1 The Uniformization Theorem

In these notes we will prove the Uniformization Theorem, which states that any elliptic curve defined over $\mathbb{C}$ is isomorphic to $\mathbb{C}/\Lambda$ for some lattice Λ. We will actually present two proofs. The first, which is shorter, uses the theory of coverings of Riemann surfaces. The second, which contains more ideas that bear fruit beyond the proof of the Uniformization Theorem, constructs a compact Riemann surface whose points correspond to equivalence classes of lattices. The proof then uses this to show that the j invariant, restricted to elliptic curves that come from lattices, is surjective. The main sources used are [1], [2], [3], [4].

1.1 Lattices

1.1.1 Definition. Let V be an n-dimensional real vector space. An additive subgroup $\Lambda \subseteq V$ is called a *lattice* if there exist non-zero vectors $\gamma_1, \ldots, \gamma_n \in V$, linearly independent over $\mathbb{R}$, such that

$$\Lambda = \mathbb{Z}\gamma_1 + \cdots + \mathbb{Z}\gamma_n.$$

The following proposition gives a characterization of lattices that will be useful in showing that they arise from the action of the group of deck transformations on the universal cover $\mathbb{C}$ of a

1.1.2 Proposition. *Let V be a finite dimensional real vector space. A subgroup $\Lambda \subseteq V$ is a lattice if and only if*

(i) *Λ is discrete, i.e. there exist a neighbourhood U of zero such that $\Lambda \cap U = \{0\}$, and*
(ii) *Λ is contained in no proper vector subspace of V.*

PROOF: The forward direction is clear. Suppose that Λ is discrete and is contained in no proper vector subspace of V. By induction on $n = \dim(V)$, we will show that there exist $\gamma_1, \ldots, \gamma_n \in V$ such that

$$\Lambda = \mathbb{Z}\gamma_1 + \cdots + \mathbb{Z}\gamma_n.$$

This is trivial when $n = 0$. Suppose that it holds for $n \geq 0$. We will show that it holds for $n+1$. Since Λ is not contained in any proper vector subspace of V, there exist $n+1$ linearly independent vectors $x_1, \ldots, x_{n+1} \in \Lambda$. Let V_0 be the vector subspace of V spanned by $x_1, \ldots, x_n$, and let $\Lambda_0 = \Lambda \cap V_0$. By applying the induction hypothesis to Λ_0, which is clearly a lattice, there exists linearly independent vectors $\gamma_1, \ldots, \gamma_n \in \Lambda_0 \subset \Lambda$ such that

$$\Lambda_0 = \mathbb{Z}\gamma_1 + \cdots + \mathbb{Z}\gamma_n.$$

Hence every vector $x \in \Lambda$ may be written uniquely in the form

$$x = c_1(x)\gamma_1 + \cdots + c_n(x)\gamma_n + c(x)x_{n+1},$$

where the $c_i(x)$ and $c(x)$ are real numbers. Since the parallelotope

$$P = \{\lambda_1 y_1 + \cdots + \lambda_n y_n + \lambda x_{n+1} : \lambda_i, \lambda \in [0,1]\}$$

is compact, $\Lambda \cap P$ is finite. Hence there exists a vector $y_{n+1} \in (\Lambda \cap P) \setminus V_0$ such that

$$c(y_{n+1}) = \min\{c(x) : x \in (\Lambda \cap P) \setminus V_0\} \in (0,1].$$

We claim that $\Lambda = \Lambda_0 + \mathbb{Z}y_{n+1}$. Suppose that $x \in \Lambda$ is arbitrary. Then there exist $m_j \in \mathbb{Z}$ such that

$$x' = x - \sum_{j=1}^{n+1} m_j y_j = \sum_{j=1}^{n} \lambda_j y_j + \lambda x_{n+1},$$

where $0 \le \lambda_j \le 1$ for $j = 1, \ldots, n$, and $0 \le \lambda < c(y_{n+1})$. Since $x' \in \Lambda \cap P$, it follows from the definition of y_{n+1} that $\lambda = 0$. Thus $x' \in \Lambda \cap V_0 = \Lambda_0$. Hence all λ_j are integers and thus are zero. This implies that $x' = 0$, i.e. that

$$x = \sum_{j=1}^{n+1} m_j y_j \in \mathbb{Z}y_1 + \cdots + \mathbb{Z}y_{n+1}.$$

□

Let Λ be a lattice in $\mathbb{C}$. Clearly, $\mathbb{C}/\Lambda$ is naturally given the structure of a compact Riemann surface, which is also a complex Lie group because Λ is an additive subgroup of $\mathbb{C}$. Recall that the Eisenstein series of weight $2k$ for Λ is the series

$$G_{2k}(\Lambda) = \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \omega^{-2k}.$$

When there is no confusion about Λ, we will simply use the notation G_{2k}. It is proven in Silverman, Theorem IV.3.6 (a) that this series is absolutely convergent for all $k > 1$. We let

$$g_2 = g_2(\Lambda) = 60G_4 \quad \text{and} \quad g_3 = g_3(\Lambda) = 140G_6.$$

Let E be the complex curve given by

$$y^2 = 4x^3 - g_2 x - g_3.$$

It is proven in Silverman, Theorem VI.3.6 that the discriminant of this curve vanishes, i.e. that it is smooth, and thus that it is an elliptic curve. Define the map $\varphi : \mathbb{C}/\Lambda \to E \subseteq \mathbb{P}^2(\mathbb{C})$ by

$$\varphi(z) = [\wp(z) : \wp'(z) : 1].$$

Silverman also proves there that φ is a complex analytic isomorphism of complex Lie groups. Let Λ_1 and Λ_2 be lattices in $\mathbb{C}$. In Corollary VI.4.1.1, Silverman proves that $\mathbb{C}/\Lambda_1$ and $\mathbb{C}/\Lambda_2$ are isomorphic if and only if Λ_1 and Λ_2 are

homothetic, i.e. $\Lambda_1 = \alpha\Lambda_2$ for some $\alpha \in \mathbb{C}^*$. We will now give a different characterization of homothety of lattices.

Let Λ be a lattice, and let $\gamma_1, \gamma_2 \in \mathbb{C}^*$ be independent vectors over $\mathbb{R}$ such that

$$\Lambda = \mathbb{Z}\gamma_1 + \mathbb{Z}\gamma_2.$$

Since γ_1 and γ_2 are independent over $\mathbb{R}$, one of γ_1/γ_2 and γ_2/γ_1 is in the upper half plane, and the other is in the lower half plane. Without loss of generality, suppose that $\gamma_1/\gamma_2 \in \mathbb{H}$, and let $\tau = \gamma_1/\gamma_2$. Define

$$\Lambda_\tau = \mathbb{Z} + \mathbb{Z}\tau.$$

Then Λ and Λ_τ are homothetic, as $\Lambda_\tau = \gamma_1^{-1}\Lambda$. Therefore, for most of our later discussions, we only need to consider lattices of the form Λ_τ for some $\tau \in \mathbb{H}$.

Recall that $\mathrm{SL}(2,\mathbb{R})$ is the group of 2×2 matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with real coefficients such that $ad - bc = 1$. The elements of $\mathrm{SL}(2,\mathbb{R})$ are realized as the Möbius transformations on $\mathbb{P}^1$, i.e. if $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, we define

$$Az = \frac{az + b}{cz + d}.$$

It is easy to verify the formula

$$\mathrm{Im}(Az) = \frac{(ad - bc)\mathrm{Im}(z)}{|cz + d|^2} = \frac{\mathrm{Im}(z)}{|cz + d|^2},$$

which implies that the upper half plane $\mathbb{H}$ is invariant under the action of $\mathrm{SL}(2,\mathbb{R})$. Since the element $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ of $\mathrm{SL}(2,\mathbb{R})$ acts as the identity transformation on $\mathbb{H}$, the group action of $\mathrm{SL}(2,\mathbb{R})$ on $\mathbb{H}$ is not faithful. However, this is essentially the only obstruction to a faithful action of $\mathrm{SL}(2,\mathbb{R})$ on $\mathbb{H}$.

1.1.3 Proposition. *The group action of* $\mathrm{SL}(2,\mathbb{R})/\{\pm 1\}$ *on* $\mathbb{H}$ *is faithful. Furthermore,* $\mathrm{SL}(2,\mathbb{R})/\{\pm 1\}$ *is precisely the group of automorphisms of* $\mathbb{H}$.

PROOF: This is an exercise in elementary complex analysis. □

Let $\mathrm{SL}(2,\mathbb{Z})$ be the subgroup of $\mathrm{SL}(2,\mathbb{R})$ formed by the matrices with integer coefficients. The action of $\mathrm{SL}(2,\mathbb{Z})$ on $\mathbb{H}$ is intimately connected to the study of elliptic curves. The following proposition is the first step in the construction of modular curves.

1.1.4 Proposition. *If* $\tau, \tau' \in \mathbb{H}$, *then* Λ_τ *and* $\Lambda_{\tau'}$ *are homothetic if and only if there is some* $A \in \mathrm{SL}(2,\mathbb{Z})$ *such that* $\tau' = A\tau$.

PROOF: Suppose that $\Lambda_t au$ and $\Lambda_{\tau'}$ are homothetic. Then there exists some $\alpha \in \mathbb{C}^*$ such that $\Lambda_\tau = \alpha\Lambda_{\tau'}$. Thus α and $\alpha\tau'$ generate Λ_τ, so there exist $a, b, c, d \in \mathbb{Z}$ such that $ad - bc = \pm 1$, $\alpha\tau' = a\tau + b$, and $\alpha = c\tau + d$. Thus,

$$\tau' = \frac{a\tau + b}{\alpha} = \frac{a\tau + b}{c\tau + d} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\tau.$$

Since τ and τ' are both in $\mathbb{H}$, we have that $ad-bc = 1$, so that $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}(2,\mathbb{Z})$.

Conversely, suppose that there is some $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}(2,\mathbb{Z})$ such that $\tau' = A\tau$. Let $\alpha = c\tau + d$. Then $\alpha\tau' = a\tau + d$, so that $\Lambda_{\tau'} \subseteq \alpha\Lambda_\tau$. Since $ad - bc = 1$, we can exchange τ and τ' and do the same with $A^{-1} \in \mathrm{SL}(2,\mathbb{Z})$ to show that $\alpha\Lambda_\tau \subseteq \Lambda_{\tau'}$. □

1.2 A Covering Space Proof

The following proposition could be included in the proof of the Uniformization Theorem, but it is of independent interest.

1.2.1 Proposition. *Let G be a group of automorphisms of $\mathbb{C}$ with no fixed points such that every orbit of G is discrete. Then G is one of the following:*

(i) *the trivial group,*
(ii) *the group of all translations of the form*

$$z \mapsto z + n\gamma,$$

where $\gamma \in \mathbb{C}^*$ is fixed and $n \in \mathbb{Z}$,
(iii) *the group of all translations of the form*

$$z \mapsto z + m\gamma_1 + n\gamma_2,$$

where $\gamma_1, \gamma_2 \in \mathbb{C}^*$ are fixed and linearly independent over $\mathbb{R}$, and $m, n \in \mathbb{Z}$.

PROOF: It is well known that the holomorphic automorphisms of $\mathbb{C}$ are the affine maps of the form

$$z \mapsto az + b,$$

where $a, b \in \mathbb{C}$ and $a \neq 0$. If $a \neq 1$, then this transformation has a fixed point. Thus G consists only of translations $z \mapsto z + b$. Let Λ be the orbit of the origin under G. Then Λ is a discrete subgroup of $\mathbb{C}$ and G consists of all translations $z \mapsto z + b$, where $b \in \Lambda$. Let $V \subseteq \mathbb{C}$ be the smallest real subspace of $\mathbb{C}$ containing Λ. By Proposition 1.1.2, depending on whether the dimension of V is 0, 1, or 2, one has case (i), (ii), or (iii). □

1.2.2 Theorem (Uniformization). *Let X be a compact Riemann surface of genus one. Then X is isomorphic to $\mathbb{C}/\Lambda$ for some lattice $\Lambda \subseteq \mathbb{C}$.*

PROOF: Since X has genus one, its universal cover is $\mathbb{C}$. Hence covering space theory says that X is isomorphic to the orbit space $\Gamma\backslash\mathbb{C}$, where Γ is the group of deck transformations of the cover of X by $\mathbb{C}$. By covering space theory, we also known that this action has discrete orbits and is free of fixed points. Therefore, by Proposition 1.2.1, Γ is of one of the three forms mentioned in the proposition. Since X is compact, this eliminates the first two possibilities,

which would lead to non-compact orbit spaces. Therefore, Γ consists of all translations of the form

$$z \mapsto z + m\gamma_1 + n\gamma_2,$$

where $\gamma_1, \gamma_2 \in \mathbb{C}^*$ are fixed and linearly independent over $\mathbb{R}$, and $m, n \in \mathbb{Z}$. But this implies that X is isomorphic to $\mathbb{C}/\Lambda$, where Λ is the orbit of the origin, i.e.

$$\Lambda = \{m\gamma_1 + n\gamma_2 : m, n \in \mathbb{Z}\}. \qquad \square$$

1.3 Discrete Subgroups of $\mathrm{SL}(2, \mathbb{R})$

We are mostly interested in the group $\mathrm{SL}(2, \mathbb{Z})$ in proving the Uniformization Theorem, but other discrete subgroups of $\mathrm{SL}(2, \mathbb{R})$ are important, e.g. for defining higher modular curves.

1.3.1 Definition. If $A \in \mathrm{SL}(2, \mathbb{R})$, we say that A is *hyperbolic* if its eigenvalues are real and distinct, *elliptic* if its eigenvalues are not real and distinct (and thus complex conjugates of each other), and *parabolic* otherwise.

Recall that a non-trivial Möbius transformation has either one or two fixed points on $\mathbb{P}^1$. It is easy to see that $A \in \mathrm{SL}(2, \mathbb{R})$ is hyperbolic if and only if it has two fixed points on $\mathbb{R}$, elliptic if and only if it has two fixed points, one in $\mathbb{H}$ and the other in $\mathbb{H}$, and parabolic if and only if it has exactly one fixed point. Given a subgroup Γ of $\mathrm{SL}(2, \mathbb{R})$, we can examine the action of Γ on $\mathbb{H}$ in terms of the fixed points of the transformations in Γ.

1.3.2 Definition. Let Γ be a subgroup of $\mathrm{SL}(2, \mathbb{R})$. If the stabilizer of $z \in \mathbb{H}$ under the action of Γ is trivial, we call z a *regular* point of Γ. If z is the unique fixed point in $\mathbb{H}$ of an elliptic element of Γ, we say that z is an *elliptic* point of Γ. If $z \in \mathbb{R} \cup \{\infty\}$ is the unique fixed point of a parabolic element of Γ, we say that z is a *cusp* of Γ.

We would like to form an orbit space of the action of Γ on $\mathbb{H}$. However, it will often be the case that the orbit space is not compact. In order to remedy this situation, we will adjoin additional points in order to compactify the orbit space. These additional points we will add are simply the cusps of Γ, which intuitively makes sense, as the points of $\mathbb{R} \cup \{\infty\}$ are the "points at infinity" of $\mathbb{H}$. For any cusp s of Γ, we define

$$\mathrm{P}(s) = \{A \in \mathrm{SL}(2, \mathbb{R}) : A(s) = s, \text{ and } A \text{ is parabolic or } A = \pm 1\},$$

and

$$\Gamma_s = \{\sigma \in \Gamma : \sigma(z) = z\}.$$

1.3.3 Proposition. *Let Γ be a discrete subgroup of Γ, and let s be a cusp of Γ. The quotient $\Gamma_s/(\Gamma \cap \{\pm 1\})$ is isomorphic to $\mathbb{Z}$. Moreover, an element of Γ_s is either ± 1 or parabolic, i.e. $\Gamma_s = \Gamma \cap P(s)$.*

PROOF: Omitted for now, but not too difficult. □

1.3.4 Definition. Let Γ be a subgroup of $\mathrm{SL}(2,\mathbb{R})$, let $\mathrm{Cusp}(\Gamma)$ be the set of cusp points of Γ, and let $\mathbb{H}^* = \mathbb{H} \cup \mathrm{Cusp}(\Gamma)$. If $z \in \mathbb{H}^*$, we let $\Gamma(z)$ denote the orbit of z, and we let $\Gamma\backslash\mathbb{H}^*$ denote the set of orbits of $\mathbb{H}^*$ under the action of Γ.

We would like to put a topology on $\Gamma\backslash\mathbb{H}^*$. In order to do this, we must first put a topology on $\mathbb{H}^*$, as the subspace topology will not give the desired behaviour at the cusp points. We will define the topology on $\mathbb{H}^*$ by defining families of local neighbourhood systems. We give any point in $\mathbb{H}$ the usual neighbourhood system. If z is a cusp of Γ other than ∞ then we take the basic neighbourhoods of z to be

$$\{z\} \cup \{\text{the interior of a circle in } \mathbb{H} \text{ tangent to the real axis at } z\}.$$

If ∞ is a cusp of Γ, then we take the basic neighbourhoods of ∞ to be

$$\{\infty\} \cup \{z \in \mathbb{H} : \mathrm{Im}(z) > C\},$$

where $C > 0$. It is easy to see that this defines a Hausdorff topology on $\mathbb{H}^*$, and that every element of Γ acts as a homeomorphism of $\mathbb{H}^*$. We can then form the quotient space $\Gamma\backslash\mathbb{H}^*$. We would like to show that the quotient space is a locally compact Hausdorff space.

We will assume that ∞ is a cusp of Γ, which is true in all of the cases we considered in class. If $\sigma \in \Gamma$, let c_σ denote the lower left entry of the matrix σ. Then $\Gamma_\infty = \{\sigma \in \Gamma : c_\sigma = 0\}$. By Proposition 1.3.3, there is a generator $\pm \left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right)$ of Γ_∞ modulo ± 1.

1.3.5 Proposition. *$|c_\sigma|$ depends only on the double coset $\Gamma_\infty \sigma \Gamma_\infty$.*

PROOF: This is a simple computation. □

1.3.6 Proposition. *Given $M > 0$, there are only finitely many double cosets $\Gamma_\infty \sigma \Gamma_\infty$ such that $\sigma \in \Gamma$ and $|c_\sigma| \le M$.*

PROOF: Since $\Gamma_\infty = \{\sigma \in \Gamma : c_\sigma = 0\}$, it is sufficient to consider only those σ for which $c_\sigma \neq 0$. Let $\tau = \pm \left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right)$ of Γ_∞ modulo ± 1. Let $\sigma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$, with c non-zero such that $|c| \le M$. We want to find an element σ'' in $\Gamma_\infty \sigma \Gamma_\infty$ such that $\sigma''(i)$ is contained in a compact set K which depends only on M and h. First, choose $n \in \mathbb{Z}$ such that

$$1 \le d + nhc \le 1 + |hc|,$$

and let $\sigma' = \sigma\tau^n = \left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right)$. Then $|c'| = |c|$, $|d'| = d + nhc$, and

$$\mathrm{Im}(\sigma'(i)) = \frac{1}{c'^2 + d'^2}.$$

We have $1 \le |d'| \le 1 + |hc|$ and $|c| \le M$, so

$$1 \le c'^2 + d'^2 < M^2 + (1 + |h|M)^2.$$

Therefore, $\sigma'(i)$ belongs to the domain defined by

$$1 \ge \mathrm{Im}(z) \ge \frac{1}{M^2 + (1 + |h|M)^2}.$$

The transformation $z \mapsto \tau^m(z) = z + mh$ does not change $\mathrm{Im}(z)$, so we can take m so that $\tau^m\sigma'(i)$ is in this domain and

$$0 \le \mathrm{Re}(z) \le |h|.$$

The set

$$K = \left\{ z \in \mathbb{H} : 0 \le \mathrm{Re}(z) \le |h| \text{ and } 1 \ge \mathrm{Im}(z) \ge \frac{1}{M^2 + (1 + |h|M)^2} \right\}$$

is a compact subset of $\mathbb{H}$. We have thus found an element $\sigma'' = \tau^m\sigma\tau^n$ such that $\sigma''(i) \in K$. It is then not hard to show that by the discreteness of Γ there must be only finitely many such σ''. □

1.3.7 Proposition. *There exists a positive number r, depending only on Γ, such that $|c_\sigma| \ge r$ for all $\sigma \in \Gamma \setminus \Gamma_\infty$. Moreover, for such an r, one has*

$$\mathrm{Im}(z) \cdot \mathrm{Im}(\sigma(z)) \le \frac{1}{r^2}$$

for all $z \in \mathbb{H}$ and all $\sigma \in \Gamma \setminus \Gamma_\infty$.

PROOF: The existence of such an r follows immediately from the previous proposition. If $\sigma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$ and $c \ne 0$, then we have

$$\mathrm{Im}(\sigma(z)) = \frac{\mathrm{Im}(z)}{|cz + d|^2} \le \frac{\mathrm{Im}(z)}{(c\mathrm{Im}(z))^2} \le \frac{1}{r^2\mathrm{Im}(z)}.$$ □

1.3.8 Proposition. *For every cusp s of Γ, there exists a neighbourhood U of s in $\mathbb{H}^*$ such that $\Gamma_s = \{\sigma \in \Gamma : \sigma(U) \cap U \ne \emptyset\}$.*

PROOF: We may assume that $s = \infty$. Let $U = \{z \in \mathbb{H}^* : \mathrm{Im}(z) > 1/r\}$, where r is chosen as in the previous proposition. If $\sigma \in \Gamma \setminus \Gamma_\infty$ and $z \in U$, we have, by the previous proposition, that $\mathrm{Im}(\sigma(z)) < 1/r$. □

It follows that two points of U are equivalent under Γ if and only if they are equivalent under Γ_s, so we may identify $\Gamma_s\backslash U$ with a subset of $\Gamma\backslash\mathbb{H}^*$.

1.3.9 Proposition. *For every cusp s of Γ and for every compact set K of $\mathbb{H}$, there exists a neighbourhood U of s such that $U \cap \Gamma(K) = \emptyset$ for every $\gamma \in \Gamma$.*

PROOF: Again, we assume that $s = \infty$. We can find two positive numbers A and B so that $A < \mathrm{Im}(z) < B$ for all $z \in K$. Let r be as in Proposition 1.3.7, and let

$$U = \{z \in \mathbb{H}^* : \mathrm{Im}(z) > \max(B, 1/(Ar^2))\}.$$

By Proposition 1.3.7, if $\sigma \in \Gamma \setminus \Gamma_\infty$, then $\mathrm{Im}(\sigma(z)) < 1/(Ar^2)$. If $\sigma \in \Gamma_\infty$, then $\mathrm{Im}(\sigma(z)) = \mathrm{Im}(z) < B$. □

1.3.10 Theorem. *The quotient topology on* $\Gamma\backslash\mathbb{H}^*$ *is Hausdorff.*

PROOF: We know that the quotient $\Gamma\backslash\mathbb{H}$ is Hausdorff from basic facts about discrete group actions. Since $\Gamma\backslash\mathbb{H}^*$ is the union of $\Gamma\backslash\mathbb{H}$, it remains to show that an equivalence class of cusps can be separated from an equivalence class of points in $\mathbb{H}$ and also from another equivalence class of cusps. Proposition 1.3.9 handles the former case, so let us only be concerned with the latter case. Suppose that there exist two cusps s and t which are not equivalent. Without loss of generality, we may assume that $t = \infty$. Let $\pm \left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right)$ be as before, and define

$$\begin{aligned} L &= \{z \in \mathbb{C} : \mathrm{Im}(z) = u\}, \\ K &= \{z \in L : 0 \le \mathrm{Re}(z) \le |h|\}, \\ V &= \{z \in \mathbb{H}^* : \mathrm{Im}(z) > u\}, \end{aligned}$$

where $u > 0$. Since K is compact, by Proposition 1.3.9 there is a neighbourhood U of s so that $K \cap \Gamma U = \emptyset$. We may assume that the boundary of U is a circle tangent to the real line. We now simply need to show that $V \cap \Gamma U = \emptyset$. Suppose, on the contrary, that $\gamma(U) \cap V \neq \emptyset$ for some $\gamma \in \Gamma$. Since $\gamma(s) \neq \infty$, the boundary of $\gamma(U)$ is a circle tangent to the real line. Therefore, if $\gamma(U) \cap V \neq \emptyset$, then $\gamma(U) \cap L \neq \emptyset$. Hence $\gamma(U)$ intersects some translation of K by an element δ of Γ_∞. Then $\delta^{-1}\gamma(U) \cap K \neq \emptyset$, which gives a contradiction. Therefore, our assumption that there are two inequivalent cusps is false. □

1.3.11 Proposition. *The quotient topology on* $\Gamma\backslash\mathbb{H}^*$ *is locally compact.*

PROOF: We already know that any point in $\Gamma\backslash\mathbb{H}$ has a system of compact neighbourhoods, so we only need ot worry about cusps. Let s be a cusp of Γ, and let $\pi : \mathbb{H}^* \to \Gamma\backslash\mathbb{H}^*$ be the natural projection map. As usual, without loss of generality we may assume that $s = \infty$. By Proposition 1.3.8 and the remarks thereafter, there exists a neighbourhood $V = \{z \in \mathbb{H}^* : \mathrm{Im}(z) \ge c\}$ with a positive constant c such that V/Γ_∞ is identified with $\pi(V)$. If $\pm \left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right)$ is a generator of Γ_∞ modulo ± 1, we see that $\pi(V)$ coincides with the image of

$$\{z \in V : z = \infty \text{ or } 0 \le \mathrm{Re}(z) \le |h|\}$$

under π. The latter set is obviously compact, so $\pi(V)$ is compact. □

We will now put a complex structure on $\Gamma\backslash HP^*$. Let $\pi : \mathbb{H}^* \to \Gamma\backslash\mathbb{H}^*$ denote the natural projection map. For every $v \in \mathbb{H}^*$, let

$$\Gamma_v = \{\gamma \in \Gamma : \gamma(v) = v\}.$$

From elementary facts about discrete group actions in the case of $v \in \mathbb{H}$ and Proposition 1.3.8 in the case of a cusp, there exists an open neighbourhood U of v such that

$$\Gamma_v = \{\gamma \in \Gamma : \gamma(U) \cap U \neq \emptyset\}.$$

Ths gives an injection $\Gamma_v\backslash U \to \Gamma\backslash\mathbb{H}^*$ such that $\Gamma_v\backslash U$ is an open neighbourhood of $\pi(v)$. If v is neither elliptic nor a cusp, thn Γ_v contains only 1 and possible -1, so that the map $\varphi : U \to \Gamma_v\backslash U$ is a homeomorphism. We take $(\Gamma_v\backslash U, \pi^{-1})$ to be a pair of a neighbourhood and local parameter in the complex structure on $\Gamma\backslash\mathbb{H}^*$.

If v is elliptic, let $\overline{\Gamma_v}$ denote the group $(\Gamma_v \cdot \{\pm 1\})/\{\pm 1\}$. Let λ be a holomorphic isomorphism of $\mathbb{H}$ onto the unit disc D such that $\lambda(v) = 0$. If $\overline{\Gamma_v}$ is of order n, then $\lambda\overline{\Gamma_v}\lambda^{-1}$ consists of the transformations $w \mapsto \zeta^k w$ for $k = 0, \ldots n-1$, where $\zeta = e^{2pii/n}$. We can then define a map $p : \Gamma_v\backslash U \to \mathbb{C}$ by $p(\pi(z)) = \lambda(z)^n$. It is easy to see that p is a homeomorphism onto an open subset of $\mathbb{C}$, so we include the pair $(\Gamma_v\backslash U, p)$ in the complex structure on $\Gamma\backslash\mathbb{H}^*$.

Let s be a cusp of Γ, and let σ be an element of $\mathrm{SL}(2,\mathbb{R})$ such that $\sigma(s) = \infty$. Then

$$\sigma\Gamma_s\sigma^{-1} \cdot \{\pm 1\} = \left\{ \pm \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}^m : m \in \mathbb{Z} \right\}$$

for some $h > 0$. Then we can define a homeomorphism p of $\Gamma_s\backslash U$ into an open subset of $\mathbb{C}$ by

$$p(\pi(z)) = \frac{\exp(2\pi i p(z))}{h},$$

and we include the pair $(\Gamma_s\backslash U, p)$ in the complex structure on $\Gamma\backslash\mathbb{H}^*$. It is easy to verify that this actually defines a complex structure.

1.4 The Modular Group

The *modular group* is the group $\mathrm{SL}(2,\mathbb{Z})$ of matrices in $\mathrm{SL}(2,\mathbb{R})$ with integer coefficients. Clearly, $\mathrm{SL}(2,\mathbb{Z})$ is a discrete subgroup of $\mathrm{SL}(2,\mathbb{R})$.

1.4.1 Proposition. *The cusps of* $\mathrm{SL}(2,\mathbb{Z})$ *are precisely the points in* $\mathbb{Q} \cup \{\infty\}$*, and all of these cusps lie in the same* $\mathrm{SL}(2,\mathbb{Z})$ *orbit.*

PROOF: It is clear that ∞ is a fixed point under the parabolic element $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ of $\mathrm{SL}(2,\mathbb{Z})$. Let $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ be a parabolic element of $\mathrm{SL}(2,\mathbb{Z})$, and let z be its unique fixed point. Since we already dealt with ∞, we may assume that z is finite, in which case it satisfies the equation

$$cz^2 + (d-a)z - b = 0,$$

and $c \neq 0$. Since the discriminant of the above equation vanishes, z must be rational. Conversely, if $p, q \in \mathbb{Z}$ satisfy $q \neq 0$ and $\gcd(p,q) = 1$, let t and u be integers such that $pt - qu = 1$. Then

$$\sigma = \begin{pmatrix} p & u \\ q & t \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}),$$

and $\sigma(\infty) = p/q$. Since the image of any cusp under the action of $\mathrm{SL}(2,\mathbb{Z})$ is a cusp, this implies that the cusps of $\mathrm{SL}(2,\mathbb{Z})$ are precisely the points of $\mathbb{Q} \cup \{\infty\}$. Also, it implies that all cusps are in a single orbit. Therefore,

$$\mathrm{SL}(2,\mathbb{Z})\backslash\mathbb{H}^* = (\mathrm{SL}(2,\mathbb{Z})\backslash\mathbb{H}) \cup \{\infty\}. \qquad \square$$

1.4.2 Definition. If Γ is a discrete subgroup of $\mathrm{SL}(2,\mathbb{R})$, we call F a *fundamenal domain* for Γ if

(i) F is a connected open subset of $\mathbb{H}$;
(ii) every point of $\mathbb{H}$ is equivalent to some point of the closure of F under Γ;
(iii) no two points of F are equivalent under Γ.

It is apparently possible to show that every discrete subgroup of $\mathrm{SL}(2,\mathbb{R})$ has a fundamental domain, but we will only identify the fundamental domain of $\mathrm{SL}(2,\mathbb{Z})$.

1.4.3 Theorem. *The set*

$$F = \left\{ z \in \mathbb{C} : -\frac{1}{2} < \mathrm{Re}(z) < \frac{1}{2}, |z| > 1 \right\}$$

is a fundamental domain for $\mathrm{SL}(2,\mathbb{Z})$.

PROOF: Clearly, F is a connected open subset of $\mathbb{H}$. Fix $z \in \mathbb{H}$ and $\sigma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}(2,\mathbb{Z})$. Then

$$\mathrm{Im}(\sigma(z)) = \frac{\mathrm{Im}(z)}{|cz+d|^2}.$$

Since $\{cz + d : c, d \in \mathbb{Z}\}$ is a lattice in $\mathbb{C}$, there exists a pair $(c,d) \neq (0,0)$ minimizing $|cz+d$. Thus, for a given z, there is a $\sigma \in \mathrm{SL}(2,\mathbb{Z})$ maximizing $\mathrm{Im}(\sigma(z))$. We will assume that σ has this property, and let $w = \sigma(z) = x + iy$, and let $\gamma = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. Then

$$\mathrm{Im}(\gamma\sigma(z)) = \mathrm{Im}\left(\frac{-1}{w}\right) = \frac{y}{|w|^2} \leq y,$$

and hence $|w| \geq 1$. If $\tau = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, we have that

$$\mathrm{Im}(\tau^h\sigma(z)) = \mathrm{Im}(\sigma(z))$$

for every $h \in \mathbb{Z}$, and hence $|\tau^h \sigma(z)| \geq 1$. Choosing a suitable h, we see that z is equivalent to a point of the region

$$\overline{F} = \left\{ z \in \mathbb{C} : -\frac{1}{2} \leq \mathrm{Re}(z) \leq \frac{1}{2}, |z| \geq 1 \right\}.$$

Now all that remains to be shown is that no two points of F are equivalent under Γ. Let z and z' be distinct points of F, and suppose that $z' = \sigma(z)$ for some $\sigma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}(2, \mathbb{Z})$. Without loss of generality, we may assume that

$$\mathrm{Im}(z) \leq \mathrm{Im}(z') = \frac{\mathrm{Im}(z)}{|cz + d|^2}.$$

Then

$$|c| \cdot \mathrm{Im}(z) \leq |cz + d| \leq 1.$$

If $c = 0$, then a and d are equal and are either -1 or 1, so that $z' = z \pm b$, which is impossible. Therefore, $c \neq 0$. By some simple plane geometry, we observe that $\mathrm{Im}(z) > \sqrt{3}//2$, so by the above equation, $|c| = 1$, and we have that $|z \pm d| \leq 1$. But if $z \in F$ and $|d| \geq$, we have that $|z + d| > 1$. Therefore, we must have that $d = 0$, so that $|z| \leq 1$. But this contradicts the assumption that $z \in F$. Therefore, our assumption that z and z' are equivalent under the action of $\mathrm{SL}(2, \mathbb{Z})$ is false, showing that F is a fundamental domain for $\mathrm{SL}(2, \mathbb{Z})$. □

1.4.4 Corollary. *The Riemann surface* $\mathrm{SL}(2, \mathbb{Z}) \backslash \mathbb{H}^* = (\mathrm{SL}(2, Z) \backslash \mathbb{H}) \cup \{\infty\}$ *is compact.*

PROOF: This follows from the easily verified fact that

$$F' = \left\{ z \in \mathbb{C} : |z| \geq 1, \mathrm{Re}(z) = -\frac{1}{2} \right\} \cup \left\{ z \in \mathbb{C} : |z| = 1, = \frac{1}{2} \leq \mathrm{Re}(z) \leq 0 \right\}$$

is a se of representatives for $\mathbb{H}$ modulo the action of $\mathrm{SL}(2, \mathbb{Z})$. □

1.4.5 Proposition. *The group* $\mathrm{SL}(2, \mathbb{Z})$ *is generated by the elements*

$$\sigma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \tau = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

PROOF: Let G be the subgroup of $\mathrm{SL}(2, \mathbb{Z})$ generated by σ and τ. Then $-1 = \tau^2 \in G$. Observe that every element in $\mathrm{SL}(2, \mathbb{Z})$ of the form $\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$ is contained in G, and if $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in G$, then

$$\begin{pmatrix} -c & -d \\ a & b \end{pmatrix} = \tau \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G.$$

Suppose that $G \neq \mathrm{SL}(2, \mathbb{Z})$, and fix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}(2, \mathbb{Z}) \setminus G$ such that $\min(|a|, |c|)$ is minimized. We may assume that $|a| \geq |c| > 0$. Let q and r be integers such that $a = cq + r$ and $0 \leq r < |c|$. Then

$$\sigma^{-q} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} r & * \\ c & * \end{pmatrix} \notin G,$$

and

$$r = \min(r, |c|) < |c| = \min(|a|, |c|),$$

contradicting the choice of $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Therefore, our assumption that G is not all of $\mathrm{SL}(2,\mathbb{Z})$ is false. □

1.5 Modular Functions

We are interested functions that we can define that are invariants of elliptic curves, and in particular, functions on elliptic curves that come from lattices that are invariants of the underlying curves. Since the points of $\mathrm{SL}(2,\mathbb{Z})\backslash\mathbb{H}$ correspond to equivalence classes of lattices under homothety, it is natural to attempt to define these as meromorphic functions on $\mathrm{SL}(2,\mathbb{Z})\backslash\mathbb{H}^*$, or meromorphic functions on $\mathbb{H}$ that satisfy certain regularity conditions under the action of $\mathrm{SL}(2,\mathbb{Z})$. We will also be interested in functions that do not quite pass to the quotient, but fail to do so in a rather trivial way.

1.5.1 Definition. Let k be an integer, and let f be a meromorphic function on $\mathbb{H}$. We say that f is *weakly modular of weight* $2k$ if

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^{2k} f(z)$$

for all $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}(2,\mathbb{Z})$ and $z \in \mathbb{H}$.

Remark. The reason we only consider modular functions of even weight is that there would be no interesting function satisfying the definition for an odd weight m, as $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \in \mathrm{SL}(2,\mathbb{Z})$ and we would have

$$f(z) = f\left(\frac{-z+0}{0-1}\right) = (-1)^m f(z) = -f(z)$$

for all $z \in \mathbb{H}$.

Since we computed a useful set of generators for $\mathrm{SL}(2,\mathbb{Z})$, we have an alternate characterization of modular functions.

1.5.2 Proposition. *Let f be a meromorphic function on $\mathbb{H}$. Then f is weakly modular of weight $2k$ if and only if*

$$f(z+1) = f(z) \quad \text{and} \quad f\left(-\frac{1}{z}\right) = z^{2k} f(z)$$

for all $z \in \mathbb{H}$.

PROOF: Immediate from Proposition 1.4.5. □

Suppose that f is a meromorphic function on $\mathbb{H}$ such that $f(z+1) = f(z)$. Then f can be expressed as a function of $q(z) = e^{2\pi iz}$ that is holomorphic in the open unit disk with the origin removed, which we will denote by $\tilde{f}$. If $\tilde{f}$ extends to a holomorphic (meromorphic) function at the origin, then we say that f is *holomorphic (meromorphic) at infinity*. If f is holomorphic at infinity, we define $f(\infty) = \tilde{f}(0)$. This notation makes sense, because both 0 and ∞ are cusps of $\mathrm{SL}(2,\mathbb{Z})$, and all cusps of $\mathrm{SL}(2,\mathbb{Z})$ are equivalent. If f is a weakly modular function of weight $2k$, we say that f is a *modular function of weight* $2k$. It is easy to see that the modular functions on $\mathbb{H}$ correspond to the meromorphic functions on $\mathrm{SL}(2,\mathbb{Z})\backslash\mathbb{H}^*$ by examining the definition of the complex structure on $\mathbb{H}^*$.

1.5.3 Definition. If f is a modular function that is holomorphic everywhere (including infinity), we say that f is a *modular form*. If, in addition, it vanishes at infinity, we say that it is a *cusp form*.

A modular form is then given by a series

$$f(z) = \sum_{n=0}^{\infty} a_n q^n = \sum_{n=0}^{\infty} a_n e^{2\pi inz},$$

which converges for $|q| < 1$, i.e. for $\mathrm{Im}(z) > 0$, and satisfies the identity

$$f\left(-\frac{1}{z}\right) = z^{2k} f(z).$$

It is a cusp form precisely when $a_0 = 0$.

We have already encountered the Eisenstein series of a lattice. We will define a modular form G_{2k} on $\mathbb{H}$ by simply letting $G_{2k}(z)$ be the Eisenstein series of the lattice Λ_z, i.e.

$$G_{2k}(z) = \mathrm{G}_{2k}(\Lambda_z) = \sum_{\substack{\omega\in\Lambda_z \\ \omega\neq 0}} \omega^{-2k} = \sum_{m,n\in\mathbb{Z}} (mz+n)^{-2k}.$$

1.5.4 Proposition. *Let $k > 1$ be an integer. The function G_{2k} is a modular form of weight $2k$, and $G_{2k}(\infty) = 2\zeta(2k)$, were ζ is the Riemann zeta function.*

PROOF: The definition of G_{2k} and what we already know about the Eisenstein series of a lattice show that G_{2k} is a weakly modular function of weight $2k$ that is holomorphic in $\mathbb{H}$. To show that G_{2k} is holomorphic at infinity, we need to show that $G_{2k}(z)$ has a limit as $\mathrm{Im}(z) \to \infty$. If we suppose that z is in the fundamental domain D, then we can apply uniform convergence and compute the limit term by term. The terms $(mz+n)^{-2k}$ relative to $m \neq 0$ give 0, and the others give n^{-2k}. Therefore,

$$\lim_{\mathrm{Im}(z)\to\infty} G_{2k}(z) = \sum_{n\in\mathbb{Z}} n^{-2k} = 2\sum_{n=1}^{\infty} n^{-2k} = 2\zeta(2k).$$

□

The Eisenstein series that we are most concerned with are those with weights 4 and 6. It is helpful to replace them with the multiples

$$g_4(z) = 60G_4(z) \qquad \text{and} \qquad g_6(z) = 140G_3(z).$$

We then have $g_4(\infty) = 120\zeta(4)$ and $g_6(\infty) = 280\zeta(6)$. Using the known values of the Riemann zeta function, we have that

$$g_4(\infty) = \frac{4}{3}\pi^4 \qquad \text{and} \qquad g_6(\infty) = \frac{8}{27}\pi^6.$$

Hence, if we let

$$\Delta(z) = g_4^3(z) - 27g_6^2(z),$$

then $\Delta(\infty) = 0$, so Δ is a cusp form of weight 12.

Let j be the function defined by

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

It follows from our previous investigation of the j invariant for elliptic curves that $j(z)$ is the j invariant of $\mathbb{C}/\Lambda_z$.

1.5.5 Proposition. *The function j is a modular function of weight 0 that is holomorphic on $\mathbb{H}$ and has a simple pole at infinity.*

PROOF: The first assertion follows from the fact that g_4^3 and Δ are both modular functions of weight 12. The second assertion follows from the fact that g_4^3 is non-zero at infinity whereas Δ has a simple zero at infinity. □

We are now ready to prove the result that has motivated most of our labour.

1.5.6 Theorem. *The function j induces an analytic isomorphism of $\mathrm{SL}(2,\mathbb{Z})\backslash\mathbb{H}^*$ with $\mathbb{P}^1$.*

PROOF: Clearly, j is injective when viewed as a holomorphic function from $\mathrm{SL}(2,\mathbb{Z})\backslash\mathbb{H}^*$ to $\mathbb{P}^1$, and it is obviously non-zero. Therefore, by the compactness of $\mathrm{SL}(2,\mathbb{Z})\backslash\mathbb{H}^*$, j is surjective. Therefore, j is an analytic isomorphism. □

1.5.7 Corollary. *Let E be a complex elliptic curve. Then E is isomorphic to E/Λ for some lattice Λ in $\mathbb{C}$.*

PROOF: This follows from the surjectivity of the j function given by previous theorem and the fact that the j invariant is a complete invariant of elliptic curves. □

Bibliography

[1] Forster, Otto. *Lectures on Riemann-Surfaces*. Springer-Verlag, 1981.

[2] Serre, J. P. *A Course in Arithmetic*. Springer-Verlag, 1996.

[3] Shimura, Goto. *The Arithmetic Theory of Automorphic Forms*. Princeton University Press, 1971.

[4] Silverman, Joseph. *The Arithmetic of Elliptic Curves*, 2 ed. Springer-Verlang, 1992.