Our first goal for this lecture is to complete the proof of the uniformization theorem, which states that every elliptic curve $E/\mathbb{C}$ is isomorphic to a torus $\mathbb{C}/L$ for some lattice L. Given what we have already proved, it suffices to show that the map that sends a lattice L to its j-invariant $j(L)$ is surjective; every complex number is the j-invariant of some lattice.

18.1 The j-function

Every lattice $[\omega_1, \omega_2]$ is homothetic to a lattice of the form $[1, \tau]$, with τ in the upper half plane $\mathbb{H} = \{z \in \mathbb{C} : \operatorname{im} z > 0\}$; we may take $\tau = \pm\omega_2/\omega_1$ with the sign chosen so that $\operatorname{im} \tau > 0$. This leads to the following definition of the j-function.

Definition 18.1. The *j-function* $j\colon \mathbb{H} \to \mathbb{C}$ is defined by $j(\tau) = j([1, \tau])$. We similarly define $g_2(\tau) = g_2([1, \tau])$, $g_3(\tau) = g_3([1, \tau])$, and $\Delta(\tau) = \Delta([1, \tau])$.

Note that for any $\tau \in \mathbb{H}$, the quantities $-1/\tau$ and $\tau + 1$ also lie in $\mathbb{H}$.

Theorem 18.2. *The j-function is holomorphic on $\mathbb{H}$, and satisfies $j(-1/\tau) = j(\tau)$ and $j(\tau + 1) = j(\tau)$.*

Proof. From the definition of $j(\tau) = j([1, \tau])$ we have

$$j(\tau) = 1728\frac{g_2(\tau)^3}{\Delta(\tau)} = 1728\frac{g_2(\tau)^3}{g_2(\tau)^3 - 27g_3(\tau)^2}.$$

The series defining

$$g_2(\tau) = 60\sum_{m,n\in\mathbb{Z}}{}' \frac{1}{(m + n\tau)^4} \qquad \text{and} \qquad g_3(\tau) = 140\sum_{m,n\in\mathbb{Z}}{}' \frac{1}{(m + n\tau)^6}$$

converge absolutely for any fixed $\tau \in \mathbb{H}$, by Lemma 16.11, and uniformly over τ in any compact subset of $\mathbb{H}$. The proof of this last fact is straight-forward but slightly technical; see [1, Thm. 1.15] for the details. It follows that $g_2(\tau)$ and $g_3(\tau)$ are both holomorphic on $\mathbb{H}$, and therefore $\Delta(\tau) = g_2(\tau)^3 - 27g_3(\tau)^2$ is also holomorphic on $\mathbb{H}$. Since $\Delta(\tau)$ is nonzero for all $\tau \in \mathbb{H}$, by Lemma 16.21, the j-function $j(\tau)$ is holomorphic on $\mathbb{H}$ as well.

The lattices $[1, \tau]$ and $[1, -1/\tau] = -1/\tau[1, \tau]$ are homothetic, and the lattices $[1, \tau + 1]$ and $[1, \tau]$ are equal; thus $j(-1/\tau) = j(\tau)$ and $j(\tau + 1) = j(\tau)$, by Theorem 17.6. □

18.2 The modular group

We now consider the *modular group*

$$\Gamma = \mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z},\ ad - bc = 1 \right\}.$$

As proved in Problem Set 8, the group Γ acts on $\mathbb{H}$ via linear fractional transformations

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

and Γ is generated by the matrices $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. This implies that the j-function is invariant under the action of the modular group. In fact, more is true.

Andrew V. Sutherland

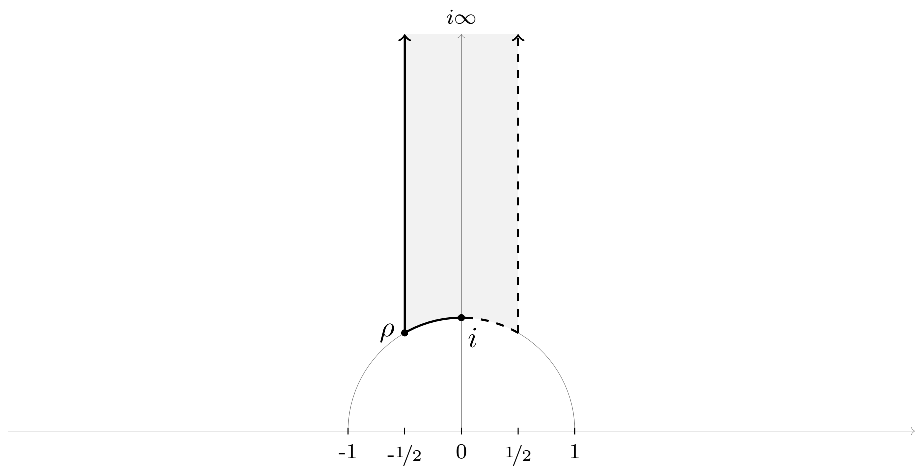

Figure 1: Fundamental domain $\mathcal{F}$ for the action of $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}$, with $\rho = e^{2\pi i/3}$.

Lemma 18.3. *We have $j(\tau) = j(\tau')$ if and only if $\tau' = \gamma\tau$ for some $\gamma \in \Gamma$.*

Proof. We have $j(S\tau) = j(-1/\tau) = j(\tau)$ and $j(T\tau) = j(\tau+1) = j(\tau)$, by Theorem 18.2, It follows that if $\tau' = \gamma\tau$ then $j(\tau') = j(\tau)$, since S and T generate Γ.

To prove the converse, let us suppose that $j(\tau) = j(\tau')$. Then by Theorem 17.6, the lattices $[1,\tau]$ and $[1,\tau']$ must be homothetic So suppose $[1,\tau'] = \lambda[1,\tau]$, for some $\lambda \in \mathbb{C}^*$. Then there exist integers a, b, c, and d such that

$$\tau' = a\lambda\tau + b\lambda$$
$$1 = c\lambda\tau + d\lambda$$

From the second equation, we see that $\lambda = \frac{1}{c\tau+d}$. Substituting this into the first, we have

$$\tau' = \frac{a\tau+b}{c\tau+d} = \gamma\tau, \qquad \text{where } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Similarly, using $[1,\tau] = \lambda^{-1}[1,\tau']$, we can write $\tau = \gamma'\tau'$ for some integer matrix γ'. The fact that $\tau' = \gamma\gamma'\tau'$ implies that $\det\gamma = \pm 1$ (since γ and γ' are integer matrices), and since τ and τ' both lie in $\mathbb{H}$, we must have $\det\gamma = 1$, and therefore $\gamma \in \Gamma$ as desired. □

Lemma 18.3 implies that when studying the j-function, we are really only interested in how it behaves on Γ-equivalence classes of $\mathbb{H}$, that is, the orbits of $\mathbb{H}$ under the action of Γ. We thus consider the quotient of $\mathbb{H}$ modulo Γ-equivalence, which we denote by $\mathbb{H}/\Gamma$. Some authors instead write $\Gamma\backslash\mathbb{H}$, to indicate that the action is on the left. The actions of γ and $-\gamma$ are identical, so taking the quotient by $\mathrm{PSL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})/\{\pm 1\}$ yields the same result, but for the sake of clarity we will stick with $\Gamma = \mathrm{SL}_2(\mathbb{Z})$.

We now wish to determine a fundamental domain for $\mathbb{H}/\Gamma$, a set of unique representatives in $\mathbb{H}$ for each Γ-equivalence class. For this purpose we will use the set

$$\mathcal{F} = \{\tau \in \mathbb{H} : \mathrm{re}(\tau) \in [-1/2, 1/2) \text{ and } |\tau| \geq 1, \text{ such that } |\tau| > 1 \text{ if } \mathrm{re}(\tau) > 0\}.$$

Lemma 18.4. *The set $\mathcal{F}$ is a fundamental domain for $\mathbb{H}/\Gamma$.*

Proof. We need to show that for every $\tau \in \mathbb{H}$, there is a unique $\tau' \in \mathcal{F}$ such that $\tau' = \gamma\tau$, for some $\gamma \in \Gamma$. We first prove existence. Let us fix $\tau \in \mathbb{H}$. For any $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$ we have

$$\operatorname{im}(\gamma\tau) = \operatorname{im}\left(\frac{a\tau + b}{c\tau + d}\right) = \frac{\operatorname{im}\big((a\tau + b)(c\bar{\tau} + d)\big)}{|c\tau + d|^2} = \frac{(ad - bc)\operatorname{im}\tau}{|c\tau + d|^2} = \frac{\operatorname{im}\tau}{|c\tau + d|^2} \tag{1}$$

Let $c\tau + d$ be a shortest vector in the lattice $[1, \tau]$. Then c and d must be relatively prime, and we can pick integers a and b so that $ad - bc = 1$. The matrix $\gamma_0 = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ then maximizes the value of $\operatorname{im}(\gamma\tau)$ over $\gamma \in \Gamma$. Let us now choose $\gamma = T^k\gamma_0$, where k is chosen so that $\operatorname{re}(\gamma\tau) \in [1/2, 1/2)$, and note that $\operatorname{im}(\gamma\tau) = \operatorname{im}(\gamma_0\tau)$ remains maximal. We must have $|\gamma\tau| \geq 1$, since otherwise $\operatorname{im}(S\gamma\tau) > \operatorname{im}(\gamma\tau)$, contradicting the maximality of $\operatorname{im}(\gamma\tau)$. Finally, if $\tau' = \gamma\tau \notin \mathcal{F}$, then we must have $|\gamma\tau| = 1$ and $\operatorname{re}(\gamma\tau) > 0$, in which case we replace γ by $S\gamma$ so that $\tau' = \gamma\tau \in \mathcal{F}$.

It remains to show that τ' is unique. This is equivalent to showing that any two Γ-equivalent points in $\mathcal{F}$ must coincide. So let τ_1 and $\tau_2 = \gamma_1\tau_1$ be two elements of $\mathcal{F}$, with $\gamma_1 = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, and assume $\operatorname{im}\tau_1 \leq \operatorname{im}\tau_2$. Then by (1), we must have $|c\tau_1 + d|^2 \leq 1$, thus

$$1 \geq |c\tau_1 + d|^2 = (c\tau_1 + d)(c\bar{\tau}_1 + d) = c^2|\tau_1|^2 + d^2 + 2cd\operatorname{re}(\tau_1) \geq c^2|\tau_1|^2 + d^2 - |cd|.$$

We cannot have $c = d = 0$, and we must have $|\tau_1| \geq 1$, thus the RHS is at least 1. So equality holds throughout and we have $|c\tau_1 + d| = 1$, which implies $\operatorname{im}\tau_2 = \operatorname{im}\tau_1$. We also must have $|c|, |d| \leq 1$, and by replacing γ_1 by $-\gamma_1$ if necessary, we may assume that $c \geq 0$. This leaves 3 cases:

1. $c = 0$: then $|d| = 1$ and $a = d$. So $\tau_2 = \tau_1 \pm b$, but $|\operatorname{re}\tau_2 - \operatorname{re}\tau_1| < 1$, so $\tau_2 = \tau_1$.
2. $c = 1, d = 0$: then $b = -1$ and $|\tau_1| = 1$. So τ_1 is on the unit circle and $\tau_2 = a - 1/\tau_1$. Either $a = 0$ and $\tau_2 = \tau_1 = i$, or $a = -1$ and $\tau_2 = \tau_1 = \rho$.
3. $c = 1, |d| = 1$: then $|\tau_1 + d| = 1$, so $\tau_1 = \rho$, and $\operatorname{im}\tau_2 = \operatorname{im}\tau_1 = \sqrt{3}/2$ implies $\tau_2 = \rho$.

$\square$

Theorem 18.5. *The restriction of the j-function to $\mathcal{F}$ defines a bijection from $\mathcal{F}$ to $\mathbb{C}$.*

Proof. Injectivity follows immediately from Lemmas 18.3 and 18.4. It remains to prove surjectivity. We have

$$g_2(\tau) \;=\; 60 \sum_{n,m \in \mathbb{Z}}{}' \frac{1}{(m + n\tau)^4} \;=\; 60\left(2\sum_{m=1}^{\infty} \frac{1}{m^4} + \sum_{\substack{n,m \in \mathbb{Z} \\ n \neq 0}} \frac{1}{(m + n\tau)^4}\right)$$

The second sum tends to 0 as $\operatorname{im}\tau \to \infty$. Thus we have

$$\lim_{\operatorname{im}\tau \to \infty} g_2(\tau) = 120 \sum_{m=1}^{\infty} m^{-4} = 120\,\zeta(4) = 120\,\frac{\pi^4}{90} = \frac{4\pi^4}{3},$$

where $\zeta(s)$ is the Riemann zeta function. Similarly,

$$\lim_{\operatorname{im}\tau \to \infty} g_3(\tau) = 280\,\zeta(6) = 280\,\frac{\pi^6}{945} = \frac{8\pi^6}{27}.$$

Thus

$$\lim_{\mathrm{im}\tau\to\infty} \Delta(\tau) = \left(\frac{4}{3}\pi^4\right)^3 - 27\left(\frac{8}{27}\pi^6\right)^2 = 0.$$

(this explains the coefficients 60 and 140 in the definitions of g_2 and g_3; they are the smallest pair of integers that ensure this limit is 0). Since $\Delta(\tau)$ is the denominator of $j(\tau)$, the quantity $j(\tau) = g_2(\tau)^3/\Delta(\tau)$ is unbounded as $\mathrm{im}\,\tau \to \infty$.

In particular, j is a non-constant holomorphic function on the open set $\mathbb{H}$. By the open-mapping theorem [3, Thm. 3.4.4], $j(\mathbb{H})$ is an open subset of $\mathbb{C}$.

We now show that $j(\mathbb{H})$ is also a closed subset of $\mathbb{C}$. Let $j(\tau_1), j(\tau_2), \ldots$ be an arbitrary convergent sequence in $j(\mathbb{H})$, converging to $w \in \mathbb{C}$. The j-function is Γ-invariant, by Lemma 18.3, so we may assume the τ_n all lie in $\mathcal{F}$. The sequence $\mathrm{im}\,\tau_1, \mathrm{im}\,\tau_2, \ldots$ must be bounded, since $j(\tau) \to \infty$ as $\mathrm{im}\,\tau \to \infty$, thus the τ_n all lie in a compact set $\Omega \subset \mathcal{F} \subset \mathbb{H}$. Thus there is a subsequence of the τ_n that converges to some $\tau \in \Omega \subset \mathbb{H}$. By continuity, $j(\tau) = w$, thus the set $j(\mathbb{H})$ contains all its limit points and is therefore closed.

The fact that the non-empty set $j(\mathbb{H}) \subseteq \mathbb{C}$ is both open and closed implies that $j(\mathbb{H}) = \mathbb{C}$, since $\mathbb{C}$ is connected. It follows that $j(\mathcal{F}) = \mathbb{C}$, since every element of $\mathbb{H}$ is equivalent to an element of $\mathcal{F}$ (Lemma 18.4) and the j-function is Γ-invariant (Lemma 18.3). □

Corollary 18.6 (Uniformization Theorem)**.** *For every elliptic curve $E/\mathbb{C}$ there exists a lattice L such that $E(\mathbb{C})$ is isomorphic to $\mathbb{C}/L$.*

Proof. Given $E/\mathbb{C}$, pick $\tau \in \mathbb{H}$ so that $j(\tau) = j(E)$ and let $L = [1, \tau]$. Then E is isomorphic to the elliptic curve corresponding to L, via Theorem 17.2, and therefore $E(\mathbb{C}) \simeq \mathbb{C}/L$. □

18.3 Complex multiplication

Having established the correspondence between complex tori $\mathbb{C}/L$ and elliptic curves $E/\mathbb{C}$, we now wish to make explicit the relationship between endomorphisms of $\mathbb{C}/L$ and endomorphisms of $E/\mathbb{C}$.

Theorem 18.7. *Let L be a lattice, let $E/\mathbb{C}$ be the corresponding elliptic curve given by Theorem 17.2, and let $\Phi\colon \mathbb{C}/L \to E(\mathbb{C})$ be the isomorphism that sends z to $\big(\wp(z), \wp'(z)\big)$. For any $\alpha \in \mathbb{C}$, the following are equivalent:*

(1) $\alpha L \subseteq L$;

(2) $\wp(\alpha z) = u\big(\wp(z)\big)/v\big(\wp(z)\big)$ *for some polynomials* $u, v \in \mathbb{C}[x]$;

(3) *There exists an endomorphism $\phi \in \mathrm{End}(E)$ such that the following diagram commutes:*

$$\begin{array}{ccc} \mathbb{C}/L & \xrightarrow{\Phi} & E(\mathbb{C}) \\ \big\downarrow{\scriptstyle\alpha} & & \big\downarrow{\scriptstyle\phi} \\ \mathbb{C}/L & \xrightarrow{\Phi} & E(\mathbb{C}) \end{array}$$

where α denotes the map $z \mapsto \alpha z$ on $\mathbb{C}/L$.

Moreover, every endomorphism ϕ in $\mathrm{End}(E)$ gives rise to an $\alpha \in \mathbb{C}$ satisfying (1)–(3), and the map that sends ϕ to α is a ring isomorphism from $\mathrm{End}(E)$ to $\{\alpha \in \mathbb{C} : \alpha L \subseteq L\}$. In particular, the endomorphism ϕ in (3) is unique, and $N(\alpha) = \deg \phi = \deg u = \deg v + 1$.

Proof. Properties (1)–(3) clearly hold for $\alpha = 0$, so assume $\alpha \neq 0$.

(1) $\Rightarrow$ (2): Let $\omega \in L$. Then $\wp(\alpha(z+\omega)) = \wp(\alpha z+\alpha\omega) = \wp(\alpha z)$. Thus $\wp(\alpha z)$ is periodic, and $\wp(\alpha z)$ is clearly meromorphic, so it is an elliptic function (with respect to L). It is also even, since $\wp(z)$ is, so it is a rational function of $\wp(z)$, by Lemma 18.10 below.

(2) $\Rightarrow$ (1): We have $v(\wp(z))\wp(\alpha z) = u(\wp(z))$. Both $\wp(z)$ and $\wp(\alpha z)$ have a double pole at 0. Thus $u(\wp(z))$ has a pole of order $2\deg u$ at 0 and $v(\wp(z))\wp(\alpha z)$ has a pole of order $2\deg v + 2$ at 0, hence $\deg u = \deg v + 1$. Thus $u(\wp(z))$ has a pole of order $2\deg v + 2$ at every $\omega \in L$, so $\wp(\alpha z)$ must have a double pole at every $\omega \in L$. It follows that $\wp(z)$ has a double pole at $\alpha\omega$ for all $\omega \in L$, and therefore $\alpha L \subseteq L$.

(2) $\Rightarrow$ (3): Let ϕ be the rational map

$$\phi = \left(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y\right),$$

where u and v are given by (2), and $s = (u'v - v'u)$ and $t = \alpha v^2$, so that

$$\wp'(\alpha z) = \frac{1}{\alpha}\big(\wp(\alpha z)\big)' = \frac{1}{\alpha}\left(\frac{u(\wp(z))}{v(\wp(z)}\right)' = \frac{s(\wp(z))}{t(\wp(z))}\wp'(z).$$

To verify that the diagram commutes, we note that going around the square clockwise yields

$$\phi(\Phi(z)) = \phi\big((\wp(z), \wp'(z))\big) = \left(\frac{u(\wp(z))}{v(\wp(z))}, \frac{s(\wp(z))}{t(\wp(z))}\wp'(z)\right),$$

and going around the square counter-clockwise yields

$$\Phi(\alpha z) = \big(\wp(\alpha z), \wp'(\alpha z)\big) = \left(\frac{u(\wp(z))}{v(\wp(z))}, \frac{s(\wp(z))}{t(\wp(z))}\wp'(z)\right).$$

(3) $\Rightarrow$ (1). Let $\phi \in \mathrm{End}(E)$ satisfy (3). For any $\omega \in L$ we have $\phi(\Phi(\omega)) = 0$, and by commutativity of the diagram, $\Phi(\alpha\omega) = \phi(\Phi(\omega)) = 0$, thus $\alpha\omega \in L$. Therefore $\alpha L \subseteq L$.

We now prove the "moreover" part of the theorem. For any $\phi \in \mathrm{End}(E)$, the map

$$\phi^* = \Phi^{-1} \circ \phi \circ \Phi$$

is an endomorphism of $\mathbb{C}/L$. By taking a small neighborhood U of 0 in $\mathbb{C}$, we obtain a map from U to $\mathbb{C}$ that is holomorphic[1] away from 0. Since $\phi^* \in \mathrm{End}(\mathbb{C}/L)$, we have

$$\phi^*(z_1 + z_2) \equiv \phi^*(z_1) + \phi^*(z_2) \bmod L,$$

and $\phi^*(0) \in L$. By replacing ϕ^* with $\phi^* - \phi^*(0)$ if necessary, we may assume that $\phi^*(0) = 0$. By continuity, $\phi^*(z)$ is arbitrarily close to 0 when z is close to 0, so by making U sufficiently small, we have

$$\phi^*(z_1 + z_2) = \phi^*(z_1) + \phi^*(z_2)$$

for all $z_i \in U$. We now use the definition of the derivative to compute

$$(\phi^*)'(z) = \lim_{h\to 0}\frac{\phi^*(z+h) - \phi^*(z)}{h} = \lim_{h\to 0}\frac{\phi^*(z) + \phi^*(h) - \phi^*(h)}{h} = \lim_{h\to 0}\frac{\phi^*(h) - \phi^*(0)}{h} = (\phi^*)'(0).$$

[1] An analog of the inverse function theorem holds for holomorphic functions.

Thus the derivative of ϕ^* is equal to some constant $\alpha = (\phi^*)'(0)$ at all $z \in U$. Thus $\phi^*(z) = \alpha z$ for all $z \in U$. For any $z \in \mathbb{C}$, we may choose $n \in \mathbb{Z}$ such that $\frac{z}{n} \in U$. Thus

$$\phi^*(z) = n\phi^*\left(\frac{z}{n}\right) = n\alpha\frac{z}{n} = \alpha z.$$

The map ϕ^* sends lattice points to lattice points, and we have just shown that ϕ^* is the "multiplication-by-α" map. Thus $\alpha L \subseteq L$, and α satisfies the equivalent conditions (1)–(3).

We now show that the map $\Psi\colon \operatorname{End}(E) \to \{\alpha \in \mathbb{C} : \alpha L \subseteq L\}$ that sends ϕ to $\alpha = (\phi^*)'(0)$ is a ring homomorphism. Clearly, $\Psi(0) = 0$ and $\Psi(1) = 1$. Let $\phi_1, \phi_2 \in \operatorname{End}(E)$. Then

$$(\phi_1 + \phi_2)^* \;=\; \Phi^{-1} \circ (\phi_1 + \phi_2) \circ \Phi \;=\; \Phi^{-1} \circ \phi_1 \circ \Phi + \Phi^{-1} \circ \phi_2 \circ \Phi \;=\; \phi_1^* + \phi_2^*,$$

since Φ is an isomorphism. It follows that $\Psi(\phi_1 + \phi_2) = \Psi(\phi_1) + \Psi(\phi_2)$, since we have $(\phi_1^* + \phi_2^*)'(0) = (\phi_1^*)'(0) + (\phi_2^*)'(0)$. Similarly,

$$(\phi_1 \circ \phi_2)^* \;=\; \Phi^{-1} \circ (\phi_1 \circ \phi_2) \circ \Phi \;=\; \Phi^{-1} \circ \phi_1 \circ \Phi \circ \Phi^{-1} \circ \phi_2 \circ \Phi \;=\; \phi_1^* \circ \phi_2^*,$$

and $(\phi_1^* \circ \phi_2^*)'(0) = (\phi_1^*)'(\phi_2^*(0))(\phi_2^*)'(0) = (\phi_1^*)'(0)(\phi_2^*)'(0)$, thus $\Psi(\phi_1 \circ \phi_2) = \Psi(\phi_1) \circ \Psi(\phi_2)$.

Thus Ψ is a ring homomorphism. If $\Psi(\phi) = 0$, then $\phi^* = 0$, and in this case the identity $\Phi \circ \phi^* = \phi \circ \Phi$ implies that $\phi = 0$, since Φ is an isomorphism. Therefore Ψ is injective. If $\alpha L \subset L$, then for the ϕ given by (3) we have $\phi^*(z) = \alpha z$, and therefore $\Psi(\phi) = (\phi^*)'(0) = \alpha$, so Ψ is surjective. Thus Ψ is an isomorphism.

It follows that for any $\phi \in \operatorname{End}(E)$, the complex number $\alpha = \Psi(\phi)$ satisfies the equation $X^2 - (\operatorname{tr}\phi)X + \deg\phi = 0$, which has integer coefficients. Therefore α is a quadratic integer with trace $T(\alpha) = \alpha + \bar{\alpha} = \operatorname{tr}(\phi)$ and norm $N(\alpha) = \alpha\bar{\alpha} = \deg\phi = \deg u = \deg v + 1$. $\square$

Corollary 18.8. *Let E be an elliptic curve defined over $\mathbb{C}$. Then $\operatorname{End}(E)$ is commutative and therefore isomorphic to either $\mathbb{Z}$ or an order in an imaginary quadratic field.*

Proof. Let L be the lattice corresponding to E. The ring $\operatorname{End}(E) \simeq \{\alpha \in \mathbb{C} : \alpha L \subseteq L\}$ is clearly commutative, and therefore not an order in a quaternion algebra. The result then follows from Corollary 14.16. $\square$

Remark 18.9. Corollary 18.8 applies to elliptic curves over $\mathbb{Q}$, and over number fields, since these are subfields of $\mathbb{C}$, and it can be extended to arbitrary fields of characteristic 0 via the Lefschetz principle; see [2, Thm. VI.6.1].

Lemma 18.10. *Let $f(z)$ be an elliptic function with respect to a lattice L. Then $f(z)$ can be written as a rational function of $\wp(z) = \wp(z; L)$ and $\wp'(z) = \wp'(z; L)$. Moreover, if $f(z)$ is an even function, then it can be written as a rational function of $\wp(z)$ alone.*

Proof. Every function $f(z)$ can be written as the sum of an even and an odd function, namely, $f(z) = f_e(z) + f_o(z)$, where

$$f_e(z) = \frac{f(z) + f(-z)}{2} \quad \text{and} \quad f_o(z) = \frac{f(z) - f(-z)}{2}.$$

It thus suffices to consider the cases where f is even or odd. We first consider the case that f is even, and we assume that f is nonzero, since the lemma clearly holds for $f = 0$.

Suppose that f is holomorphic at all points not in L. Then it has a Laurent expansion about 0 of the form

$$f(z) = \sum_{k=-n}^{\infty} a_{2k} z^{2k},$$

where $2n$ is the order of f. If $n \geq 0$, then f is holomorphic on $\mathbb{C}$, and since f is periodic with respect to L it is bounded, so by Liouville's theorem it is a constant function $f(z) = f(0)$. If $n > 0$, then $f(z) - a_{-2n}\wp^n(z)$ is an even elliptic function of order at most $2(n-1)$ that is holomorphic except at points in L. By repeating the process until $n = 0$, we obtain a function of the form $f(z) - P\big(\wp(z)\big)$, for some polynomial $p \in \mathbb{C}[x]$, and this function must be equal to a constant $a_0 \in \mathbb{C}$. Thus $f(z) = p(\wp(z)) + f(0)$ is a polynomial in $\wp(z)$.

Now suppose that f has a pole of order n at some $\omega \notin L$. If $2\omega \in L$, we first replace f by a function of the form $g = (af+b)/(cf+d)$, with $a, b, c, d \in \mathbb{C}$ chosen so that $ad - bc \neq 0$, such that g does has neither a zero nor a pole at ω. This transformation is invertible, so if we can write g as a rational function of $\wp$, then we can write f as a rational function of $\wp$. After repeating this process up to three times, if necessary, we may assume without loss of generality that $2\omega \notin L$ for every $\omega \notin L$ at which f has a pole.

Consider the function

$$(\wp(z) - \wp(\omega))^n.$$

Since $2\omega \notin L$, we have $\wp'(\omega) \neq 0$, so ω is a simple root of $\wp(z) - \wp(\omega)$ and the function $(\wp(z)-\wp(\omega))^n$ has a zero of order n at ω. This implies that $(\wp(z)-\wp(\omega))^n f(z)$ is holomorphic at ω. After repeating this process for all of the (finitely many) poles of f in a fundamental domain, we obtain a polynomial $v \in \mathbb{C}[x]$ such that $v(\wp(z))f(z)$ is holomorphic at all points not in L. By the argument above, we may write $v(\wp(z))f(z)$ in the form $u(\wp(z))$, for some polynomial $u \in \mathbb{C}[x]$. Thus $f(z) = u(\wp(z))/v(\wp(z))$ is a rational function of $\wp(z)$.

If $f(z)$ is instead an odd function, we may write

$$f(z) = \wp'(z)\frac{f(z)}{\wp'(z)}.$$

The function $f(z)/\wp'(z)$ is even ($f(z)$ and $\wp'(z)$ are both odd), so we may write $f(z)/\wp'(z)$ as a rational function of $\wp(z)$, and $f(z)$ is therefore a rational function of $\wp(z)$ and $\wp'(z)$. $\square$

References

[1] Tom M. Apostol, *Modular functions and Dirichlet series in number theory*, second edition, Springer, 1990.

[2] Joseph H. Silveman, *The arithmetic of elliptic curves*, second edition, Springer, 2009.

[3] Elias M. Stein and Rami Shakarchi, *Complex analysis*, Princeton University Press, 2003.