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 $\tau$ in the upper half plane $\mathbb{H} = \{z \in \mathbb{C} : \text{im} \, z > 0\}$; we may take $\tau = \pm \omega_2/\omega_1$ with the sign chosen so that $\text{im} \, \tau > 0$. This leads to the following definition of the $j$-function.

**Definition 18.1.** The $j$-function $j : \mathbb{H} \to \mathbb{C}$ 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

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

converge absolutely for any fixed $\tau \in \mathbb{H}$, by Lemma 16.11, and uniformly over $\tau$ in any compact subset of $\mathbb{H}$. The proof of this last fact is straightforward 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

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

As proved in Problem Set 8, the group $\Gamma$ 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 $\Gamma$ is generated by the matrices $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. This implies that the $j$-function is invariant under the action of the modular group. In fact, more is true.
Figure 1: Fundamental domain $\mathcal{F}$ for the action of $\Gamma = \text{SL}_2(\mathbb{Z})$ 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 $\Gamma$.

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 $\lambda = \frac{1}{ca+d}$. Substituting this into the first, we have

$$\tau' = \frac{a \tau + b}{c \tau + d} = \gamma \tau,$$
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 $\gamma'$. The fact that $\tau' = \gamma\gamma' \tau'$ implies that $\det \gamma = \pm 1$ (since $\gamma$ and $\gamma'$ are integer matrices), and since $\tau$ and $\tau'$ both lie in $\mathbb{H}$, we must have $\det \gamma = 1$, and therefore $\gamma \in \Gamma$ as desired. 

---

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

---

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

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

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

---

2
\textbf{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 \( \gamma = (\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}) \in \Gamma \) we have

\[
im(\gamma \tau) = \nim\left(\frac{a \tau + b}{c \tau + d}\right) = \nim\left(\frac{(a \tau + b)(c \tau + d)}{|c \tau + d|^2}\right) = \frac{(ad - bc) \nim \tau}{|c \tau + d|^2} = \frac{\nim \tau}{|c \tau + d|^2} \quad (1)
\]

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 \( \gamma_0 = (\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}) \) then maximizes the value of \( \nim(\gamma \tau) \) over \( \gamma \in \Gamma \). Let us now choose \( \gamma = T^k \gamma_0 \), where \( k \) is chosen so that \( \re(\gamma \tau) \in [1/2, 1/2) \), and note that \( \nim(\gamma \tau) = \nim(\gamma_0 \tau) \) remains maximal. We must have \( |\gamma \tau| \geq 1 \), since otherwise \( \nim(S \gamma \tau) > \nim(\gamma \tau) \), contradicting the maximality of \( \nim(\gamma \tau) \). Finally, if \( \tau' = \gamma \tau \not\in \mathcal{F} \), then we must have \( |\gamma \tau| = 1 \) and \( \re(\gamma \tau) > 0 \), in which case we replace \( \gamma \) by \( S \gamma \) so that \( \tau' = \gamma \tau \in \mathcal{F} \).

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

\[
1 \geq |c \tau_1 + d|^2 = (c \tau_1 + d)(c \tau_1 + d) = c^2 |\tau_1|^2 + d^2 + 2cd \re(\tau_1) \geq c^2 |\tau_1|^2 + d^2 - |cd|.
\]

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 \( \nim \tau_2 = \nim \tau_1 \). We also must have \( |c|, |d| \leq 1 \), and by replacing \( \gamma_1 \) 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 \( \re \tau_2 - \re \tau_1 < 1 \), so \( \tau_2 = \tau_1 \).
2. \( c = 1, d = 0 \): then \( b = -1 \) and \( |\tau_1| = 1 \). So \( \tau_1 \) 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 \( \nim \tau_2 = \nim \tau_1 = \sqrt{3}/2 \) implies \( \tau_2 = \rho \).

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

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

\[
g_2(\tau) = 60 \sum_{n,m\in\mathbb{Z}}' \frac{1}{(m+n\tau)^4} = 60 \left( 2 \sum_{m=1}^{\infty} \frac{1}{m^4} + \sum_{n,m\in\mathbb{Z}} \frac{1}{(m+n\tau)^4} \right)
\]

The second sum tends to 0 as \( \nim \tau \to \infty \). Thus we have

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

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

\[
\lim_{\nim \tau \to \infty} g_3(\tau) = 280 \zeta(6) = 280 \frac{\pi^6}{945} = \frac{8\pi^6}{27}.
\]
Thus
\[
\lim_{\im\tau \to \infty} \Delta(\tau) = \left( \frac{4}{3} \pi^4 \right)^3 - 27 \left( \frac{8}{27} \pi^6 \right)^2 = 0.
\]
(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 \(\im \tau \to \infty\).

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 \(j(\tau_j), j(\tau_2), \ldots\) be an arbitrary convergent sequence in \(j(\mathbb{H})\), converging to \(w \in \mathbb{C}\). The \(j\)-function is \(\Gamma\)-invariant, by Lemma 18.3, so we may assume the \(\tau_j\) all lie in \(F\). The sequence \(\im \tau_1, \im \tau_2, \ldots\) must be bounded, since \(j(\tau) \to \infty\) as \(\im \tau \to \infty\), thus the \(\tau_j\) all lie in a compact set \(\Omega \subset F \subset \mathbb{H}\). Thus there is a subsequence of the \(\tau_n\) 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 \(j(\mathbb{H}) \subset \mathbb{C}\) is both open and closed implies that \(j(\mathbb{H}) = \mathbb{C}\), since \(\mathbb{C}\) is connected. It follows that \(j(F) = \mathbb{C}\), since every element of \(\mathbb{H}\) is equivalent to an element of \(F\) (Lemma 18.4) and the \(j\)-function is \(\Gamma\)-invariant (Lemma 18.3). \(\square\)

**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 \(E(\mathbb{C}) \simeq \mathbb{C}/L\). \(\square\)

**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 \(\Phi: \mathbb{C}/L \to E(\mathbb{C})\) be the isomorphism that sends \(z\) to \((\varphi(z), \varphi'(z))\). For any \(\alpha \in \mathbb{C}\), the following are equivalent:

1. \(\alpha L \subseteq L\);
2. \(\varphi(\alpha z) = u(\varphi(z))/v(\varphi(z))\) for some polynomials \(u, v \in \mathbb{C}[x]\);
3. There exists an endomorphism \(\phi \in \text{End}(E)\) such that the following diagram commutes:

\[
\begin{array}{ccc}
\mathbb{C}/L & \xrightarrow{\phi} & E(\mathbb{C}) \\
\downarrow{\alpha} & & \downarrow{\phi} \\
\mathbb{C}/L & \xrightarrow{\phi} & E(\mathbb{C})
\end{array}
\]

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

Moreover, every endomorphism \(\phi\) in \(\text{End}(E)\) gives rise to an \(\alpha \in \mathbb{C}\) satisfying (1)–(3), and the map that sends \(\phi\) to \(\alpha\) is a ring isomorphism from \(\text{End}(E)\) to \{\(\alpha \in \mathbb{C}: \alpha L \subseteq L\}\). In particular, the endomorphism \(\phi\) in (3) is unique, and \(\text{N}(\alpha) = \deg \phi = \deg u = \deg v + 1\).
Proof. Properties (1)–(3) clearly hold for \( \alpha = 0 \), so assume \( \alpha \neq 0 \).

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

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

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

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

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

\[
\varphi'(\alpha z) = \frac{1}{\alpha} \left( \varphi(\alpha z) \right)' = \frac{1}{\alpha} \left( \frac{u(\varphi(z))}{v(\varphi(z))} \right)' = \frac{s(\varphi(z))}{t(\varphi(z))} \varphi'(z).
\]

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

\[
\phi(\Phi(z)) = \phi((\varphi(z), \varphi'(z))) = \left( \frac{u(\varphi(z))}{v(\varphi(z))}, \frac{s(\varphi(z))}{t(\varphi(z))} \varphi'(z) \right),
\]

and going around the square counter-clockwise yields

\[
\Phi(\alpha z) = (\varphi(\alpha z), \varphi'(\alpha z)) = \left( \frac{u(\varphi(z))}{v(\varphi(z))}, \frac{s(\varphi(z))}{t(\varphi(z))} \varphi'(z) \right).
\]

(3) \( \Rightarrow \) (1). Let \( \phi \in \text{End}(E) \) 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 \( \phi \in \text{End}(E) \), 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 \( \phi^* \in \text{End}(\mathbb{C}/L) \), we have

\[
\phi^*(z_1 + z_2) \equiv \phi^*(z_1) + \phi^*(z_2) \mod L,
\]

and \( \phi^*(0) \in L \). By replacing \( \phi^* \) 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

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

\(^1\)An analog of the inverse function theorem holds for holomorphic functions.
Thus the derivative of \( \phi^* \) 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 \( \phi^* \) sends lattice points to lattice points, and we have just shown that \( \phi^* \) is the “multiplication-by-\( \alpha \)” map. Thus \( \alpha L \subseteq L \), and \( \alpha \) satisfies the equivalent conditions (1)–(3).

We now show that the map \( \Psi : \text{End}(E) \to \{ \alpha \in \mathbb{C} : \alpha L \subseteq L \} \) that sends \( \phi \) to \( \alpha = (\phi^*)'(0) \) is a ring homomorphism. Clearly, \( \Psi(0) = 0 \) and \( \Psi(1) = 1 \). Let \( \phi_1, \phi_2 \in \text{End}(E) \). Then
\[
(\phi_1 + \phi_2)^* = \Phi^{-1} \circ (\phi_1 + \phi_2) \circ \Phi = \Phi^{-1} \circ \phi_1 \circ \Phi + \Phi^{-1} \circ \phi_2 \circ \Phi = \phi_1^* + \phi_2^*,
\]
which \( \Phi \) 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 \( \phi_1 \circ \phi_2 \) is even or odd. We first consider the case that \( \phi \) 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
\[
f(z) = \sum_{k=-n}^{\infty} a_{2k} z^{2k},
\]

Corollary 18.8. Let \( E \) be an elliptic curve defined over \( \mathbb{C} \). Then \( \text{End}(E) \) 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 \( \text{End}(E) \cong \{ \alpha \in \mathbb{C} : \alpha L \subseteq L \} \) is clearly commutative, and therefore not an order in a quaternion algebra. The result then follows from Corollary 14.16.

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].
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 $f(z) - P(\wp(z))$, 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 $\omega$. 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 $\omega$ is a simple root of $\wp(z) - \wp(\omega)$ and the function $(\wp(z) - \wp(\omega))^n$ has a zero of order $n$ at $\omega$. This implies that $(\wp(z) - \wp(\omega))^nf(z)$ is holomorphic at $\omega$. 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 $\wp'(z)$.

References


18.783 Elliptic Curves
Spring 2013

For information about citing these materials or our Terms of Use, visit: http://ocw.mit.edu/terms.