THE RIEMANN-ROCH THEOREM AND ELLIPTIC CURVES

JET CHUNG

Abstract. The Riemann-Roch theorem lets us compute the dimension of the space of meromorphic functions with controlled zeros and poles. This paper will present a proof of the Riemann-Roch theorem using sheaf cohomology. We will also introduce the basic theory of elliptic curves, including the uniformization theorem and the group law. In particular, we will see that the Riemannn-Roch theorem provides more enlightening proofs than elementary methods.

Contents

Date: May 2021.

Introduction

Motivating Question: Rational Points on Elliptic Curves. Consider an elliptic curve E defined over $\mathbb{C}$; for now, we'll say this is the locus of the points $(x, y) \in \mathbb{C}^2$ such that $y^2 = 4x^3 - g_2x - g_3$ for some fixed constants $g_2, g_3 \in \mathbb{C}$ where $g_2^3 - 27g_3^2 \neq 0$. We are interested in the rational points of E, denoted $E(\mathbb{Q}) = \{(x, y) \in \mathbb{Q}^2 : y^2 = 4x^3 - g_2x - g_3\}$. Given a set of rational points, one way to generate more is to take a rational point $\mathcal{O}$, and define an operation as follows. Given two rational points A and B, let the line ℓ through A and B intersect E at C. Then, draw the line ℓ' through $\mathcal{O}$ and C, and let it intersect E at $A + B$. Then $A + B$ is a rational point. One may ask:

- Is $E(\mathbb{Q})$ finite or infinite?
- If $E(\mathbb{Q})$ is finite, how do we compute its size?
- Can we generate $E(\mathbb{Q})$ by the process defined above? Is the set of starting points needed to do this finite?
- How many rational points do we expect a random elliptic curve E to have?
- Does $E(\mathbb{Q})$ carry any structure?

The Riemann-Roch Theorem. Consider a compact Riemann surface X of genus g; the *Riemann-Roch theorem* will aim to determine the dimension of the complex vector space of meromorphic functions on X with controlled zeros and poles. In particular, let D be a formal sum of points $\sum n_iP_i$. Then $\mathscr{O}_D$ gives the complex vector space of meromorphic functions f such that at each point P, $\mathrm{ord}_{P_i}(f) + n_i \geq 0$ (see Section 2).

The Riemann-Roch theorem states that:

$$\dim H^0(X, \mathscr{O}_D) - \dim H^1(X, \mathscr{O}_D) = 1 - g + \deg D.$$

Serre duality will allow us to interpret the first cohomology group of the sheaf $\mathscr{O}_D$ as global sections of the sheaf $\mathscr{O}_{K-D}$. We find

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

where $\ell(D) = \dim H^0(X, \mathscr{O}_D)$. The second form of the theorem allows us to more easily derive consequences of Riemann-Roch, as the zeroth cohomology group simply gives us the global sections.

We see that Riemann-Roch theorem implies that any compact Riemann surface can be embedded into $\mathbb{P}^N$ for some N, and in particular, that elliptic curves can be embedded in $\mathbb{P}^2$. We will also see the theorems of Abel and Jacobi imply that a compact Riemann surface can be embedded into its Jacobian, and that any genus 1 Riemann surface is isomorphic to a complex torus.

Elliptic Curves. Using the theory we develop, we prove the uniformization theorem for elliptic curves that says, roughly, that elliptic curves correspond to complex tori. More precisely, given a complex torus $\mathbb{C}/\Lambda$, we can embed it into $\mathbb{P}^2$ by

$$\varphi : z \mapsto \begin{cases} (\wp(z) : \wp'(z) : 1) \text{ if } z \notin \Lambda \\ \mathcal{O} \text{ if } z \in \Lambda \end{cases}.$$

Since $\wp'(z)^2 = 4\wp(z) - g_2(\Lambda)\wp(z) - g_3$, by $y = \wp'(z)$ and $x = \wp(z)$, this induces an elliptic curve E_Λ, and furthermore, φ is a group isomorphism. Conversely, one wonders if, given an elliptic curve $E : y^2 = 4x^3 - g_2x - g_3$, if there is a complex torus $\mathbb{C}/\Lambda$ such that $E_\Lambda \cong E$. We will see that this is the case.

We will also give a natural explanation of the group law for elliptic curves.

Assumed Background. We will assume the reader knows some basic concepts from complex analysis and algebra. We freely use results from Section 5.1 before they are stated - in part, because they can be proven with elementary complex analysis. Other than that, we have tried to keep the prerequisites to a minimum - in particular, we have tried to avoid categorical constructions when possible.

1. Sheaf Cohomology

1.1. Complexes.

Definition 1.1. A *cochain complex* $C^\bullet$ is a sequence of abelian groups or modules along with homomorphisms such that the image of the previous homomorphism is contained in the kernel of the next homomorphism:

$$\cdots \xrightarrow{\delta_{i-1}} C^i \xrightarrow{\delta_i} C^{i+1} \xrightarrow{\delta_{i+1}} C^{i+2} \xrightarrow{\delta_{i+2}} C^{i+3} \xrightarrow{\delta_{i+3}} \cdots$$

and $\operatorname{Im}\delta_i \subseteq \ker\delta_{i+1}$ for all i. Note that this is equivalent to $\delta_{i+1}\circ\delta_i = 0$. Each δ_i is called a *boundary operator*. A complex is *exact* if $\operatorname{Im}\delta_i = \ker\delta_{i+1}$ for each i. Elements in the kernel of δ are called *cocycles*, and elements in the image of δ are called *coboundaries*. Finally, the *i-th cohomology* $H^i(C^\bullet)$ is defined as $\ker\delta_{i+1}/\operatorname{Im}\delta_i$.

Remark. There is also a notion of a *chain complex*, where the indices are decreasing rather than increasing, but this won't be important for our discussion.

Definition 1.2. An exact sequence of the form

$$0 \longrightarrow L \xrightarrow{\alpha} M$$

is called a *monomorphism* and an exact sequence of the form

$$M \xrightarrow{\beta} N \longrightarrow 0$$

is called an *epimorphism.*

Proposition 1.3. *Consider a complex*

$$0 \longrightarrow L \xrightarrow{\alpha} M \xrightarrow{\beta} N \longrightarrow 0$$

Then the complex is exact if and only if α *is a monomorphism,* β *is an epimorphism, and* $\operatorname{Im}\alpha = \ker\beta$.

Proof. Follows from the definitions. ■

We call such a complex a *short exact sequence.*

Proposition 1.4. *Let*

$$0 \xrightarrow{\delta_0} U \xrightarrow{\delta_1} V \xrightarrow{\delta_2} W \xrightarrow{\delta_3} 0$$

be a short exact sequence of finite-dimensional vector spaces. Then $\dim(V) = \dim(U) + \dim(W)$.

Proof. By the first isomorphism theorem, we have $\operatorname{Im}\delta_2 \cong V/\ker\delta_2$ and $\operatorname{Im}\delta_1 \cong U/\ker\delta_1$. Since the sequence is exact, we have $0 = \operatorname{Im}\delta_0 = \ker\delta_1$ and $\operatorname{Im}\delta_1 = \ker\delta_2$. Then

$$W = \ker\delta_3 = \operatorname{Im}\delta_2 \cong V/\ker\delta_2 = V/\operatorname{Im}\delta_1 \cong V/U$$

so

$$\dim(W) = \dim(V/U) = \dim(V) - \dim(U)$$

and

$$\dim(V) = \dim(U) + \dim(W)$$

as desired. ■

Definition 1.5. Let the Euler characteristic of a complex $C^\bullet$ be

$$\chi(C^\bullet) = \sum_i (-1)^i \dim(H^i(C^\bullet)).$$

Proposition 1.6. *If* $C^\bullet$ *is an exact sequence, then* $\chi(C^\bullet) = 0$.

Proof. [Alu09] p. 335. ■

Proposition 1.7 (The Snake Lemma)**.** *Consider the following diagram*

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & \ker\lambda \arrow[r] \arrow[d] & \ker\mu \arrow[r] \arrow[d] & \ker\nu \arrow[d] \arrow[dddll, rounded corners, "\delta"] & \\
0 \arrow[r] & L_0 \arrow[r, "\alpha_0"] \arrow[d] & M_0 \arrow[r, "\beta_0"] \arrow[d] & N_0 \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & L_1 \arrow[r, "\alpha_1"] \arrow[d] & M_1 \arrow[r, "\beta_1"] \arrow[d] & N_1 \arrow[r] \arrow[d] & 0 \\
 & \mathrm{coker}\lambda \arrow[r] \arrow[d] & \mathrm{coker}\mu \arrow[r] \arrow[d] & \mathrm{coker}\nu \arrow[d] & \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

where

$$\begin{tikzcd}
0 \arrow[r] & L_0 \arrow[r, "\alpha_0"] \arrow[d, "\lambda"] & M_0 \arrow[r, "\beta_0"] \arrow[d, "\mu"] & N_0 \arrow[r] \arrow[d, "\nu"] & 0 \\
0 \arrow[r] & L_1 \arrow[r, "\alpha_1"] & M_1 \arrow[r, "\beta_1"] & N_1 &
\end{tikzcd}$$

commutes. Then there is an exact sequence of the form

$$\begin{tikzcd}
0 \arrow[r] & \ker\lambda \arrow[r] & \ker\mu \arrow[r] & \ker\nu \arrow[r, "\delta"] & \mathrm{coker}\lambda \arrow[r] & \mathrm{coker}\mu \arrow[r] & \mathrm{coker}\nu
\end{tikzcd}$$

Proof. Omitted. ■

1.2. **Sheaves.**

Definition 1.8. A *presheaf* tells us the following data: to each open set $U \subseteq X$, we associate a set $\mathscr{F}(U)$ called the *sections* of $\mathscr{F}$ over U; we call $\mathscr{F}(X)$ the *global sections*. Typically, the sections are abelian groups. We also need restriction maps $\mathrm{res}_U^V : \mathscr{F}(V) \to \mathscr{F}(U)$ for any open sets $U \subseteq V \subseteq X$ satisfying:

- $\mathrm{res}_U^U = \mathrm{id}$
- $\mathrm{res}_U^V \circ \mathrm{res}_V^W = \mathrm{res}_U^W$ for any $U \subseteq V \subseteq W$; i.e. the following diagram commutes:

$$\begin{tikzcd}
\mathscr{F}(W) \arrow[rr, "\mathrm{res}_U^W"] \arrow[dr, "\mathrm{res}_V^W"'] & & \mathscr{F}(U) \\
 & \mathscr{F}(V) \arrow[ur, "\mathrm{res}_U^V"'] &
\end{tikzcd}$$

Definition 1.9. A presheaf is a *sheaf* if it satisfies the following two properties:

- **Identity**: If $\{U_i\}_{i\in I}$ is an open cover of U, $f, g \in \mathscr{F}(U)$ and $f\big|_{U_i} = g\big|_{U_i}$ for all $i \in I$, then $f = g$ (elements of $\mathscr{F}(U)$ are determined by their restriction to an open cover $\{U_i\}_{i\in I}$)
- **Gluability**: Let $f_i \in \mathscr{F}(U_i)$. If $f_i\big|_{U_i\cap U_j} = f_j\big|_{U_i\cap U_j}$ for all $i, j \in I$, then $\exists f \in \mathscr{F}(U)$ such that $f\big|_{U_i} = f_i$ for all $i \in I$.

Identity means there is at most one way to join sections, and gluability means that there is at least one way to join sections.

Our most important examples of sheaves will be the holomorphic and meromorphic functions.

Example 1.10.

- Let $\mathscr{O}(U)$ be the set of holomorphic functions defined on U. The restriction maps are defined in the natural way: if $U \subseteq V$ and $f \in \mathscr{F}(V)$, then let $\operatorname{res}_U^V(f) = f\big|_U \in \mathscr{F}(U)$. Then, $\mathscr{O}$ can be seen to be a sheaf.
- Let Ω be the sheaf of holomorphic 1-forms on a compact Riemann surface X, that is, symbols that locally look like $\omega = f(z)dz$ for f holomorphic (recall that X locally looks like $\mathbb{C}$ as a Riemann surface is a one dimensional complex manifold).
- Let $\mathscr{M}$ be the sheaf of meromorphic functions.
- Let $\mathscr{M}^{(1)}$ be the sheaf of meromorphic 1-forms.
- On a connected topological space, we can define a constant sheaf which simply associates the same set to each open set U. In particular, we are interested in the sets $\mathbb{Z}$ and $\mathbb{C}$; these contain topological information about X.

Example 1.11. An example of a presheaf that is not a sheaf is the set of bounded functions on $\mathbb{C}$. For example, if we cover $\mathbb{C}$ by $U_n = \{z \in \mathbb{C} : |z| < n\}$ for $n \in \mathbb{N}$, then the function $f(z) = z$ is bounded on each U_n and agrees on intersections, but cannot be glued over all of $\mathbb{C}$ to give a bounded function.

1.3. **Stalks and Germs.** Say we have a presheaf $\mathscr{F}$ on a topological space X, and consider a point $a \in X$. We define an equivalence relation on the disjoint union

$$\bigsqcup_{U \ni a} \mathscr{F}(U)$$

over all open neighborhoods U of a as follows: for $f \in \mathscr{F}(U)$ and $g \in \mathscr{F}(V)$, $f \sim_a g$ if and only if there is an open set W with $a \in W \subseteq U \cap V$ such that $f\big|_W = g\big|_W$.

Definition 1.12. The *stalk* of $\mathscr{F}$ at a is given by

$$\mathscr{F}_a = \left(\bigsqcup_{U \ni a} \mathscr{F}(U) \right) \Big/ \sim_a .$$

Definition 1.13. Let U be an open set, and let $a \in U$. Then consider the function $\rho_a : \mathscr{F}(U) \to \mathscr{F}_a$ which sends a section to its equivalence class modulo $\sim_a$. We call $\rho_a(f)$ the *germ* of f at a.

The idea is that we want to have more information than just the point a itself; we want to know the behaviour around a. However, no open set is small enough to only contain information about a. Thus, a germ can be thought of as a point with additional information. Similarly, we can think of the stalk at a point as being the set of possible germs.

Example 1.14. Let $X = \mathbb{R}$, and let $\mathscr{F}$ be the sheaf of real valued smooth functions on X. Then the germ at a point tells us the derivatives at a point $p \in \mathbb{R}$. This is not enough to tell us the sections. However, if we consider the sheaf of holomorphic functions on $\mathbb{C}$, then we *can* determine the sections!

1.4. **Cohomology.** Let X be a topological space, and let $\mathfrak{U} = (U_i)_{i \in I}$ be an open cover of X. Also, fix a sheaf of abelian groups $\mathscr{F}$ on X. For each non-negative integer q, we define

$$C^q(\mathfrak{U}, \mathscr{F}) = \prod_{i_0 < i_1 < \ldots < i_q} \mathscr{F}(U_{i_0, i_1, \ldots, i_q})$$

where $U_{i_0, i_1, \ldots, i_q} = U_{i_0} \cap U_{i_1} \cap \cdots \cap U_{i_q}$ An element $\alpha \in C^q(\mathfrak{U}, \mathscr{F})$ is determined by taking an element $\alpha_{i_0, \ldots, i_q} \in \mathscr{F}(U_{i_0 \ldots, i_q})$ for each $q+1$ tuple in I. We can also define the coboundary map $\delta_q : C^q(\mathfrak{U}, \mathscr{F}) \to C^{q+1}(\mathfrak{U}, \mathscr{F})$ by

$$(\delta_q \alpha)_{i_0, \ldots, i_{q+1}} = \sum_{k=0}^{q+1} (-1)^k \alpha_{i_0, \ldots, \hat{i}_k, \ldots, i_{q+1}} \Big|_{U_{i_0, \ldots, i_{q+1}}}$$

Example 1.15. Say we have a sheaf of abelian groups on a topological space X, and consider the coboundary map from $C^3(\mathfrak{U}, \mathscr{F}) \to C^4(\mathfrak{U}, \mathscr{F})$. Then

$$(\delta\alpha)_{i_0, i_1, i_2, i_3, i_4} = \alpha_{i_1, i_2, i_3, i_4} - \alpha_{i_0, i_2, i_3, i_4} + \alpha_{i_0, i_1, i_3, i_4} - \alpha_{i_0, i_1, i_2, i_4} + \alpha_{i_0, i_1, i_2, i_3}.$$

We might hope that this actually gives a complex. Given $\alpha \in C^2(\mathfrak{U}, \mathscr{F})$, we can calculate $(\delta_3 \circ \delta_2)(\alpha)$:

$$\delta_3(\delta_2\alpha))_{i_0,i_1,i_2,i_3,i_4} = (\delta_2\alpha)_{,i_1,i_2,i_3,i_4} - (\delta_2\alpha)_{i_0,i_2,i_3,i_4} + (\delta_2\alpha)_{i_0,i_1,i_3,i_4} - (\delta_2\alpha)_{i_0,i_1,i_2,i_4} + (\delta_2\alpha)_{i_0,i_1,i_2,i_3}$$

and substituting, we find

$$\begin{aligned}
\delta_3(\delta_2\alpha))_{i_0,i_1,i_2,i_3,i_4} &= (\alpha_{i_2,i_3,i_4} - \alpha_{i_1,i_3,i_4} + \alpha_{i_1,i_2,i_4} - \alpha_{i_1,i_2,i_3}) \\
&\quad - (\alpha_{i_2,i_3,i_4} - \alpha_{i_0,i_3,i_4} + \alpha_{i_0,i_2,i_4} - \alpha_{i_0,i_2,i_3}) \\
&\quad + (\alpha_{i_1,i_3,i_4} - \alpha_{i_0,i_3,i_4} + \alpha_{i_0,i_1,i_4} - \alpha_{i_0,i_1,i_3}) \\
&\quad - (\alpha_{i_1,i_2,i_4} - \alpha_{i_0,i_2,i_4} + \alpha_{i_0,i_1,i_4} - \alpha_{i_0,i_1,i_2}) \\
&\quad + (\alpha_{i_1,i_2,i_3} - \alpha_{i_0,i_2,i_3} + \alpha_{i_0,i_1,i_3} - \alpha_{i_0,i_1,i_2}) \\
&= 0
\end{aligned}$$

Proposition 1.16. *$\delta_{q+1} \circ \delta_q = 0$: in particular, $C^\bullet(\mathfrak{U}, \mathscr{F})$ is a cochain complex of abelian groups.*

Proof. Consider the matrix of indices that are skipped in the α's. Given a coordinate (n, m), if $n < m$, then the sign is $+$ if and only if $n \not\equiv m \pmod 2$, while if $n > m$, then the sign is $+$ if and only if $n \equiv m \pmod 2$. Thus, the sum is 0. ■

Definition 1.17. Call

$$Z^q(\mathfrak{U}, \mathscr{F}) = \ker(C^q(\mathfrak{U}, \mathscr{F}) \to C^{q+1}(\mathfrak{U}, \mathscr{F}))$$

the *q-cocycles* and

$$B^q(\mathfrak{U}, \mathscr{F}) = \operatorname{Im}(C^{q-1}(\mathfrak{U}, \mathscr{F}) \to C^q(\mathfrak{U}, \mathscr{F}))$$

the *q-coboundaries.* Note that, in particular, each coboundary is a cocycle. Then we define

$$H^q(\mathfrak{U}, \mathscr{F}) = Z^q(\mathfrak{U}, \mathscr{F})/B^q(\mathfrak{U}, \mathscr{F})$$

to be the *q-th cohomlogy group* with coefficients in $\mathscr{F}$ with respect to $\mathfrak{U}$.

Remark. We note that the cohomology groups defined above depend on the open covering $\mathfrak{U}$ of X - thus, we have constructed the Čech cohomology. However, once we have defined the Čech cohomology, sheaf cohomology can be defined in a natural way. The construction is omitted but can be found in ([For81], §12).

Definition 1.18. Let

$$H^q(X, \mathscr{F}) = \varinjlim_{\mathfrak{U}} H^q(\mathfrak{U}, \mathscr{F})$$

be the *sheaf cohomology.*

If we're going to just take the direct limit of the Čech cohomology to obtain the sheaf cohomology, why do we bother with Čech? The upshot is that it's easier to compute with Čech cohomology.

Theorem 1.19 (Leray)**.** *Let $\mathscr{F}$ be a sheaf of abelian groups, and let $\mathfrak{U} = \{U_i\}_{i \in I}$ be an open covering of X such that $H^1(U_i, \mathscr{F}) = 0$ for each $i \in I$. Then*

$$H^1(X, \mathscr{F}) \cong H^1(\mathfrak{U}, \mathscr{F}).$$

$\mathfrak{U}$ is then called a Leray covering *for $\mathscr{F}$.*

Example 1.20 (The Exponential Sheaf Sequence)**.** Let $\mathscr{O}^*$ be the sheaf of nonvanishing holomorphic functions. Then the exponential map $\exp : \mathscr{O} \to \mathscr{O}^*$ is a sheaf homomorphism, and in particular induces a short exact sequence

$$0 \longrightarrow 2\pi i\mathbb{Z} \longrightarrow \mathscr{O} \longrightarrow \mathscr{O}^* \longrightarrow 0$$

on stalks: given a nonvanishing function germ, we can locally compute its logarithm. However, it is not necessarily globally exact: for example, in a nonsimply connected space, a function may not have a global logarithm.

Let X be a compact Riemann surface, and let $\mathscr{F}$ be a sheaf of abelian groups on X. We construct a complex like so:

$$0 \longrightarrow C^0(X,\mathscr{F}) \xrightarrow{\delta_0} C^1(X,\mathscr{F}) \xrightarrow{\delta_1} C^2(X,\mathscr{F}) \longrightarrow \dots$$

Similarly to above, let $Z^1(X,\mathscr{F}) = \ker\delta_1$ be the 1-cocycles, and $B^1(X,\mathscr{F}) = \operatorname{Im}\delta_0$ be the 1-coboundaries. Then the *first cohomology* group $H^1(X,\mathscr{F})$ is $\ker\delta_1/\operatorname{Im}\delta_0 = Z^1(X,\mathscr{F})/B^1(X,\mathscr{F})$.

Proposition 1.21. *Let $\mathscr{F}$ be a sheaf. Then the* zeroth cohomology group *$H^0(X,\mathscr{F})$ simply gives the sections $\mathscr{F}(X)$.*

Proof. We consider $H^0(X,\mathscr{F})$ by looking at the complex

$$0 \longrightarrow C^0(X,\mathscr{F}) \xrightarrow{\delta_0} C^1(X,\mathscr{F}) \longrightarrow \cdots$$

so that $H^0(X,\mathscr{F}) = \ker\delta_0$. Note that $(\delta_0\alpha)_{i_0,i_1} = \alpha_{i_1} - \alpha_{i_0}$, so an element α of the kernel is one where $\alpha_i = \alpha_j$ for each $i,j \in I$. Thus, by the definition of a sheaf, α is a constant on X. We conclude $H^0(X,\mathscr{F}) = \mathscr{F}(X)$. ■

Proposition 1.22. *For a compact Riemann surface X, $H^1(X,\mathscr{O})$ is a finite dimensional complex vector space.*

Proof. The proof uses some sophisticated tools from functional analysis and thus falls outside the scope of this paper. Details can be found in [For81]. ■

Definition 1.23. We call $g = \dim H^1(X,\mathscr{O})$ the *genus* of X.

1.5. The Exact Cohomology Sequence.

Definition 1.24. Let $\mathscr{F}$ and $\mathscr{G}$ be sheaves on a topological space X. Then a *sheaf homomorphism* $\alpha : \mathscr{F} \to \mathscr{G}$ sends

$$\alpha_U : \mathscr{F}(U) \to \mathscr{G}(U)$$

for each open set $U \subseteq X$. For open sets U, V such that $U \subseteq V \subseteq X$, we require

$$\begin{tikzcd}
\mathscr{F}(V) \arrow[r, "\alpha_V"] \arrow[d, "\operatorname{res}^V_U"'] & \mathscr{G}(V) \arrow[d, "\operatorname{res}^V_U"] \\
\mathscr{F}(U) \arrow[r, "\alpha_U"] & \mathscr{G}(U)
\end{tikzcd}$$

to commute.

Definition 1.25. Let a sequence of sheaf homomorphisms on X be *exact* if the induced homomorphism on stalks is exact for each $x \in X$.

Lemma 1.26. *Let X be a topological space and let*

$$0 \longrightarrow \mathscr{F} \xrightarrow{\alpha} \mathscr{G} \xrightarrow{\beta} \mathscr{H}$$

be an exact sequence of sheaves on X. Then for each open set $U \subseteq X$,

$$0 \longrightarrow \mathscr{F}(U) \xrightarrow{\alpha_U} \mathscr{G}(U) \xrightarrow{\beta_U} \mathscr{H}(U)$$

is exact.

Proof of Lemma 1.26.

- First, we prove that $0 \longrightarrow \mathscr{F}(U) \xrightarrow{\alpha_U} \mathscr{G}(U)$ is exact. Let $f \in \mathscr{F}(U)$ be such that $\alpha_U(f) = 0$. Note that each sequence of stalks

  $$0 \longrightarrow \mathscr{F}_x \xrightarrow{\alpha_x} \mathscr{G}_x$$

  is exact, so for each $x \in U$, there is an open neighborhood $U_x \subseteq U$ so that $f\big|_{U_x} = 0$. By the definition of a sheaf, $f = 0$. Thus, α is injective.

- Now, we prove that $\operatorname{Im} \alpha_U \subseteq \ker \beta_U$. Say that $f \in \mathscr{F}(U)$, and let $g = \alpha(f)$: note that $g \in \alpha_U$. Then since the sequence is exact on stalks, we have $g \in \operatorname{Im} \alpha = \ker \beta$, so there is an open neighborhood U_x such that $\beta(g)\big|_{U_x} = 0$. By the same argument as above, we have $\beta(g) = 0$, so $g \in \ker \beta_U$.
- Finally, we prove that $\ker \beta_U \subseteq \operatorname{Im} \alpha_U$. Say that $g \in \ker \mathscr{G}(U)$ and $\beta(g) = 0$. Then, for each x, by exactness on stalks, we have $\ker \beta_x = \operatorname{Im} \alpha_x$, so $g \in \operatorname{Im} \alpha_x$. In particular, there is a covering $(U_i)_{i \in I}$ such that for each i, there exists $f_i \in \mathscr{F}(U_i)$ such that $\alpha(f_i) = g\big|_{U_i}$. Then, $\alpha(f_i - f_j) = 0$ on $U_i \cap U_j$, so $f_i = f_j$ on $U_i \cap U_j$. Thus, there is an $f \in \mathscr{F}(U)$ such that $f\big|_{U_i} = f_i$ for each $i \in I$, and $\alpha(f) = g$.

■

Lemma 1.27. *Let X be a compact Riemann surface and let*

$$0 \longrightarrow \mathscr{F} \xrightarrow{\alpha} \mathscr{G} \xrightarrow{\beta} \mathscr{H} \longrightarrow 0$$

be a short exact sequence of sheaves on X. Then

$$\begin{tikzcd}
0 \arrow[r] & H^0(X,\mathscr{F}) \arrow[r, "\alpha_0"] & H^0(X,\mathscr{G}) \arrow[r, "\beta_0"] & H^0(X,\mathscr{H}) \arrow[dll, "\delta_*"] \\
& H^1(X,\mathscr{F}) \arrow[r] & H^1(X,\mathscr{G}) \arrow[r] & H^1(X,\mathscr{H})
\end{tikzcd}$$

is exact.

Proof outline. Since a compact Riemann surface is paracompact and Hausdorff, the derived functor cohomology agrees with the Čech cohomology (see [Whi60]). Then we use the two short exact sequences given in [Ara] on p. 28. and apply the Snake Lemma. ■

2. Riemann-Roch

Definition 2.1. Let X be a compact Riemann surface. A *divisor* on X is a formal sum of a finite number of points, $D = \sum_{i=1}^{k} n_i P_i$. The *degree* of D is $\sum_{i=1}^{k} n_i$.

$$\operatorname*{ord}_x(f) = \begin{cases} 0 & \text{if } f \text{ is holomorphic and nonzero at } x \\ -k & \text{if } f \text{ has a pole of order } k \text{ at } x \\ k & \text{if } f \text{ has a zero of degree } k \text{ at } x \\ \infty & \text{if } f \text{ is identically zero in a neighborhood of } x \end{cases}$$

Example 2.2. Let f be a meromorphic function on an open subset Y of a Riemann surface X. For a point $x \in Y$, we can define $\operatorname{ord}_x(f)$ to be the order of f at x. Then the function $x \mapsto \operatorname{ord}_x(f)$ is a divisor on X.

Definition 2.3. A divisor D is called *principal* if there is a meromorphic function $f \in \mathscr{M}(X)$ such that $D = (f)$, and two divisors D and D' are *equivalent*, written $D \sim D'$, if there $D - D' = (f)$ for some $f \in \mathscr{M}(X)$. We say a divisor D is *effective* if $D \geq 0$.

Let X be a compact Riemann surface. Then, we define $\deg : \operatorname{Div}(X) \to \mathbb{Z}$ by $\deg D = \sum_{x \in X} D(x)$. Recall that meromorphic functions on a compact Riemann surface have the same number of zeros as poles, so $\deg(f) = 0$ for any $f \in \mathscr{M}(X)$. In particular, if D and $D' \in \operatorname{Div}(X)$ are equivalent, we have $D - D' = (f)$ for some meromorphic f, so $\deg(D) - \deg(D') = \deg(f) = 0 \implies \deg(D) = \deg(D')$.

Definition 2.4. Let D be a divisor on a compact Riemann surface X. Then we construct the sheaf $\mathscr{O}_D$ along with the natural restriction map as follows: for any open set $U \subseteq X$,

$$\mathscr{O}_D(U) = \{f \in \mathscr{M}(U) : \operatorname*{ord}_x(f) \geq -D(x) \text{ for all } x \in U\}.$$

We can think of $\mathscr{O}_D$ as giving us the vector space of meromorphic functions with controlled zeros and poles. If some point P has a zero of order n, then we require $\operatorname{ord}_P(f) \geq -D(P) = -n$, so f must have a pole of order at most n. If P has a pole of order n, then f must have a zero of multiplicity at least n.

Definition 2.5. Let ω be a nontrivial meromorphic 1-form on X. Then the divisor $K = (\omega) = \sum_{x \in X} \operatorname{ord}_x(\omega)$ is the *canonical divisor* on X. This is well defined because for $\omega, \omega' \in \mathscr{M}^{(1)}(X) \setminus \{0\}$, we have

$$\frac{\omega}{\omega'} = \frac{f(z)dz}{g(z)dz} = (f/g)(z) \in \mathscr{M}(X) \setminus \{0\},$$

so that $(\omega) = (\omega')$.

Definition 2.6. Let Ω_D be the sheaf of meromorphic 1-forms ω such that $\operatorname{ord}(\omega) \geq -D$. In particular, we denote by Ω the sheaf of holomorphic 1-forms.

Lemma 2.7. *There is an isomorphism between $\mathscr{O}_{D+K}$ and Ω_D defined by $f \mapsto f\omega$, for ω a nontrivial meromorphic 1-form.*

Proposition 2.8. *If D and D' are equivalent as divisors on X, then $\mathscr{O}_D$ and $\mathscr{O}_{D'}$ are isomorphic as sheaves.*

Proof. Say that $D - D' = (f)$ for some meromorphic f. Then

$$\mathscr{O}_D = \mathscr{O}_{D'+(f)} \cong \mathscr{O}_{D'}$$

as

$$(gf) + D' = (g) + (f) + D' = (g) + D.$$

■

Proposition 2.9. *If $D \leq D'$, then there is an inclusion $\mathscr{O}_D \to \mathscr{O}_{D'}$.*

Proof. If $f \in \mathscr{O}_D$, then $\operatorname{ord}_x(f) \geq -D(x)$ for all $x \in X$. However, as $D(x) \leq D'(x)$ for all x, we have $\operatorname{ord}_x(f) \geq -D'(x)$, so $f \in \mathscr{O}_{D'}$ as desired. ■

Definition 2.10. Let X be a Riemann surface, and let P be a point of X. Then we define the *skyscraper sheaf* $\mathbb{C}_P$ by

$$\mathbb{C}_P(U) = \begin{cases} \mathbb{C} & \text{if } P \in U, \\ 0 & \text{if } P \notin U. \end{cases}$$

Lemma 2.11. *We have*

(1) $H^0(X, \mathbb{C}_P) \cong \mathbb{C}$*;*
(2) $H^1(X, \mathbb{C}_P) = 0$*.*

Proof. Note that (1) follows as the zeroth cohomology group just gives us the global sections: $H^0(X, \mathbb{C}_P) = \mathbb{C}_P(X) = \mathbb{C}$. To prove (2), consider a Leray covering $\mathfrak{U} = (U_i)_{i \in I}$ of X, and say $h \in H^1(X, \mathbb{C}_P)$. Then $Z_1(\mathfrak{U}, \mathbb{C}_P) = 0$, so $h = 0$. ■

Lemma 2.12. *For any divisor D on X and point $P \in X$,*

$$0 \longrightarrow \mathscr{O}_D \longrightarrow \mathscr{O}_{D+P} \longrightarrow \mathbb{C}_P \longrightarrow 0$$

is a short exact sequence.

Proof. First, we define $\beta : \mathscr{O}_{D+P} \to \mathbb{C}_P$ as follows: let $f \in \mathscr{O}_{D+P}$ have a Laurent expansion around $U \ni P$

$$f(z) = \sum_{n=-k-1}^{\infty} c_n z^n,$$

and let $\beta(f) = c_{-k}$. Then β is clearly surjective onto $\mathbb{C}_P$. To show that $\mathscr{O}_D \to \mathscr{O}_{D+P}$ is injective, it suffices to check on stalks. If $Q \neq P$, then

$$(\mathscr{O}_D)_Q = (\mathscr{O}_{D+P})_Q,$$

and if $Q = P$, then

$$(\mathscr{O}_D)_P \oplus \mathbb{C} = (\mathscr{O}_{D+P})_P.$$

■

Theorem 2.13 (Riemann-Roch)**.** *Let X be a compact Riemann surface with genus g, and say D is a divisor on X. Then $H^0(X, \mathscr{O}_D)$ and $H^1(X, \mathscr{O}_D)$ are finite dimensional vector spaces and*

$$(\star) \qquad \dim H^0(X, \mathscr{O}_D) - \dim H^1(X, \mathscr{O}_D) = 1 - g + \deg D$$

Proof. First, consider the case when $D = 0$. Note that $\deg D = 0$. As $g = \dim H^1(X, \mathscr{O})$, it suffices to show that $\dim H^0(X, \mathscr{O}) = 1$. Note that $H^0(X, \mathscr{O}) = \mathscr{O}(X)$, and as holomorphic functions on compact Riemann surfaces are constant, we have $[H^0(X, \mathscr{O}) : \mathbb{C}] = [\mathscr{O}(X) : \mathbb{C}] = 1$, as desired.

Now, say $P \in X$, and let D and $D + P$ be divisors on X. We will show that $(\star)$ holds for divisor D if and only if it holds for $D + P$. First, note that $\deg(D + P) - \deg(D) = 1$. By applying Lemma 1.27 to the short exact sequence in Lemma 2.12, we obtain an exact sequence:

$$\begin{tikzcd}
0 \arrow[r] & H^0(X, \mathscr{O}_D) \arrow[r] & H^0(X, \mathscr{O}_{D+P}) \arrow[r] & H^0(X, \mathbb{C}_P) \arrow[dll] \\
& H^1(X, \mathscr{O}_D) \arrow[r] & H^1(X, \mathscr{O}_{D+P}) \arrow[r] & H^1(X, \mathbb{C}_P)
\end{tikzcd}$$

By Lemma 2.11, this is equivalent to:

$$0 \longrightarrow H^0(X, \mathscr{O}_D) \longrightarrow H^0(X, \mathscr{O}_{D+P}) \xrightarrow{\varphi} \mathbb{C} \xrightarrow{\phi} H^1(X, \mathscr{O}_D) \longrightarrow H^1(X, \mathscr{O}_{D+P}) \longrightarrow 0$$

Let $V = \operatorname{Im}\varphi$ and $W = \mathbb{C}/V$. Note in particular that $\dim W + \dim V = 1$. We can split this long exact sequence into two short exact sequences:

$$\begin{tikzcd} 0 \arrow[r] & H^0(X,\mathscr{O}_D) \arrow[r] & H^0(X,\mathscr{O}_{D+P}) \arrow[r] & V \arrow[r] & 0 \\ 0 \arrow[r] & W \arrow[r] & H^1(X,\mathscr{O}_D) \arrow[r] & H^1(X,\mathscr{O}_{D+P}) \arrow[r] & 0 \end{tikzcd}$$

where the first sequence is exact because

$$\operatorname{Im}(H^0(X,\mathscr{O}_{D+P} \to V) = \operatorname{Im}\varphi = V = \ker(V \to 0)$$

and the second sequence is exact because $V = \operatorname{Im}\varphi = \ker\phi$ so

$$\operatorname{Im}(W \to H^1(X,\mathscr{O}_D)) = \operatorname{Im}(\mathbb{C}/V \to H^1(X,\mathscr{O}_D)) = \operatorname{Im}\phi = \ker(H^1(X,\mathscr{O}_D) \to H^1(X,\mathscr{O}_{D+P})).$$

By Proposition 1.4, we have

$$\dim H^0(X,\mathscr{O}_D) + \dim V = \dim H^0(X,\mathscr{O}_{D+P})$$

and

$$\dim W + \dim H^1(X,\mathscr{O}_{D+P}) = \dim H^1(X,\mathscr{O}_D)$$

so subtracting gives us

$$\dim H^0(X,\mathscr{O}_{D+P}) - \dim H^1(X,\mathscr{O}_{D+P}) - \dim W = \dim H^0(X,\mathscr{O}_D) - \dim H^1(X,\mathscr{O}_D) + \dim V.$$

Now, we have

$$\begin{aligned} &\dim H^0(X,\mathscr{O}_{D+P}) - \dim H^1(X,\mathscr{O}_{D+P}) - \deg(D+P) - 1 + g \\ &= \dim H^0(X,\mathscr{O}_D) - \dim H^1(X,\mathscr{O}_D) - \deg(D) - 1 + g \end{aligned} \tag{$\dagger$}$$

so in particular, $(\star)$ holds for D if and only if it holds for $D + P$.

Remark. We can also obtain $(\dagger)$ by applying Proposition 1.6 to the long exact sequence.

The general case follows by induction, as any arbitrary $D \in \operatorname{Div}(X)$ can be written as $D = P_1 + \ldots + P_m - P_{m-1} - \ldots - P_n$. ■

Remark. For $D \in \operatorname{Div}(X)$, $i(D) = \dim H^1(X,\mathscr{O}_D)$ is called the *index of speciality* of D. It is typically thought of as a correction term, as it disappears when the degree of D is sufficiently large.

2.1. **Serre Duality.** Let $\ell(D) = \dim H^0(X,\mathscr{O}_D)$. The zeroth cohomology group is easy to interpret: $H^0(X,\mathscr{O}_D) = \mathscr{O}_D$. But what about $H^1(X,\mathscr{O}_D)$? Serre duality tells us that $H^0(\Omega_{-D}) = H^1(\mathscr{O}_D)^\vee$, but we won't be able to prove this. We will instead prove a weaker form that says:

Proposition 2.14 (Weak Serre Duality)**.** *We have* $\dim H^1(X,\mathscr{O}_D) = \dim H^0(X,\mathscr{O}_{K-D})$*, and in particular,* $\ell(K - D) = \dim H^1(X,\mathscr{O}_D)$*.*

First, we will need the following lemma:

Lemma 2.15. *There is an injective map*

$$i_D : H^0(X,\Omega_D) \to H^1(X,\mathscr{O}_{-D});$$

in particular, $\dim H^0(X,\Omega_D) \le \dim H^1(X,\mathscr{O}_{-D})$*.*

Proof. [McM], p. 89. ■

Proof of Proposition 2.14. By Riemann-Roch, we have

$$\dim H^0(X,\mathscr{O}_{K+D}) - \dim H^1(X,\mathscr{O}_{K+D}) = 1 - g + \deg(K + D)$$

and

$$\dim H^0(X,\mathscr{O}_{-D}) - \dim H^1(X,\mathscr{O}_{-D}) = 1 - g + \deg(-D),$$

so adding gives

$$\dim H^0(X, \mathscr{O}_{K+D}) + \dim H^0(X, \mathscr{O}_{-D}) = 2 - 2g + \deg K + \dim H^1(X, \mathscr{O}_{K+D}) + \dim H^1(X, \mathscr{O}_{-D})$$

and thus

$$\dim H^0(X, \mathscr{O}_{K+D}) + \dim H^0(X, \mathscr{O}_{-D}) = \deg K + \dim H^1(X, \mathscr{O}_{K+D}) + \dim H^1(X, \mathscr{O}_{-D}).$$

By Lemma 2.7, we have $\mathscr{O}_{K+D} \cong \Omega_D$ and $\mathscr{O}_{-D} \cong \Omega_{-K-D}$, so along with Lemma 2.15, we have

$$\dim H^0(X, \mathscr{O}_{K+D}) = \dim H^0(X, \Omega_D) \leq \dim H^1(X, \mathscr{O}_{-D})$$

and

$$(*) \qquad \dim H^0(X, \mathscr{O}_{-D}) = \dim H^0(X, \Omega_{-K-D}) \leq \dim H^1(X, \mathscr{O}_{K+D}),$$

so we must have equality in both cases. Thus, by the substitution $D \mapsto D - K$ in $(*)$, we have

$$\dim H^0(X, \mathscr{O}_{K-D}) = \dim H^1(X, \mathscr{O}_D)$$

so $\ell(K - D) = \dim H^1(X, \mathscr{O}_D)$. ■

As $\ell(D) = \dim H^0(X, \mathscr{O}_D)$ and $\ell(K - D) = \dim H^1(X, \mathscr{O}_D)$, we have:

Theorem 2.16 (Riemann-Roch (Second Form))**.**

$$\boxed{\ell(D) - \ell(K - D) = 1 - g + \deg D}$$

2.2. **Consequences of Riemann-Roch.**

Proposition 2.17. *If* $\deg D < 0$*, then* $\ell(D) = 0$.

Proof. If we had some $f \in \mathscr{O}_D$, then we would have $\operatorname{ord}_x(f) \geq -D(x) > 0$ for all $x \in X$, so $\deg(f) > 0$. This is impossible, as f is meromorphic, and $\deg(f) = 0$ for any meromorphic function on a compact Riemann surface. ■

Proposition 2.18. *If* $\deg D \geq 2g - 1$*, then* $\ell(K - D) = 0$.

Proof. By $\ell(D) - \ell(K - D) = 1 - g + \deg D \geq 1 - g + 2g - 1 = g$, so

$$\begin{aligned} \ell(K - D) - \ell(D) &= 1 - g + \deg(K - D) \leq -g \\ \implies \deg(K - D) &\leq -1 \\ \implies \deg(K - D) &< 0 \end{aligned}$$

and by Proposition 2.17, we have $\ell(K - D) = 0$, as desired.

■

Proposition 2.19. $\ell(K) = g$.

Proof. Note that by considering the divisor $D = 0$, we have

$$\ell(0) - \ell(K) = \deg 0 + 1 - g \implies 1 - \ell(K) = 1 - g \implies \ell(K) = g.$$

■

Thus, there are exactly g linearly independent holomorphic 1-forms on a compact Riemann surface of genus g.

Proposition 2.20. $\deg K = 2g - 2$.

Proof. By considering the canonical divisor K, we have

$$\ell(K) - \ell(K - K) = \deg K + 1 - g \implies g - 1 = \deg K + 1 - g \implies \deg K = 2g - 2.$$

■

Proposition 2.21. *For any lattice* Λ*,* $\mathbb{C}/\Lambda$ *has genus* 1.

Proof. For any holomorphic 1-form ω on $\mathbb{C}/\Lambda$, we locally have $\omega = f(z)dz$ for f holomorphic. However, as the only holomorphic elliptic functions are the constant functions, we have $\omega = dz$. Thus, ω has no zeros or poles, and $0 = \deg(\omega) = 2g - 2 \implies g = 1$. ■

2.3. **Riemann Surfaces of Genus 0.** Consider a compact Riemann surface X of genus 0. We will verify the Rieman-Roch theorem for X explicitly.

Proposition 2.22. *For any divisor D on X, we have*

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

in particular,

(1) $\deg K = -2$
(2) $\ell(K) = 0$
(3) If $\deg D \geq 0$*, then* $\ell(D) = 1 + \deg D$*; otherwise,* $\ell(D) = 0$.

Lemma 2.23. *If* $\deg D \geq 0$*,* $\ell(D + P) = \ell(D) + 1$ *for any point* $P \in X$*.*

Proof. First, we claim that $\ell(D + P) \geq \ell(D) + 1$: we do this by constructing a function f that is in $\mathscr{O}_{D+P}$ but not $\mathscr{O}_D$. If $D = nP + \sum_{i=1}^{k} n_i P_i$, since $D + P = (n + 1)P + \sum_{i=1}^{k} n_i P_i$,

$$f(z) = (z - P_i)^{n+1} \prod_{i=1}^{k} (z - P_i)^{n_i}$$

suffices. To show that $\ell(D+P) \leq \ell(D)+1$, we note that if there are functions that attain a pole of maximal order at P, then the dimension increases by 1; otherwise, it is equal to $\ell(D)$. Thus, $\ell(D + P) = \ell(D) + 1$, as desired. ■

Proof of Proposition 2.22.

(1) Consider a 1-form $\omega = dz$; we claim it has as pole of order 2 at ∞. By the change of variables $z \mapsto \frac{1}{y}$, we have $dz = -\frac{1}{y^2}dy$, so that dz has a pole at of order 2 at $y = 0$; that is, a pole of order 2 at ∞. It has no other poles, so $K = -2 \cdot \infty$ and $\deg K = -2$.
(2) $\ell(K) = \dim H^0(X, \mathscr{O}_K) = \dim \mathscr{O}_K$, and as there are no holomorphic 1-forms on X, we have $\ell(K) = 0$.
(3) First, say $\deg D \geq 0$. Note that any divisor can be written as a finite sum of points, say $D = \sum_{i=1}^{n} P_i$ where by slight abuse of notation, we may include a point a negative number of times. Then, repeatedly applying Lemma 2.23 gives

$$\begin{aligned} \ell(D) = \ell(P_1 + \ldots + P_n) &= \ell(P_1 + \ldots + P_{n-1}) + 1 \\ &= \ell(P_1 + \ldots + P_{n-2}) + 2 \\ &= \ell(0) + n \\ &= 1 + \deg D \end{aligned}$$

as desired. If $\deg D < 0$, then $\ell(D) = 0$: $(f) + D \geq 0$, but for any meromorphic function f on X, $\deg(f) = 0$.

■

Example 2.24. Consider the divisor $D = -nP$, where n is an integer. Then the Riemann-Roch theorem follows if we can show that

$$\ell(-2 \cdot \infty + nP) = n - 1$$

for $n < 0$, which follows as

$$\left\{ \frac{1}{(z-P)^2}, \frac{1}{(z-P)^3}, \ldots, \frac{1}{(z-P)^n} \right\}$$

is a $\mathbb{C}$-basis of $\mathscr{O}_{(-2\cdot\infty - nP)}$.

3. Embedding into Projective Space

Definition 3.1. Let $\mathbb{A}^n = \{(a_1, \ldots, a_n) : a_i \in \mathbb{C}\}$ be *affine n-space* over $\mathbb{C}$.

Definition 3.2. Let $\mathbb{P}^n = \{(a_0, \ldots, a_n) \setminus \{(0, \ldots, 0)\} : a_i \in \mathbb{C}\}/\sim$ be *projective n-space* over $\mathbb{C}$, where $(a_0, \ldots, a_n) \sim (a'_0, \ldots, a'_n)$ if and only if there exists some $c \in \mathbb{C}^\times$ such that $a_i = ca'_i$ for $1 \leq i \leq n$. We write an equivalence class of a point by $(a_0 : \cdots : a_n)$.

Let $U_j = \{(z_0 : \cdots : z_N) \in \mathbb{P}^N : z_j \neq 0\}$, and define a map $\varphi_j : U_j \to \mathbb{C}^N$ by

$$\varphi_j(z_0 : \cdots : z_N) = \left(\frac{z_0}{z_j}, \ldots, \frac{\hat{z}_j}{z_j}, \ldots, \frac{z_N}{z_j}\right).$$

Note that the U_j form an open cover of $\mathbb{P}^N$, and $\varphi_j : U_j \to \mathbb{C}^N$ is a homeomorphism. They are called the *standard affine charts.* If we have a continuous function $f : X \to \mathbb{P}^N$, then the sets $W_j = f^{-1}(U_j)$ are open. Then we obtain maps

$$f_j = \varphi_j \circ f : W_j \to \mathbb{C}^N.$$

Note that each f_j gives N functions from W_j to $\mathbb{C}$, as $f_j : W_j \to \mathbb{C}^N$. Let $f_j = (f_{j1}, \ldots, f_{jN})$.

Definition 3.3. We call f *holomorphic* if each f_{jk} is holomorphic, and an *immersion* if it is holomorphic, and for each $x \in X$, there is some F_{jk} such that $x \in W_j$ and $\frac{\partial F_{jk}(x)}{\partial x} \neq 0$. Finally, f is an *embedding* if it is an injective immersion.

Theorem 3.4. *Let D be a divisor with $\deg D \geq 2g + 1$, and let $f_0, \ldots, f_N$ be a basis of $H^0(X, \mathcal{O}_D)$. Then*

$$f = (f_0 : \cdots : f_N) : X \to \mathbb{P}^N$$

is an embedding.

Proof. Omitted; [For81] p. 144 or [Nar92] p. 56. ■

Theorem 3.5. *Any compact Riemann surface can be embedded in $\mathbb{P}^3$.*

Proof. [Har77] p. 310.

■

4. Abel-Jacobi

Definition 4.1. By a curve, we mean a continuous map $c : [0,1] \to X$. Then a 1-*chain* on X is a formal sum

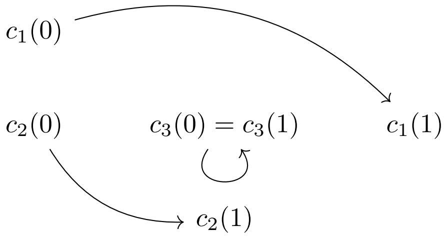
$$c = \sum_{j=1}^{m} n_j c_j$$

where the c_j are curves, and $n_j \in \mathbb{Z}$. We will denote the group of all 1-chains on X by $C_1(X)$. The integral over c of a closed differential form ω is

$$\int_c \omega = \sum_{j=1}^{m} n_j \int_{c_j} \omega.$$

We define a boundary operator $\varphi : C_1(X) \to \mathrm{Div}(X)$. Let $\partial c = \sum_{j=1}^{m} n_j \partial c_j$, where ∂ is defined on curves as follows: if c_j is a closed curve, i.e. $c_j(0) = c_j(1)$, then let $\partial c_j = 0$. Otherwise, let it be the divisor $c_j(1) - c_j(0)$. Note that, in particular, as $\deg(\partial c_j) = 0$ for any curve, we also have $\deg(\partial c) = 0$ for any 1-chain.

Example 4.2.



Proposition 4.3. *Given $D \in \mathrm{Div}_0(X)$, there is a $c \in C_1(X)$ such that $\partial c = D$.*

Proof. Say that $D = P_1 + \ldots + P_n - Q_1 - \ldots - Q_n$, where points may be repeated. Then let c_i connect Q_i and P_i with $c_i(0) = Q_i$ and $c_i(1) = P_i$. With $c = \sum_{i=1}^{n} c_i$, we have $\partial c = \sum_{i=1}^{n}(P_i - Q_i) = D$, as desired. ■

Definition 4.4. Let $Z_1(X) = \ker \partial$ be the 1-*chains*.

Remark. Note that although every $c \in C_1(X)$ satisfies $\deg(\partial c) = 0$, we do *not* always have $\partial c = 0$.

Now, define an equivalence relation as follows: for two chains $c_1, c_2 \in C_1(X)$, let $c_1 \sim c_2$ if for all closed differential forms ω (recall a closed differential form satisfies $d\omega = 0$), $\int_{c_1} \omega = \int_{c_2} \omega$; in this case, we say c_1 and c_2 are *homologous*. Then $H_1(X, \mathbb{Z}) = Z_1(X, \mathbb{Z})/\sim$ is the *first homology group* of X. Note that for any $c \in H_1(X, \mathbb{Z})$ and closed differential 1-form ω, $\int_c \omega$ is well defined.

Remark. This is similar to the fundamental group $\pi_1(X)$; in fact, $H_1(X, \mathbb{Z})$ is the abelianization of $\pi_1(X)$.

We say that $D \in \mathrm{Div}(X)$ has a solution if there is some meromorphic function $f \in \mathscr{M}(X)$ such that $(f) = D$. Clearly, since X is a compact Riemann surface, it is necessary that $\deg D = 0$. Abel's theorem will give us sufficient conditions.

Theorem 4.5 (Abel)**.** *Let X be a compact Riemann surface, and let D be a divisor with $\deg D = 0$. Then D has a solution if and only if there is some $c \in C_1(X)$ with $\partial c = D$ and $\int_c \omega = 0$ for each holomorphic 1-form ω.*

Recall that $\dim \Omega(X) = g$; take a basis $\omega_1, \ldots, \omega_g$. Then define the *period lattice* of the ω_i as follows:

$$\Gamma = \mathrm{Per}(\omega_1, \ldots, \omega_g) = \left\{ \left(\int_\alpha \omega_1, \ldots, \int_\alpha \omega_g \right) : \alpha \in H_1(X) \right\}$$

Proposition 4.6. *Γ is a lattice in $\mathbb{C}^g$, i.e.*

$$\Gamma = \gamma_1 \mathbb{Z} + \gamma_2 \mathbb{Z} + \ldots + \gamma_{2g} \mathbb{Z}$$

for some $\gamma_1, \ldots, \gamma_{2g} \in Z_1(X, \mathbb{Z})$ linearly independent over $\mathbb{R}$.

Corollary 4.7. *In particular,* $H_1(X, \mathbb{Z}) \cong \mathbb{Z}^{2g}$.

Definition 4.8. Let the Jacobian of X be defined by

$$\mathrm{Jac}(X) = \Omega(X)^\vee \Big/ \left\{ \int_c \in \Omega(X)^\vee : c \in H_1(X, \mathbb{Z}) \right\} \cong \mathbb{C}^g / \Gamma.$$

Proposition 4.9. *If* $X = \mathbb{C}/\Lambda$ *for a lattice* Λ*, then it is isomorphic to its Jacobian* $\mathrm{Jac}(X)$*.*

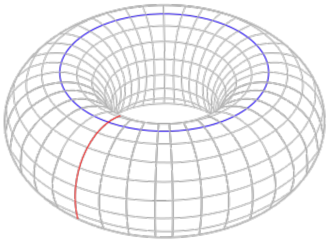


FIGURE 1. The red and blue cycles represent classes in $H_1(\mathbb{C}/\Lambda, \mathbb{Z})$.

Proof. Let $\Lambda = \{1, \tau\}$ where $\tau \in \mathbb{H}$. Recall that by Proposition 2.21, $\mathbb{C}/\Lambda$ has genus 1. For $0 \leq t \leq 1$, let $t \mapsto t$ be the blue cycle c_1, and let $t \mapsto t\tau$ be the red cycle c_2; these generate $H_1(\mathbb{C}/\Lambda, \mathbb{Z}) \cong \mathbb{Z}^2$. Then any $c \in H_1(\mathbb{C}/\Lambda, \mathbb{Z})$ can be written in the form $c = c_1^{k_1} c_2^{k_2}$ for integers k_1 and k_2. For any $\omega \in \Omega(X)$, we have

$$\int_c \omega = k_1 \int_{c_1} \omega + k_2 \int_{c_2} \omega.$$

Now, consider $\mathbb{C} \mapsto \mathbb{C}/\Lambda$. This sends the 1-form dz to ω, so the integral $\int_0^1 dz$ gets sent to $\int_{c_1} \omega \mod \Lambda$ and $\int_0^\tau dz$ is sent to $\int_{c_2} \omega$. In particular, $\int_{c_1} \omega = 1$ and $\int_{c_2} \omega = \tau$. Thus, $\Gamma \cong \Lambda$, and

$$\mathrm{Jac}(X) = \Omega(X)^\vee / \Gamma \cong \mathbb{C}/\Gamma \cong \mathbb{C}/\Lambda = X.$$

■

Definition 4.10. Let $\mathrm{Div}(X)$, $\mathrm{Div}_0(X)$, $\mathrm{Div}_P(X)$ be the divisors, degree 0 divisors, and principal divisors, respectively, and let $\mathrm{Pic}(X) = \mathrm{Div}(X)/\mathrm{Div}_0(X)$ and $\mathrm{Pic}_0(X) = \mathrm{Div}_0(X)/\mathrm{Div}_P(X)$ be the *Picard group* and *degree 0 Picard group* respectively.

We define a map $\Phi : \mathrm{Div}_0(X) \to \mathrm{Jac}(X)$ by

$$D \mapsto \left(\int_c \omega_1, \ldots, \int_c \omega_g \right)$$

where c is a 1-chain with $\partial c = D$. Note that Φ is well defined because the integral over a boundary chain is zero. Recall that by Abel's theorem, $\ker \Phi = \mathrm{Div}_P(X)$. Then modding out by $\mathrm{Div}_P(X)$ gives an injective map $j : \mathrm{Pic}_0(X) \to \mathrm{Jac}(X)$.

Theorem 4.11 (Jacobi)**.** *The map* j *is surjective (and thus defines an isomorphism between* $\mathrm{Pic}_0(X)$ *and* $\mathrm{Jac}(X)$*).*

Thus, the group of degree zero divisors modulo the principal divisors is isomorphic to a complex g-dimensional torus.

Example 4.12. In the genus 0 case, $\mathrm{Jac}(X)$ is trivial, so $\mathrm{Pic}_0(X)$ is as well.

Proposition 4.13. *Any compact Riemann surface* X *of genus* 1 *can be written in the form* $\mathbb{C}/\Lambda$*.*

Proof. Note that as X has genus 1, it is isomorphic to its Jacobian $\mathrm{Jac}(X)$, and furthermore, $\mathrm{Jac}(X) \cong \mathbb{C}/\Lambda$ for a lattice Λ. Thus, $X \cong \mathrm{Jac}(X) \cong \mathbb{C}/\Lambda$. ■

Proposition 4.14. *Any compact Riemann surface of genus* $g \geq 1$ *embeds into its Jacobian.*

5. Elliptic Curves

5.1. **Elliptic Functions.**

Definition 5.1. Recall that, given two nonzero complex numbers ω_1, ω_2 such that $\frac{\omega_1}{\omega_2} \notin \mathbb{R}$, we may define the *lattice* Λ by $\Lambda = [\omega_1, \omega_2] = \{m\omega_1 + n\omega_2 : m, n \in \mathbb{Z}\}$. Then an *elliptic function* with respect to Λ is a meromorphic function f such that $f(z + \omega) = f(z)$ for all $\omega \in \Lambda$.

We know some basic facts about the zeros and poles of elliptic functions, which can be derived using tools from complex analysis. We will show alternate proofs using the theory we have developed. In what follows, let $\mathcal{P}$ denote a fundamental parallelogram (a parallelogram with vertices at $0, \omega_1, \omega_2$ and $\omega_1 + \omega_2$), and let Γ be the boundary of $\mathcal{P}$.

Theorem 5.2. *An entire elliptic function $f : X \to \mathbb{C}$ is constant.*

Proof. Note that X is compact. Then $f(X)$ is also compact, so in particular, it is bounded. Since f is an elliptic function, it defines an entire function $f : \mathbb{C} \to \mathbb{C}$. Thus, by Liouville's theorem, f is constant. ■

Proof with Riemann-Roch. Consider the divisor $D = 0$: this gives us the holomorphic functions on X. Then, we have $\ell(D) - \ell(K - D) = 1 - g + \deg D \implies \ell(0) = \deg D + \ell(K) = 1$. Thus, the only entire functions on X are the constant functions. ■

Theorem 5.3. *There are no elliptic functions with a single simple pole in each fundamental parallelogram.*

Proof. Say we have a simple pole at z_0. By the residue theorem,

$$\int_\Gamma f(z)dz = 2\pi i \mathrm{Res}(f; z_0).$$

However, by double periodicity, the integral is 0, so the residue at z_0 is 0, which is a contradiction to z_0 being a pole. Thus, there is no such f with a simple pole at z_0. ■

Proof with Riemann-Roch. Say we have a simple pole at P. Then, we consider the divisor $D = P$: this controls the functions that have at most a pole of order 1 at P, and are holomorphic everywhere else. Then as $\deg P = 1 \geq 2g - 1$, $\ell(K - P) = 0$, so $\ell(P) = \deg P = 1$. However, the constant functions have no poles, so there are no elliptic functions with a single simple pole in each fundamental parallelogram. ■

Definition 5.4. Let f be a meromorphic function. Given a contour Γ, we let $n_0(f)$ and $n_\infty(f)$ respectively denote the number of zeros and poles of f in the interior of Γ, counted with multiplicity.

Theorem 5.5 (Argument Principle). *Suppose that $\Gamma \subset \mathbb{C}$ is a contour, f is holomorphic on Γ and its interior except for some isolated singularities. Then*

$$\frac{1}{2\pi i}\int_\Gamma \frac{f'(z)}{f(z)}dz = n_0(f) - n_\infty(f).$$

Proof. Say $f(z)$ has a root z_i with multiplicity k_i; we have $f(z) = (z - z_i)^{k_i} g(z)$ for $g(z_i) \neq 0$. Then $f'(z) = (z - z_i)^{k_i} g'(z) + k_i(z - z_i)^{k_i - 1} g(z)$ so

$$\frac{f'(z)}{f(z)} = \frac{g'(z)}{g(z)} + \frac{k_i}{z - z_i}$$

and integrating over a small contour Γ gives

$$\frac{1}{2\pi i}\int_\Gamma \frac{f'(z)}{f(z)}dz = \frac{1}{2\pi i}\int_\Gamma \frac{g'(z)}{g(z)}dz + k_i.$$

Now, let us see what happens if we have a pole z_j with multiplicity k_j: we can write $f(z) = \frac{g(z)}{(z - z_j)^{k_j}}$ with $g(z_j) \neq 0$.

$$f'(z) = \frac{g'(z)}{(z - z_j)^{k_j}} - \frac{g(z) \cdot k_j}{(z - z_j)^{k_j + 1}}$$

Then

$$\frac{f'(z)}{f(z)} = \frac{g'(z)}{g(z)} - \frac{k_j}{z-z_j}$$

and

$$\frac{1}{2\pi i}\int_\Gamma \frac{f'(z)}{f(z)} = \frac{1}{2\pi i}\int_\Gamma \frac{g'(z)}{g(z)} - k_j.$$

Doing this for all poles and zeros gives the desired result. ■

Theorem 5.6. *If f is a nonzero elliptic function, then the number of poles is equal to the number of zeros.*

Proof. This follows by the symmetry of the integral over Γ and the argument principle. ■

So far, we've only proved results we already knew how to prove with more elementary methods. Using the theory we have developed, we will be able to prove a converse to the following theorem:

Theorem 5.7. *Let f be an elliptic function with respect to the lattice Λ, and suppose f has zeros and poles $a_1, \ldots, a_n$ with multiplicities m_k. Then $\sum_{k=1}^n a_k m_k \in \Lambda$.*

Theorem 5.8. *Fix a lattice Λ, and let $a_1, \ldots, a_n$ be a sequence of complex numbers, and let $m_1, \ldots, m_n$ be a sequence of integers. Then there is a doubly periodic meromorphic function f with respect to Λ with zeros and poles at each a_k with multiplicity m_k if and only if $\sum_{k=1}^n a_k m_k \in \Lambda$ and $\sum_{i=1}^n m_k = 0$.*

Proof of Theorem 5.7. By the residue theorem, we have

$$\frac{1}{2\pi i}\int_\Gamma z\frac{f'(z)}{f(z)}dz = \sum_{k=1}^n a_k m_k.$$

Note that

$$\int_{\omega_1}^{\omega_1+\omega_2} z\frac{f'(z)}{f(z)}dz = \int_0^{\omega_2}(z+\omega_1)\frac{f'(z+\omega_1)}{f(z+\omega_1)}dz = \int_0^{\omega_2}(z+\omega_1)\frac{f'(z)}{f(z)}dz,$$

and similarly,

$$\int_{\omega_1+\omega_2}^{\omega_2} z\frac{f'(z)}{f(z)}dz = \int_{\omega_1}^{0}(z+\omega_2)\frac{f'(z+\omega_2)}{f(z+\omega_2)}dz = \int_{\omega_1}^{0}(z+\omega_2)\frac{f'(z)}{f(z)}dz.$$

Now,

$$\int_0^{\omega_1} z\frac{f'(z)}{f(z)}dz + \int_{\omega_1+\omega_2}^{\omega_2} z\frac{f'(z)}{f(z)}dz = \int_0^{\omega_1} z\frac{f'(z)}{f(z)}dz + \int_{\omega_1}^{0}(z+\omega_2)\frac{f'(z)}{f(z)}dz = \omega_2\int_{\omega_1}^{0}\frac{f'(z)}{f(z)}dz,$$

and

$$\int_{\omega_1}^{\omega_1+\omega_2} z\frac{f'(z)}{f(z)}dz + \int_{\omega_2}^{0} z\frac{f'(z)}{f(z)}dz = \int_0^{\omega_2}(z+\omega_1)\frac{f'(z)}{f(z)}dz + \int_{\omega_2}^{0} z\frac{f'(z)}{f(z)}dz = \omega_1\int_0^{\omega_2}\frac{f'(z)}{f(z)}dz.$$

Now, note that $\int_{\omega_1}^0 \frac{f'(z)}{f(z)}dz = \log(0) - \log(\omega_1) = 2\pi i n_2$ and $\int_0^{\omega_2} \frac{f'(z)}{f(z)}dz = \log(\omega_2) - \log(0) = 2\pi i n_1$. Thus,

$$\sum_{k=1}^n a_k m_k = \frac{1}{2\pi i}\int_\Gamma z\frac{f'(z)}{f(z)}dz = \frac{1}{2\pi i}(2\pi i n_1\omega_1 + 2\pi i n_2\omega_2) = n_1\omega_1 + n_2\omega_2 \in \Lambda.$$

■

Proof of Theorem 5.8. Let D be the divisor given by the a_k and m_k: note that $\deg D = 0$. Then, by Abel's theorem, D has a solution if and only if there is a chain $c \in C_1(X)$ such that $\partial c = D$ and $\int_c \omega = 0$ for each $\omega \in \Omega(X)$. Since the sum of the m_i is 0, we can pair up the zeros and poles; it doesn't matter how we do this.

Let $\pi : \mathbb{C} \to \mathbb{C}/\Lambda$ be the canonical projection, and let

$$c = \pi\circ\gamma_1 + \ldots + \pi\circ\gamma_N,$$

where N is the total number of pairs. Then $\partial c = D$ and for any holomorphic 1-form ω induced by a 1-form dz on $\mathbb{C}$, we have

$$\int_c \omega = \sum_{i=1}^{N} \int_{c_i} dz = \sum_{k=1}^{n} a_k m_k = 0.$$

■

5.2. **The Weierstrass $\wp$-function.** Note that there are no elliptic functions with a simple pole in each fundamental parallelogram. However, the Weierstrass $\wp$-function gives us the next best thing: an elliptic function with a double pole in each fundamental parallelogram. We will also see that it is universal in a sense: every elliptic function can be written as a rational function in $\wp(z)$ and its derivative, $\wp'(z)$.

Definition 5.9. Let the *Weierstrass $\wp$-function* with respect to a given lattice Λ be defined by

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega\in\Lambda^*} \left(\frac{1}{(z+\omega)^2} - \frac{1}{\omega^2} \right).$$

Definition 5.10. Let

$$E_k = \sum_{\omega\in\Lambda\setminus\{0\}} \frac{1}{\omega^k}$$

be the *k-th Eisenstein series.*

Remark. The Eisenstein series are an example of *modular forms*, which are important in number theory as well as other branches of mathematics.

Proofs of the following propositions can be found in standard references such as [Cox97] or [SS03].

Proposition 5.11. *$\wp(z)$ is a meromorphic even function; furthermore, $\wp(z)$ is doubly periodic with respect to ω_1 and ω_2 and has a double pole at each lattice point $\omega \in \Lambda$. It has no poles anywhere else.*

Proposition 5.12. *$\wp'(z)$ is a meromorphic and odd function with a triple pole at each lattice at each lattice point $\omega \in \Lambda$. It has no poles anywhere else. Furthermore, it is doubly periodic with respect to ω_1 and ω_2.*

Proposition 5.13. *$\wp(z)$ has a Laurent series expansion around $z = 0$ given by*

$$\wp(z) = \frac{1}{z^2} + \sum_{k=1}^{\infty} (2k+1) E_{2k+2} z^{2k}.$$

Let's look at the basis of the space of meromorphic elliptic functions with a pole of order at most n at each lattice point P: By the Riemann-Roch theorem, we expect there to be a linear dependence relation

n	$\ell(nP)$	$\mathbb{C}$-basis
0	1	$\{1\}$
1	1	$\{1\}$
2	2	$\{1, \wp\}$
3	3	$\{1, \wp, \wp'\}$
4	4	$\{1, \wp, \wp', \wp^2\}$
5	5	$\{1, \wp, \wp', \wp^2, \wp\wp'\}$
6	6	$\{1, \wp, \wp', \wp^2, \wp\wp', \wp^3\}$

$$\wp'^2 = a_1 + a_2\wp + a_3\wp' + a_4\wp^2 + a_5\wp\wp' + a_6\wp^3$$

and indeed we have

Proposition 5.14. *Let*

$$g_2(\Lambda) = 60E_4 = 60 \sum_{\omega\in\Lambda\setminus\{0\}} \frac{1}{\omega^4}$$

and

$$g_3(\Lambda) = 140E_6 = 140 \sum_{\omega\in\Lambda\setminus\{0\}} \frac{1}{\omega^6}$$

Then we have

$$\begin{aligned}\wp'(z)^2 &= 4\wp(z)^3 - 60E_4\wp(z) - 140E_6\\ &= 4\wp(z)^3 - g_2(\Lambda)\wp(z) - g_3(\Lambda).\end{aligned}$$

Proposition 5.15. *Every coefficient in the Laurent expansion of $\wp(z)$ can be expressed as a polynomial in E_4 and E_6.*

5.3. **Elliptic Curves.** Consider a lattice $\Lambda \subset \mathbb{C}$. Then note that $X = \mathbb{C}/\Lambda$ is a compact Riemann surface: in particular, it is a complex torus. Studying the elliptic functions with respect to Λ corresponds to studying meromorphic functions on X.

From the Weierstrass differential equation, it can be shown that the coordinate ring of X takes the form

$$\mathbb{C}[X] = \mathbb{C}[x, y]/(y^2 - (4x^3 - g_2x - g_3)).$$

Thus, every regular function on X is a polynomial in x and y, where $y^2 = 4x^3 - g_2x - g_3$.

Proposition 5.16. *For a nonsingular projective plane curve C of degree d, the genus of C is given by*

$$g = \frac{(d-1)(d-2)}{2}.$$

Definition 5.17. An elliptic curve is a nonsingular curve of genus 1 along with a specified base point.

Proposition 5.18. *Let E be an elliptic curve with base point $\mathcal{O}$. Then there are functions $x, y \in \mathbb{C}(E)$ such that $E \to \mathbb{P}^2$ by $P \mapsto (x(P) : y(P) : 1)$ for $P \neq \mathcal{O}$ and $\mathcal{O} \mapsto (0 : 1 : 0)$ gives an isomorphism of E onto a curve in nonsingular Weierstrass form,*

$$C : Y^2Z = 4X^3 - g_2XZ^2 - g_3Z^3,$$

where $\Delta = g_2^3 - 27g_3^2 \neq 0$. Furthermore, every point in $E \setminus \{\mathcal{O}\}$ is sent to a point in affine space. We then call x and y the Weierstrass coordinates *for E.*

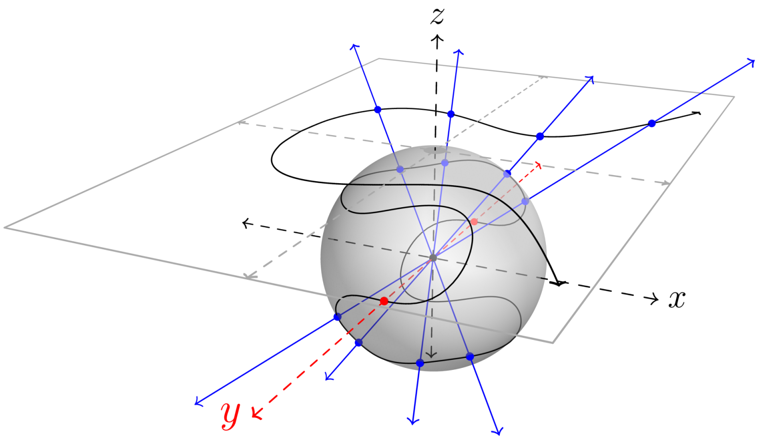


Figure 2. An elliptic curve in $\mathbb{P}^2$; the y-axis corresponds to the point at infinity.

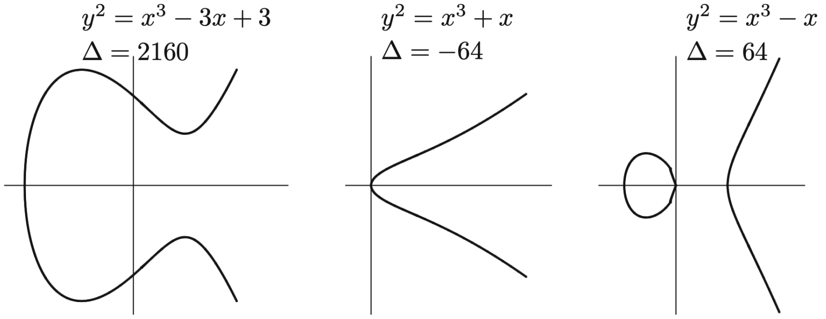


FIGURE 3. If we work in affine coordinates $x = X/Z, y = Y/Z$, then we obtain the locus of a cubic $y^2 = 4x^3 - g_2x - g_3$, along with a formal point at infinity.

Proof. Consider the vector spaces $n\mathcal{O}$ for $n \geq 1$. By Riemann-Roch, we have $\ell(\mathscr{O}_{n\mathcal{O}}) = n$.

- $\mathscr{O}_{\mathcal{O}}$: a basis is $\{1\}$.
- $\mathscr{O}_{2\mathcal{O}}$: since this vector space has dimension 2, a basis must be of the form $\{1, x\}$. In particular, x has a pole of order exactly 2 at $\mathcal{O}$.
- $\mathscr{O}_{3\mathcal{O}}$: $\{1, x, y\}$, where x has a pole of order 2 at P, and y has a pole of order 3 at $\mathcal{O}$.
- $\mathscr{O}_{4\mathcal{O}}$: $\{1, x, y, x^2\}$.
- $\mathscr{O}_{5\mathcal{O}}$: $\{1, x, y, x^2, xy\}$.
- $\mathscr{O}_{6\mathcal{O}}$: this case is more interesting: note that $1, x, y, x^2, xy, x^3, y^2$ are all in $\mathscr{O}_{6\mathcal{O}}$, but $\mathscr{O}_{6\mathcal{O}}$ has dimension 6. This implies that there is a linear dependence relation:

$$a_1 + a_2x + a_3y + a_4x^2 + a_5xy + a_6y^2 + a_7x^3 = 0 \tag{1}$$

We want to write the above equation in a nicer form. First, we claim that $a_6, a_7 \neq 0$: otherwise, each a_j term in Equation (1) would have a different order pole at $\mathcal{O}$, so each a_j would be 0. Now, consider the substitution

$$(x, y) \mapsto (-a_6a_7x, a_6a_7^2y).$$

We have

$$a_1 - a_2a_6a_7x + a_3a_6a_7^2y + a_4a_6^2a_7^2x^2 - a_5a_6^2a_7^3xy + a_6^3a_7^4y^2 - a_6^3a_7^4x^3 = 0$$

so dividing through by $a_6^3a_7^4$ gives

$$\frac{a_1}{a_6^3a_7^4} - \frac{a_2}{a_6^2a_7^3}x + \frac{a_3}{a_6^2a_7^2}y + \frac{a_4}{a_6a_7^2}x^2 - \frac{a_5}{a_6a_7}xy + y^2 - x^3 = 0$$

or

$$y^2 + \frac{a_4}{a_6a_7^2}xy + \frac{a_3}{a_6^2a_7^3}y = x^3 - \frac{a_4}{a_6a_7^2}x^2 + \frac{a_2}{a_6^2a_7^3}x - \frac{a_1}{a_6^3a_7^4}.$$

For ease of reading, replace the constants as appropriate:

$$y^2 + b_1xy + b_3y = x^3 + b_2x^2 + b_4x + b_6.$$

Then, the substitution

$$(x, y) \mapsto \left(y + \frac{b_1x + b_3}{2}, x - \frac{b_1^2/4 + b_2}{3}\right)$$

gives

$$y^2 = x^3 + Ax + B,$$

or in projective coordinates,

$$Y^2Z = x^3 + AXZ^2 + BZ^3$$

where

$$A = \frac{-b_1^4}{48} - \frac{b_1b_2^2}{6} + \frac{b_1b^3}{4} - \frac{b_2^2}{3} + b_4$$

and

$$B = \frac{b_1^6}{864} + \frac{b_1^4 b_2}{72} - \frac{b_1^3 b_3}{48} + \frac{b_1^2 b_2^2}{18} - \frac{b_1^2 b_4}{12} - \frac{b_1 b_2 b_3}{12} + \frac{2b_2^3}{27} + \frac{b_3^2}{4} - \frac{b_2 b_4}{3} + b_6.$$

Finally, $y \mapsto \frac{y}{2}$ gives the desired form:

$$y^2 = 4x^3 - g_2 x + g_3 \tag{2}$$

or

$$C : Y^2 Z = 4X^3 - g_2 X Z^2 - g_3 Z^3, \tag{3}$$

Now we prove that $\mathbb{C}(E) = \mathbb{C}(x, y)$. Consider the maps

$$P \mapsto (x(P) : y(P) : 1) \mapsto x(P)$$

and

$$P \mapsto (x(P) : y(P) : 1) \mapsto y(P)$$

from $E \setminus \{\mathcal{O}\} \to C \to \mathbb{C}$. We have $[\mathbb{C}(E) : \mathbb{C}(x)] = 2$ and $[\mathbb{C}(E) : \mathbb{C}(y)] = 3$ (see [Sil09]). Note that

$$[\mathbb{C}(E) : \mathbb{C}(x, y)] \cdot [\mathbb{C}(x, y) : \mathbb{C}(x)] = [\mathbb{C}(E) : \mathbb{C}(x)] = 2$$

and

$$[\mathbb{C}(E) : \mathbb{C}(x, y)] \cdot [\mathbb{C}(x, y) : \mathbb{C}(y)] = [\mathbb{C}(E) : \mathbb{C}(y)] = 3,$$

so $[\mathbb{C}(E) : \mathbb{C}(x, y)]$ divides both 2 and 3. This implies that $[\mathbb{C}(E) : \mathbb{C}(x, y)] = 1$, so $\mathbb{C}(E) = \mathbb{C}(x, y)$, as desired. Furthermore, note that x has a pole of order 2 at $\mathcal{O}$ and y has a pole of order 3 at $\mathcal{O}$. Thus, $\mathcal{O}$ is mapped to the point at infinity. ■

Proposition 5.19. *A Weierstrass cubic $y^2 = 4x^3 - g_2 x - g_3$ has three distinct roots if and only if $\Delta = g_2^3 - 27g_3^2 \neq 0$.*

Proof. Let $\{e_1, e_2, e_3\}$ be the roots of $4x^3 - g_2 x - g_3 = 0$. Then through tedious algebraic manipulation, it can be shown that

$$\Delta = 16(e_1 - e_2)^2 (e_2 - e_3)^2 (e_3 - e_1)^2.$$

■

Remark. One may wonder what goes wrong if $\Delta = 0$. In this case, we obtain singular cubic curves, which are *not* elliptic curves:

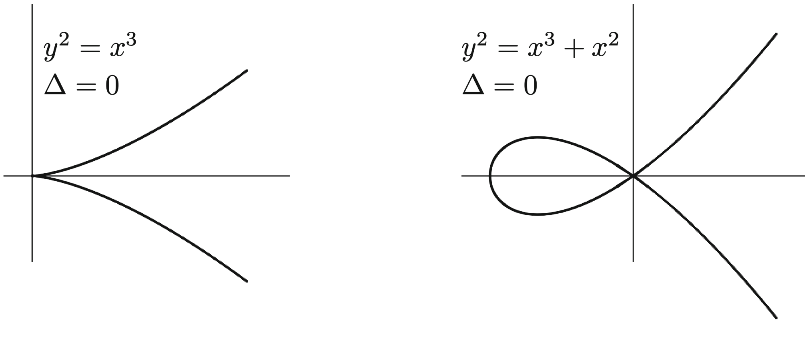


FIGURE 4. Singular cubic curves in $\mathbb{A}^2$.

However, analysis of singular cubic curves is still important; particular, it is often useful to consider a Weierstrass cubic equation over $\mathbb{F}_p$. Further discussion can be found in [Sil09], p. 55.

Proposition 5.20. *Consider the curve*

$$C : Y^2Z = 4X^3 - g_2XZ^2 - g_3$$

where $\Delta \neq 0$. *Then* C *is an elliptic curve with base point* $(0 : 1 : 0)$.

Proof. Note that C is a nonsingular projective plane curve of degree 3 in $\mathbb{P}^2$. Thus, by Lemma 5.16, the genus of C is $\frac{1}{2}(3-1)(3-2) = 1$. ∎

5.4. **The Uniformization Theorem.** Recall the Weierstrass differential equation

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

and consider the mapping $(\wp(z), \wp'(z)) \mapsto (x, y)$. Then Equation (4) defines an elliptic curve

$$E_\Lambda : y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda). \tag{5}$$

Thus, every lattice in $\mathbb{C}$ corresponds to an elliptic curve. However, this leads one to wonder: given an elliptic curve E, is there a lattice $\mathbb{C}$ such that $E = E_\Lambda$? The answer is yes; this is the content of the *uniformization theorem* for elliptic curves.

5.4.1. *The discriminant of a lattice.*

Definition 5.21. Recall that a lattice gives rise to a differential equation of the Weierstrass function: with $g_2(\Lambda) = 60E_4 = 60\sum_{\omega\in\Lambda\setminus\{0\}} \frac{1}{\omega^4}$ and $g_3(\Lambda) = 140E_6 = 140\sum_{\omega\in\Lambda\setminus\{0\}} \frac{1}{\omega^6}$, we have

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

Recall that a cubic of the form

$$E : y^2 = 4x^3 - g_2x - g_3$$

has discriminant $g_2^3 - 27g_3^2$; thus, we define the *discriminant* of Λ by $\Delta(\Lambda) = g_2(\Lambda)^3 - 27g_3(\Lambda)^2$. Also, let $\{e_1, e_2, e_3\}$ be the roots of $4\wp(z)^3 - g_2(\Lambda)\wp(z) - g_3(\Lambda) = 0$. It is well known (without loss of generality) that $e_1 = \wp\left(\frac{\omega_1}{2}\right)$, $e_2 = \wp\left(\frac{\omega_2}{2}\right)$, and $e_3 = \wp\left(\frac{\omega_1+\omega_2}{2}\right)$.

Proposition 5.22. *For any lattice* Λ, $\Delta(\Lambda) \neq 0$.

Proof. Note that $\Delta(\Lambda) = 16(e_1-e_2)^2(e_2-e_3)^2(e_3-e_1)^2$, where $e_1 = \wp\left(\frac{\omega_1}{2}\right)$, $e_2 = \wp\left(\frac{\omega_2}{2}\right)$, and $e_3 = \wp\left(\frac{\omega_1+\omega_2}{2}\right)$. As the e_i are distinct, it follows that $\Delta(\Lambda) \neq 0$. ∎

Corollary 5.23. *The differential equation of the Weierstrass* $\wp$ *function gives rise to an elliptic curve.*

5.4.2. *The* j*-invariant of a lattice.* Call two lattices Λ and Λ' *homothetic* if there is some $\lambda \in \mathbb{C}$ such that $\Lambda = \lambda\Lambda'$.

Definition 5.24. Now, define the j*-invariant* of the lattice Λ by

$$j(\Lambda) = 1728\frac{g_2(\Lambda)^3}{\Delta(\Lambda)}.$$

Proposition 5.25. *Two lattices* Λ *and* Λ' *are homothetic if and only if* $j(\Lambda) = j(\Lambda')$.

Proof. If Λ and Λ' are homothetic, write $\Lambda = \lambda\Lambda'$. Then

$$g_2(\Lambda) = g_2(\lambda\Lambda') = \frac{1}{\lambda^4}g_2(\Lambda')$$

and

$$g_3(\Lambda) = g_3(\lambda\Lambda') = \frac{1}{\lambda^6}g_3(\Lambda').$$

Then by the definition of the j-invariant, we have

$$j(\Lambda) = 1728\frac{g_2(\Lambda)^3}{g_2(\Lambda)^3 - 27g_3(\Lambda)^2} = 1728\frac{g_2(\Lambda')^3/\lambda^{12}}{(g_2(\Lambda)^3 - 27g_3(\Lambda)^2)/\lambda^{12}} = 1728\frac{g_2(\Lambda')^3}{g_2(\Lambda')^3 - 27g_3(\Lambda')^2} = j(\Lambda').$$

Conversely, say Λ and Λ' satisfy $j(\Lambda) = j(\Lambda')$. Let $\lambda \in \mathbb{C}$ be such that

$$\lambda^4 = \frac{g_2(\Lambda)}{g_2(\Lambda')}.$$

Since

$$1728\frac{g_2(\Lambda)^3}{\Delta(\Lambda)} = j(\Lambda) = j(\Lambda') = 1728\frac{g_2(\Lambda')^3}{\Delta(\Lambda')},$$

we have

$$g_2(\Lambda)^3(g_2(\Lambda')^3 - 27g_3(\Lambda')^2) = g_2(\Lambda')^3(g_2(\Lambda)^3 - 27g_3(\Lambda)^2)$$

so

$$g_2(\Lambda)^3 g_3(\Lambda')^2 = g_2(\Lambda')^3 g_3(\Lambda)^2$$

and

$$\lambda^{12} = \left(\frac{g_2(\Lambda)}{g_2(\Lambda')}\right)^3 = \left(\frac{g_3(\Lambda)}{g_3(\Lambda')}\right)^2$$

so that

$$\left(\frac{g_3(\Lambda)}{g_3(\Lambda')}\right)^2 = \pm\lambda^6.$$

If the above is negative, then replace λ by $i\lambda$ so that $\lambda^4 = (i\lambda)^4$ and $\lambda^6 = -(i\lambda)^6$. Then we have either

$$g_2(\Lambda) = \lambda^4 g_2(\Lambda') \text{ and } g_3(\Lambda) = \lambda^6 g_3(\Lambda')$$

or

$$g_2(\Lambda) = (i\lambda)^4 g_2(\Lambda') \text{ and } g_3(\Lambda) = (i\lambda)^6 g_3(\Lambda').$$

Now, by the definition of g_2 and g_3 (namely as Eisenstein series) we have $g_2(\Lambda') = g_2(\lambda\Lambda)$ and $g_3(\Lambda') = g_3(\lambda\Lambda)$. By Lemma 5.15, we have $\wp_\Lambda(z) = \wp_{\lambda\Lambda'}(z)$. Since the lattice is the set of poles of the Weierstrass function, we have $\Lambda = \lambda\Lambda'$ as desired. ■

We can also define the j-function $j : \mathbb{H} \to \mathbb{C}$ by $j(\tau) = j([1, \tau])$. This notion will be useful for existence.

Lemma 5.26. *The j-function $j : \mathbb{H} \to \mathbb{C}$ is surjective.*

Proof. [Cox97] p. 204. ■

5.4.3. *The Uniformization Theorem.*

Proposition 5.27. *Let $g_2, g_3 \in \mathbb{C}$ be such that $g_2^3 - 27g_3^2 \neq 0$. Then there is a lattice Λ such that $g_2(\Lambda) = g_2$ and $g_3(\Lambda) = g_3$.*

Proof of Proposition 5.27 with the j-function. Take τ so that $j(\tau) = 1728g_2^3/(g_2^3 - 27g_3^2)$. Then the lattice $[1, \tau]$ suffices: we can find λ so that $g_2(\Lambda) = g_2/\lambda^4$ and $g_3(\Lambda) = g_3/\lambda^6$. ■

We can also give a proof of this fact using the Riemann-Hurwitz formula.

Theorem 5.28 (Riemann-Hurtwitz onto Riemann Sphere)**.** *Let $\pi : X \to \mathbb{P}^1$ where X is the Riemann surface of $\sqrt{P(z)} = c\sqrt{(z - a_1)\cdots(z - a_k)}$ and the a_i are distinct. Then the genus of X is given by $g = \lfloor \frac{k-1}{2} \rfloor$.*

Proof of Proposition 5.27 with Riemann-Hurtwitz. Fix $g_2, g_3 \in \mathbb{C}$ and assume $g_2^3 - 27g_3^2 \neq 0$. Let $X \to \mathbb{P}^1$ be the Riemann surface of $\sqrt{4z^3 - g_2 z - g_3}$. Then since the roots of $4z^3 - g_2 z - g_3$ are all distinct, we have $g = 1$. In particular, X is isomorphic to its Jacobian $\mathrm{Jac}(X)$, which is isomorphic to $\mathbb{C}/\Lambda$ for some lattice Λ. ■

Theorem 5.29 (The Uniformization Theorem for Elliptic Curves)**.** *Given a lattice $\Lambda \subseteq \mathbb{C}$, there is a corresponding elliptic curve E_Λ such that $\mathbb{C}/\Lambda \cong E_\Lambda$, and given an elliptic curve E, there is a lattice (unique up to homothety) Λ such that $E \cong \mathbb{C}/\Lambda$.*

Let $\varphi : \mathbb{C}/\Lambda \to E_\Lambda(\mathbb{C})$ be defined by $z \mapsto (\wp(z), \wp'(z))$ for $z \notin \Lambda$ and $z \mapsto \mathcal{O}$ for $z \in \Lambda$.

Lemma 5.30. *φ is a bijection from $\mathbb{C}/\Lambda$ onto $E_\Lambda(\mathbb{C})$.*

Proof. Say that $\varphi(z_1) = \varphi(z_2)$. Then we have $\wp(z_1) = \wp(z_2)$, so $z_1 \equiv \pm z_2 \bmod \Lambda$. Since we must also have $\wp'(z_1) = \wp'(z_2)$, and $\wp'$ is an odd function, we must have $z_1 \equiv z_2 \bmod \Lambda$. Thus, φ is injective. To show that φ is surjective, let $(x_0, y_0) \in E_\Lambda(\mathbb{C})$. Let z_0 be a solution of $\wp(z) - x_0 = 0$. Then $\wp(z_0) = x_0$ and

$$\wp'(z)^2 = 4\wp(z_0)^2 - g_2(\Lambda)\wp(z_0) - g_3(\Lambda) = 4x_0^3 - g_2(\Lambda)x_0 - g_3(\Lambda) = y_0^2,$$

so $\wp'(z) = \pm y_0$. It follows that $\varphi(\pm z_0) = (x_0, \pm y_0)$, so φ is surjective. Thus, φ is bijective. ■

Lemma 5.31. *φ is structure preserving; in particular, it induces an isomorphism of groups.*

Proof. Let $z_1, z_2 \in \mathbb{C}/\Lambda$. If z_1 or $z_2 \in \Lambda$, then $\varphi(z_1 + z_2) = \varphi(z_2) = \mathcal{O} + \varphi(z_2) = \varphi(z_1) + \varphi(z_2)$ or $\varphi(z_1 + z_2) = \varphi(z_1) = \varphi(z_1) + \mathcal{O} = \varphi(z_1) + \varphi(z_2)$. If $z_1 + z_2 \in \Lambda$, then $\varphi(z_1) = \varphi(-z_2) = -\varphi(z_2)$, so $\varphi(z_1) + \varphi(z_2)$. Thus, we may assume $z_1, z_2, z_1 + z_2 \notin \Lambda$. Let $y = mx + b$ be the line connecting P_1 and P_2; $m \neq \infty$ since P_1 and P_2 are not inverses, as $z_1 + z_2 \notin \Lambda$. Let z_3 be the third zero of $f(z) = -\wp(z) + m\wp'(z) + b$. Note that $f(z)$ is an elliptic function with zeros z_1, z_2, z_3. This implies that $z_1 + z_2 + z_3 \in \Lambda$, so

$$\varphi(z_1 + z_2) = \varphi(-z_3) = -\varphi(z_3) = -P_3 = P_1 + P_2 = \varphi(z_1) + \varphi(z_2).$$

■

Proof of Theorem 5.29. Consider an elliptic curve $y^2 = 4x^3 - g_2 x - g_3$. By Proposition 5.27, we can find a lattice Λ, unique up to homothety, such that $g_2(\Lambda) = g_2$ and $g_3(\Lambda) = g_3$. By Lemma 5.31, we have $\mathbb{C}/\Lambda \cong E_\Lambda = E$. Conversely, by $z \mapsto (\wp(z), \wp'(z))$ and Lemma 5.31, given a lattice Λ, there is an elliptic curve E_Λ such that $\mathbb{C}/\Lambda \cong E_\Lambda$. ■

Corollary 5.32. *Any elliptic curve can be embedded into $\mathbb{P}^2$ by $z \mapsto (\wp(z) : \wp'(z) : 1)$.*

Proof. $\{1, \wp, \wp'\}$ is a basis of $H^0(X, \mathscr{O}_{3\mathcal{O}})$. Then by Theorem 3.4, $F = (\wp : \wp' : 1) : X \to \mathbb{P}^2$ is an embedding. ■

5.5. **The Group Law.** Recall that for an elliptic curve E, there is a corresponding lattice Λ such that $\mathbb{C}/\Lambda \cong E$. In particular, this is an isomorphism of groups. We describe the geometric group law on E below:

Given two points A and B on E, consider the line through both of them (if they are the same line, consider the tangent line); let this line intersect E at C. Then let the line through $\mathcal{O}$ and C intersect E at $A \oplus B$.

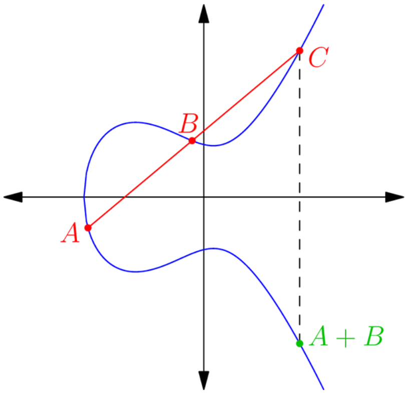


Figure 5. The group law on the elliptic curve $y^2 = x^3 - x + 1$.

Theorem 5.33. *This turns E into an abelian group with identity $\mathcal{O}$. In particular:*

(a) If A, B, C are collinear, then $(A \oplus B) \oplus C = \mathcal{O}$.
(b) $A \oplus \mathcal{O} = A$ for all $A \in E$.
(c) $A \oplus B = B \oplus A$ for all $A, B \in E$.
(d) Given A, there exists B such that $A \oplus B = \mathcal{O}$.
(e) For all A, B, C, we have $(A \oplus B) \oplus C = A \oplus (B \oplus C)$.

Proof of Theorem 5.33.

(a) This follows by the construction of $A + B$ and as C and $A \oplus B$ have opposite y coordinate.
(b) Let the line through A and $\mathcal{O}$ intersect E again at B. Then the constructed line intersects E at $\mathcal{O}$, B, $A \oplus \mathcal{O}$, which implies $A \oplus \mathcal{O} = A$.
(c) This is clear by the construction of $A \oplus B$.
(d) Let the line through A and $\mathcal{O}$ intersect E at B. Then $A \oplus B = (A \oplus \mathcal{O}) \oplus B = \mathcal{O}$.
(e) Associativity is the only hard part. One can prove this explicitly using algebra, but we will use the theory we have developed to give a more enlightening proof.

Since $X = \mathbb{C}/\Lambda$ is a compact Riemann surface of genus 1, it is isomorphic to its Jacobian. Also, by the Abel-Jacobi theorem, $\mathrm{Jac}(X) \cong \mathrm{Pic}_0(X)$, so $X \cong \mathrm{Pic}_0(X)$.

Proposition 5.34. *For an elliptic curve E, there is a bijection between E and $\mathrm{Pic}_0(E)$. In particular,*

$$P \mapsto P - \mathcal{O}$$

suffices (where $P - \mathcal{O}$ is to be considered as a divisor).

Proof. We wish to show that if D is a divisor of degree 0, then there is a unique P such that $D \sim P - \mathcal{O}$. By the Riemann-Roch theorem, we have

$$\ell(D + \mathcal{O}) - \ell(K - D - \mathcal{O}) = 1 - g + \deg(D + \mathcal{O}) = 1.$$

By Proposition 2.17, since $\deg(K - D - \mathcal{O}) = \deg(K) - \deg(D) - \deg(\mathcal{O}) = (2 \cdot 1 - 2) - 0 - 1 = -1$, we have $\ell(K - D - \mathcal{O}) = 0$, so $\ell(D + \mathcal{O}) = 1$. Thus, there is a unique rational function f (up to multiplication by an element of $\mathbb{C}^\times$) such that $(f) + D + \mathcal{O} \geq 0$. This implies that $(f) + D + \mathcal{O}$ takes the form P, i.e. $D + \mathcal{O} \sim P$ or $D \sim P - \mathcal{O}$. ■

Since $\mathrm{Pic}_0(E)$ is an abelian group, it induces an group action $\oplus$ on E. Let us demonstrate how it works:

$$(P \oplus Q) \oplus R = P + Q + R = P \oplus (Q \oplus R).$$

$$P \oplus (-P) = \mathcal{O}$$

$$P \oplus Q = P + Q = Q + P = Q \oplus P$$

$$P \oplus \mathcal{O} = (P - \mathcal{O}) + (\mathcal{O} - \mathcal{O}) = P$$

thus the induced group action is compatible with the group law defined above.

Proposition 5.35. *For an elliptic curve E, $P \oplus Q = R$ if and only if $P + Q \sim R + \mathcal{O}$.*

Proof. Since $P \mapsto P - \mathcal{O}$ and $Q \mapsto Q - \mathcal{O}$, and the operation on $\mathrm{Pic}_0(E)$ is addition of divisors, we want $R = P \oplus Q \mapsto P + Q - 2\mathcal{O}$. However, we already know that $P \oplus Q \mapsto P \oplus Q - \mathcal{O}$, so we have $P \oplus Q - \mathcal{O} \sim P + Q - 2\mathcal{O}$, and in particular, $P \oplus Q + \mathcal{O} = R + \mathcal{O} \sim P + Q$.

Conversely, if $P + Q \sim R + \mathcal{O}$, then $P + Q - R \sim \mathcal{O}$ and the isomorphism defined above sends $P + Q - R \mapsto P + Q - R - \mathcal{O}$. Thus, $P + Q = R$ as desired. ■

■

Let us now work out explicitly the group law on an elliptic curve with affine coordinates. Consider an elliptic curve $E : y^2 = 4x^3 - g_2 x - g_3$. For any two points $p_1, p_2 \in E(\mathbb{C})$, if $p_{1,2}$ is not the point at infinity, let $p_{1,2} = (x_{1,2}, y_{1,2})$.

- If p_1 or p_2 is $\mathcal{O}$, then let $p_1 + p_2 = p_2 = \mathcal{O}$ or $p_1 + p_2 = p_1 = \mathcal{O}$ respectively.
- If $x_1 = x_2$, the Weierstrass equation implies that $y_1 = \pm y_2$. This gives two subcases:
  - If $x_1 = x_2$ and $y_1 = -y_2$ or $y_1 = y_2 = 0$, then let $p_1 + p_2 = \mathcal{O}$.

- If $x_1 = x_2$ and $y_1 = y_2 \neq 0$, let $p_1 + p_2 = 2p_1 = (x_3, y_3)$ where
$$x_3 = -2x_1 + \frac{1}{16}\left(\frac{12x_1^2 - g_2}{y_1}\right)^2$$
and
$$y_3 = -y_1 - (x_3 - x_1)\left(\frac{12x_1 - g_2}{2y_1}\right).$$

Otherwise we have:

- If $x_1 \neq x_2$, let $p_1 + p_2 = (x_3, y_3)$, where
$$x_3 = -x_1 - x_2 + \frac{1}{4}\left(\frac{y_1 - y_2}{x_1 - x_2}\right)^2$$
and
$$y_3 = -y_1 - (x_3 - x_1)\left(\frac{y_1 - y_2}{x_1 - x_2}\right).$$
This comes by intersecting $y = mx + b$ with $y^2 = 4x^3 - g_2x - g_3$ and noting this implies
$$x_1 + x_2 + x_3 = \frac{m^2}{4} = \frac{1}{4}\left(\frac{y_1 - y_2}{x_1 - x_2}\right)^2$$
and
$$y_3 = m(x_3 - x_1) + y_1 = \left(\frac{y_1 - y_2}{x_1 - x_2}\right)(x_1 - x_3) + y_1$$

Corollary 5.36. *By $z \mapsto (\wp(z), \wp'(z))$, we have the addition law for the Weierstrass $\wp$ function:*
$$\wp(w + z) + \wp(w) + \wp(z) = \frac{1}{4}\left(\frac{\wp'(w) - \wp'(z)}{\wp(w) - \wp(z)}\right)^2,$$
and the duplication formula:
$$\wp(2z) = -2\wp(z) + \frac{1}{16}\left(\frac{12\wp(z)^2 - g_2}{2\wp'(z)}\right)^2.$$

6. Applications to Number Theory

We will state some celebrated results in arithmetic geometry; we have no hope of proving them here.

Theorem 6.1 (Mordell-Weil)**.** *If K is a number field (i.e. $[K:\mathbb{Q}]<\infty$, then $E(K)$ is finitely generated.*

Theorem 6.2 (Faltings)**.** *Any curve of genus $g>1$ over $\mathbb{Q}$ has only finitely many rational points.*

Definition 6.3. Define the *Fermat curve* in affine coordinates by $x^n+y^n=1$, or in projective coordinates by $X^n+Y^n=Z^n$.

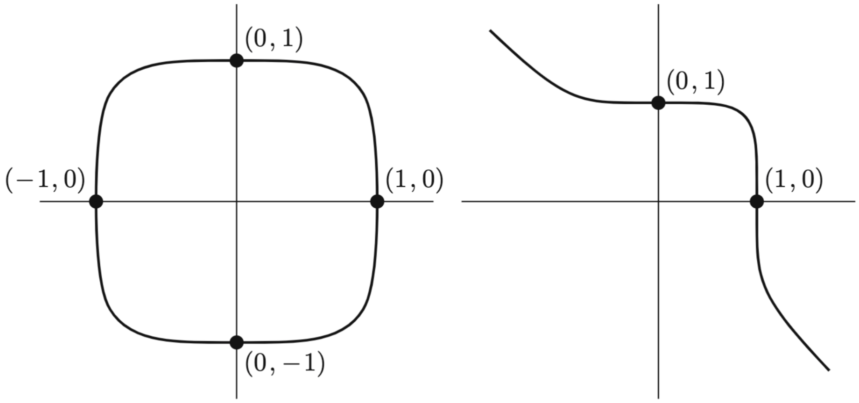


Figure 6. The affine Fermat curves $x^4+y^4=1$ and $x^5+y^5=1$

We claim the curve $f_n : X^n+Y^n-Z^n$ is nonsingular over $\mathbb{C}$; if a singular point P existed, we would have:

$$\left(\frac{\partial f}{\partial X}\right)_P = nX^{n-1}=0$$
$$\left(\frac{\partial f}{\partial Y}\right)_P = nY^{n-1}=0$$
$$\left(\frac{\partial f}{\partial Z}\right)_P = nZ^{n-1}=0$$

which would imply that $P=(0:0:0)$. However, $(0:0:0)$ does not lie in projective space, so it follows that f_n is nonsingular. By Lemma 5.16, the genus of the n-th Fermat curve is $\frac{1}{2}(n-1)(n-2)$, so for $n\geq 4$, Faltings's theorem implies that there are only finitely many rational points on each Fermat curve. This is a weak form of the famous:

Theorem 6.4 (Fermat's Last Theorem)**.** *There are no nontrivial integer solutions to the Diophantine equation $a^n+b^n=c^n$.*

Acknowledgements

The author would like to thank Simon Rubinstein-Salzedo and Casey C. Wojcik for their guidance in writing this paper and helpful discussions.

References

[Alu09] Paolo Aluffi. *Algebra: Chapter 0*. American Mathematical Society, Jul 2009.

[Ara] Donu Arapura. Sheaf cohomology. `https://www.math.purdue.edu/~arapura/preprints/sheaves5.pdf`.

[Cox97] David A. Cox. *Primes of the Form* $x^2 + ny^2$. John Wiley & Sons, Inc., Apr 1997.

[Ele] Georges Elencwajg. Equivalence of Grothendieck-style versus Čech-style sheaf cohomology. MathOverflow. URL: `https://mathoverflow.net/q/4229` (visited on 2021-05-27).

[For81] Otto Forster. *Lectures on Riemann Surfaces*. Springer New York, 1981.

[Har77] Robin Hartshorne. *Algebraic Geometry*. Springer New York, 1977.

[Hur22] Adolf Hurwitz. *Vorlesungen über allgemeine Funktionentheorie und elliptische Funktionen*. Springer Berlin Heidelberg, 1922.

[IR90] Kenneth Ireland and Michael Rosen. *A Classical Introduction to Modern Number Theory*. Springer New York, 1990.

[Kob93] Neal Koblitz. *Introduction to Elliptic Curves and Modular Forms*. Springer New York, 1993.

[McM] Curtis T. McMullen. Math 213b: Complex Analysis on Riemann Surfaces. `http://people.math.harvard.edu/~ctm/papers/home/text/class/harvard/213b/course/course.pdf`.

[Mil06] J.S. Milne. *Elliptic Curves*. BookSurge Publishers, 2006.

[Mir95] Rick Miranda. *Algebraic Curves and Riemann Surfaces*. American Mathematical Society, April 1995.

[Nar92] Raghavan Narasimhan. *Compact Riemann Surfaces*. Birkhäuser Basel, 1992.

[Ser56] Jean-Pierre Serre. Géométrie algébrique et géométrie analytique. *Annales de l'Institut Fourier*, 6:1–42, 1956.

[Shu13] Jerry Shurman. The Elliptic Group Law via the Riemann-Roch Theorem. `https://people.reed.edu/~jerry/311/rr.pdf`, 2013.

[Sil09] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Springer New York, 2009.

[SS03] Stein and Shakarchi. *Complex Analysis*. Princeton University Press, 2003.

[ST15] Joseph H. Silverman and John T. Tate. *Rational Points on Elliptic Curves*. Springer Publishing Company, Incorporated, 2nd edition, 2015.

[Vak] Ravi Vakil. MATH 216: Foundations of Algebraic Geometry. `http://math.stanford.edu/~vakil/216blog/FOAGnov1817public.pdf`.

[Whi60] J. H. C. Whitehead. Topologie Algebrique et Theorie des Faisceaux. By Roger Godement. pp. 283. 3600 fr. 1959. (Hermann, Paris). *The Mathematical Gazette*, 44(347):69–70, 1960.