v \notin S} p_v^{r_v} = (\beta)$$
for some $\beta \in K$. Then $\alpha' = \alpha \beta^{-m} \in \mathcal{O}_S^\times$ and $K(\alpha^{1/m}) = K((\alpha')^{1/m}) \subseteq L'$. This holds for all $\alpha \in K^\times$, so $L \subseteq L'$. On the other hand, $L' \subseteq L$ is obvious so we get $L' = L$ and (1) is proven.

For (2), apply Dirichlet’s $S$-unit theorem to get
\[ \text{Gal}(L/K) = \mathcal{O}_S^\times / (\mathcal{O}_S^\times)^m = (\mathbb{Z}/m\mathbb{Z})^{r(S) + 1} \]
where the extra copy of $\mathbb{Z}/m\mathbb{Z}$ comes from the torsion part since $\mu_m \subseteq K$. \hfill \Box

**Remark.** Consider the situation when $M = A[m]$ and $A[m] \subseteq A(K)$. As in the proof of Lemma 5.2.6, we may assume $\mu_m \subseteq K$ and that $\mathcal{O}_S$ is a PID. Then
\[ H_1^1(K, A[m]) = \text{Hom}_{cts}(\text{Gal}(L/K), A[m]) = \text{Hom}_{cts}((\mathbb{Z}/m\mathbb{Z})^{1+r(S)}, (\mathbb{Z}/m\mathbb{Z})^2) \]
so $|H_1^1(K, A[m])| = m^{2(1+r(S))}$. On the other hand, $#A(K)/[m]A(K) = m^{2(1+r(A))}$ and since there is an embedding $A(K)/[m]A(K) \hookrightarrow H_1^1(K, A[m])$, we get a bound on the rank of the elliptic curve $A$:
\[ r(A) \leq 2r(S) = 2(r + s - 1 + #S). \]

**Corollary 5.2.7.** For any isogeny of elliptic curves $\varphi : A \to B$ over a number field $K$, the Selmer group $\text{Sel}^{(\varphi)}(A/K)$ is a finite group.

**Corollary 5.2.8 (Weak Mordell-Weil Theorem).** For any elliptic curve $E$ over $\mathbb{Q}$, $E(\mathbb{Q})/mE(\mathbb{Q})$ is finite for all $m \geq 2$.

**Remark.** Let $\varphi : E \to E'$ be an isogeny over $\mathbb{Q}$. There is a bilinear, alternating pairing
\[ \text{III}(E/\mathbb{Q}) \times \text{III}(E'/\mathbb{Q}) \to \mathbb{Q}/\mathbb{Z} \]
called Cassel’s pairing, whose kernel consists of divisible elements. As a result, one obtains the following useful fact:

**Theorem 5.2.9.** For any elliptic curve $E$, the order of $\text{III}(E/\mathbb{Q})$ is divisible by 2.

### 5.3 Twists, Covers and Principal Homogeneous Spaces

Before making the leap from the weak Mordell-Weil theorem to the full Mordell-Weil theorem, we take a couple sections to describe the Selmer and Tate-Shafarevich groups explicitly. This allows one to write down explicit generators for $E(K) / \varphi E(K)$ which ultimately lead to an effective proof of Mordell-Weil.

**Definition.** Let $X$ be an algebro-geometric object over a field $k$. Then a **twist** of $X$ is an element of the set
\[ \text{Twist}(X/k) = \{ \text{objects } Y \text{ of the same category } \mid Y \cong X \text{ over } \bar{k} \}. \]

**Example 5.3.1.** By Proposition 0.2.7 (or 2.6.5), every conic in $\mathbb{P}^2$ is isomorphic over $\bar{k}$ to $\mathbb{P}^1$, but is only isomorphic over $k$ if it has a $k$-point. Therefore $\text{Twist}(\mathbb{P}^1/k)$ is the set of conics in $\mathbb{P}^2$. 

84
The next result is a sort of “meta-proposition” about twists of algebro-geometric objects. One can repeat the proof in any specific category of algebro-geometric objects to obtain a bijection between the twists and the given cohomology set.

**Proposition 5.3.2.** Let $X$ be an algebro-geometric object over a field $k$. Then there is a bijection $H^1(k, \text{Aut}_{\bar{k}}(X)) \cong \text{Twist}(X/k)$.

**Proof.** Given $Y \in \text{Twist}(X/k)$, there is an isomorphism $\varphi : Y \to X$ defined over $\bar{k}$. Then each $\sigma \in G_k$ acts on $\varphi$ in the natural way, and

$$\xi : \sigma \mapsto \varphi^{\sigma} \circ \varphi^{-1} \in \text{Aut}_{\bar{k}}(X)$$

is a 1-cocycle in $H^1(k, \text{Aut}_{\bar{k}}(X))$.

Conversely, for $\xi : \sigma \mapsto \xi_{\sigma}$ in $H^1(k, \text{Aut}_{\bar{k}}(X))$, we may view $\xi$ as a continuous map $G_k \to \text{Aut}_{\bar{k}}(X)$. Since $\text{Aut}_{\bar{k}}(X)$ has the discrete topology, $\ker \xi$ is an open normal subgroup of $G_k$, so by Galois theory, there is an extension $L/k$ with $\ker \xi = \text{Gal}(L/k)$. We define a twisted action of $\text{Gal}(L/k)$ on $X(L)$ by

$$\text{Gal}(L/k) \times X(L) \to X(L), \quad (\sigma, P) \mapsto \xi_{\sigma}(P^{\sigma}).$$

Then the coset space $Y := X(L)/\text{Gal}(L/k)$ is an object defined over $k$ of the same type as $X$ that is isomorphic to $X$ over $\bar{k}$, hence a twist of $X$ over $k$. It is easy to check that the assignments are inverses of each other. \qed

**Definition.** Let $A$ be an algebraic group over a field $k$. A principal homogeneous space (or PHS) for $A$ is a variety $X$ over $k$ equipped with a simply transitive action of $A$ as an algebraic group action over $k$. In other words, there is a morphism

$$\mu : X \times A \to X, \quad (x, P) \mapsto x \boxplus P$$

satisfying

1. $x \boxplus 0 = x$ for all $x \in X$.
2. $x \boxplus (P + Q) = (x \boxplus P) \boxplus Q$ for all $P, Q \in A$ and $x \in X$.
3. For any $x_0 \in X$, the map

$$\theta_{x_0} : A \to X, \quad P \mapsto x_0 \boxplus P$$

is an isomorphism defined over any field $L$ such that $x_0 \in X(L)$.

In particular, (3) says that $X$ is a twist of $A$. Notice that if $x_0 \in X(k)$, then $X \cong A$ over $k$, i.e. $X$ is a trivial twist of $A$, and vice versa. In this case, we will say $X$ is a trivial principal homogeneous space of $A$.

**Lemma 5.3.3.** Every twist of $A$ over $k$ is a principal homogeneous space.
Proof. Let $X$ be a twist of $A$, with isomorphism $\theta = \theta_{x_0} : A \to X$ defined over $\bar{k}$. Then for any $x \in X$ and $P \in A$,
$$\theta(\theta^{-1}(x) + P) = x_0 \boxplus (\theta^{-1}(x) + P) = (x_0 \boxplus \theta^{-1}(x)) \boxplus P = x \boxplus P.$$ 
Therefore the action $\mu : X \times A \to X$ can be written $\mu(x, P) = \theta(\theta^{-1}(x) + P)$. □

Lemma 5.3.4. Given an isomorphism $\theta = \theta_{x_0} : A \to X$ over $\bar{k}$, there is a subtraction map 
$$\nu : X \times X \longrightarrow A, \quad (x, y) \mapsto x \boxminus y = \theta^{-1}(x) - \theta^{-1}(y)$$ 
which is defined over $k$.

Definition. Two principal homogeneous spaces $(X, \mu)$ and $(X', \mu')$ of $A$ over $k$ are isomorphic over $k$ if there exists an isomorphism $i : X \to X'$ defined over $k$ such that the following diagram commutes:

$$
\begin{array}{ccc}
X \times A & \xrightarrow{\mu} & X \\
\downarrow{i \times 1} & & \downarrow{i} \\
X' \times A & \xrightarrow{\mu'} & X'
\end{array}
$$

There is a related notion of a “torsor” for $A$, which turns out to be equivalent to the definition of a PHS of $A$.

Definition. A torsor for $A$ over $k$ is a pair $(X, \theta)$ where $X$ is an algebraic variety over $k$ and $\theta : A \to X$ is an isomorphism defined over $\bar{k}$.

Definition. Two torsors $(X, \theta)$ and $(X', \theta')$ for $A$ over $k$ are isomorphic as torsors if there exists an isomorphism of varieties $i : X \to X'$ defined over $k$ and a point $P \in A$ such that the following diagram commutes:

$$
\begin{array}{ccc}
A & \xrightarrow{\theta} & X \\
\downarrow{\tau_P} & & \downarrow{i} \\
A & \xrightarrow{\theta'} & X'
\end{array}
$$

Proposition 5.3.5. The equivalence classes of principal homogeneous spaces of $A$ over $k$ are in bijection (as pointed sets) with the equivalence classes of torsors for $A$ over $k$.

Proof. Let $X$ be a PHS and pick $x_0 \in X$. Then $\theta = \theta_{x_0} : A \to X$ is an isomorphism, so $(X, \theta)$ is a torsor. For a different choice of point $y_0 \in X$, we get an isomorphic torsor $(X, \theta_{y_0})$, where the isomorphism is given by the diagram
5.3 Twists, Covers and Principal Homogeneous Spaces

The Mordell-Weil Theorem

\[
\begin{array}{c}
A \xrightarrow{\theta_{x_0}} X \\
\tau_P \\
A \xrightarrow{\theta_{y_0}} X
\end{array}
\]

(Here, \( P = x_0 \square y_0 \).) Conversely, a torsor \((X, \theta)\) determines a PHS \((X, \mu)\) of \( A \) by \( \mu(x, P) = \theta(\theta^{-1}(x) + P) \).

\[\square\]

**Definition.** The set of equivalence classes of principal homogeneous spaces of \( A \) over \( k \), or equivalently the equivalence classes of torsors for \( A \) over \( k \), is called the \textbf{Weil-Châtelet group} of \( A \), denoted \( \text{WC}(A/k) \).

**Remark.** Let \( A \) be an algebraic group over \( k \).

1. Given a twist \( X \in \text{Twist}(A/k) \), then up to isomorphism of torsors, there are \(|\text{Aut}(A)|\) different torsor structures we can put on \( X \). For an elliptic curve \( E \), the typical case is that \( \text{Aut}(E) = \mathbb{Z}/2\mathbb{Z} \), so there are two torsor structures on each twist of \( E \).

2. The automorphism group of \( A \) as a torsor for \( A \) is isomorphic to \( A \) itself. Hence by Proposition 5.3.2,

\[
\text{WC}(A/k) \rightarrow H^1(k, A) \\
(X, \mu) \rightarrow (\xi : \sigma \mapsto x_0^\sigma \square x_0)
\]

is a bijection. Viewing \( \text{WC}(A/k) \) as an equivalence class of torsors, the isomorphism is given by \((X, \theta) \mapsto (\xi : \sigma \mapsto P_\sigma)\), where \( P_\sigma \) is the point such that \((\theta^\sigma)^{-1} \circ \theta(Q) = Q + P_\sigma \) in \( A \).

Recall that when \( A \) is an elliptic curve over a number field \( K \), \( \text{III}(A/K) \subseteq H^1(K, A) \) and elements of \( \text{III}(A/K) \) are those cocycles \( \xi \in H^1(K, A) \) such that \( \xi_v \in H^1(K_v, A) \) is trivial for each place \( v \) of \( K \). Interpreting each \( H^1(K_v, A) \) as \( \text{WC}(A/K_v) \), the restriction map is given by

\[
\text{WC}(A/K) \rightarrow \prod_v \text{WC}(A/K_v) \\
X/K \mapsto \prod_v (X/K_v).
\]

**Lemma 5.3.6.** A torsor \( X \) for \( A \) is trivial in \( \text{WC}(A/K) \) if and only if \( X(K) \neq \emptyset \).

**Theorem 5.3.7.** Let \( \varphi : A \rightarrow B \) be an isogeny of elliptic curves over a number field \( K \). Then \( \text{III}(A/K) \) is the set of equivalence classes of PHSs for \( A \) over \( K \) having a point over \( K_v \) for every place \( v \) of \( K \).

On the other hand, recall that \( \text{Sel}^{(\varphi)}(A/K) \subseteq H^1(K, A[\varphi]) \). By Proposition 5.3.2, \( H^1(K, A[\varphi]) \) can be viewed as the set of twists of \( A \) with automorphism group isomorphic to \( A[\varphi] \). This naturally leads to the idea of twists of an isogeny, also known as \( \varphi \)-covers.
Definition. Let \( \varphi : A \to B \) be an isogeny. Then a \( \varphi \)-cover is a curve \( C \) and a covering map \( \pi : C \to B \) defined over \( K \) such that there exists an isomorphism \( \alpha : C \to A \) defined over \( K \) making the following diagram commute:

\[
\begin{array}{ccc}
C & \xrightarrow{\pi} & B \\
\downarrow{\alpha} & & \downarrow{id} \\
A & \xrightarrow{\varphi} & B \\
\end{array}
\]

If \( \pi : C \to B \) is a \( \varphi \)-cover, then \( C \) is a torsor for \( A \) over \( K \), so \( C \in WC(A/K) \). Note that if \( \alpha' : C \to A \) is another isomorphism over \( \bar{K} \) then it differs from \( \alpha \) by \( \tau_P \) for some \( P \in A[\varphi] \); thus \( [(C, \alpha)] = [(C, \alpha')] \) in \( WC(A/K) \).

Definition. Let \( \varphi : A \to B \) be an isogeny. An isomorphism of \( \varphi \)-covers \( (C, \pi) \to (C', \pi') \) is an isomorphism of curves \( i : C \to C' \) making the following diagram commute:

\[
\begin{array}{ccc}
C & \xrightarrow{\pi} & B \\
\downarrow{i} & & \downarrow{id} \\
C' & \xrightarrow{\pi'} & B \\
\end{array}
\]

Remark. For any isogeny \( \varphi \), \( \text{Twist}(\varphi/K) \) is the set of \( \varphi \)-covers up to isomorphism of \( \varphi \)-covers. This is a pointed set with trivial element \( \varphi : A \to B \) itself. Moreover, the automorphism group of \( \varphi \) as a \( \varphi \)-cover is in correspondence with \( A[\varphi] \), since any \( \varphi \)-cover isomorphism \( \varphi \to \varphi \) must be of the form \( \tau_P \) for some \( P \in A[\varphi] \).

Proposition 5.3.8. For any isogeny \( \varphi : A \to B \), there is a bijection

\[
\{ \text{equivalence classes of } \varphi \text{-covers} \} \longleftrightarrow H^1(K, A[\varphi]).
\]

The Selmer-Tate-Shafarevich sequence (Proposition 5.2.3) can now be written:

\[
0 \longrightarrow B(K)/\varphi A(K) \xrightarrow{\delta} H^1(K, A[\varphi]) \longrightarrow WC(A/K) \longrightarrow 0
\]

\[
[C \xrightarrow{\pi} B] \longleftrightarrow [C]
\]

Proposition 5.3.9. If \( C \xrightarrow{\pi} B \) is a \( \varphi \)-cover and there is a point \( x \in C(K) \), then \( [C \xrightarrow{\pi} B] = \delta(P) \) for \( P = \pi(x) \in B(K) \).
5.4 Descent

Proof. For any $P \in B(K)$, $\delta(P) : \sigma \mapsto x^\sigma - x$. In particular, if $P = \varphi \circ \alpha(x) = \pi(x)$, then

$$
\delta(P)(\sigma) = (\varphi \circ \alpha(x))(\sigma) \\
= [\alpha(x)]^\sigma - \alpha(x) \\
= \alpha^\sigma(x^\sigma) - \alpha(x) \\
= \tau_{P_\sigma} \circ \alpha(x^\sigma) - \alpha(x) \quad \text{since } \tau_{P_\sigma} = \alpha^\sigma \circ \alpha^{-1} \\
= \alpha(x^\sigma) + \xi_\sigma - \alpha(x) \\
= \alpha(x) + \xi_\sigma - \alpha(x) = \xi_\sigma
$$

where $\xi$ is the cocycle in $H^1(K, A[\varphi])$ corresponding (via Proposition 5.3.8) to $C \xrightarrow{\pi} B$. Thus $\delta(P) = [C \xrightarrow{\xi} B]$. \qed

Now viewing $\text{Sel}^{(\varphi)}(A/K)$ as a subset of $H^1(K, A[\varphi])$, the Selmer group consists of those $\varphi$-covers (up to isomorphism) which are everywhere locally trivial, that is, have a point over $K_v$ for all completions $K_v$ of $K$. Moreover, the map $\text{Sel}^{(\varphi)}(A/K) \to \text{III}(A/K)[\varphi]$ takes a $\varphi$-cover $C \xrightarrow{\xi} B$ to the space $C$ as a PHS of $A$.

In order to compute $B(K)/\varphi A(K)$, and in particular the weak Mordell-Weil groups $E(\mathbb{Q})/mE(\mathbb{Q})$, one constructs principal homogeneous spaces $C \in \text{III}(A/K)[\varphi]$ which have points in every $K_v$ and use the Selmer-Tate-Shafarevich sequence (Proposition 5.2.3) to pull $C$ back to a generator of $B(K)/\varphi A(K)$. This strategy is known as descent.

5.4 Descent

The goal of descent is to construct torsion elements of the Tate-Shafarevich group $\text{III}(A/K)$ and lift them to generators of $B(K)/\varphi A(K)$. We will describe this construction in the relatively tractable case of 2-torsion elements of an elliptic curve. The general procedure can be found in Silverman and in Cremona’s “Higher Descent on Elliptic Curves”.

Let $E$ be an elliptic curve with a rational 2-torsion point $P \in E(K)$; then $\langle P \rangle$ is a subgroup of order 2 in $E(K)$. We can construct a 2-isogeny of $E$ as follows. Change coordinates of $E$ to move $P$ to the point $(0, 0)$. Then $E$ is given by the Weierstrass form

$$
E : y^2 = x(x^2 + ax + b).
$$

If we set $a' = -2a, b' = a^2 - 4b$ and assume $bb' \neq 0$, then

$$
E' : y^2 = x(x^2 + a'x + b')
$$

is an elliptic curve and there is an isogeny

$$
\varphi : E \longrightarrow E' \\
(x, y) \mapsto \left( \frac{y^2}{x^2}, \frac{y(b - x^2)}{x^2} \right).
$$

Lemma 5.4.1. If $\varphi : E \rightarrow E'$ is an isogeny, then $E$ and $E'$ have good/bad reduction at the same primes.
5.4 Descent 5 The Mordell-Weil Theorem

Proof. (Move?) Silverman VII.7.2.

Let $S$ be the set of primes of bad reduction for $E$ and $E'$; that is,
$$S = \{\text{archimedean primes}\} \cup \{\text{primes dividing } \Delta_{E'} = 16(b')^2((a')^2 - 4b')\}.$$

Set
$$K(S, 2) = \{\beta \in K^\times/(K^\times)^2 : \text{ord}_v(\beta) \equiv 0 \mod 2 \text{ for all } v \notin S\}.$$

Then $E[\varphi] = \{0, 0\}$ as a Galois module, so by Kummer theory, there is a bijection
$$K(S, 2) \longrightarrow H^1_S(K, E)$$
$$\beta \longmapsto \xi(\beta) : \sigma \mapsto \begin{cases} 0, & \text{if } (\sqrt{\beta})^\sigma = \sqrt{\beta} \\ \frac{P}{2}, & \text{if } (\sqrt{\beta})^\sigma = -\sqrt{\beta}. \end{cases}$$

We use this correspondence to construct a $\varphi$-cover $C_\pi \longrightarrow B$ corresponding to $\xi(\beta)$. Consider the field $\overline{K(E)}_\xi$ defined as the set $\overline{K(E)}$ with twisted Galois action $Z : \overline{K(E)} \longrightarrow \overline{K(E)}$,
$$Z(f) = f \circ \tau_{\xi(\beta)}.$$

Then $\overline{K(E)}_{\xi}^{G_K}$, the fixed field of $\overline{K(E)}_\xi$ under the Galois action of $G_K$ defined above, is a function field. Let $C_\beta$ be the corresponding curve (by Proposition 2.2.2). Looking at the addition formula (Proposition 3.3.2) for $E$, one can compute the translation map $\tau_P = \tau_{(0,0)}$ to be
$$\tau_P(x, y) = \left(\frac{b}{x}, -\frac{by}{x^2}\right).$$

Let $L = K(\sqrt{\beta})$, so that $G_{L/K} = \langle \sigma \rangle$ where $\sigma : \sqrt{\beta} \mapsto -\sqrt{\beta}$. Then $L(E)_\xi = L(x, y)/(y^2 - x(x^2 + ax + b))$ with
$$(\sqrt{\beta})^\sigma = -\sqrt{\beta}, \quad x^\sigma = \frac{b}{x} \quad \text{and} \quad y^\sigma = -\frac{by}{x^2}.$$ Observe that $z = \frac{\sqrt{\beta}x}{y}$ and $w = \sqrt{\beta} \left(x - \frac{b}{x}\right)^2(y) \in \overline{K(E)}_{\xi}$ are $G_{L/K}$-invariant and satisfy the equation
$$Y : \beta w^2 = \beta^2 - 2a\beta z^2 + (a^2 - 4b)z^4.$$ In fact, $Y$ is a nonsingular (since $b(a^2 - 4b) \neq 0$ by nonsingularity of $E$) hyperelliptic curve of genus 1. We claim that $Y = C_\beta$.

Over $L$, there is a bijection
$$\theta : E \setminus \{(0, 0), O\} \longrightarrow C_\beta$$
$$(x, y) \longmapsto (z, w) = \left(\frac{\sqrt{\beta}x}{y}, \sqrt{\beta} \left(x - \frac{b}{x}\right)^2\right).$$
Since $\frac{z}{y} = \frac{xy}{y^2} = \frac{y}{x^2 + ax + b}$, this can be extended to all points $Q \in E$ by

$$\theta(Q) = \begin{cases} 
\left( \frac{\sqrt{3}y}{x^2 + ax + b}, \frac{\sqrt{3}(x^2 - b)}{x^2 + ax + b} \right), & Q \neq (0, 0), O \\
(0, -\sqrt{3}), & Q = (0, 0) \\
(0, \sqrt{3}), & Q = O. 
\end{cases}$$

One can also compute the inverse $\alpha = \theta^{-1}$ explicitly:

$$\alpha : C_\beta \to E$$

$$(z, w) \mapsto \left( \frac{\sqrt{3}w - az^2 + \beta}{2z^2}, \frac{\beta w - a\sqrt{3}z^2 + \beta\sqrt{3}}{2z^3} \right).$$

Thus $\theta$ and $\alpha$ are isomorphisms.

Now consider the diagram

$$\begin{array}{ccc}
C_\beta & \xrightarrow{\pi} & E' \\
\alpha \downarrow & & \downarrow\text{id} \\
E & \xrightarrow{\varphi} & E'
\end{array}$$

where $\pi$ is given by $(z, w) \mapsto \left( \frac{\beta}{z^2}, -\frac{\beta w}{z^3} \right)$. Then $\pi = \varphi \circ \alpha$ so $\pi : C_\beta \to E'$ is a $\varphi$-cover.

**Lemma 5.4.2.** The cocycle associated to $C_\beta \xrightarrow{\pi} E'$ is $\xi(\beta)$.

Now recall that the connecting morphism $\delta : E'(K)/\varphi E(K) \to \text{Sel}^{(\psi)}(E/K)$ is given by $\delta(P') : \sigma \mapsto Q^\sigma - Q$ where $\varphi(Q) = P'$. Note that $\varphi(O) = O$, so when $P' = O$, $\delta(O) : \sigma \mapsto O$ and thus $1 \in K(S, 2)$. If $P' = P = (0, 0)$, the 2-torsion point, then $Q$ must have $y = 0$ and $x$ a root of $x^2 + ax + b$, so $Q = \left( \frac{-a \pm \sqrt{a^2 - 4b}}{2}, 0 \right)$. This implies

$$\xi(\beta)\xi = Q^\sigma - Q = \begin{cases} 
O, & \text{if } \sigma \text{ acts trivially on } \sqrt{a^2 - 4b} \\
(0, 0), & \text{otherwise.} 
\end{cases}$$

From this, we see that $\beta = a^2 - 4b$, so $\delta(P) = \beta \in K(S, 2)$. Finally, for $P' = (x, y) \neq (0, 0)$, one can show that $\delta(P') = \delta(x, y) = x$. These explicit $\varphi$-covers $C_\beta \xrightarrow{\pi} E'$ allow us to pull back to generators of $E'(K)/\varphi E(K)$, as demonstrated in the next examples.

**Example 5.4.3.** Let $E$ be the elliptic curve over $\mathbb{Q}$ defined by

$$E : y^2 = x^3 - 6x^2 + 17x.$$  

Our goal is to compute $E(\mathbb{Q})/2E(\mathbb{Q})$. First, $\Delta = -147968 = -2^9 \cdot 17^2$, so $S = \{\infty, 2, 17\}$ and $\mathbb{Q}(S, 2) = \{\pm 1, \pm 2, \pm 17, \pm 34\}$. The above formulas for $E'$ and the $\varphi$-covers $C_\beta$ give the following curves:

$$E' : y^2 = x^3 + 12x^2 - 32x$$

$$C_\beta : \beta w^2 = \beta^2 + 12\beta z^2 - 32z^4, \quad \beta \in \mathbb{Q}(S, 2).$$
Notice that \( \delta(0,0) = a^2 - 4b = -32 \equiv -2 \mod (\mathbb{Q}^\times)^2 \) so the \( \varphi \)-cover \( C_{-2} \) is the image under \( \delta \) of \((0,0)\). Hence \([C_{-2}]\) is trivial in \( \text{III}(E/\mathbb{Q})[\varphi] \). (In particular, this shows that \( E \) has a point over \( \mathbb{Q} \)!)

For \( \beta = 2 \), we get the \( \varphi \)-cover

\[
C_2 : 2w^2 = 4 + 24z^2 - 32z^4.
\]

Setting \( t = 2z \), we can write this as

\[
C_2 : w^2 = 2 + 3t^2 - t^4.
\]

Notice that \((t,w) = (1,2)\) is a point on \( C_2 \), corresponds to a point \((z,w) = (\frac{1}{2}, 2)\) on \( E \), and hence \( \pi \left( \frac{1}{2}, 2 \right) = (8, -32) \in E'(\mathbb{Q}) \). Once again, by Proposition 5.3.9, \([C_2]\) is trivial in the Tate-Shafarevich group.

Next, let \( \beta = 17 \). The corresponding \( \varphi \)-cover is

\[
C_{17} : 17w^2 = 17^2 + 12 \cdot 17z^2 - 32z^4.
\]

Here we show that \([C_{17}] \not\in \text{Sel}(\varphi)(E/\mathbb{Q})\). Suppose to the contrary that there exists a point \((z,w) \in C_{17}(\mathbb{Q}_{17})\). Then \( \text{ord}_{17}(17w^2) \) is odd and \( \text{ord}_{17}(32z^4) \) is even, which implies that \( \text{ord}_{17}(17^2 + 12 \cdot 17z^2 - 32z^4) \neq \text{ord}_{17}(32z^4) = 4 \text{ord}_{17}(z) \). On the other hand,

\[
\text{ord}_{17}(17^2 + 12 \cdot 17z^2 - 32z^4) \geq \min\{2, 1 + 2 \text{ord}_{17}(z), 4 \text{ord}_{17}(z)\}
\]

and the only way this is possible is if \( \text{ord}_{17}(z) > 0 \). However, this contradicts the defining equation for \( C_{17} \). Hence \( C_{17}(\mathbb{Q}_{17}) = \emptyset \), so by Theorem 5.3.7, \([C_{17}] \not\in \text{Sel}(\varphi)(E/\mathbb{Q})\). Further, since \( \text{Sel}(\varphi)(E/\mathbb{Q}) \) is a group, we must have \([C_{-17}], [C_{34}], [C_{-34}] \not\in \text{Sel}(\varphi)(E/\mathbb{Q})\) as well. We have therefore shown that

\[
\text{Sel}(\varphi)(E/\mathbb{Q}) = \{C_1, C_{-1}, C_2, C_{-2}\} \cong \{\pm 1, \pm 2\}.
\]

Further, \( \text{III}(E/\mathbb{Q})[\varphi] = 0 \) so we have an isomorphism \( E'(\mathbb{Q})/\varphi E(\mathbb{Q}) \cong \text{Sel}(\varphi)(E/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \).

Now consider the dual isogeny \( \hat{\varphi} : E' \to E \). Here, we still have \( \text{Q}(S,2) = \{\pm 1, \pm 2, \pm 17, \pm 34\} \) and one can determine the following formulas for \( \hat{\varphi} \)-covers:

\[
C'_\beta : \beta w^2 = \beta^2 - 24\beta z^2 + 272w^4, \quad \beta \in \text{Q}(S,2).
\]

Observe that if \( \beta < 0 \), \( C'_\beta(\mathbb{R}) = \emptyset \) since the signs don’t alternate. Also, \( \delta(0,0) = 272 = 2^4 \cdot 17 \equiv 17 \mod (\mathbb{Q}^\times)^2 \) so \( C'_{17} \) is the image of \((0,0) \in E'(\mathbb{Q})/\hat{\varphi} E(\mathbb{Q}) \) under \( \delta \). Lastly, for \( \beta = 2 \), we have

\[
C'_2 : 2w^2 = 4 - 12t + 17t^4
\]

(with \( t = 2z \)). A similar proof as above shows that \( C'_2(\mathbb{Q}_2) = \emptyset \), so \([C'_2] \not\in \text{Sel}(\hat{\varphi})(E'/\mathbb{Q})\). In all, this shows that

\[
\text{Sel}(\hat{\varphi})(E'/\mathbb{Q}) = \{C_1, C_{17}\} \cong \{1, 17\},
\]

but \( C_1 \) and \( C_{17} \) are images under \( \delta \) of the points \( O \) and \((0,0), \) respectively, so \( \text{III}(E'/\mathbb{Q})[\hat{\varphi}] = 0 \) in this case.
Let’s put this together to determine the weak Mordell-Weil group $E(\mathbb{Q})/2E(\mathbb{Q})$. From above, $E'(\mathbb{Q})/\varphi E(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, where the generators are $(0, 0)$ and $(8, -32)$. On the other hand, the previous paragraph implies that $E(\mathbb{Q})/\hat{\varphi}E'(\mathbb{Q}) \cong \text{Sel}^{(\hat{\varphi})}(E'/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$, with explicit generator $(0, 0)$. The composition $\varphi \circ \hat{\varphi} = [2]$ gives us an exact sequence

$$0 \rightarrow \frac{E'(\mathbb{Q})}{\varphi(E(\mathbb{Q})[\varphi])} \rightarrow \frac{E(\mathbb{Q})}{\varphi E'(\mathbb{Q})} \rightarrow \frac{E(\mathbb{Q})}{2E(\mathbb{Q})} \rightarrow \varphi E(\mathbb{Q}) \rightarrow 0.$$ 

Inserting the terms we know, this becomes

$$0 \rightarrow \mathbb{Z}/2\mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z} \rightarrow \frac{E(\mathbb{Q})}{2E(\mathbb{Q})} \rightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \rightarrow 0.$$ 

Hence by exactness, $E(\mathbb{Q})/2E(\mathbb{Q}) = \langle (0, 0), (8, -32) \rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Furthermore, since $E_{\text{tors}}(\mathbb{Q}) = E(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z} = \langle (0, 0) \rangle$, we deduce that $(8, -32)$ is a point of infinite order on $E(\mathbb{Q})$. This implies the final result:

$$E(\mathbb{Q}) = \langle (0, 0), (8, -32) \rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}.$$ 

In the above example, we were able to determine $\text{III}(E/\mathbb{Q})[\varphi] = 0$ and $\text{III}(E'/\mathbb{Q})[\hat{\varphi}] = 0$ and use this to deduce $E(\mathbb{Q})/2E(\mathbb{Q})$, and ultimately $E(\mathbb{Q})$. However, sometimes one may discover a $\varphi$-cover $C_\beta$ not mapping to the trivial class in $\text{III}(E/\mathbb{Q})[\varphi]$. In such a situation, one may require a method known as ‘second descent’ (cf. Cremona’s paper entitled “Higher Descents on Elliptic Curves”). Let $\varphi : A \rightarrow B$ and $\hat{\varphi} : B \rightarrow A$ be dual isogenies such that $\varphi \circ \hat{\varphi} = [m]$. Then we have a commutative diagram with exact rows and columns:

$$\begin{array}{ccccccccc}
0 & 0 & 0 & 0 & 0 \\
0 & \to & H & \to & A(\mathbb{Q})/\hat{\varphi}B(\mathbb{Q}) & \to & B(\mathbb{Q})/mB(\mathbb{Q}) & \to & B(\mathbb{Q})/\varphi A(\mathbb{Q}) & \to & 0 \\
0 & \to & H & \to & \text{Sel}(\hat{\varphi})(B/\mathbb{Q}) & \to & \text{Sel}^{(m)}(B/\mathbb{Q}) & \to & \text{Sel}^{(\varphi)}(A/\mathbb{Q}) & \to & 0 \\
0 & \to & \text{III}(B'/\mathbb{Q})[\hat{\varphi}] & \to & \text{III}(B'/\mathbb{Q})[m] & \to & \text{III}(A'/\mathbb{Q})[\varphi] & \to & 0 \\
0 & 0 & 0 & 0 & 0
\end{array}$$

(Here, $H = B(\mathbb{Q})[\hat{\varphi}]/\varphi(A(\mathbb{Q})[\varphi])$.) Take $C \in \text{Sel}^{(\varphi)}(A/\mathbb{Q})$ and use exactness of the middle row to find a lift $D \in \text{Sel}^{(m)}(B/\mathbb{Q})$; then these are $\varphi$- and $\hat{\varphi}$-covers, respectively:
5.4 Descent

\[
\begin{array}{ccc}
D \xrightarrow{\varpi} C & \xrightarrow{\pi} & B \\
\cong & \cong & \downarrow \text{id} \\
B \xrightarrow{\hat{\varphi}} A & \xrightarrow{\varphi} & B
\end{array}
\]

Such a \( D \) is called a descendant of \( C \). The key insight is that a point on \( D \) (over any field, but in particular over local fields) gives a point on \( C \) via \( \varpi \). In general, points on \( D \) will have smaller height than those on \( C \) (see Section 5.5), so it will be easier in theory to find points on \( D \).

If points cannot be found on \( D \), replace \( \varphi \) with \([m]\), \( \hat{\varphi} \) with \([m]\) and \( m = \deg \varphi \) with \( m^2 = \deg[m] \) and repeat the argument. In principle, this can be repeated indefinitely. However, each step yields an exact sequence:

\[
0 \to B(\mathbb{Q})/\varphi A(\mathbb{Q}) \to \text{Sel}^{(\varphi,j)}(A/\mathbb{Q}) \to m^j \text{III}(A/\mathbb{Q})[m^j] \to 0
\]

where, for \( j \geq 2 \), \( \text{Sel}^{(\varphi,j)}(A/\mathbb{Q}) \) denotes the elements of \( \text{Sel}^{(\varphi)}(A/\mathbb{Q}) \) coming from \( \text{Sel}^{(m^j)}(A/\mathbb{Q}) \). Eventually, the last term in these sequences becomes \( 0 \) as long as the Tate-Shafarevich group \( \text{III}(A/\mathbb{Q}) \) is not infinitely \( m \)-divisible. It is conjectured that this is true for all elliptic curves, but has not been proven. Thus it is believed that the descent procedure always terminates in a finite number of steps. (In fact, the Birch-Swinnerton-Dyer Conjecture would imply that the Tate-Shafarevich group is always finite, in which case descent always terminates.)

**Example 5.4.4.** For \( D \in \mathbb{Z} \), let

\[
E : y^2 = x^3 + Dx
\]

be the congruent number elliptic curve (see Section 0.1). For simplicity, we will assume \( D = p \), a prime number congruent to 1 mod 8. Then \( \Delta_E = -4p^3 \) and \( S = \{ \infty, 2, p \} \), so \( \mathbb{Q}(S, 2) = \{ \pm 1, \pm 2, \pm p, \pm 2p \} \). One can show using normal means that \( E_{\text{tors}}(\mathbb{Q}) = \langle (0,0) \rangle \cong \mathbb{Z}/2\mathbb{Z} \). Further, we have the following formulas for the \( \varphi \)- and \( \hat{\varphi} \)-covers in the Selmer groups:

\[
\begin{align*}
C_{\beta} : \beta w^2 &= \beta^2 - 4pz^4 \quad \text{in} \ \text{Sel}^{(\varphi)}(E/\mathbb{Q}) \\
C_{\beta}' : \beta w^2 &= \beta^2 + pz^4 \quad \text{in} \ \text{Sel}^{(\hat{\varphi})}(E'/\mathbb{Q}).
\end{align*}
\]

For the 2-torsion point \( P = (0,0) \), notice that \( \delta(P) = -4p^3 \equiv -p \mod (\mathbb{Q}^\times)^2 \) and \( \hat{\delta}(P) \equiv p \mod (\mathbb{Q}^\times)^2 \). So \( C_{-p} \in \text{Sel}^{(\varphi)}(E/\mathbb{Q}) \) and \( C_{p}' \in \text{Sel}^{(\hat{\varphi})}(E'/\mathbb{Q}) \). Also, if \( \beta < 0 \), the coefficients in the second equation above fail to alternate, so \( C_{\beta}'(\mathbb{R}) = \emptyset \). Consider the \( \hat{\varphi} \)-cover for \( \beta = 2 \):

\[
C_{2}' : 2w^2 = 4 + pz^4.
\]

Over \( \mathbb{Q}_2 \), any point \((z, w)\) must then satisfy \( 1 + 2 \text{ord}_2(w) \geq \min\{2, 4 \text{ord}_2(z)\} \), but 2 and 4 \( \text{ord}_2(z) \) are both even and never equal, so the inequality is an equality. However, \( 1 + 2 \text{ord}_2(w) \) is odd, so this is impossible. Hence \( C_{2}'(\mathbb{Q}_2) = \emptyset \), and thus \( C_{2}' \notin \text{Sel}^{(\hat{\varphi})}(E'/\mathbb{Q}) \). We have now shown that \( \text{Sel}^{(\hat{\varphi})}(E'/\mathbb{Q}) = \{1, p\} \).

To finish computing \( \text{Sel}^{(\varphi)}(E/\mathbb{Q}) \), we have

\[
C_{-1} : -w^2 = 1 - 4pz^4, \quad \text{or} \quad w^2 + 1 = 4pz^4.
\]
Over \( \mathbb{F}_p \), the reduction \( \overline{C}_{-1}(\mathbb{F}_p) \) is given by \( w^2 + 1 = 0 \), and since we assumed \( p \equiv 1 \) (mod \( 8 \)), there is a solution by quadratic reciprocity. Check that this point is nonsingular on the reduction, so that it lifts to a point of \( C_{-1}(\mathbb{Q}_p) \). Now over \( \mathbb{Q}_2 \), make the change of variables \((z, w) \mapsto (\frac{z}{1}, \frac{w}{8})\) so that the \( \varphi \)-cover \( C_{-1} \) is given by

\[
C_{-1} : w^2 + 64 = pz^4.
\]

Then \((1, 1)\) is a solution mod 8 and satisfies Hensel’s criterion, so \( C_{-1}(\mathbb{Q}_2) \neq \emptyset \). This proves \( C_{-1} \in \text{Sel}^{(\varphi)}(E/\mathbb{Q}) \).

Now for \( \beta = -2 \), the cover is given by

\[
C_{-2} : -2w^2 = 4 - 4pz^4, \quad \text{or} \quad w^2 + 2 = 2pz^4.
\]

Over \( \mathbb{F}_p \), the equation becomes \( w^2 + 2 = 0 \) which again has a solution since \( p \equiv 1 \) (mod \( 8 \)). As above, one can check that the point is nonsingular and then lift it to a point of \( C_{-2}(\mathbb{Q}_p) \). Likewise, the proof that \( C_{-2}(\mathbb{Q}_2) \) is nonempty is similar.

The above work shows that \( \text{Sel}^{(\varphi)}(E/\mathbb{Q}) = \{ \pm 1, \pm 2, \pm p, \pm 2p \} \). Now consider the sequences

\[
\begin{align*}
0 \to E'(\mathbb{Q})[\varphi] & \to E'(\mathbb{Q}) & \to E(\mathbb{Q}) & \to E(\mathbb{Q}) & \to 0 \quad \text{(A)} \\
0 \to E'(\mathbb{Q}) & \to \text{Sel}^{(\varphi)}(E/\mathbb{Q}) & \to \text{III}(E/\mathbb{Q})[\varphi] & \to 0 \quad \text{(B)} \\
0 \to \text{III}(E/\mathbb{Q})[\varphi] & \to \text{III}(E/\mathbb{Q})[2] & \to \text{III}(E'/\mathbb{Q})[\varphi] & \to 0. \quad \text{(C)}
\end{align*}
\]

The terms in all three sequences are \( \mathbb{F}_2 \)-vector spaces, so we can add dimensions as follows:

\[
\dim \left( \frac{E'(\mathbb{Q})[\varphi]}{\varphi(E(\mathbb{Q})[2])} \right) + \dim \left( \frac{E(\mathbb{Q})}{2E(\mathbb{Q})} \right) = \dim \left( \frac{E'(\mathbb{Q})}{\varphi(E(\mathbb{Q}))} \right) + \dim \left( \frac{E(\mathbb{Q})}{\varphi(E'(\mathbb{Q}))} \right)
\]

\[
= \dim \text{Sel}^{(\varphi)}(E/\mathbb{Q}) - \dim \text{III}(E/\mathbb{Q})[\varphi]
\]

\[
+ \dim \text{Sel}^{(\varphi)}(E'/\mathbb{Q}) - \dim \text{III}(E'/\mathbb{Q})[\varphi]
\]

(where \( \dim = \dim_{\mathbb{F}_2} \)). On the other hand, \( E(\mathbb{Q})/2E(\mathbb{Q}) = (\mathbb{Z}/2\mathbb{Z})^{1+\text{rank}(E)} \), by the proof of Lemma 5.2.6, and since \( E_{\text{tors}}(\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} \), we must have \( \mathbb{Z}/2\mathbb{Z} \subseteq E(\mathbb{Q})/\varphi E'(\mathbb{Q}) \). By sequence (B) however, \( E(\mathbb{Q})/\varphi E'(\mathbb{Q}) \) injects into \( \text{Sel}^{(\varphi)}(E'/\mathbb{Q}) = \{ 1, p \} \), so we must have \( E(\mathbb{Q})/\varphi E'(\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} \). This further implies that \( \text{III}(E'/\mathbb{Q})[\varphi] = 0 \) in sequence (B). Finally, sequence (C) gives us \( \dim \text{III}(E/\mathbb{Q})[\varphi] = \dim \text{III}(E/\mathbb{Q})[2] \). Putting these together with the dimension formula, we get

\[
1 + (1 + \text{rank}(E)) = \dim \text{Sel}^{(\varphi)}(E/\mathbb{Q}) + \dim \text{Sel}^{(\varphi)}(E'/\mathbb{Q}) - \dim \text{III}(E/\mathbb{Q})[2]
\]

\[
= 3 + 1 - \dim \text{III}(E/\mathbb{Q})[2].
\]

So \( \dim \text{III}(E/\mathbb{Q})[2] + \text{rank}(E) = 2 \). By Cassel’s pairing (Theorem 5.2.9), \( \dim \text{III}(E/\mathbb{Q})[2] \) is even, so each of \( \{ \dim \text{III}(E/\mathbb{Q})[2], \text{rank}(E) \} \) can be either 0 or 2. In fact, both situations occur. For example, the congruent number curve

\[
E : y^2 = x^3 + 73x
\]
has rank 2 and has rational points \((\frac{9}{16}, \frac{411}{64})\) and \((36, 222)\) which generate \(E(\mathbb{Q})\).

To find an example which has \(\text{rank}(E) = 0\), assume 2 is a quartic non-residue mod \(p\) (e.g. \(p = 17\) will work). Consider the \(\beta = \pm 2\) covers:

\[
C_{\pm 2} : \pm w^2 = 2 - 2pz^4.
\]

Suppose \((z, w) \in C_{\pm 2}(\mathbb{Q})\). Writing \(z\) in lowest terms, we may assume \((z, w) = (\frac{r}{t}, \frac{2s}{t^2})\), where \(r, s, t \in \mathbb{Z}\) are coprime integers satisfying

\[
\pm 2s^2 = t^4 - pr^4. \quad (\ast)
\]

Let \(q\) be an odd prime factor of \(s\). Then reducing \((\ast)\) mod \(p\) shows that \(\left(\frac{q}{p}\right) = 1\). On the other hand, since \(p \equiv 1 \pmod{8}\), quadratic reciprocity implies \(\left(\frac{2}{p}\right) = 1\) as well. Reciprocity also implies \(\left(\frac{2}{p}\right) = 1\), so if \(s = 2^{e_0} q_1^{e_1} \cdots q_n^{e_n}\) for distinct primes \(q_1, \ldots, q_n\), then we can write

\[
\left(\frac{s}{p}\right) = \left(\frac{2}{p}\right)^{e_0} \left(\frac{q_1}{p}\right)^{e_1} \cdots \left(\frac{q_n}{p}\right)^{e_n} = 1 \cdot 1 \cdots 1 = 1.
\]

Hence \(s\) is a quadratic residue mod \(p\), which means \(s^2\) is a quartic residue mod \(p\). From \((\ast)\), we get \(\left(\frac{\pm 2s^2}{p}\right)_4 = 1\), but Gauss’s quartic reciprocity implies \(\left(\frac{-1}{p}\right)_4 = 1\) when \(p \equiv 1 \pmod{8}\).

So this means \(\left(\frac{2}{p}\right)_4 = 1\) by multiplicativity of the 4th power Legendre symbol. Thus in the case when 2 is not a quartic residue mod \(p\) (as with \(p = 17\)), we must have \(C_{\pm 2}(\mathbb{Q}) = \emptyset\).

This is exactly the condition that \(C_{\pm 2}\) are nontrivial in \(\text{III}(E/\mathbb{Q})[2]\), so we have found an entire class of elliptic curves for which \(\text{III}(E/\mathbb{Q})[2]\) is nontrivial. In particular, we find that \(E\) has rank 0.

We can similarly show that \(C_{-1}\) is nontrivial in the Tate-Shafarevich group. Write

\[
C_{-1} : -w^2 = 1 - 4pz^4.
\]

Suppose \((z, w) \in C_{-1}(\mathbb{Q})\) and rewrite this as \((z, w) = (\frac{r}{2t}, \frac{a}{2t^2})\) for \(r, s, t \in \mathbb{Z}\) coprime such that

\[
s^2 + 4t^2 = pr^4. \quad (\ast\ast)
\]

Write \(p = a^2 + b^2\) for \(a = 1 \pmod{2}\) and \(b \equiv 0 \pmod{2}\); this is possible by Fermat’s theorem on primes of the form \(p = x^2 + y^2\), since \(p \equiv 1 \pmod{4}\). Using Gauss’s composition formulas for quadratic forms, one can write

\[
(pr^2 + 2bt^2)^2 = p(br^2 + 2t^2)^2 + a^2 s^2
\]

\[
\implies (pr + 2bt^2 - as)(pr + 2bt^2 + as) = p(br^2 + 2t^2)^2.
\]

These together imply that for some \(u, v \in \mathbb{Z}\),

\[
\begin{cases}
br^2 + 2t^2 = uv \text{ or } 2uv \\
pr^2 + 2bt^2 \pm as = pu^2 \text{ or } 2pu^2 \\
pr^2 + 2bt^2 \mp as = v^2 \text{ or } 2v^2.
\end{cases}
\]
The second and third lines combine to give us

\[
(†) = \begin{cases} 
2pt^2 + 4bt^2 = pu^2 + v^2 \\
b^2 + 2t^2 = uv.
\end{cases}
\]

By quartic reciprocity, \( (\frac{2}{p})_4 = (-1)^{ab/4} \), but by assumption \( (\frac{2}{p})_4 \neq 1 \), so \( 8 \nmid b \). Thus \( b \equiv 0 \pmod{2} \) implies that \( b \equiv 4 \pmod{8} \). Reducing (†) mod 8 yields

\[
\begin{cases} 
2r^2 = u^2 + v^2 \\
4t^2 = uv.
\end{cases}
\]

These imply \( u \) and \( v \) are both even, so \( r \) is even and therefore so is \( t \). But this contradicts the assumption that \( r \) and \( t \) are coprime. Hence \( C_{−1}(\mathbb{Q}) = \emptyset \).

### 5.5 Heights

Fix an elliptic curve in short Weierstrass form

\[ E : y^2 = x^3 + Ax + B, \quad A, B \in \mathbb{Z}. \]

**Definition.** For any \( t \in \mathbb{Q} \), write \( t = \frac{p}{q} \) for coprime integers \( p, q \in \mathbb{Z} \). The **height** of \( t \) is defined by

\[ H(t) = \max\{|p|, |q|\}. \]

Next, for a point \( P = [x_0, \ldots, x_N] \in \mathbb{P}^N_\mathbb{Q} \), we may assume \( \gcd(x_0, \ldots, x_N) = 1 \). Then the **height function** \( H : \mathbb{P}^N_\mathbb{Q} \to \mathbb{R}_{\geq 0} \) is defined by

\[ H(P) = \max\{|x_i| : 0 \leq i \leq N\} \]

for all \( P = [x_0, \ldots, x_N] \in \mathbb{P}^N_\mathbb{Q} \), and \( H(\infty) = 1 \).

Setting \( h(P) = \log H(P) \) defines a function

\[ h : \mathbb{P}^N_\mathbb{Q} \to \mathbb{R}_{\geq 0}. \]

This can be extended to any field extension \( K/\mathbb{Q} \) by

\[ h(P) = \frac{1}{[K : \mathbb{Q}]} \sum_v \log \max\{|x_i|_v : 0 \leq i \leq N\} \]

for any \( P = [x_0, \ldots, x_N] \in \mathbb{P}^N(K) \), where the sum is over all valuations \( v \) on \( K \) and \( |x_i|_v = (\# \mathcal{O}_K/p_v)^{-\ord_v(x)} \) is the normalized \( p_v \)-adic valuation on \( K \).

**Proposition 5.5.1.** Let \( E \) be an elliptic curve over \( \mathbb{Q} \) and fix \( P_0 \in E(\mathbb{Q}) \). Then

1. There is some constant \( C_1 \), which depends on \( P_0, A \) and \( B \), such that \( h(P + P_0) \leq 2h(P) + C_1 \) for all \( P \in E(\mathbb{Q}) \).
2. There is some constant \( C_2 \), which depends only on \( A \) and \( B \), such that \( h([2]P) \geq 4h(P) - C_2 \) for all \( P \in E(\mathbb{Q}) \).
(3) \( \{ P \in E(\mathbb{Q}) : h(P) < B \} \) is a finite set for all \( B > 0 \).

**Proof.** Silverman. \qed

**Remark.** More generally, any projective embedding \( X \hookrightarrow \mathbb{P}_k^N \) of a variety gives a height function. Recall (Section 2.3) that such embeddings arise from very ample divisors. The whole theory of heights can be derived from this perspective (see *Diophantine Geometry* by Hindry-Silverman).

**Definition.** The **canonical height function** for any elliptic curve \( E \) is defined for a point \( P \in \mathbb{P}_\mathbb{Q}^N(K) \) by

\[
\hat{h}(P) := \lim_{n \to \infty} \frac{1}{4^n} h([2^n]P).
\]

**Proposition 5.5.2.** The canonical height function for any elliptic curve \( E \) satisfies

(i) For all \( B > 0 \), the set \( \{ P \in E(\mathbb{Q}) : \hat{h}(P) < B \} \) is finite.

(ii) For each \( m \in \mathbb{Z} \) and each point \( P \in E(\mathbb{Q}) \), \( \hat{h}(mP) = m^2 \hat{h}(P) \).

(iii) The pairing \( \langle P, Q \rangle = \frac{1}{2}(\hat{h}(P + Q) - \hat{h}(P) - \hat{h}(Q)) \) is symmetric and bilinear.

**Proof.** Silverman. \qed

We are now prepared to give the proof the full Mordell-Weil theorem using the weak version (Corollary 5.2.8) and heights.

**Theorem 5.5.3** (Mordell-Weil). For every elliptic curve \( E \) over \( \mathbb{Q} \), the group \( E(\mathbb{Q}) \) is finitely generated. 

**Proof.** Fix \( m \in \mathbb{Z} \). By Corollary 5.2.8, the weak Mordell-Weil group \( E(\mathbb{Q})/mE(\mathbb{Q}) \) is finitely generated, so pick generators \( P_1, \ldots, P_s \in E(\mathbb{Q})/mE(\mathbb{Q}) \). Set \( c_0 = \max\{|P_i| : 1 \leq i \leq s\} \), where \( |P| = \sqrt{\hat{h}(P)} \) for any \( P \in E(\mathbb{Q}) \). By Proposition 5.5.2(i), it’s enough to show that \( S := \{ P \in E(\mathbb{Q}) : |P| \leq c_0 \} \) generates \( E(\mathbb{Q}) \), since this set is finite. The proof follows Fermat’s strategy of ‘descent’.

Suppose \( Q_0 \in E(\mathbb{Q}) \). If \( Q_0 \notin S \), then \( |Q_0| > c_0 \). Since \( E(\mathbb{Q})/mE(\mathbb{Q}) \) is finitely generated, we may write \( Q_0 = P_{i_1} + mQ_1 \) for some \( P_{i_1}, Q_1 \in E(\mathbb{Q}) \). Now

\[
m|Q_1| = m\sqrt{\hat{h}(Q_1)} = \sqrt{m^2 \hat{h}(Q_1)}
\]

\[
= \sqrt{\hat{h}(mQ_1)} = |mQ_1| \quad \text{by Proposition 5.5.2(ii)}
\]

\[
= |Q_0 - P_{i_1}| \leq |Q_0| + |P_{i_1}| \quad \text{from Proposition 5.5.2(iii)}
\]

\[
< 2|Q_0| \quad \text{since } |Q_0| > c_0 \geq |P_{i_1}|.
\]

So \( |Q_1| \leq |Q_0| \). Now repeat: either \( Q_1 \in S \) or \( |Q_1| > c_0 \). In the latter case, \( Q_1 = P_{i_2} + mQ_2 \) for \( P_{i_2}, Q_2 \in E(\mathbb{Q}) \) satisfying \( |Q_2| \leq |Q_1| \leq |Q_0| \). Now, by Proposition 5.5.2(i), the set \( \{ P \in E(\mathbb{Q}) : |P| \leq |Q_0| \} \) is finite, so this descent process must terminate. This shows that \( Q_0 \) is a sum of elements of \( S \), so \( S \) generates \( E(\mathbb{Q}) \) and the theorem is proven. \qed
6 Elliptic Curves and Complex Analysis

In this chapter we review the classical theory of complex algebraic curves, starting with the construction and basic properties of elliptic functions, their connection to elliptic curves and their Jacobians, and then describing the construction in arbitrary dimension.

6.1 Elliptic Functions

Let \( \Lambda \subseteq \mathbb{C} \) be a lattice, i.e. a free abelian subgroup of rank 2. Then \( \Lambda \) can be written

\[ \Lambda = \mathbb{Z} \omega_1 + \mathbb{Z} \omega_2 \]

for some \( \omega_1, \omega_2 \in \mathbb{C} \) such that \( \frac{\omega_1}{\omega_2} \notin \mathbb{R} \).

**Definition.** A function \( f : \mathbb{C} \to \mathbb{C} \cup \{\infty\} \) is doubly periodic with lattice of periods \( \Lambda \) if \( f(z + \ell) = f(z) \) for all \( \ell \in \Lambda \) and \( z \in \mathbb{C} \).

**Definition.** An elliptic function is a function \( f : \mathbb{C} \to \mathbb{C} \cup \{\infty\} \) that is meromorphic and doubly periodic.

It is not obvious that doubly periodic functions even exist! We will prove this shortly.

**Definition.** Let \( \Lambda \subseteq \mathbb{C} \) be a lattice. The set

\[ \Pi = \Pi(\omega_1, \omega_2) = \{ t_1 \omega_1 + t_2 \omega_2 \mid 0 \leq t_i < 1 \} \]

is called the fundamental parallelogram, or fundamental domain, of \( \Lambda \). We say a subset \( \Phi \subseteq \mathbb{C} \) is fundamental for \( \Lambda \) if the quotient map \( \mathbb{C} \to \mathbb{C}/\Lambda \) restricts to a bijection on \( \Phi \).

**Lemma 6.1.1.** For any choice of basis \( [\omega_1, \omega_2] \) of \( \Lambda \), \( \Pi(\omega_1, \omega_2) \) is fundamental for \( \Lambda \).

**Lemma 6.1.2.** Let \( \Lambda \) be a lattice. Then
6.1 Elliptic Functions

(a) If $\Pi$ is the fundamental domain of $\Lambda$, then for any $\alpha \in \mathbb{C}$, $\Pi_\alpha := \Pi + \alpha$ is fundamental for $\Lambda$.

(b) If $\Phi$ is fundamental for $\Lambda$, then $\mathbb{C} = \bigcup_{\ell \in \Lambda} \Phi + \ell$.

Corollary 6.1.3. Suppose $f$ is an elliptic function with lattice of periods $\Lambda$ and $\Phi$ fundamental for $\Lambda$. Then $f(\mathbb{C}) = f(\Phi)$.

Proposition 6.1.4. A holomorphic elliptic function is constant.

Proof. Let $f$ be such an elliptic function and let $\Phi$ be the fundamental domain for its lattice of periods. Then $\Pi$ is compact and hence $f(\Pi)$ is as well. In particular, $f(\mathbb{C}) = f(\Pi) \subseteq f(\Pi)$ is bounded, so by Liouville’s theorem, $f$ is constant.

The prominence of tools from complex analysis (e.g. Liouville’s theorem in the above proof) is obvious in the study of elliptic functions. Another important result for computations is the residue theorem:

Theorem (Residue Theorem). For any meromorphic function $f$ on a region $R \subseteq \mathbb{C}$, with isolated singularities $z_1, \ldots, z_k \in R$. Then if $\Delta = \partial R$,

$$\int_{\Delta} f(z) \, dz = 2\pi i \sum_{i=1}^{k} \text{Res}(f; z_i).$$

Proposition 6.1.5. Let $f$ be an elliptic function. If $\alpha \in \mathbb{C}$ is a complex number such that $\partial \Pi_\alpha$ does not contain any of the poles of $f$, then the sum of the residues of $f$ inside $\partial \Pi_\alpha$ equals 0.

Proof. Fix a basis $[\omega_1, \omega_2]$ of $\Lambda$ and set $\Delta = \partial \Pi_\alpha$. By the residue theorem, it’s enough to show $\int_{\Delta} f(z) \, dz = 0$. We parametrize the boundary of $\Pi$ as follows:

$$\begin{align*}
\gamma_1 &= \alpha + t\omega_1 \\
\gamma_2 &= \alpha + \omega_1 + t\omega_2 \\
\gamma_3 &= \alpha + (1-t)\omega_1 + \omega_2 \\
\gamma_4 &= \alpha + (1-t)\omega_2.
\end{align*}$$
We show that \( \int_{\gamma_1} f(z) \, dz + \int_{\gamma_3} f(z) \, dz = 0 \) and leave the proof that \( \int_{\gamma_2} f(z) \, dz + \int_{\gamma_2} f(z) \, dz = 0 \) for exercise. Consider

\[
\int_{\gamma_1} f(z) \, dz + \int_{\gamma_3} f(z) \, dz = \int_0^1 f(\alpha + t\omega_1)(\omega_1 \, dt) + \int_0^1 f(\alpha + (1 - t)\omega_1 + \omega_2)(-\omega_1 \, dt) \\
= \omega_1 \int_0^1 f(\alpha + t\omega_1) \, dt + \omega_1 \int_1^0 f(\alpha + s\omega_1) \, ds \quad \text{since } f \text{ is elliptic} \\
= \omega_1 \left( \int_0^1 f(\alpha + t\omega_1) \, dt - \int_0^1 f(\alpha + s\omega_1) \, ds \right) = 0.
\]

Hence the sum of the residues equals 0.

\[\square\]

**Corollary 6.1.6.** Any elliptic function has either a pole of order at least 2 or two poles on the fundamental domain of its lattice of periods.

**Proposition 6.1.7.** Suppose \( f \) is an elliptic function with fundamental domain \( \Pi \) and \( \alpha \in \mathbb{C} \) such that \( \Delta = \partial \Pi_\alpha \) does not contain any zeroes or poles of \( f \). Let \( \{a_j\}_{j=1}^n \) be a finite set of zeroes and poles in \( \Pi_\alpha \), with \( m_j \) the order of the pole \( a_j \). Then \( \sum_{j=1}^n m_j = 0 \).

**Proof.** For a pole \( z_0 \), we can write \( f(z) = (z - z_0)^m g(z) \) for some holomorphic function \( g(z) \), with \( g(z_0) \neq 0 \). Then

\[
\frac{f'(z)}{f(z)} = (z - z_0)^{-1} \left( m + (z - z_0) \frac{g'(z)}{g(z)} \right).
\]

Hence \( \text{Res} \left( \frac{f'}{f}; z_0 \right) = m \). Then the statement follows from Proposition 6.1.5. \[\square\]

Proposition 6.1.7 may be viewed as a complex-geometric analogue of the statement for algebraic curves in Corollary 2.2.6: the divisor of a rational function on an algebraic curve has degree zero.

Continuing in the complex setting, let \( f \) be an elliptic function and let \( a_1, \ldots, a_r \) be the poles and zeroes of \( f \) in the fundamental domain of \( \Lambda \). Write \( \text{ord}_{a_i} f = m_i \) if \( a_i \) is a pole of order \(-m_i\) or if \( a_i \) is a zero of multiplicity \( m_i \). The sum \( \text{ord}(f) = \sum_{i=1}^r m_i \) is called the order of \( f \). Then Corollary 6.1.6 says that there are no elliptic functions of order 1. We will show that the field of elliptic functions with period lattice \( \Lambda \) is generated by an order 2 and an order 3 function.

Let \( f \) be elliptic and \( z_0 \in \mathbb{C} \) with \( \text{ord}_{z_0} f = m \). Then for any \( \ell \in \Lambda \), \( \text{ord}_{z_0 + \ell} f = m \) as well. Indeed, if \( z_0 \) is a zero then

\[
0 = f(z_0) = f(z_0) = \ldots = f^{(m-1)}(z_0)
\]

but \( f^{(k)}(z) \) is also elliptic for all \( k \geq 1 \). If \( z_0 \) is a pole of \( f \), the same result can be obtained using \( \frac{1}{f} \) instead of \( f \).

If \( \Phi_1 \) and \( \Phi_2 \) are any two fundamental domains for \( \Lambda \), then for all \( a_1 \in \Phi_1 \), there is a unique \( a_2 \in \Phi_2 \) such that \( a_2 = a_1 + \ell \) for some \( \ell \in \Lambda \). Thus Propositions 6.1.5 and 6.1.7 hold for any fundamental domain of \( \Lambda \), so it follows that \( \text{ord}(f) \) is well-defined on the quotient \( \mathbb{C}/\Lambda \).

101
Now given any meromorphic function \( f(z) \) on \( \mathbb{C} \), we would like to construct an elliptic function \( F(z) \) with lattice \( \Lambda \). Put
\[
F(z) = \sum_{\ell \in \Lambda} f(z + \ell).
\]
There are obvious problems of convergence and (in a related sense) the order of summation. It turns out we can do this construction with \( f(z) = \frac{1}{z^m}, m \geq 3 \) though. First, we need the following result from complex analysis, which can be proven using Cauchy’s integral formula and Morera’s theorem.

**Lemma 6.1.8.** Let \( U \subseteq \mathbb{C} \) be an open set and suppose \((f_n)\) is a sequence of holomorphic functions on \( U \) such that \( f_n \to f \) uniformly on every compact subset of \( U \). Then \( f \) is holomorphic on \( U \) and \( f' \to f' \) uniformly on every compact subset of \( U \).

**Proposition 6.1.9.** Let \( \Lambda \) be a lattice with basis \([\omega_1, \omega_2]\). Then the sum
\[
\sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{|\omega|^s}
\]
converges for all \( s > 2 \).

**Proof.** Extend the fundamental domain by translation by the vectors \( \omega_1, \omega_2 \) and \( \omega_1 + \omega_2 \), and call the boundary of the resulting region \( \Delta \):

\[
\begin{array}{ccc}
\Lambda & \Lambda & \Delta \\
\Lambda & \Lambda & \\
\Lambda & \Lambda & \\
\end{array}
\]

Then \( \Delta \) is compact, so there exists \( c > 0 \) such that \( |z| \geq c \) for all \( z \in \Delta \). We claim that for all \( m, n \in \mathbb{Z} \),
\[
|m \omega_1 + n \omega_2| \geq c \cdot \max\{|m|, |n|\}.
\]
The cases when \( m = 0 \) or \( n = 0 \) are trivial, so without loss of generality assume \( m \geq n > 0 \). Then
\[
|m \omega_1 + n \omega_2| = |m| \left| \omega_1 + \frac{n}{m} \omega_2 \right| \geq |m|c.
\]
Hence the claim holds. Set \( M = \max\{|m|, |n|\} \) and arrange the sum in question so that the \( \frac{1}{|\omega|^s} \) are added in order of increasing \( M \) values. Then the sum can be estimated by
\[
\sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{|\omega|^s} \leq \sum_{M=1}^{\infty} \frac{8M}{c^s M^s} \sim \sum_{M=1}^{\infty} \frac{1}{M^{s-1}}.
\]
This converges for \( s > 2 \) by \( p \)-series.
Proposition 6.1.10. Let $n \geq 3$ and define

$$F_n(z) = \sum_{\omega \in \Lambda} \frac{1}{(z - \omega)^n}.$$ 

Then $F_n(z)$ is holomorphic on $\mathbb{C} \setminus \Lambda$ and has poles of order $n$ at the points of $\Lambda$. Moreover, $F_n$ is doubly periodic and hence elliptic.

Proof. Fix $r > 0$ and let $B_r = B_r(0)$ be the open complex $r$-ball centered at the origin in $\mathbb{C}$. Let $\Lambda_r = \Lambda \cap B_r$ be the lattice points contained in the closed $r$-ball. Then the function

$$F_{n,r}(z) = \sum_{\omega \in \Lambda \setminus \Lambda_r} \frac{1}{(z - \omega)^n}$$

is holomorphic on $B_r$. To see this, one has $\frac{1}{|z - \omega|^n} \leq \frac{C}{|\omega|^n}$ for some constant $C$ and for all $z \in B_r, \omega \in \Lambda \setminus \Lambda_r$. Then $\frac{C}{|\omega|^n}$ converges by Proposition 6.1.9, so by the Weierstrass $M$-test, $\frac{1}{|z - \omega|^n}$ converges uniformly and hence $F_{n,r}(z)$ is holomorphic. It follows from the definition that $F_n$ has a pole of order $n$ at each $\omega \in \Lambda$. Finally, for $\ell \in \Lambda$, we have

$$F_n(z + \ell) = \sum_{\omega \in \Lambda} \frac{1}{(z + \ell - \omega)^n} = \sum_{\eta \in \Lambda} \frac{1}{(z - \eta)^n} = F_n(z)$$

since the series is absolutely convergent and we can rearrange the terms. \qed

This shows that elliptic functions exist and more specifically that for each $n \geq 3$, there is at least one elliptic function of order $n$. Unfortunately the previous proof won’t work to construct an elliptic function of order 3. However, Weierstrass discovered the following elliptic function.

Definition. The Weierstrass $\wp$-function for a lattice $\Lambda$ is defined by

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left[ \frac{1}{(z - \omega)^2} - \frac{1}{\omega^2} \right].$$

Theorem 6.1.11. For any lattice $\Lambda$, $\wp(z)$ is an elliptic function with poles of order 2 at the points of $\Lambda$ and no other poles. Moreover, $\wp(-z) = \wp(z)$ and $\wp'(z) = -2F_3(z)$.

Proof. (Sketch) To show $\wp(z)$ is meromorphic, one estimates the summands by

$$\left| \frac{1}{(z - \omega)^2} - \frac{1}{\omega^2} \right| \leq \frac{D}{|\omega|^3}$$

for some constant $D$ and all $z \in B_r, \omega \in \Lambda \setminus \Lambda_r$ as in the previous proof.

Next, $\wp(z)$ can be differentiated term-by-term to obtain the expression $\wp'(z) = -2F_3(z)$. And proving that $\wp(z)$ is odd is straightforward:

$$\wp(-z) = \frac{1}{(-z)^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left[ \frac{1}{(-z - \omega)^2} - \frac{1}{\omega^2} \right]$$

$$= \frac{1}{z^2} + \sum_{-\omega \in \Lambda \setminus \{0\}} \left[ \frac{1}{(z - (-\omega))^2} - \frac{1}{(-\omega)^2} \right] = \wp(z)$$

103
after switching the order of summation.

Finally, proving $\varphi(z)$ is doubly periodic is difficult since we don’t necessarily have absolute convergence. However, one can reduce to proving $\varphi(z + \omega_1) = \varphi(z)$ for $z = (\omega_1 + \omega_2)$. Then using the formula for $\varphi'(z)$, we have
\[
\frac{d}{dz}[\varphi(z + \omega_1) - \varphi(z)] = -2F_3(z + \omega_1) + 2F_3(z) = -2F_3(z) + 2F_3(z) = 0
\]
since $F_3(z)$ is elliptic by Proposition 6.1.10. Hence $\varphi(z + \omega_1) - \varphi(z) = c$ is constant. Evaluating at $z = -\frac{\omega_1}{2}$, we see that $c = \varphi\left(\frac{\omega_1}{2}\right) - \varphi\left(-\frac{\omega_1}{2}\right) = 0$ since $\varphi(z)$ is odd. Hence $c = 0$, so it follows that $\varphi(z)$ is doubly periodic and therefore elliptic.

\begin{proof}
\end{proof}

\begin{lemma}
Let $\varphi(z)$ be the Weierstrass $\varphi$-function for a lattice $\Lambda \subseteq \mathbb{C}$ and let $\Pi$ be the fundamental domain of $\Lambda$. Then
\begin{enumerate}
\item For any $u \in \mathbb{C}$, the function $\varphi(z) - u$ has either two simple roots or one double root in $\Pi$.
\item The zeroes of $\varphi'(z)$ in $\Pi$ are simple and they only occur at $\frac{\omega_1}{2}$, $\frac{\omega_2}{2}$, and $\frac{\omega_1 + \omega_2}{2}$.
\item The numbers $u_1 = \varphi\left(\frac{\omega_1}{2}\right)$, $u_2 = \varphi\left(\frac{\omega_2}{2}\right)$ and $u_3 = \varphi\left(\frac{\omega_1 + \omega_2}{2}\right)$ are precisely those $u$ for which $\varphi(z) - u$ has a double root.
\end{enumerate}
\end{lemma}

\begin{proof}
(1) follows from Corollary 6.1.6.

(2) By Theorem 6.1.11, $\deg \varphi'(z) = 3$ so it suffices to show that $\frac{\omega_1}{2}$, $\frac{\omega_2}{2}$, and $\frac{\omega_1 + \omega_2}{2}$ are all roots. For $z = \frac{\omega_1}{2}$, we have
\[
\varphi'\left(\frac{\omega_1}{2}\right) = -\varphi'\left(-\frac{\omega_1}{2}\right) = -\varphi'\left(\frac{\omega_1}{2} - \omega_1\right) = -\varphi'\left(\frac{\omega_1}{2}\right)
\]
since $\varphi'(z)$ is elliptic. Thus $\varphi'\left(\frac{\omega_1}{2}\right) = 0$. The others are similar.

(3) The double roots occur exactly when $\varphi'(u) = 0$, so use (2).
\end{proof}

We now prove that any elliptic function can be written in terms of $\varphi(z)$ and $\varphi'(z)$.

\begin{theorem}
Fix a lattice $\Lambda \subseteq \mathbb{C}$ and let $\mathcal{E}(\Lambda)$ be the field of all elliptic functions with lattice of periods $\Lambda$. Then $\mathcal{E}(\Lambda) = \mathbb{C}(\varphi, \varphi')$.
\end{theorem}

\begin{proof}
Take $f(z) \in \mathcal{E}(\Lambda)$. Then $f(-z) \in \mathcal{E}(\Lambda)$ as well and thus we can write $f(z)$ as the sum of an even and an odd elliptic function:
\[
f(z) = f_{\text{even}}(z) + f_{\text{odd}}(z) = \frac{f(z) + f(-z)}{2} + \frac{f(z) - f(-z)}{2}.
\]
We will prove that every even elliptic function is rational in $\varphi(z)$, but this will imply the theorem, since then $f_{\text{even}}(z) = \varphi(\varphi(z))$ and $\frac{f_{\text{odd}}(z)}{\varphi'(z)} = \psi(\varphi(z))$ for some $\varphi, \psi \in \mathbb{C}(\varphi(z))$ and we can then write $f(z) = \varphi(\varphi(z)) + \varphi'(z)\psi(\varphi(z))$.

Assume $f(z)$ is an even elliptic function. It’s enough to construct $\varphi(\varphi(z))$ such that $\frac{f(z)}{\varphi(\varphi(z))}$ only has (potential) zeroes and poles at $z = 0$ in the fundamental parallelogram.
for \( \Lambda \), since then by Corollary 6.1.6, \( \frac{f(z)}{\varphi(\varphi(z))} \) is holomorphic and then by Proposition 6.1.4 it is constant. Suppose \( f(a) = 0 \) for a some zero of order \( m \). Consider \( \varphi(z) = u \). If \( u \neq \varphi \left( \frac{w_1}{2} \right), \varphi \left( \frac{w_2}{2} \right), \varphi \left( \frac{w_1 + w_2}{2} \right) \) then \( \varphi(z) = u \) has precisely two solutions in the fundamental parallelogram, \( z = a \) and \( z = a^* \) where

\[
a^* = \begin{cases} 
\omega_1 + \omega_2 - a & \text{if } a \in \text{Int}(\Pi) \\
\omega_1 - a & \text{if } a \text{ is parallel to } \omega_1 \\
\omega_2 - a & \text{if } a \text{ is parallel to } \omega_2.
\end{cases}
\]

(Notice that since \( f \) is even, \( f(a) = 0 \) implies \( f(a^*) = 0 \) as well.) Moreover, if \( \text{ord}_a f = 0 \) then \( \text{ord}_{a^*} f = m \). Note that \( a = a^* \) holds precisely when \( a \) is in the set \( \Theta := \left\{ 0, \frac{w_1}{2}, \frac{w_2}{2}, \frac{w_1 + w_2}{2} \right\} \).

Let \( Z \) (resp. \( P \)) be the set of zeroes (resp. poles) of \( f(z) \) in \( \Pi \). Then the assignment \( a \mapsto a^* \) is in fact an involution on \( Z \) and \( P \), so we can write

\[
Z = Z'_1 \cup \cdots \cup Z'_s \cup Z''_1 \cup \cdots \cup Z''_t \\
P = P'_1 \cup \cdots \cup P'_u \cup P''_1 \cup \cdots \cup P''_v
\]

where the \( Z'_i \) and \( P'_i \) are the 2-element orbits of the involution and the \( Z''_j \) and \( P''_j \) are the 1-element orbits. Of course then \( s, v \leq 3 \). For \( a'_i \in Z'_i \), set \( \text{ord}_{a'_i} f = m'_i \) and for \( a''_j \in Z''_j \), set \( \text{ord}_{a''_j} f = m''_j \), which is even. Likewise, for \( b'_i \in P'_i \), set \( \text{ord}_{b'_i} f = n'_i \) and for \( b''_j \in P''_j \), set \( \text{ord}_{b''_j} f = n''_j \), which is even. Then we define \( \varphi(\varphi(z)) \) by

\[
\varphi(\varphi(z)) = \frac{\prod_{i=1}^s (\varphi(z) - \varphi(a''_j))^{m''_j} \prod_{j=1}^t (\varphi(z) - \varphi(b''_j))^{m''_j/2}}{\prod_{i=1}^u (\varphi(z) - \varphi(b'_i))^{n'_i} \prod_{j=1}^v (\varphi(z) - \varphi(b''_j))^{n''_j}}.
\]

Then \( \varphi(\varphi(z)) \) has only potential zeroes/poles at \( z = 0 \) in the fundamental parallelogram, so we are done.

\[\square\]

## 6.2 Elliptic Curves

Let \( \Lambda \subseteq \mathbb{C} \) be a lattice. There is a canonical way to associate to the complex torus \( \mathbb{C}/\Lambda \) an elliptic curve \( E \) such that \( \mathbb{C}/\Lambda \cong E(\mathbb{C}) \). We would also like to reverse this process, i.e. given an elliptic curve \( E \), define a lattice \( \Lambda \subseteq \mathbb{C} \) such that \( \mathbb{C}/\Lambda \cong E(\mathbb{C}) \). This procedure generalizes for a curve \( C \) of genus \( g > 1 \) and produces its Jacobian, \( C \hookrightarrow \mathbb{C}^g/\Lambda = J(C) \).

We need the following lemma from complex analysis.

**Lemma 6.2.1.** Suppose \( f_0, f_1, f_2, \ldots \) is a sequence of analytic functions on the ball \( B_r(z_0) \) with Taylor expansions

\[
f_n(z) = \sum_{k=0}^{\infty} a_k^{(n)}(z - z_0)^k.
\]

Then if \( F(z) = \sum_{n=0}^{\infty} f_n(z) \) converges uniformly on \( B_\rho(z_0) \) for all \( \rho < r \), each series \( A_k = \sum_{n=0}^{\infty} a_k^{(n)} \) converges and \( F(z) \) has Taylor expansion

\[
F(z) = \sum_{k=0}^{\infty} A_k(z - z_0)^k.
\]

105
Let \( \wp(z) \) be the Weierstrass \( \wp \)-function for \( \Lambda \). Then \( \wp'(z)^2 \) is an even elliptic function, so by Theorem 6.1.13, \( \wp'(z)^2 \in \mathbb{C}(\wp) \). On a small enough neighborhood around \( z_0 = 0 \),

\[
\wp(z) - \frac{1}{z^2} = \sum_{\omega \in \Lambda \setminus \{0\}} \left[ \frac{1}{(z - \omega)^2} - \frac{1}{\omega^2} \right]
\]

is analytic. Moreover, for each \( \omega \in \Lambda \setminus \{0\} \) we have

\[
\frac{1}{(z - \omega)^2} = \frac{1}{\omega^2} + \frac{2z}{\omega^3} + \frac{3z^2}{\omega^4} + \ldots
\]

\[
\implies \frac{1}{(z - \omega)^2} - \frac{1}{\omega^2} = \frac{2z}{\omega^2} + \frac{3z^2}{\omega^4} + \ldots
\]

which is uniformly convergent. Hence Lemma 6.2.1 shows that

\[
\wp(z) - \frac{1}{z^2} = \sum_{\omega \in \Lambda \setminus \{0\}} \sum_{k=1}^{\infty} \frac{k + 1}{\omega^k+2} z^k = \sum_{k=1}^{\infty} (k + 1)G_{k+2}z^k
\]

where \( G_m = G_m(\Lambda) := \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{\omega^m} \). These \( G_m \) are examples of modular forms.

**Definition.** The series \( G_m(\Lambda) = \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{\omega^m} \) is called the Eisenstein series for \( \Lambda \) of weight \( m \).

From the above work, we obtain the following formulas:

\[
\wp(z) = \frac{1}{z^2} + 3G_4z^2 + 5G_6z^4 + 7G_8z^6 + \ldots
\]

\[
\wp(z)^2 = \frac{1}{z^4} + 6G_4 + \ldots
\]

\[
\wp(z)^3 = \frac{1}{z^6} + \frac{9G_4}{z^2} + 15G_6 + \ldots
\]

\[
\wp'(z) = -\frac{2}{z^3} + 6G_4z + \ldots
\]

\[
\wp'(z)^2 = \frac{4}{z^6} - \frac{24G_4}{z^2} - 80G_6 - \ldots
\]

This implies:

**Proposition 6.2.2.** The functions \( \wp \) and \( \wp' \) satisfy the following relation:

\[
\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3
\]

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

Consider the polynomial \( p(x) = 4x^3 - g_2x - g_3 \), where the \( g_n \) are defined for the lattice \( \Lambda \subseteq \mathbb{C} \).

**Proposition 6.2.3.** \( p(x) = 4(x - u_1)(x - u_2)(x - u_3) \) where \( u_1 = \wp\left(\frac{\omega_1}{2}\right) \), \( u_2 = \wp\left(\frac{\omega_2}{2}\right) \) and \( u_3 = \wp\left(\frac{\omega_1 + \omega_2}{2}\right) \) are distinct roots.
Thus \((x, y) = (\varphi(z), \varphi'(z))\) determine an equation \(y^2 = 4x^3 - g_2x - g_3\) which is the defining equation for an elliptic curve \(E_0\) over \(\mathbb{C}\). Let \(E = E_0 \cup \{0, 1, 0\} \subseteq \mathbb{P}^2\) be the projective closure of \(E_0\). Denote the point \([0, 1, 0]\) by \(\infty\).

**Theorem 6.2.4.** The map

\[
\varphi : \mathbb{C}/\Lambda \longrightarrow E(\mathbb{C})
\]

\[
z + \Lambda \longmapsto \varphi(z + \Lambda) = \begin{cases} 
[\varphi(z), \varphi'(z), 1], & z \notin \Lambda \\
[0, 1, 0], & z \in \Lambda 
\end{cases}
\]

is a bijective, biholomorphic map.

**Proof.** Assume \(z_1, z_2 \in \mathbb{C}\) are such that \(z_1 + \Lambda \neq z_2 + \Lambda\). Without loss of generality we may assume \(z_1, z_2 \in \Pi\), the fundamental domain of \(\Lambda\) (otherwise, translate). If \(\varphi(z_1) = \varphi(z_2)\) and \(\varphi'(z_1) = \varphi'(z_2)\), then with the notation of Theorem 6.1.13, we must have \(z_2 = z_1^2 \neq z_1\) and thus \(z_1, z_2 \notin \Theta = \{0, \frac{w_1}{2}, \frac{w_1 + w_2}{2}\}\). Since \(\varphi(z)\) is odd, we get \(\varphi'(z_1) = \varphi'(z_2) = -\varphi'(-z_2) = -\varphi'(z_1)\), but this implies \(\varphi(z_1) = 0\), contradicting \(z_1 \notin \Theta\). Therefore \(\varphi\) is one-to-one.

Next, we must show that for any \((x_0, y_0) \in E(\mathbb{C})\), \(x_0 = \varphi(z)\) and \(y_0 = \varphi'(z)\) for some \(z \in \mathbb{C}\). If \(\varphi(z_1) = x_0\), then it’s clear that \(\varphi'(z_1) = y_0\) or \(-y_0\). Now one shows as in the previous paragraph that we must have \(\varphi'(z_1) = y_0\).

Now consider \(F(x, y) = y^2 - p(x)\), where \(p(x) = 4x^3 - g_2x - g_3\). If \((x_0, y_0)\) satisfies \(F(x_0, y_0) = 0\) and \(y_0 \neq 0\), then \(\frac{\partial F}{\partial y}(x_0, y_0) \neq 0\) and thus the assignment \((x, y) \mapsto x\) is a local chart about \((x_0, y_0)\). Likewise, \((x, y) \mapsto y\) defines a local chart about \((x_0, y_0)\) when \(x_0 \neq 0\). Finally, we conclude by observing that a locally biholomorphic map is biholomorphic. 

Recall from Chapter 3 that an elliptic curve can be defined by a Weierstrass equation

\[
E : y^2 = f(x) = ax^3 + bx^2 + cx + d.
\]

This embeds into projective space via \((x, y) \mapsto [x, y, 1]\). Setting \(x = \frac{X}{Z}\) and \(y = \frac{Y}{Z}\), we also obtain a homogeneous equation for the curve:

\[
E : ZY^2 = aX^3 + bX^2Z + cXZ^2 + dZ^3.
\]

The single point at infinity, \([0, 1, 0]\), can be studied by dehomogenizing via the coordinates \(\tilde{z} = \frac{Z}{Y}\) and \(\tilde{x} = \frac{X}{Y}\), which yield

\[
E : \tilde{z} = a\tilde{x}^3 + b\tilde{x}^2\tilde{z} + a\tilde{x}\tilde{z}^2 + d\tilde{z}^3.
\]

We have shown that a lattice \(\Lambda \subseteq \mathbb{C}\) determines elliptic functions \(\varphi(z)\) and \(\varphi'(z)\) that satisfy \(\varphi'(z)^2 = 4\varphi(z)^3 - g_2\varphi(z) - g_3\) and that this polynomial expression has no multiple roots. Therefore the mapping \(z \mapsto (\varphi(z), \varphi'(z))\) determines a bijective correspondence \(\mathbb{C}/\Lambda \setminus \{0\} \rightarrow E(\mathbb{C}) \setminus \{\infty\}\) which can be extended to all of \(\mathbb{C}/\Lambda \rightarrow E(\mathbb{C})\) (this is Theorem 6.2.4). There is a natural group structure on \(\mathbb{C}/\Lambda\) induced from \(\mathbb{C}\), but what is not so obvious is that this coincides precisely with the “chord-and-tangent” group law on \(E(\mathbb{C})\) from Section 3.3.

**Theorem 6.2.5.** The map \(\varphi : \mathbb{C}/\Lambda \rightarrow E(\mathbb{C})\) is an isomorphism of abelian groups.
Proof. Consider the diagram

\[
\begin{array}{ccc}
\mathbb{C}/\Lambda \times \mathbb{C}/\Lambda & \xrightarrow{\varphi \times \varphi} & E(\mathbb{C}) \times E(\mathbb{C}) \\
\alpha \downarrow & & \downarrow \beta \\
\mathbb{C}/\Lambda & \xrightarrow{\varphi} & E(\mathbb{C})
\end{array}
\]

where \(\alpha\) and \(\beta\) are the respective group operations. Since \(\mathbb{C}/\Lambda \times \mathbb{C}/\Lambda\) is a topological group, it’s enough to show the diagram commutes on a dense subset of \(\mathbb{C}/\Lambda \times \mathbb{C}/\Lambda\). Consider

\[
\tilde{X} = \{(u_1, u_2) \in \mathbb{C}^2 \mid u_1, u_2, u_1 \pm u_2, 2u_1 + u_2, u_1 + 2u_2 \not\in \Lambda\}.
\]

Then \(\tilde{X} \cong \mathbb{C}^2\) so \(X = \tilde{X} \mod \Lambda \times \Lambda\) is dense in \(\mathbb{C}/\Lambda \times \mathbb{C}/\Lambda\). Take \((u_1 + \Lambda, u_2 + \Lambda) \in X\) and set \(u_3 = -(u_1 + u_2)\). Then \(u_1 + u_2 + u_3 = 0\) in \(\mathbb{C}/\Lambda\). Set \(P = \varphi(u_1), Q = \varphi(u_2)\) and \(R = \varphi(u_3) \in E(\mathbb{C})\). By the assumptions on \(X\), the points \(P, Q, R\) are distinct. We want to show \(\varphi(u_1 + u_2) = \varphi(u_1) + \varphi(u_2) = P + Q\). Since \(\varphi(z)\) is even and \(\varphi'(z)\) is odd, we see that \(\varphi(-z) = -\varphi(z)\) for all \(z \in \mathbb{C}/\Lambda\). Thus \(\varphi(u_1 + u_2) = -\varphi(-(u_1 + u_2)) = -R\) so we need to show \(P + Q + R = O\), i.e. \(P, Q, R\) are colinear. Since \(u_1 \neq u_2\), the line \(PQ\) is not vertical, so there exist \(a, b\) such that \(\varphi'(u_i) = a\varphi(u_i) + b\) for \(i = 1, 2\). Consider the elliptic function

\[
f(z) = \varphi'(z) - (a\varphi(z) + b).
\]

Then on the fundamental domain \(\Pi\), \(f\) only has a pole at 0, so \(\text{ord}_0 f = -3\). Also, \(u_1\) and \(u_2\) are distinct zeroes of \(f\), so there is a third point \(\omega \in \Pi\) such that \(\text{deg}(f) = u_1 + u_2 + \omega - 3\cdot 0 = 0\), i.e. \(u_1 + u_2 + \omega = 0\). Solving for \(\omega\), we get \(\omega = -(u_1 + u_2) = u_3\). It follows that \(R = \varphi(u_3)\) is on the same line as \(P\) and \(Q\), so we are done. \(\square\)

The compatibility of the group operations of \(\mathbb{C}/\Lambda\) and \(E(\mathbb{C})\) is highly useful. For example, fix \(N \in \mathbb{N}\) and let

\[
E[N] = \{P \in E(\mathbb{C}) \mid [N]P = O\},
\]

be the \(N\)-torsion points of \(E\). For \(N = 2\), the points \(P\) such that \(P = -P\) are exactly the intersection points of \(E\) with the \(x\)-axis along with \(O = [0, 1, 0]\):
Theorem 4.0.2 said that \( \# E[N] = N^2 \). This is hard to see from the geometric picture, but working with the isomorphism \( E(\mathbb{C}) \cong \mathbb{C}/\Lambda \) from Theorem 6.2.5, we see that since \( \mathbb{C}/\Lambda = \mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z} \) as an abelian group, the \( N \)-torsion is given by \( (\mathbb{C}/\Lambda)[N] = \frac{1}{N} \mathbb{Z}/\mathbb{Z} \times \frac{1}{N} \mathbb{Z}/\mathbb{Z} \). This is a group of order \( N^2 \), so we have proven (3) of Theorem 4.0.2. The other statements of the theorem are straightforward to prove.

Recall that morphism in the category of elliptic curves is called an isogeny. Explicitly, \( \varphi : E_1 \rightarrow E_2 \) is an isogeny between two elliptic curves if it is a (nonconstant) morphism of schemes that takes the basepoint \( O_1 \in E_1 \) to the basepoint \( O_2 \in E_2 \).

**Proposition 6.2.6.** Suppose \( \Lambda_1, \Lambda_2 \subseteq \mathbb{C} \) are lattices and \( f : \mathbb{C}/\Lambda_1 \rightarrow \mathbb{C}/\Lambda_2 \) is a holomorphic map. Then there exist \( a, b \in \mathbb{C} \) such that \( a\Lambda_1 \subseteq \Lambda_2 \) and

\[
f(z \mod \Lambda_1) = az + b \mod \Lambda_2.
\]

**Proof.** As topological spaces, \( \mathbb{C}/\Lambda_1 \) and \( \mathbb{C}/\Lambda_2 \) are complex tori with the same universal covering space \( \mathbb{C} \), so any \( f : \mathbb{C}/\Lambda_1 \rightarrow \mathbb{C}/\Lambda_2 \) lifts to \( F : \mathbb{C} \rightarrow \mathbb{C} \) making the diagram commute:

\[
\begin{array}{ccc}
\mathbb{C} & \xrightarrow{F} & \mathbb{C} \\
\pi_1 \downarrow & & \downarrow \pi_2 \\
\mathbb{C}/\Lambda_1 & \xrightarrow{f} & \mathbb{C}/\Lambda_2
\end{array}
\]

Since covers are local homeomorphisms, it follows that \( F \) is holomorphic as well. Thus for any \( z \in \mathbb{C}, \ell \in \Lambda_1, \)

\[
\pi_2(F(z + \ell) - F(z)) = f(\pi_1(z + \ell) - \pi_1(z)) = f(\pi_1(z) - \pi_1(z)) = f(0) = 0.
\]

So \( F(z + \ell) - F(z) \in \Lambda_1 \) for any \( \ell \in \Lambda_1 \) and the function \( L(z) = F(z + \ell) - F(z) \) is constant. It follows that \( F'(z + \ell) = F'(z) \), so \( F' \) is holomorphic and elliptic, but this means by Proposition 6.1.4 that \( F'(z) = a \) for some constant \( a \). Hence \( F(z) = az + b \) as claimed. \( \square \)
Corollary 6.2.7. For two lattices $\Lambda_1, \Lambda_2$, the elliptic curves $\mathbb{C}/\Lambda_1$ and $\mathbb{C}/\Lambda_2$ are isomorphic if and only if there exists an $a \in \mathbb{C}$ such that $\Lambda_1 = a\Lambda_2$.

Definition. Two lattices $\Lambda_1$ and $\Lambda_2$ are said to be homothetic if $\Lambda_1 = a\Lambda_2$ for some $a \in \mathbb{C}$.

Thus the set of homothety classes of lattices is naturally identified with the set of isomorphisms of complex elliptic curves.

Corollary 6.2.8. Any holomorphic map $f : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ is, up to translation, a group homomorphism. In particular, if $f(0) = 0$ then $f$ is a homomorphism.

Corollary 6.2.9. For any elliptic curve $E$, the group of endomorphisms $\text{End}(E)$ has rank at most 2.

Proof. Viewing $E(\mathbb{C}) = \mathbb{C}/\Lambda$ for some $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$, we get

\[
\text{End}(E) = \{ f : E \to E \mid f \text{ is an isogeny} \}
\]

\[
= \{ f : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda \mid f \text{ is holomorphic and } f(0) = 0 \} \quad \text{by Corollary 6.2.8}
\]

\[
= \{ z \in \mathbb{C} \mid z\Lambda \subseteq \Lambda \}
\]

\[
= \{ z \in \mathbb{C} \mid z(\mathbb{Z} + \mathbb{Z}\tau) \subseteq (\mathbb{Z} + \mathbb{Z}\tau) \}
\]

\[
\subseteq \mathbb{Z} + \mathbb{Z}\tau.
\]

Hence $\text{rank} \text{End}(E) \leq 2$. $\square$

It turns out that there are two possible cases for the structure of $\text{End}(E)$:

- $\text{End}(E) = \mathbb{Z}$.
- $\text{End}(E)$ is an order $\mathcal{O}$ in some imaginary quadratic number field $K/\mathbb{Q}$. In this case, $E$ is said to have complex multiplication.

6.3 The Classical Jacobian

For the isomorphism $\varphi : \mathbb{C}/\Lambda \to E(\mathbb{C})$ in Theorem 6.2.5, let $\psi = \varphi^{-1} : E(\mathbb{C}) \to \mathbb{C}/\Lambda$ be the inverse map. To understand this map explicitly, we will show how to construct a torus for every elliptic curve, i.e. find a lattice $\Lambda \subseteq \mathbb{C}$ such that $\mathbb{C}/\Lambda \cong E(\mathbb{C})$.

Lemma 6.3.1. Any lattice $\Lambda \subseteq \mathbb{C}$ can be written

\[
\Lambda = \left\{ \int_0^P dz : P \in \Lambda \right\}.
\]

Notice that each differential form $dz$ on $\mathbb{C}$ satisfies $d(z + \ell) = dz$ for all $\ell \in \Lambda$ by Lemma 6.3.1. Thus $dz$ descends to a differential form on $\mathbb{C}/\Lambda$, which by abuse of notation we will also denote by $dz$. Formally, this is the pushforward of $dz$ along the quotient $\pi : \mathbb{C} \to \mathbb{C}/\Lambda$. This implies:
Lemma 6.3.2. Any lattice $\Lambda \subseteq \mathbb{C}$ can be written

$$\Lambda = \left\{ \int_\gamma dz : \gamma \text{ is a closed curve in } \mathbb{C}/\Lambda \text{ passing through } 0 \right\}.$$

For an elliptic curve $E$ defined by the equation $y^2 = f(x)$, fix a holomorphic differential form $\omega$ on $E(\mathbb{C})$. (In general, the space of holomorphic differential forms on a curve has dimension equal to the genus of the curve, so in the elliptic curve case, there is exactly one such $\omega$, up to scaling.)

**Definition.** The **lattice of periods** for an elliptic curve $E$ is

$$\Lambda = \left\{ \int_\gamma \omega : \gamma \text{ is a closed curve in } E \text{ passing through } P \right\}$$

where $P \in E(\mathbb{C})$ is fixed.

**Example 6.3.3.** Under the map $\varphi : \mathbb{C}/\Lambda \to E(\mathbb{C}), z \mapsto (x, y) = (\varphi(z), \varphi'(z))$, we see that

$$dx = \varphi'(z) \, dz = y \, dz$$

so $\omega = \frac{dx}{y}$ is a differential form on $E(\mathbb{C})$. In fact, $\omega = \frac{dx}{f'(x)}$, where $E$ is defined by $y^2 = f(x)$, is holomorphic because $f'(x) \neq 0$. This differential form is also holomorphic at $O = [0, 1, 0]$, so up to scaling, this is the unique holomorphic form on $E$.

Historically, mathematicians were interested in studying solutions to **elliptic integrals**, or integrals of the form

$$\int \frac{dx}{\sqrt{ax^3 + bx + c}}.$$

When $f(x) = ax^3 + bx + c$, the expression $\omega = \frac{dx}{\sqrt{ax^3 + bx + c}}$ is precisely the holomorphic differential form defining the lattice of periods of the elliptic curve $E : y^2 = f(x)$.

For a more functorial description, let $V_E = \Gamma(E, \Omega_E)$ be the space of all holomorphic differential forms on $E$. If $\gamma$ is a curve in $E(\mathbb{C})$, there is an associated linear functional $\varphi_\gamma \in V_E^*$ defined by

$$\varphi_\gamma : V_E \to \mathbb{C}$$

$$\omega \mapsto \int_\gamma \omega.$$

Fixing the basepoint $O \in E(\mathbb{C})$, the lattice of periods for $E$ can be written

$$\Lambda = \{ \varphi_\gamma : \gamma \in \pi_1(E(\mathbb{C}), O) \}.$$

In other words, this defines a map $\pi_1(E(\mathbb{C}), O) \to V_E^*, \gamma \mapsto \varphi_\gamma$.

**Definition.** The **Jacobian** of an elliptic curve $E$ is the quotient $J(E) = V_E^*/\Lambda$.

For each point $P \in E(\mathbb{C})$, the coset $\varphi_\gamma + \Lambda$ is an element of the Jacobian, where $\gamma$ is a path from $O$ to $P$. This defines an injective map $i : E \hookrightarrow J(E)$. 

111
Proposition 6.3.4. Suppose \( \sigma : E_1 \rightarrow E_2 \) is an isogeny between elliptic curves, so that \( \sigma(O_1) = O_2 \). Then there is a map \( \tau : J(E_1) \rightarrow J(E_2) \) making the following diagram commute:

\[
\begin{array}{ccc}
E_1 & \xrightarrow{\sigma} & E_2 \\
\downarrow{i_1} & & \downarrow{i_2} \\
J(E_1) & \xrightarrow{\tau} & J(E_2)
\end{array}
\]

Proof. The pullback gives a contravariant map \( \sigma^* : V_{E_2} \rightarrow V_{E_1} \), \( \omega \mapsto \sigma^* \omega = \omega \circ \sigma \). Taking the dual of this gives a linear map \( \tau^* : V_{E_1}^* \rightarrow V_{E_2}^* \) defined by \( (\tau^* \rho) (\omega) = \rho(\sigma^* \omega) \) for any \( \rho \in V_{E_1}^* \) and \( \omega \in V_{E_2}^* \). Taking \( \rho = \varphi_{\gamma_1} \) for a path \( \gamma_1 \) in \( E_1 \) gives

\[
\tau^* \varphi_{\gamma_1} = \varphi_{\sigma(\gamma_1)}.
\]

Thus \( \tau^* \varphi_{\gamma_1} = \varphi_{\sigma(\gamma_1)} \). If \( \gamma_1 \) is a closed curve through \( O_1 \), then \( \sigma(\gamma_1) \) is a closed curve passing through \( O_2 = \sigma(O_1) \). Hence if \( \Lambda_{E_1}, \Lambda_{E_2} \) are the lattices of periods for \( E_1, E_2 \), respectively, we have \( \tau^* (\Lambda_{E_1}) \subseteq \Lambda_{E_2} \). So \( \tau^* \) factors through the quotients, defining \( \tau \):

\[
\tau = \overline{\sigma^*} : V_{E_1}^*/\Lambda_{E_1} \longrightarrow V_{E_2}^*/\Lambda_{E_2}.
\]

It is immediate the diagram commutes. \( \square \)

Lemma 6.3.5. For any elliptic curve \( E \), the inclusion \( i : E \hookrightarrow J(E) \) induces an isomorphism

\[
i^* : \pi_1(E, O) \longrightarrow \pi_1(J(E), i(O)).
\]

Unfortunately, the construction of the Jacobian given so far is not algebraic so it would be hard to carry over to curves over an arbitrary ground field. To construct Jacobians algebraically, we will prove Abel’s theorem:

Theorem 6.3.6 (Abel). Suppose \( \Lambda \subseteq \mathbb{C} \) is a lattice with fundamental domain \( \Pi \) and take any set \( \{a_i\} \subset \Pi \) such that there are integers \( m_i \in \mathbb{Z} \) satisfying \( \sum m_i = 0 \) and \( \sum m_i a_i \in \Lambda \).

Then there exists an elliptic function \( f(z) \) whose set of zeroes and poles is \( \{a_i\} \) and whose orders of vanishing/poles are \( \text{ord}_z f = m_i \).

Given a lattice \( \Lambda \subseteq \mathbb{C} \), we may assume \( \Lambda = \mathbb{Z} + \mathbb{Z} \tau \) for some \( \tau \in \mathbb{C} \) with \( \text{im} \tau > 0 \).

Definition. The theta function for a lattice \( \Lambda \) is

\[
\theta(z, \tau) = \sum_{n=-\infty}^{\infty} e^{\pi i (n^2 \tau + 2nz)}.
\]

One has \( |e^{\pi i (n^2 \tau + 2nz)}| = e^{-\pi (n^2 \text{im} \tau + 2n \text{im} z)} \) for any \( z \in \mathbb{C} \), which implies that the above series converges absolutely.

Proposition 6.3.7. Fix a theta function \( \theta(z) = \theta(z, \tau) \). Then
(1) $\theta(z) = \theta(-z)$.

(2) $\theta(z + 1) = \theta(z)$.

(3) $\theta(z + \tau) = e^{-\pi i (\tau + 2z)} \theta(z)$.

Properties (2) and (3) together say that $\theta(z)$ is what’s known as a semielliptic function. For our purposes, this will be good enough. Notice that for $z = \frac{1+\tau}{2}$, we have

$$
\theta \left( \frac{1+\tau}{2} \right) = \theta \left( -\frac{1+\tau}{2} + (1+\tau) \right) = e^{\pi i (\tau + 2 \left(-\frac{1+\tau}{2}\right))} \theta \left( -\frac{1+\tau}{2} \right) = e^{\pi i \theta \left( -\frac{1+\tau}{2} \right)} = -\theta \left( \frac{1+\tau}{2} \right).
$$

Thus $z = \frac{1+\tau}{2}$ is a zero of $\theta(z)$.

**Lemma 6.3.8.** All zeroes of $\theta(z, t)$ are simple and are of the form $\frac{1+\tau}{2} + \ell \in \Lambda$.

**Lemma 6.3.9.** For $x \in \mathbb{C}$, set $\theta^{(x)}(z, \tau) = \theta \left( z - \frac{1+\tau}{2} - x \right)$. Then $\theta^{(x)}(z) = \theta^{(x)}(z, \tau)$ satisfies:

(1) $\theta^{(x)}(z + 1) = \theta^{(x)}(z)$.

(2) $\theta^{(x)}(z + \tau) = e^{-\pi i (2(z-x) - 1)} \theta^{(x)}(z)$.

We now prove Abel’s theorem (6.3.6).

**Proof.** Given such a set $\{a_i\} \subset \Pi$, let $x_1, \ldots, x_n$ be the list of all $a_i$ with $m_i > 0$, listed with repetitions corresponding to the number $m_i$. For example, if $m_1 = 2$ then $x_1 = x_2 = a_1$. Likewise, let $y_1, \ldots, y_n$ be the list of all $a_i$ with $m_i < 0$, once again with repetitions. By the hypothesis $\sum m_i = 0$, there are indeed an equal number of each. Set

$$
f(z) = \frac{\prod_{i=1}^{n} \theta^{(x_i)}(z)}{\prod_{i=1}^{n} \theta^{(y_i)}(z)}.
$$

Then by Lemma 6.3.9, $f(z + 1) = f(z)$. On the other hand, the lemma also gives

$$
f(z + \tau) = \frac{\prod_{i=1}^{n} \theta^{(x_i)}(z + \tau)}{\prod_{i=1}^{n} \theta^{(y_i)}(z)} = e^{2\pi i \left( \sum_{i=1}^{n} x_i - \sum_{i=1}^{n} y_i \right)} f(z) = e^{2\pi i \sum m_i a_i} f(z) = f(z) \text{ since } \sum m_i a_i = 0.
$$

Therefore $f(z)$ is elliptic. \qed
Note that $\theta(z)$ is a meromorphic function, so by complex analysis, the integral
\[
\frac{1}{2\pi i} \int_{\partial \Pi} \frac{\theta'(z)}{\theta(z)} \, dz
\]
counts the number of zeroes of $\theta(z)$ in the fundamental domain $\Pi$, up to multiplicity. To ensure no zeroes lying on $\partial \Pi$ are missed, we may shift $\Pi \to \Pi_\alpha$ for an appropriate $\alpha \in \mathbb{C}$. Parametrize $\partial \Pi$ as in Proposition 6.1.5. Then once again the integrals along $\gamma_2$ and $\gamma_4$ cancel since $\theta(z + 1) = \theta(z)$. On the other hand,
\[
\begin{align*}
\theta(z + \tau) &= e^{-\pi i (\tau + 2z)} \theta(z) \\
\implies \theta'(z + \tau) &= e^{-\pi i (\tau + 2z)} (-2\pi i \theta(z) + \theta'(z)) \\
\implies \frac{\theta'(z + \tau)}{\theta(z + \tau)} &= -2\pi i + \frac{\theta'(z)}{\theta(z)}.
\end{align*}
\]
This implies
\[
\int_{\partial \Pi} \frac{\theta'(z)}{\theta(z)} \, dz = \int_{\gamma_1} \frac{\theta'(z)}{\theta(z)} \, dz + \int_{\gamma_2} \frac{\theta'(z)}{\theta(z)} \, dz + \int_{\gamma_3} \frac{\theta'(z)}{\theta(z)} \, dz + \int_{\gamma_4} \frac{\theta'(z)}{\theta(z)} \, dz
\]
\[
= \left( \int_{\gamma_1} \frac{\theta'(z)}{\theta(z)} \, dz + \int_{\gamma_3} \frac{\theta'(z)}{\theta(z)} \, dz \right) + \left( \int_{\gamma_2} \frac{\theta'(z)}{\theta(z)} \, dz + \int_{\gamma_4} \frac{\theta'(z)}{\theta(z)} \, dz \right)
\]
\[
= \left( \int_{\gamma_1} \frac{\theta'(z)}{\theta(z)} \, dz - \int_{\gamma_1} \frac{\theta'(z)}{\theta(z)} \, dz + 2\pi i \right) + 0
\]
\[
= 2\pi i.
\]
It follows that $\theta(z)$ has exactly one zero in $\Pi$, and it must be $z = \frac{1+\tau}{2}$.

The inverse map $\psi : E \to \mathbb{C}/\Lambda$ extends to the group of divisors on $E$:
\[
\Psi : \text{Div}(E) \to \mathbb{C}/\Lambda \\
\sum n_P P \mapsto \sum n_P \psi(P).
\]

**Definition.** The map $\Psi : \text{Div}(E) \to \mathbb{C}/\Lambda$ is called the **Abel-Jacobi map**.

Recall that $\psi : P \mapsto \int_{\gamma_P} \omega + \Lambda \in \mathbb{C}/\Lambda$ where $\omega$ is a fixed holomorphic differential form on $E$ and $\gamma_P$ is a path connecting $O \in E(\mathbb{C})$ to $P$. If $O'$ is another basepoint and $\psi'$ is the corresponding map, we have $\psi(P) = \psi'(O') + \psi'(P)$ for all $P \in E$. So it appears that $\Psi$ is not well-defined. However, this issue vanishes when we restrict $\Psi$ to $\text{Div}^0(E)$: if $D = \sum n_P P$ is a degree 0 divisor, then
\[
\Psi(D) = \sum n_P \psi(P)
\]
\[
= \sum n_P (\psi(O') + \psi'(P))
\]
\[
= \psi(O') \sum n_P + \sum n_P \psi'(P)
\]
\[
= 0 + \sum n_P \psi'(P) = \Psi'(D).
\]
114
Corollary 6.3.10. The map $\Psi : \text{Div}^0(E) \to \mathbb{C}/\Lambda$ induces an isomorphism $\text{Pic}^0(E) \cong \mathbb{C}/\Lambda$.

Proof. One can prove that $\Psi$ is a surjective group homomorphism. Moreover, Abel’s theorem (6.3.6) implies that $\ker \Psi = \text{PDiv}(E)$. \qed

Consider the map $i_O : E \to \text{Div}^0(E)$ that sends $P \mapsto P - O$. This fits into a commutative diagram:

$$
\begin{array}{ccc}
\text{Div}^0(E) & \xrightarrow{\Psi} & \mathbb{C}/\Lambda \\
i_O \downarrow & & \downarrow \psi_O \\
E & \xrightarrow{\psi_O} & \mathbb{C}/\Lambda
\end{array}
$$

On the level of the Picard group, this diagram looks like

$$
\begin{array}{ccc}
\text{Pic}^0(E) & \xrightarrow{\overline{\Psi}} & \mathbb{C}/\Lambda \\
i_O \downarrow & & \downarrow \psi_O \\
E & \xrightarrow{\psi_O} & \mathbb{C}/\Lambda
\end{array}
$$

and every arrow is a bijection.

6.4 Jacobians of Higher Genus Curves

Let $C$ be a complex curve of genus $g \geq 2$ and let $V = \Gamma(C, \Omega_C)$ be the vector space of holomorphic differential forms on $C$. Then $\dim \mathbb{C} V = g$, so $V^* \cong \mathbb{C}^g$. As in the previous section, for any path $\omega$ in $C$ the assignment $\varphi_\gamma : \omega \mapsto \int_\gamma \omega$ defines a functional $\varphi_\gamma \in V^*$. As for elliptic curves, we define:

Definition. The lattice of periods for $C$ is

$$
\Lambda = \{\varphi_\gamma \in V^* \mid \gamma \text{ is a closed curve in } C\}.
$$

Lemma 6.4.1. $\Lambda$ is a lattice in $V^*$.

Definition. The Jacobian of $C$ is the quotient space $J(C) = V^*/\Lambda$.

As with elliptic curves, we have a map $\psi : C \to J(C)$ called the Abel-Jacobi map, which sends $P \mapsto \varphi_{\gamma_P} + \Lambda$, where $\gamma_P$ is a curve through $P$. Also, $\psi$ extends to the divisor group of $C$ as a map

$$
\Psi : \text{Div}(C) \longrightarrow J(C)
$$

which is canonical when restricted to $\text{Div}^0(C)$. The Abel-Jacobi theorem generalizes Theorem 6.3.6 and Corollary 6.3.10.
Theorem 6.4.2. Let $C$ be a curve of genus $g > 0$ and let $\Psi : \text{Div}^0(C) \to J(C)$ be the Abel-Jacobi map. Then

1. (Abel) $\ker \Psi = \text{PDiv}(C)$.
2. (Jacobi) $\Psi$ is surjective.

Therefore $\Psi$ induces an isomorphism $\text{Pic}^0(C) \cong J(C)$.

Just as with elliptic curves, if we fix a basepoint $O \in C$, the map $i_O : C \to \text{Div}^0(C), P \mapsto P - O$ determines a commutative diagram

\[
\begin{array}{ccc}
\text{Pic}^0(C) & \xrightarrow{\Phi} & J(C) \\
\downarrow{i_O} & & \downarrow{\psi_O} \\
C & \xrightarrow{\psi_O} & J(C)
\end{array}
\]

However, this time not every map is a bijection. In particular, $\dim C = 1 < g = \dim J(C)$. To remedy this, let $C^g$ be the $g$-fold product of $C$ and consider the map

$$\psi^g : C^g \longrightarrow J(C)$$

$$(P_1, \ldots, P_g) \mapsto \psi(P_1) + \ldots + \psi(P_g)$$

where $+$ denotes the group law on $J(C)$.

Theorem 6.4.3 (Jacobi). $\psi^g : C^g \longrightarrow J(C)$ is surjective.

There is still work to do to show that the natural map $C^g \to \text{Pic}^0(C)$ is surjective. It turns out that $J(C)$ is birationally equivalent to the symmetric power $C^{(g)} = C^g / \sim$, where $(P_1, \ldots, P_g) \sim (P_{\sigma(1)}, \ldots, P_{\sigma(g)})$ for any permutation $\sigma \in S_g$. Jacobi proved that this birational equivalence is enough to endow $\text{Pic}^0(C) \cong J(C)$ with the structure of an algebraic group.

Theorem 6.4.4. $J(C)$ is an abelian variety.
7 Complex Multiplication

We saw in Section 4.1 that many endomorphisms of an elliptic curve are of the form \([m] : P \mapsto mP\) for \(m \in \mathbb{Z}\). In fact, for most elliptic curves, these are the only endomorphisms, but a special class of curves admit extra endomorphisms which are the starting place for a beautiful theory of complex multiplication in number theory.

In class field theory, one classifies all abelian extensions of a number field \(K\) by studying complex roots of unity, i.e. torsion points of the group scheme \(\mathbb{G}_m(\mathbb{C})\), and using them to construct cyclotomic extensions of \(K\) – by the Kronecker-Weber theorem, all abelian extensions are subfields of such cyclotomic fields. In a completely analogous way, the theory of complex multiplication allows one to construct, for an elliptic curve \(E\) for which \(\text{End}(E)\) has extra elements coming from a number field \(K\), abelian extensions of \(K\). Namely, torsion points of \(E\) along with the \(j\)-invariant will generate all such fields.

7.1 Classical Complex Multiplication

For an elliptic curve \(E/\mathbb{C}\), let \(\Lambda \subset \mathbb{C}\) be the lattice associated to \(E\) by Theorem 6.2.5. Write \(\Lambda = [\omega_1, \omega_2]\) for \(\omega_1, \omega_2 \in \mathbb{C}\).

**Definition.** An order in a number field \(K/\mathbb{Q}\) is a subring \(O\) of \(K\) that is finitely generated as an abelian group and satisfies \(O \otimes \mathbb{Z} \mathbb{Q} = K\).

**Proposition 7.1.1.** For a complex elliptic curve \(E = \mathbb{C}/\Lambda\), where \(\Lambda = [\omega_1, \omega_2]\), either

1. \(\text{End}(E) \cong \mathbb{Z}\); or
2. \(\text{End}(E)\) is an order in the imaginary quadratic field \(\mathbb{Q} \left( \frac{\omega_2}{\omega_1} \right)\).

**Proof.** We may assume \(\omega_1 = 1\) and \(\omega_2 = \tau \in \mathbb{C} \setminus \mathbb{R}\). As we saw in the proof of Corollary 6.2.9,

\[
\text{End}(E) = \{ z \in \mathbb{C} | z\Lambda \subseteq \Lambda \}.
\]

So for any \(z \in \text{End}(E)\), we can find integers \(a, b, c\) and \(d\) such that \(z = a + b\tau\) and \(\tau z = c + d\tau\). Solving for \(\tau\) in each and combining the equations, we obtain

\[
z^2 - (a + d)z + (ad - bc) = 0,
\]

so in particular \(z\) is an algebraic integer. This shows \(\text{End}(E)\) is an integral extension of \(\mathbb{Z}\). If \(\text{End}(E) \neq \mathbb{Z}\), take \(z \in \text{End}(E) \setminus \mathbb{Z}\). Then \(b \neq 0\) and we can solve for \(z\) in each of the equations above to produce

\[
br^2 - (a - d)\tau - c = 0.
\]

Since \(b \neq 0\), this means \(\tau\) is a complex root of a quadratic polynomial, so \(\mathbb{Q}(\tau)\) is an imaginary quadratic field. Further, \(\text{End}(E)\) is contained in \(\mathbb{Q}(\tau)\) and is an integral extension of \(\mathbb{Z}\), so it is therefore an order.

**Definition.** An elliptic curve \(E\) over the complex numbers has complex multiplication, abbreviated CM, if \(\text{End}(E)\) is an order in an imaginary quadratic field.
Proposition 7.1.2. Let $E/\mathbb{C}$ be an elliptic curve with complex multiplication via an order $\mathcal{O} \subset K$. Then there is a unique isomorphism of abelian groups $[\cdot] : \mathcal{O} \to \text{End}(E)$ such that for any invariant differential $\omega \in \Omega_E$, we have $[\alpha]^*\omega = \alpha \omega$ for all $\alpha \in \mathcal{O}$.

Proof. Fix an isomorphism $\varphi : \mathbb{C}/\Lambda \isom E$ for a lattice $\Lambda$ and for each $\alpha \in \mathcal{O}$, define $[\alpha] : \text{End}(E)$ by the following commutative diagram:

$$
\begin{array}{ccc}
\mathbb{C}/\Lambda & \xrightarrow{m_\alpha} & \mathbb{C}/\Lambda \\
\downarrow{\varphi} & & \downarrow{\varphi} \\
E & \xrightarrow{[\alpha]} & E
\end{array}
$$

where $m_\alpha$ denotes multiplication by $\alpha$. Let $\omega \in \Omega_E$ be an invariant differential on $E$. By Lemma 2.4.1, $\omega \in \Omega_E$ and $dz \in \Omega_{\mathbb{C}/\Lambda}$ are each unique up to scaling, so $\varphi^*\omega = a dz$ for some $a \in \mathbb{C}$. By commutativity, we get $\varphi^*[\alpha]^*\omega = m_\alpha^*\varphi^*\omega = m_\alpha a dz = \alpha a dz$ which implies $[\alpha]^*\omega = \alpha \omega$ as desired. \qed

Corollary 7.1.3. Suppose $\varphi : E_1 \to E_2$ is an isogeny between elliptic curves with complex multiplication via the same order $\mathcal{O}$. Write $[\cdot]_1 : \mathcal{O} \isom \text{End}(E_1)$ and $[\cdot]_2 : \mathcal{O} \isom \text{End}(E_2)$. Then for all $\alpha \in \mathcal{O}$, $\varphi \circ [\alpha]_1 = [\alpha]_2 \circ \varphi$.

Proof. Take $\omega \in \Omega_{E_2}$. Then by Proposition 7.1.2,

$$(\varphi \circ [\alpha]_1)^*\omega = [\alpha]_1^* \varphi^*\omega = \alpha \varphi^*\omega = \varphi^*(\alpha \omega) = \varphi^*[\alpha]_2^*\omega = ([\alpha]_2 \circ \varphi)^*\omega.$$ 

Therefore $(\varphi \circ [\alpha]_1)^* = ([\alpha]_2 \circ \varphi)^*$, but since $\varphi^*$ is nonzero by Theorem 4.1.10, we must have $(\varphi \circ [\alpha]_1) = [\alpha]_2 \circ \varphi$. \qed

For an order $\mathcal{O}$ in an imaginary quadratic field $K$, let $\text{Ell}(\mathcal{O})$ denote the set of isomorphism classes of elliptic curves $E/\mathbb{C}$ with $\text{End}(E) \cong \mathcal{O}$.

Theorem 7.1.4. Let $K$ be a number field with ring of integers $\mathcal{O}_K$, class group $C_K$ and nonzero fractional ideals $a, b \subset K$. Then for any lattice $\Lambda \subset \mathbb{C}$ with associated elliptic curve $E = \mathbb{C}/\Lambda$ lying in $\text{Ell}(\mathcal{O}_K)$,

(a) $a\Lambda$ and $b\Lambda$ are lattices.

(b) If $E_a = \mathbb{C}/a\Lambda$, then $\text{End}(E_a) \cong \mathcal{O}_K$.

(c) $E_a \cong E_b$ if and only if $[a] = [b]$ in $C_K$.

(d) $C_K$ acts simply transitively on $\text{Ell}(\mathcal{O}_K)$.

(e) In particular, $# \text{Ell}(\mathcal{O}_K) = h_K$, the class number of $K$. 

118
Proof. (a) follows from the fact that \(a\Lambda\) is a discrete subgroup of \(\Lambda\); this is standard to prove.

(b) For all \(\alpha \in \mathbb{C}\), \(\alpha a\Lambda \subseteq \Lambda\) is equivalent to \(a\Lambda \subseteq \Lambda\), after multiplying through by \(a^{-1}\).

This shows that
\[
\text{End}(E_a) = \{\alpha \in \mathbb{C} \mid \alpha a\Lambda \subseteq a\Lambda\} = \{\alpha \in \mathbb{C} \mid a\Lambda \subseteq \Lambda\} = \text{End}(E) = \mathcal{O}_K
\]

by Corollary 6.2.9.

(c) By Corollary 6.2.7, \(E_a \cong E_b\) if and only if the lattices \(a\Lambda\) and \(b\Lambda\) are homothetic, i.e. \(a\Lambda = cb\Lambda\) for some \(c \in \mathbb{C}\). So
\[
E_a \cong E_b \iff a\Lambda = cb\Lambda \text{ for some } c \in \mathbb{C}
\]
\[
\iff \Lambda = ca^{-1}b\Lambda \text{ and } \Lambda = c^{-1}ab^{-1}\Lambda \text{ for some } c \in \mathbb{C}
\]
\[
\iff ca^{-1}b, c^{-1}ab^{-1} \subseteq \mathcal{O}_K \text{ for some } c \in \mathbb{C}
\]
\[
\iff ca^{-1}b = \mathcal{O}_K = c^{-1}ab^{-1} \text{ for some } c \in \mathbb{C}
\]
\[
\iff a = cb \text{ for some } c \in \mathbb{K}
\]
\[
\iff [a] = [b] \text{ in } C_K.
\]

(d) Define the action of \(C_K\) on \(\text{Ell}(\mathcal{O}_K)\) by \([a] \cdot E = E_{a^{-1}}\). Fix \(E_1, E_2 \in \text{Ell}(\mathcal{O}_K)\) with \(E_1 = \mathbb{C}/\Lambda_1\) and \(E_2 = \mathbb{C}/\Lambda_2\). For \(j = 1, 2\), choose \(\lambda_j \in \Lambda_j\) and set \(a_j = \lambda_j^{-1}\Lambda_j\). By the proof of Proposition 7.1.1, \(a_j \subseteq K\) and it is a finitely generated abelian group since \(\Lambda_j\) is, so \(a_j\) is a fractional ideal of \(K\). Set \(a = a_2^{-1}a_1\). Then \(\Lambda_2 = \lambda_1^{-1}\lambda_2a_1^{-1}a_2\Lambda_1\) so we have
\[
[a] \cdot E_1 = E_{a^{-1}} = \mathbb{C}/a^{-1}\Lambda_1 = \mathbb{C}/\lambda_1^{-1}\lambda_2\Lambda_2 \cong \mathbb{C}/\Lambda_2 = E_2.
\]

Thus the action is transitive. To see that it is simply transitive, note that by (c), if \([a] \cdot E = [b] \cdot E\) then \([a] = [b]\). Then (e) follows immediately.

Example 7.1.5. For the lattice \(\Lambda = \mathbb{Z}[i]\), the Gaussian integers, set \(E = \mathbb{C}/\Lambda\). Then \(\text{End}(E) \cong \mathbb{Z}[i]\) so \(E\) has complex multiplication. Moreover, \(\text{Aut}(E) = \{\pm 1, \pm i\} \cong \mathbb{Z}/4\mathbb{Z}\) and \(j(E) = 1728\) by analysis of the Weierstrass equation, so \(E\) is isomorphic to the elliptic curve given by \(y^2 = x^3 + x\). To see this explicitly, note that \(i\Lambda = \Lambda\) implies \(g_3(\Lambda) = g_3(i\Lambda) = i^9g_3(\Lambda) = -g_3(\Lambda)\), where \(g_3(\Lambda)\) is the normalized Eisenstein series for \(\Lambda\) (see Section 6.2). Thus \(g_3(\Lambda) = 0\) so by Theorem 6.2.4, \(E\) has Weierstrass equation
\[
E : y^2 = 4x^3 - g_2(\Lambda)x.
\]

This also confirms that \(j(E) = 1728\). Note that although \(E\) is isomorphic to a rational elliptic curve, e.g. \(y^2 = x^3 + x\), the above Weierstrass equation is not rational. In fact,
\[
g_2(\Lambda) = 64 \left( \int_0^1 \frac{dt}{\sqrt{1-t^4}} \right)^4.
\]

Example 7.1.6. Similarly, consider the lattice \(\Lambda = \mathbb{Z}[\rho]\) where \(\rho = e^{2\pi i/3}\) is a primitive third root of unity. Then for \(E = \mathbb{C}/\Lambda\), we have \(\text{End}(E) = \mathbb{Z}[\rho]\) so once again, \(E\) has complex multiplication. Let us describe \(E\) explicitly as in the previous example. First, \(\rho\Lambda = \Lambda\) implies \(g_3(\Lambda) = g_3(\rho\Lambda) = \rho^4g_2(\Lambda) = \rho g_2(\Lambda)\), so \(g_2(\Lambda) = 0\). By Theorem 6.2.4, \(E\) is given by the Weierstrass equation
\[
E : y^2 = 4x^3 - g_3(\Lambda)
\]
so \(j(E) = 0\). Moreover, \(\text{Aut}(E) = \{\pm 1, \pm \rho, \pm \rho^2\} \cong \mathbb{Z}/6\mathbb{Z}\) and \(E\) is isomorphic to the rational elliptic curve \(y^2 = x^3 + 1\).
7.2 Torsion and Rational Points

Elliptic curves with complex multiplication possess richer structure than those without CM, in several ways. In this section we will study how the group of torsion points on a CM curve change. Then we will see how rational points can be studied systematically.

We begin by generalizing the torsion subgroup $E[m] = E_m$ introduced in Chapter 4. Suppose $E \in \text{Ell}(O_K)$ for an imaginary quadratic field $K$. For each ideal $a \subseteq O_K$, define

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

where $[\cdot]$ is the isomorphism $O_K \xrightarrow{\sim} \text{End}(E)$ defined in Proposition 7.1.2.

**Proposition 7.2.1.** For any $O_K$-ideal $a$, there is an isogeny $\varphi_a : E \to [a] \cdot E$ such that

(a) $\ker \varphi_a = E[a]$.

(b) $E[a]$ is a free module over $O_K/a$ of rank 1.

**Proof.** The isogeny is given by $\varphi_a : C/\Lambda \to C/a^{-1}\Lambda$, $z \mapsto z$ which is well-defined since $\Lambda \subseteq a^{-1}\Lambda$ when $a$ is an (integral) ideal of $O_K$. Then (a) is easily verified and (b) can be proven using the Chinese remainder theorem – see Silverman’s *Advanced Topics* for details. □

**Corollary 7.2.2.** Let $\mathfrak{N} = \mathfrak{N}_{K/Q}$ be the ideal norm of the extension $K/Q$. Then

(a) For any ideal $a \subset O_K$, the isogeny $\varphi_a : E \to [a] \cdot E$ has degree $\mathfrak{N}a$.

(b) In particular, for all $\alpha \in O_K$, the isogeny $[\alpha] : E \to E$ has degree $|N\alpha|$ where $N = N_{K/Q}$ is the field norm.

**Proof.** (a) By Proposition 7.2.1, $\deg \varphi_a = \#E[a] = \mathfrak{N}a$.

(b) This follows from the fact that if $a = (\alpha)$, then $[a] = [\alpha]$, the image of $\alpha$ in $\text{End}(E)$ under the isomorphism in Proposition 7.1.2. In this case, we have $\deg[\alpha] = \mathfrak{N}(\alpha) = |N_{K/Q}\alpha|$ by part (a). □

Next, we turn to a discussion of rational points of elliptic curves with complex multiplication. Note that for any complex elliptic curve $E$, there is an isomorphism $\text{End}(E^\sigma) \cong \text{End}(E)$ for any automorphism $\sigma : \mathbb{C} \to \mathbb{C}$.

**Proposition 7.2.3.** Let $K$ be an imaginary quadratic field. Then

(a) For any elliptic curve $E/\mathbb{C}$ with complex multiplication by $O_K$, $j(E) \in \overline{\mathbb{Q}}$.

(b) $\text{Ell}(O_K)$ is equal to the set of $\overline{\mathbb{Q}}$-isomorphism classes of elliptic curves defined over $\overline{\mathbb{Q}}$ with $\text{End}(E) \cong O_K$.

**Proof.** (a) Set $L = \mathbb{Q}(j(E))$; we must show that $[L : \mathbb{Q}] < \infty$. For any $\sigma \in \text{Aut}(\mathbb{C})$, $E^\sigma$ is the curve obtained by letting $\sigma$ act on the Weierstrass equation for $E$, so by definition $j(E^\sigma) = j(E)^\sigma$. Since $\text{End}(E^\sigma) \cong O_K$ for each $\sigma$, there are only finitely many $\mathbb{C}$-isomorphism classes that $E^\sigma$ can take on. By Proposition 3.2.1, elliptic curves over $\mathbb{C}$ are in bijective
7.2 Torsion and Rational Points 7 Complex Multiplication

correspondence with $j$-invariants, so $\{j(E)^\sigma \mid \sigma \in \text{Aut}(\mathbb{C})\}$ is a finite set. Hence $[L : \mathbb{Q}] < \infty$ as desired.

(b) For each subfield $L \subseteq \mathbb{C}$, let $\text{Ell}_L(\mathcal{O}_K)$ denote the set of $L$-isomorphism classes of elliptic curves defined over $L$ with $\text{End}(E) \cong \mathcal{O}_K$. Any fixed embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ induces a map $\text{Ell}_{\overline{\mathbb{Q}}}(\mathcal{O}_K) \rightarrow \text{Ell}_C(\mathcal{O}_K)$. To show this is a bijection, first take $E \in \text{Ell}_C(\mathcal{O}_K)$. Then by (a), $j(E) \in \overline{\mathbb{Q}}$ and by Propositions 3.2.1 and 3.2.2, there exists an elliptic curve $E'$ defined over $\mathbb{Q}(j(E))$ with $j(E') = j(E)$ and $E' \cong E$ over $\mathbb{C}$. Thus $\text{Ell}_{\overline{\mathbb{Q}}}(\mathcal{O}_K) \rightarrow \text{Ell}_C(\mathcal{O}_K)$ is surjective. Injectivity follows from Proposition 3.2.1.

We will later show that in the above situation, $j(E) \in \overline{\mathbb{Z}}$. To lay the groundwork for this, we next find the field of definition for each isogeny $[\alpha] : E \rightarrow E$ from Proposition 7.1.2.

**Theorem 7.2.4.** Let $E$ be an elliptic curve with complex multiplication via some order $\mathcal{O} \subseteq \mathbb{C}$. Then

1. For all $\alpha \in \mathcal{O}$ and $\sigma \in \text{Aut}(\mathbb{C})$, $[\alpha]_E^\sigma = [\sigma \alpha]_{E^\sigma}$.

2. Suppose $E$ is defined over a subfield $L \subseteq \mathbb{C}$ and $\mathcal{O} \subseteq K$ for an imaginary quadratic field $K$. Then every element of $\text{End}(E)$ is defined over $LK$.

3. If, in addition, $E'$ is an elliptic curve defined over $L$, then every isogeny $E \rightarrow E'$ is defined over some finite extension $M/L$.

**Proof.** (1) For any $\omega \in \Omega_E$, $\sigma \cdot \omega \in \Omega_{E^\sigma}$ so by Proposition 7.1.2,

$$[\sigma \alpha]_{E^\sigma}^E(\sigma \cdot \omega) = \sigma \alpha(\sigma \cdot \omega) = \sigma \cdot (\alpha \omega) = \sigma \cdot [\alpha]_{E^\sigma}^E \omega = ([\alpha]_{E^\sigma}^E)^\sigma(\sigma \cdot \omega).$$

Hence $[\sigma \alpha]_{E^\sigma}^E = ([\alpha]_{E}^E)^\sigma$ so Theorem 4.1.10 implies $[\sigma \alpha]_{E^\sigma} = [\alpha]_E^\sigma$ since we are in characteristic 0.

(2) Take $\sigma \in \text{Aut}(\mathbb{C}/L)$. Then $E^\sigma = E$ so by (a), we have $[\alpha]_{E}^\sigma = [\sigma \alpha]_{E^\sigma} = [\sigma \alpha]_{E}$ for all $\alpha \in \mathcal{O}$. Given that $\mathcal{O} \subseteq K$, if $\sigma$ also fixes $K$ then $\sigma \alpha = \alpha$. Thus $[\alpha]_{E}^\sigma = [\alpha]_{E}$ for all $\sigma \in \text{Aut}(\mathbb{C}/LK)$, meaning $[\alpha] = [\alpha]_{E}$ is defined over $LK$. But by Proposition 7.1.2, these are all the elements of $\text{End}(E)$.

(3) Fix an isogeny $\varphi : E \rightarrow E'$ and suppose $\sigma \in \text{Aut}(\mathbb{C}/L)$. Then $\varphi^\sigma$ is an isogeny $E \rightarrow E'$ as well, since the Weierstrass equations of $E, E'$ are fixed under $\sigma$. By Proposition 4.1.9, $\varphi$ is determined by its kernel which is a finite subgroup of $E(\mathbb{C})$. There are only finitely many finite subgroups of $E(\mathbb{C})$, so we see that there are only finitely many isogenies $E \rightarrow E'$ of a given degree. Therefore $\{\varphi^\sigma \mid \sigma \in \text{Aut}(\mathbb{C}), \sigma \text{ fixes } L\}$ is a finite set (noting that $\deg \varphi^\sigma = \deg \varphi$) which implies $\varphi$ is defined over a finite extension of $L$. Repeating the argument for any $\varphi$ gives an extension $M/L$, but since $\text{Hom}(E, E')$ is finitely generated, we may take $M/L$ to be a finite extension.

**Corollary 7.2.5.** If $E$ is an elliptic curve with complex multiplication via $\mathcal{O}_K$ where $K$ is an imaginary quadratic field, then $[\mathbb{Q}(j(E)) : \mathbb{Q}] \leq h_K$, the class number of $K$.

We will later show that $[\mathbb{Q}(j(E)) : \mathbb{Q}] = h_K$, so in particular $j(E)$ is rational if and only if $K$ is an imaginary quadratic field with class number 1. As there are only a finite number of such number fields, it follows that only a finite number of $\mathbb{Q}$-isomorphism classes of elliptic curves have complex multiplication.

121
Example 7.2.6. Consider the elliptic curve $E$ defined by $y^2 = x^3 + x$, which admits an isomorphism $[\cdot] : \mathbb{Z}[i] \to \text{End}(E)$ by Proposition 7.1.2. Explicitly, $[\cdot]$ is determined by $[i] : (x,y) \mapsto (-x, iy)$ since if $\sigma \in \text{Aut}(\mathbb{C})$ is complex conjugation, then

$([i](x,y))^\sigma = (-x, iy)^\sigma = (-\tau \cdot x, \tau \cdot (iy)) = (-\tau \cdot x, -i(\tau \cdot x)) = [-i](\tau \cdot x, \tau \cdot y) = [i]^\tau(x, y)^\tau$.

Thus $[i]^\tau = [\tau \cdot i]$, which confirms (2) of Theorem 7.2.4.

Theorem 7.2.7. Let $E$ be a complex elliptic curve with complex multiplication by $\mathcal{O}_K$ and let $L = K(j(E), E_{\text{tors}})$ be the field extension generated by $j(E)$ along with all torsion points of $E$. Then $L$ is an abelian extension of $K(j(E))$.

Proof. Set $L' = K(j(E))$ and for each $m \geq 1$, let $L_m = L'(E[m])$ be the extension of $L'$ generated by the $m$-torsion points of $E$. Then $L = \bigcup_{m \geq 1} L_m$ so it suffices to show each $L_m/L'$ is abelian. For each $\sigma \in \text{Gal}(L_m/L')$, $P \in E[m]$ and $\alpha \in \mathcal{O}_K$, Theorem 7.2.4 gives us

$([\alpha]P)^\sigma = [\alpha](P^\sigma)$

so the actions of $\text{Gal}(L_m/L')$ and $\mathcal{O}_K$ on $E[m]$ commute. This induces a group homomorphism

$\rho : \text{Gal}(\overline{K}/L') \to \text{Aut}_{\mathcal{O}_K/m\mathcal{O}_K}(E[m])$

where $\overline{K}$ is an algebraic closure of $K$, which descends to an injective homomorphism

$\text{Gal}(L_m/L') \to \text{Aut}_{\mathcal{O}_K/m\mathcal{O}_K}(E[m])$

but by Proposition 7.2.1(b), $E[m]$ is a free $\mathcal{O}_K/m\mathcal{O}_K$-module of rank 1. Thus $\text{Aut}_{\mathcal{O}_K/m\mathcal{O}_K}(E[m]) \cong (\mathcal{O}_K/m\mathcal{O}_K)^\times$ which is abelian, so $\text{Gal}(L_m/L')$ is abelian as required. \qed

Let $K$ be an imaginary quadratic field with ring of integers $\mathcal{O}_K$ and define

$F : \text{Gal}(\overline{K}/K) \to C_K$

by sending $\sigma$ to the unique element $F(\sigma) = [a] \in C_K$ such that $[a] \cdot E = E^\sigma$ for all elliptic curves $E \in \text{Ell}(\mathcal{O}_K)$. (Existence and uniqueness of this element follow from Theorem 7.1.4). The following results highlight an interesting fact: $F$ converts the algebraic information of the absolute Galois group of $K$ into the analytic information of elliptic curves over $\mathbb{Q}$, via their $j$-invariants.

Lemma 7.2.8. For all $\sigma \in \text{Gal}(\overline{K}/K)$ and all elliptic curves $E \in \text{Ell}(\mathcal{O}_K)$,

$j(E)^\sigma = j(E_F(\sigma))$.

Proposition 7.2.9. The map $F : \text{Gal}(\overline{K}/K) \to C_K$ is a group homomorphism.

Proof. For all $\sigma, \tau \in \text{Gal}(\overline{K}/K)$ and $E \in \text{Ell}(\mathcal{O}_K)$, we have

$F(\sigma \tau) \cdot E = E^{\sigma \tau} = (E^\tau)^\sigma = (F(\tau) \cdot E)^\sigma = F(\sigma) F(\tau) \cdot E$

so by definition, $F(\sigma \tau) = F(\sigma) F(\tau)$. \qed
Proposition 7.2.10. For all elliptic curves $E \in \text{Ell}(\mathcal{O}_K)$, classes $[a] \in C_K$ and automorphisms $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, $([a] \cdot E)\sigma = [a]\sigma \cdot E\sigma$.

Proof. By Proposition 7.2.3 we may assume $E$ is defined over $\overline{\mathbb{Q}}$, so $E\sigma$ makes sense. Choose a lattice $\Lambda \subset \mathbb{C}$ so that $E \cong \mathbb{C}/\Lambda$. Also, since $a$ is a finitely generated $\mathcal{O}_K$-module, we have an exact sequence

$$\mathcal{O}_K^m \rightarrow \mathcal{O}_K^n \rightarrow a \rightarrow 0$$

for some $m, n \in \mathbb{N}$. Note that for any $\mathcal{O}_K$-module $M$, the map

$$a^{-1}M \rightarrow \text{Hom}_{\mathcal{O}_K}(a, M)$$

$$x \mapsto (\alpha \mapsto \alpha x)$$

is an isomorphism of $\mathcal{O}_K$-modules. In particular, $\text{Hom}_{\mathcal{O}_K}(a, \Lambda) \cong a^{-1}\Lambda$ and $\text{Hom}_{\mathcal{O}_K}(a, \mathbb{C}) \cong \mathbb{C}$. Now applying $\text{Hom}_{\mathcal{O}_K}(a, -)$ to the exact sequence

$$0 \rightarrow \Lambda \rightarrow \mathbb{C} \rightarrow E \rightarrow 0$$

yields the top row in the following commutative diagram:

$$
\begin{array}{c}
0 \\
\downarrow \\
0 \\
\downarrow \\
0 \\
\downarrow \\
0 \\
\downarrow \\
0 \\
\downarrow \\
0 \\
\downarrow \\
0
\end{array}
\begin{array}{cccc}
0 & 0 & 0 & 0 \\
a^{-1}\Lambda & \mathbb{C} & \text{Hom}(a, E) & \\
\Lambda^n & \mathbb{C}^n & E^n & 0 \\
\Lambda^m & \mathbb{C}^m & E^m & 0
\end{array}
$$

(The other rows come from applying $\text{Hom}(\mathcal{O}_K^m, -)$ and $\text{Hom}(\mathcal{O}_K^n, -)$ to the same sequence.) Applying the Snake Lemma to the bottom rows gives an exact sequence

$$0 \rightarrow a^{-1}\Lambda \rightarrow \mathbb{C} \rightarrow \ker(E^n \rightarrow E^m) \rightarrow \text{coker}(\Lambda^n \rightarrow \Lambda^m).$$

This identifies the $\mathbb{C}$-points of the variety $[a] \cdot E = \mathbb{C}/a^{-1}\Lambda$ with the identity component of $\ker(E^n \rightarrow E^m)$. The same argument shows that the $\mathbb{C}$-points of $[a]\sigma \cdot E\sigma$ may be identified with the identity component of $\ker((E^n)^\sigma \rightarrow (E^m)^\sigma)$, but the latter is precisely $\ker(E^n \rightarrow E^m)^\sigma$, so we conclude that $[a]\sigma \cdot E\sigma = ([a] \cdot E)^\sigma$. $\square$

7.3 Class Field Theory with Elliptic Curves

Let $K$ be an imaginary quadratic field with ring of integers $K$. Our goal in this section is to prove that for any elliptic curve $E \in \text{Ell}(\mathcal{O}_K)$, $K(j(E))$ is the maximal unramified abelian
extension of $K$, also known as the *Hilbert class field* of $K$. To start, note that the kernel of the homomorphism $F : \text{Gal}(\overline{K}/K) \to C_K$ from Proposition 7.2.9 is a finite quotient of $\text{Gal}(\overline{K}/K)$ since any elliptic curve $E \in \text{Ell}(\mathcal{O}_K)$ is defined over a finite extension $L/K$, so $F(\sigma) = 1$ for any $\sigma \in \text{Gal}(\overline{K}/L)$. Also observe that since $C_K$ is an abelian group, $F$ factors through a homomorphism

$$\text{Gal}(K^{ab}/K) \to C_K$$

where $K^{ab}$ is the maximal abelian extension of $K$. We will also denote this by $F$.

Recall that for a field extension $L/K$ and a prime ideal $p \subset \mathcal{O}_K$, a *Frobenius element* of $p$ is an element $\text{Frob}_{L/K}(p) \in \text{Gal}(L/K)$, uniquely determined up to conjugacy by the identity

$$\text{Frob}_{L/K}(p)(x) \equiv x^{N_p} \mod \mathfrak{P}$$

for all $x \in \mathcal{O}_L$, where $\mathfrak{N} = \mathfrak{N}_{K/Q}$ is the numerical norm on $K$ and $\mathfrak{P}$ is any prime ideal of $\mathcal{O}_L$ lying over $p$. For an arbitrary fractional ideal $a = \prod p_{\mathfrak{P}}^{n_{\mathfrak{P}}}$ of $K$, the definition of Frobenius elements extends to the *Artin symbol*:

$$\left(\frac{L/K}{a}\right) = \prod \text{Frob}_{L/K}(p)^{n_p}.$$

Below we summarize the Artin reciprocity theorem and its main consequence for ray class fields, which constitute most of the information from global class field theory needed for this section. If $a \subset \mathcal{O}_K$ is an integral ideal, let $I_K(a)$ and $P_K(a)$ denote respectively the ideal class group and principal subgroup mod $a$, meaning the group (and principal subgroup) of ideal classes $[b]$ such that $(a, b) = 1$.

**Theorem 7.3.1** (Artin Reciprocity). *Let $L/K$ be a finite abelian extension of number fields with conductor $f_{L/K}$. Then*

(a) *The Artin map $\left(\frac{L/K}{a}\right) : I_K(f_{L/K}) \to \text{Gal}(L/K)$, $a \mapsto \left(\frac{L/K}{a}\right)$ is surjective.*

(b) *The kernel of $\left(\frac{L/K}{a}\right)$ is $\mathfrak{N}_{L/K}(I_L)P_K(f_{L/K})$, where $\mathfrak{N}_{L/K}$ is the ideal norm of $L/K$.*

(c) *For any ideal $a \subset \mathcal{O}_K$, there exists a unique finite abelian extension $K_a$ of $K$, called a ray class field for $a$, such that for any finite abelian extension $M/K$, if $f_{M/K} | a$ then $M \subseteq K_a$.*

(d) *The set of primes in $K$ that split completely in $K_a$ are precisely the prime ideals in $P_K(a)$.***

**Proposition 7.3.2.** *For all but finitely many prime integers $p \in \mathbb{Z}$, if $p$ splits in $K$ then $F(\text{Frob}_{L/K}(p)) = [p]$ in $C_K$ for each of the two primes $p \subset \mathcal{O}_K$ lying over $p$.***

**Theorem 7.3.3.** *Let $K$ be an imaginary quadratic field with ring of integers $\mathcal{O}_K$ and let $E$ be an elliptic curve with complex multiplication via $\mathcal{O}_K$. Then*
(a) $K(j(E))$ is the Hilbert class field of $K$.

(b) $[K(j(E)) : K] = \left[ \mathbb{Q}(j(E)) : \mathbb{Q} \right] = h_K$, the class number of $K$.

(c) If $E_1, \ldots, E_m$ is a list of representatives of the isomorphism classes in $\text{Ell}(O_K)$, then $m = h_K$ and $j(E_1), \ldots, j(E_m)$ are all the Galois conjugates of $j(E)$.

(d) For any nonzero fractional ideal $a$ of $K$,

$$j(E)^{\theta(a)} = j([a] \cdot E)$$

where $\theta = \left( \frac{K(j(E))/K}{\cdot} \right)$ is the Artin symbol for the Hilbert class field of $K$.

Proof. (a) As noted above, $F : \text{Gal}(\overline{K}/K) \to C_K$ has a finite kernel. Let $L = \overline{K}^{\ker F}$ be the corresponding finite extension of $K$. Then

$$\text{Gal}(\overline{K}/L) = \ker F = \{ \sigma \in \text{Gal}(\overline{K}/K) \mid F(\sigma) = 1 \}$$

$$= \{ \sigma \in \text{Gal}(\overline{K}/K) \mid F(\sigma) \cdot E = E \} \quad \text{by Theorem 7.1.4(d)}$$

$$= \{ \sigma \in \text{Gal}(\overline{K}/K) \mid E^\sigma = E \} \quad \text{by definition of } F(\sigma)$$

$$= \{ \sigma \in \text{Gal}(\overline{K}/K) \mid j(E)^\sigma = j(E) \} = \{ \sigma \in \text{Gal}(\overline{K}/K) \mid j(E) = j(E) \} \quad \text{by Proposition 3.2.1}$$

$$= \text{Gal}(\overline{K}/K(j(E))) = \text{Gal}(\overline{K}/K).$$

By the fundamental theorem of Galois theory, this shows $L = K(j(E))$. On the other hand, $F$ restricts to an injection $\text{Gal}(L/K) \hookrightarrow C_K$ so $L/K$ is an abelian extension. Let $\mathfrak{f} = \mathfrak{f}_{L/K}$ be the conductor of the extension $L/K$ and consider the composition

$$I(\mathfrak{f}) \xrightarrow{\text{Frob}} \text{Gal}(L/K) \xrightarrow{F} C_K$$

of $F$ with the Artin map. We claim $\varphi(\mathfrak{a}) = [\mathfrak{a}]$ for all ideals $\mathfrak{a} \in I(\mathfrak{f})$. By Proposition 7.3.2, there exists a finite set of prime integers $S \subset \mathbb{Z}$ such that $F(\text{Frob}(\mathfrak{p})) = [\mathfrak{p}] \in C_K$ for all $\mathfrak{p}$ lying over primes $p \not\in S$ which split in $K$. By Dirichlet’s theorem on number fields, there exists such a prime $\mathfrak{p}$ with $[\mathfrak{p}] = [\mathfrak{a}]$ in $C_K$, say with $\mathfrak{a} = (\alpha)p$ for $\alpha \in K^\times, \alpha \equiv 1 \mod \mathfrak{f}$. Then $F(\text{Frob}((\alpha))) = 1$ in $C_K$ so

$$F(\text{Frob}(\mathfrak{a})) = F(\text{Frob}((\alpha)p)) = F(\text{Frob}(p)) = [\mathfrak{p}] = [\mathfrak{a}].$$

In fact this now implies that $F(\text{Frob}((\alpha))) = 1$ for any principal ideal in $I(\mathfrak{f})$, but since $F$ is injective, this means $\left( \frac{L/K}{\alpha} \right) = 1$ for all $(\alpha) \in I(\mathfrak{f})$. By definition of the conductor, we get $\mathfrak{f} = 1$ so $L/K$ is unramified and thus $L$ is contained in the Hilbert class field. On the other hand, $I(\mathfrak{f}) = I_K \to C_K$ is now surjective, hence an isomorphism, so we get

$$[L : K] = |\text{Gal}(L/K)| = |C_K| = h_K$$

which is precisely the degree of the Hilbert class field over $K$, so $L$ is the Hilbert class field.
(b) The above shows $[K(j(E)) : K] = h_K$ and in Corollary 7.2.5 we already showed that $[\mathbb{Q}(j(E)) : \mathbb{Q}] \leq h_K$, but since $[K : \mathbb{Q}] = 2$, we must have $[\mathbb{Q}(j(E)) : \mathbb{Q}] = h_K$ as well.

(c) From Theorem 7.1.4 we have $m = h_K$ and $C_K$ acts transitively on these curves, but then by Proposition 3.2.1, $C_K$ acts transitively on the $j$-invariants of these curves, $j(E_1), \ldots, j(E_m)$. In fact the homomorphism $F : \text{Gal}(\overline{K} / K) \to C_K$ identifies the action of $\text{Gal}(\overline{K} / K)$ on $j$-invariantes with the action of $C_K$ on elliptic curves, so $\text{Gal}(\overline{K} / K)$ also acts transitively on $j(E_1), \ldots, j(E_m)$ and hence these are the $h_K$ Galois conjugates of $j(E)$.

(d) By (a), $\theta(a) = [a]$ for any $a \in I_K$, so the statement holds. \qed