

## 1. Elliptic Curves over $\mathbb{C}$

In this chapter, we specialize to the case when  $k = \mathbb{C}$ , and go back to the historical roots of the theory of elliptic curves. We will explain (sometimes without proof) why the algebraic theory of elliptic curves over  $\mathbb{C}$  is the same as the analytic theory of compact Riemann surfaces of topological genus 1. As we will see, the development of the algebraic theory is informed by the analytic one.

### Compact Riemann Surfaces

Let's briefly review the basic facts about compact Riemann surfaces; no proofs will be given here. A compact Riemann surface  $M$  is a 1-dimensional compact complex manifold.

**Topological genus:** We may consider  $M$  as a 2-dimensional real manifold. Such manifolds can be classified by a single non-negative integer, namely the **topological genus** of  $M$ . More precisely, the singular homology group  $H_1(M, \mathbb{Z})$  is known to be isomorphic to  $\mathbb{Z}^{2g}$ , and we define  $g$  to be the topological genus of  $M$ . Note that the genus only determines the real manifold structure of  $M$ ; it does not necessarily determine the complex structure.

**Uniformization theorem:** This is the most important theorem on compact Riemann surfaces. It describes the simply-connected cover of  $M$ . It says:

**Theorem 1.1.** (i) *If  $M$  has genus 0, then  $M$  is the sphere.*

(ii) *If  $M$  has genus 1, then  $M \cong \mathbb{C}/\Lambda$  where  $\Lambda \subset \mathbb{C}$  is a  $\mathbb{Z}$ -lattice of rank 2. Moreover, every  $\mathbb{C}/\Lambda$  is a compact Riemann surface of genus 1.*

(iii) *If  $M$  has genus  $\geq 2$ , then the simply-connected cover of  $M$  is the upper half plane (or equivalently the disc).*

**Genus 1 case:** We focus now on the genus 1 case. In this case, the addition map on  $\mathbb{C}$  descends to give a group law on  $M = \mathbb{C}/\Lambda$ . Thus  $M$  is a compact abelian complex Lie group. Consider the set  $\text{Hom}_{an}(M_1, M_2)$  of complex analytic maps  $f : M_1 \rightarrow M_2$  such that  $f(0) = 0$ ; these are the analogs of isogenies. The following proposition is a consequence of the Uniformization theorem.

**Proposition 1.2.** (i) *The set  $\text{Hom}_{an}(M_1, M_2)$  is naturally given by  $\{\alpha \in \mathbb{C} : \alpha \cdot \Lambda_1 \subset \Lambda_2\}$ . Given  $\alpha$  in this set, the associated map is simply  $z \mapsto \alpha z$ . In particular, each element of  $\text{Hom}_{an}(M_1, M_2)$  is a group homomorphism.*

(ii) *Two surfaces  $\mathbb{C}/\Lambda_1$  and  $\mathbb{C}/\Lambda_2$  are isomorphic as Riemann surfaces iff there exists  $\lambda \in \mathbb{C}^\times$  such that  $\Lambda_1 = \lambda \cdot \Lambda_2$ .*

*Proof.* Since (ii) is an immediate consequence of (i), it remains to prove (i). Suppose that  $f : \mathbb{C}/\Lambda_1 \rightarrow \mathbb{C}/\Lambda_2$  is a complex analytic map with  $f(0) = 0$ . By the Uniformization theorem, we deduce the existence of a holomorphic  $\tilde{f} : \mathbb{C} \rightarrow \mathbb{C}$  lifting the map  $f$  with  $\tilde{f}(0) = 0$ . We need to show that  $\tilde{f}(z) = \alpha z$  for some  $\alpha$ .

For each  $w \in \Lambda_1$ , consider the function  $z \mapsto \tilde{f}(z+w) - \tilde{f}(z)$ . This takes values in  $\Lambda_2$ , which is discrete, and thus this function is constant. So  $\tilde{f}'(z+w) = \tilde{f}'(z)$ . In particular,  $\tilde{f}'$  is a holomorphic function on  $\mathbb{C}$  which is  $\Lambda_1$ -periodic. By Liouville's theorem,  $\tilde{f}'$  is constant, and  $f(z) = \alpha z + \beta$ . Since  $f(0) = 0$ ,  $\beta = 0$ .  $\square$

We say that two lattices are **homothetic** if they are (complex) scalar multiples of each other. The above proposition says that there is an equivalence of the category of compact Riemann surfaces of genus 1 (with morphisms complex analytic maps) and the category of homothety classes of  $\mathbb{Z}$ -lattices in  $\mathbb{C}$  (with morphisms given by scalar multiplication as above).

Let's examine the homothety classes of lattices in greater detail. Given a lattice  $L$ , choose a basis  $\{z_1, z_2\}$ . One of  $z_1/z_2$  or  $z_2/z_1$  has positive imaginary part, say  $z_2/z_1$ . Since we are considering  $L$  up to homothety, we can replace  $L$  by  $z_1^{-1}L$  which has basis  $\{1, z_2/z_1\}$ . Thus, in every homothety class of lattices, one can find a representative  $L_z$  which has basis  $\{1, z\}$  with  $\text{Im}(z) > 0$ . When are two lattices  $L_{z_1}$  and  $L_{z_2}$  in the same homothety class? This happens iff there is a scalar  $\lambda$  such that

$$\begin{cases} \lambda \cdot z_2 = az_1 + b \\ \lambda \cdot 1 = cz_1 + d \end{cases}$$

for some  $a, b, c, d \in \mathbb{Z}$ , with  $ad - bc = 1$ . Thus, we see that  $L_{z_1}$  and  $L_{z_2}$  are in the same homothety class iff

$$z_2 = \frac{az_1 + b}{cz_1 + d}$$

for some

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}).$$

The above formula defines an action of  $SL_2(\mathbb{R})$  on the upper plane  $\mathcal{H}$  and we have shown that the isomorphism classes of elliptic curves over  $\mathbb{C}$  are indexed naturally by  $SL_2(\mathbb{Z})$ -orbits on  $\mathcal{H}$ .

**Torsion points and Endomorphisms** The concrete description  $M = \mathbb{C}/\Lambda$  allows us to read off many group theoretic properties of  $M$ . For example, let  $M[m] = \{P \in M : mP = 0\}$ . Then it is clear that

$$M[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

Also, the set of torsion points is dense in  $M$ .

**Proposition 1.3.** *The ring  $\text{End}(M)$  is either  $\mathbb{Z}$  or an order in an imaginary quadratic extension. Every such order arises as  $\text{End}(M)$  for some  $M$ .*

*Proof.* Let's assume that  $M = \mathbb{C}/\Lambda_\tau$  with  $\tau \in \mathcal{H}$ . Clearly,  $\text{End}(M)$  contains the subring  $\mathbb{Z} = \{[m] : m \in \mathbb{Z}\}$ . We first show that  $\text{End}(M)$  is larger than  $\mathbb{Z}$  iff  $\mathbb{Q}(\tau)$  is an imaginary quadratic extension of  $\mathbb{Q}$ .

If  $\lambda \in \mathbb{C}^\times \setminus \mathbb{Z}$  satisfies  $\lambda\Lambda \subset \Lambda$ , we have

$$\begin{cases} \lambda = a\tau + b \\ \lambda \cdot \tau = c\tau + d \end{cases}$$

with  $a, b, c, d \in \mathbb{Z}$ . This implies that  $\tau$  satisfies the quadratic polynomial with integer coefficients:

$$a\tau^2 + (b - c)\tau - d = 0.$$

Since  $\tau \notin \mathbb{Z}$ , we have  $a \neq 0$ , so that  $\mathbb{Q}(\tau)$  is an imaginary quadratic extension of  $\mathbb{Q}$ . Thus it is clear that the set  $End(M)$  is an order in  $\mathbb{Q}(\tau)$ , since it contains  $\mathbb{Z} + \mathbb{Z}a\tau$ .

Conversely, if  $\mathbb{Q}(\tau)$  is an imaginary quadratic extension, then  $\tau$  satisfies some equation  $a\tau^2 + b\tau + c = 0$  for  $a, b, c \in \mathbb{Z}$  and  $a \neq 0$ . Then  $a\tau \in End(M)$ , so that  $End(M)$  is larger than  $\mathbb{Z}$ .

Finally, given any order  $\mathcal{O} \subset K$ , an imaginary quadratic extension, we have a field embedding  $K \hookrightarrow \mathbb{C}$  and may regard  $\mathcal{O}$  as a lattice in  $\mathbb{C}$ . Then  $M = \mathbb{C}/\mathcal{O}$  satisfies  $End(M) = \mathcal{O}$  (because  $1 \in \mathcal{O}$ ).  $\square$

**Remarks:** This proposition explains why those elliptic curves with  $End(M)$  larger than  $\mathbb{Z}$  are said to have complex multiplication.

### An Equivalence of Categories

At this point, the theory of compact Riemann surfaces of topological genus 1 is beginning to look remarkably similar to the theory of elliptic curves. For the rest of this chapter, we shall see that there is an equivalence of the following categories:

- (i) The category of compact Riemann surfaces of topological genus 1, with morphisms given by  $Hom_{an}(M_1, M_2)$ .
- (ii) The category of elliptic curves over  $\mathbb{C}$  with morphisms given by isogenies.
- (iii) The category whose objects are homothety classes of lattices in  $\mathbb{C}$  with  $Mor(\Lambda_1, \Lambda_2) = \{\alpha \in \mathbb{C} : \alpha\Lambda_1 \subset \Lambda_2\}$ .

We have already seen the equivalence of (i) and (iii), so the main point is to explain the equivalence of (i) and (ii). For lack of time, we shall not give the full details of the proof. We shall see that the notion of “modular forms” arises naturally in the study of this equivalence.

### Weierstrass $\mathcal{P}$ -function

We will now explain how to identify  $\mathbb{C}/\Lambda_\tau$  with an elliptic curve. More specifically, we shall construct a complex analytic embedding  $f : \mathbb{C}/\Lambda_\tau \rightarrow \mathbb{P}^2(\mathbb{C})$  whose image is a smooth curve defined by the equation  $y^2 = 4x^3 - g_2(\tau)x - g_3(\tau)$ . The map  $f$  sends the identity element of the group  $\mathbb{C}/\Lambda_\tau$  to the point at infinity of the plane curve.

The map  $f$  has the form  $f(z) = (X(z) : Y(z) : 1)$  for some meromorphic functions  $X(z)$  and  $Y(z)$ . What properties must the functions  $X$  and  $Y$  have? For one thing, we have to make sure that  $X$  and  $Y$  are periodic with respect to translation by  $\Lambda_\tau$ . This leads us to the question of constructing such meromorphic functions. As we noted before, by Liouville’s theorem, such a  $\Lambda$ -periodic function cannot be holomorphic. Further, by the residue theorem, it cannot have just a single pole in  $\mathbb{C}/\Lambda$ . Thus, the simplest such functions must have either a double pole at some point in  $\mathbb{C}/\Lambda$  or else have 2 simple poles.

**Definition:** The Weierstrass  $\mathcal{P}$ -function is defined by:

$$\mathcal{P}(z) = \frac{1}{z^2} + \sum_{0 \neq \lambda \in \Lambda} \left( \frac{1}{(z + \lambda)^2} - \frac{1}{\lambda^2} \right).$$

This converges locally uniformly in  $z$  and defines a  $\Lambda$ -periodic meromorphic function with a double pole at each point in  $\Lambda$  (and holomorphic everywhere else). Note that  $\mathcal{P}$  is an even function. Its Laurent expansion at 0 looks like:

$$\mathcal{P}(z) = \frac{1}{z^2} + \sum_{k=2}^{\infty} (2k-1) \cdot G_{2k}(\tau) z^{2k-2}$$

with

$$G_{2k}(\tau) = \sum_{0 \neq \lambda \in \Lambda_\tau} \frac{1}{\lambda^{2k}}.$$

Consider the derivative of  $\mathcal{P}$ :

$$\mathcal{P}'(z) = -2 \cdot \sum_{\lambda \in \Lambda} \frac{1}{(z+\lambda)^3}.$$

This has a triple pole at points in  $\Lambda$ . The functions  $\mathcal{P}$  and  $\mathcal{P}'$  are important because of the following fact (cf. [Silverman, Thm. 3.2, Pg. 154]):

**Theorem 1.4.** *Any  $\Lambda$ -periodic meromorphic function is a rational function of  $\mathcal{P}'(z)$  and  $\mathcal{P}(z)$ .*

Now we define a complex analytic map

$$f : \mathbb{C}/\Lambda_\tau \longrightarrow \mathbb{P}^2(\mathbb{C})$$

by:

$$f(z) = (\mathcal{P}(z) : \mathcal{P}'(z) : 1).$$

To show that the image is contained in a plane cubic, consider the two functions  $\mathcal{P}'(z)^2$  and  $4\mathcal{P}^3 + 60G_4\mathcal{P} - 140G_6$ . Their Laurent expansion at 0 looks like:

$$\begin{cases} \mathcal{P}'(z)^2 = \frac{4}{z^6} - \frac{24G_4}{z^2} - 80G_6 + \dots \\ 4\mathcal{P}^3 = \frac{4}{z^6} + \frac{36G_4}{z^2} + 60G_6 + \dots \end{cases}.$$

Thus,  $\mathcal{P}'(z)^2 - 4\mathcal{P}(z) + 60G_4\mathcal{P}(z) + 140G_6$  is a  $\Lambda$ -periodic holomorphic function which vanishes at 0. Thus it must be identically zero, and we get

$$\mathcal{P}'(z)^2 = 4\mathcal{P}(z) - g_2(\tau)\mathcal{P}(z) - g_3(\tau)$$

with  $g_2(\tau) = 60G_4(\tau)$  and  $g_3(\tau) = 140G_6(\tau)$ .

Now there are a number of things to check:

- the cubic equation  $4x^3 - g_2(\tau)x - g_3(\tau) = 0$  does not repeated roots.
- the map  $f$  is bijective and is a local isomorphism; thus it is a complex analytic isomorphism.
- the map  $f$  is a group homomorphism.

These will be left as guided exercises in Problem Sheet 4.

To have a functor from the category of compact Riemann surfaces of genus 1 to the category of elliptic curves, we further need to show that every complex analytic isogeny gives rise to an algebraic one:

**Proposition 1.5.** *If  $\alpha \in \mathbb{C}$  satisfies  $\alpha\Lambda_1 \subset \Lambda_2$ , then we need to show that the map  $E_{\Lambda_1} \rightarrow E_{\Lambda_2}$  given by:*

$$(\mathcal{P}_{\Lambda_1}(z) : \mathcal{P}'_{\Lambda_1}(z) : 1) \mapsto (\mathcal{P}_{\Lambda_2}(\alpha z) : \mathcal{P}'_{\Lambda_2}(\alpha z) : 1)$$

is a rational map.

*Proof.* Not surprisingly, this will depend on the previous theorem. The functions  $\mathcal{P}_{\Lambda_2}(\alpha z)$  and  $\mathcal{P}'_{\Lambda_2}(\alpha z)$  are both  $\Lambda_1$ -periodic, and thus are rational functions of  $\mathcal{P}_{\Lambda_1}(z)$  and  $\mathcal{P}'_{\Lambda_1}(z)$ .  $\square$

### Glimpses of Modular Forms

If we replace  $\lambda$  by  $\gamma \cdot \lambda$  for some  $\gamma \in SL_2(\mathbb{Z})$ , then  $C/\Lambda_\tau$  and  $\mathbb{C}/\Lambda_{\gamma \cdot \tau}$  are isomorphic as compact Riemann surfaces. How are their associated elliptic curves related? To address this, we prove:

**Proposition 1.6.** *The functions  $G_{2k}(\tau)$  satisfies:*

$$G_{2k}\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^{2k} \cdot G_{2k}(\tau)$$

if

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}).$$

*In particular, the elliptic curves  $E_\tau$  and  $E_{\gamma \cdot \tau}$  are isomorphic as elliptic curves. Thus, we have an injection from the set of isomorphism classes of compact Riemann surface of topological genus 1 to the set of isomorphism classes of elliptic curves over  $\mathbb{C}$ .*

*Proof.* The transformation law of  $G_{2k}$  follows by a direct computation, using the definition

$$G_{2k}(\tau) = \sum_{0 \neq \lambda \in \Lambda} \frac{1}{\lambda^{2k}}.$$

$\square$

A holomorphic function  $f$  on  $\mathcal{H}$  satisfying

$$f\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^k \cdot f(\tau)$$

for all

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}),$$

and which is in addition “holomorphic at the cusps” is called a **modular form of weight  $k$  with respect to  $SL_2(\mathbb{Z})$** . The functions  $G_{2k}$  are the simplest examples of modular forms of

weight  $2k$ . They are non-vanishing at the cusps, and are called **Eisenstein series**. The connection of modular forms with elliptic curves runs much deeper than the above consideration suggests.

### Integration of Invariant Differential

Finally, we shall explain how to go back from an elliptic curve  $E$  over  $\mathbb{C}$  to a lattice  $\Lambda$ . Namely, given an elliptic curve  $E$  in  $\mathbb{P}^2(\mathbb{C})$  defined by  $y^2 = 4x^3 - g_2x - g_3$ , we shall show that there is a lattice  $\Lambda_\tau$  such that  $g_2 = g_2(\tau)$  and  $g_3 = g_3(\tau)$ . The lattice  $\Lambda$  is basically constructed by considering the line integral of the invariant differential  $\frac{dx}{y}$  on  $E$ .

Given the equation  $y^2 = 4x^3 - ax - b$ , let us consider the problem of evaluating the contour integral in the complex plane:

$$I(z) = \int_z \frac{dx}{y} = \int_0^z \frac{dx}{2\sqrt{(x-a)(x-b)(x-c)}}.$$

As it stands, the above expression does not make sense, because the square root term on the right is not even well-defined on  $\mathbb{C} \setminus \{a, b, c\}$ .

From a course in complex analysis, we learn that there are 2 ways of resolving this difficulty. One of these is to take branch cuts in the complex plane. In this case, 2 branch cuts are necessary; one joining  $b$  and  $c$  say, and the other joining  $a$  and  $\infty$ . Having removed these cuts from  $\mathbb{C}$ , one can define the square root unambiguously on the remaining subset of  $\mathbb{C}$ , and the above contour integral makes sense as long as the path of integration does not meet the branch cuts.

The other way is to note that the natural domain of definition of the square root function is not the complex plane  $\mathbb{C}$  but rather a double cover of it. It is this consideration which leads to the development of the theory of Riemann surfaces. In our case, we take two copies of  $\mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$ , cut a slit along the 2 branch cuts in each copy of  $\mathbb{P}^1(\mathbb{C})$  as above, and then glue the 2  $\mathbb{P}^1$ 's together along the slits. Pictorially, it is quite clear that we are going to get a torus, and indeed one can give the resulting topological space the structure of a Riemann surface  $M$  which has topological genus 1. The Riemann surface  $M$  has a natural projection  $\pi$  onto  $\mathbb{P}^1(\mathbb{C})$  and this is a branched cover ramified at the preimages of the 4 points  $a, b, c$  and  $\infty$ .

On this Riemann surface, the function  $\sqrt{(x-a)(x-b)(x-c)}$  is well-defined, and we may consider the contour integral

$$I(z) = \int_\infty^z \frac{dz}{2\sqrt{(x-a)(x-b)(x-c)}}.$$

There is an additional problem with this: one needs to choose a path from  $\infty \in M$  to  $z \in M$ . It turns out that homologous paths give the same value. If  $H_1(M, \mathbb{Z}) = \mathbb{Z}\beta_1 \oplus \mathbb{Z}\beta_2$ , let  $\omega_i$  be the value of above contour integral over the cycle  $\beta_i$ . One checks:

**Lemma 1.7.**  $\omega_1$  and  $\omega_2$  are  $\mathbb{R}$ -linearly independent. In particular,  $\Lambda$  is a rank 2 lattice in  $\mathbb{C}$ .

The lattice  $\Lambda$  is the one associated to the given elliptic curve. Then the integral  $I$  is a map

$$I : M \longrightarrow \mathbb{C}/\Lambda$$

One checks:

**Lemma 1.8.** *The map  $I$  is a complex analytic isomorphism. Thus it makes sense to talk about the holomorphic function  $I^{-1} : \mathbb{C}/\Lambda \longrightarrow M$ .*

It remains to see that if we embed  $\mathbb{C}/\Lambda$  into  $\mathbb{P}^2(\mathbb{C})$  using the Weierstrass  $\mathcal{P}$ -function attached to  $\Lambda$ , then the image satisfies the given cubic equation. Consider the function

$$f : \mathbb{C} \longrightarrow \mathbb{C}/\Lambda \xrightarrow{I^{-1}} M \xrightarrow{\pi} \mathbb{P}^1(\mathbb{C}).$$

One checks:

**Proposition 1.9.** *The function  $f$  is equal to the Weierstrass  $\mathcal{P}$ -function of  $\Lambda$ . Moreover,  $f$  satisfies the equation:  $f'^2 = 4(f - a)(f - b)(f - c)$ . In particular, the original elliptic curve  $E$  is obtained from the lattice  $\Lambda$  using the embedding of  $\mathbb{C}/\Lambda$  into  $\mathbb{P}^2$  provided by the Weierstrass  $\mathcal{P}$ -function of  $\Lambda$ .*