18.783 Elliptic Curves
Lecture 14

Andrew Sutherland

October 31, 2023

Elliptic curves over $\mathbb{C}$

Our goal for the next two lectures is to prove **Uniformization Theorem**, an explicit correspondence between elliptic curves over $\mathbb{C}$ and tori $\mathbb{C}/L$ defined by lattices $L \subseteq \mathbb{C}$.

In particular, we will show that:

- Every lattice $L \subseteq \mathbb{C}$ can be used to define an elliptic curve $E_L/\mathbb{C}$.
- Every elliptic curve $E/\mathbb{C}$ arises as E_L for some lattice L.
- There is an analytic isomorphism

$$\mathbb{C}/L \xrightarrow{\Phi} E_L/\mathbb{C}$$

that induces an isomorphism of abelian groups $\mathbb{C}/L \simeq E(\mathbb{C})$
(addition in $\mathbb{C}$ modulo L induces the elliptic curve group law on $E(\mathbb{C})$).

Lattices in $\mathbb{C}$

Definition

A lattice $[\omega_1, \omega_2]$ in $\mathbb{C}$ is a $\mathbb{Z}$-module $\omega_1\mathbb{Z} + \omega_2\mathbb{Z} \subseteq \mathbb{C}$ with $\mathbb{R}$-span $\mathbb{C}$.

Example

Let τ be a root of $x^2 - bx + c$ with $b, c \in \mathbb{Z}$ and $b^2 - 4c < 0$. The imaginary quadratic order $\mathcal{O} = \mathbb{Z}[\tau]$ corresponds to the lattice $[1, \tau]$ in $\mathbb{C}$.

Note that $\mathbb{C}$ and L are both topological groups ($\mathbb{C}$ has the Euclidean topology, L has the discrete topology), and the torus $\mathbb{C}/L$ is a compact group.

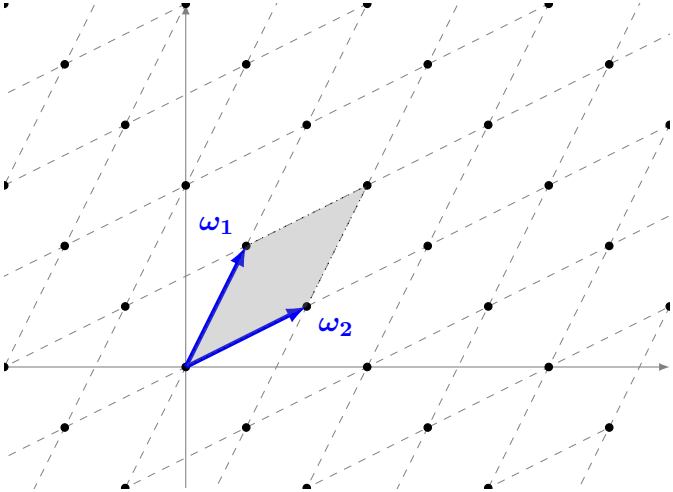
Definition

A fundamental parallelogram for $L = [\omega_1, \omega_2]$ is any set of the form

$$\mathcal{F}_\alpha = \{\alpha + t_1\omega_1 + t_2\omega_2 : \alpha \in \mathbb{C},\ 0 \leq t_1, t_2 < 1\}.$$

We may identify the points in a fundamental parallelogram with the points of $\mathbb{C}/L$.

Lattices in $\mathbb{C}$



Holomorphic and meromorphic functions

Definition

A function $f\colon \Omega \to \mathbb{C}$ on an open neighborhood Ω of $z_0 \in \mathbb{C}$ is holomorphic at z_0 if

$$f'(z_0) := \lim_{z \to z_0} \frac{f(z) - f(z_0)}{z - z_0}$$

exists. We say that f is holomorphic on Ω if it is holomorphic at every $z_0 \in \Omega$.

Definition

Let $k \in \mathbb{Z}_{>0}$. A complex function f has a zero of order k at z_0 if there is a holomorphic function g with $g(z_0) \neq 0$ such that $f(z) = (z - z_0)^k g(z)$ on some open neighborhood of z_0. We say f has a pole of order k at z_0 if $1/f$ has a zero of order k at z_0.

Definition

A complex function f is meromorphic on an open set Ω if it is holomorphic on Ω except for a discrete set of poles (every pole has an open neighborhood with no other poles).

The order of vanishing of a meromorphic function

Definition

If f is meromorphic on an open neighborhood of $z_0 \in \mathbb{C}$ we define

$$\operatorname{ord}_{z_0}(f) := \begin{cases} n & \text{if } f \text{ has a zero of order } n \text{ at } z_0, \\ -n & \text{if } f \text{ has a pole of order } n \text{ at } z_0, \\ 0 & \text{otherwise.} \end{cases}$$

For any open $\Omega \subseteq \mathbb{C}$ the set of meromorphic functions $f\colon \Omega \to \mathbb{C}$ form a field $\mathbb{C}(\Omega)$.

For each $z_0 \in \Omega$ we have

- $\operatorname{ord}_{z_0}(fg) = \operatorname{ord}_{z_0}(f) + \operatorname{ord}_{z_0}(g)$ for all $f, g \in \mathbb{C}(\Omega)^\times$;
- $\operatorname{ord}_{z_0}(f+g) \geq \min(\operatorname{ord}_{z_0}(f), \operatorname{ord}_{z_0}(g))$ for all $f, g \in \mathbb{C}(\Omega)^\times$.

Defining $\operatorname{ord}_{z_0}(0) := \infty$ yields a discrete valuation on the field $\mathbb{C}(\Omega)$.

Elliptic functions

Definition

An elliptic function for a lattice L in $\mathbb{C}$ is a complex function f such that

- f is meromorphic on $\mathbb{C}$;
- f is L-periodic, meaning $f(z+\omega) = f(z)$ for all $\omega \in L$.

Elliptic functions can be viewed as meromorphic functions on $\mathbb{C}/L$.

Constant functions are elliptic functions, as are sums, differences, products, and quotients of elliptic functions; $\mathbb{C}(L)$ denotes the field of elliptic functions for L.

Definition

The order of an elliptic function is the sum of the orders of the poles it has in any fundamental parallelogram (the number of poles counted with multiplicity).

The elliptic functions of order zero are the constant functions (by Liouville's Theorem).

Elliptic functions

Theorem

Let f be an elliptic function for a lattice L in $\mathbb{C}$. When counted with multiplicity the number of zeros of f in any fundamental parallelogram for L is equal to its order.

Proof: Let $\mathcal{F}$ be a fundamental parallelogram for L whose boundary ∂F contains no zeros or poles of f. Then

$$\frac{1}{2\pi i}\int_{\partial\mathcal{F}} \frac{f'(z)}{f(z)} = 0 = \sum_{\omega\in\mathcal{F}^0} \mathrm{ord}_\omega(f).$$

by Cauchy's argument principle (see notes). The theorem follows.

Eisenstein series

Definition

Let L be a lattice in $\mathbb{C}$ and let $k \in \mathbb{Z}_{>2}$. The weight-k Eisenstein series for L is the sum

$$G_k(L) = \sum_{\omega \in L^*} \frac{1}{\omega^k},$$

where $L^* = L - \{0\}$. For $L = [\omega_1, \omega_2]$ we put $\tau = \pm\omega_2/\omega_1 \in \mathcal{H}$ so $L \simeq [1, \tau]$ and

$$G_k(\tau) := G_k([1,\tau]) = \sum_{\substack{m,n \in \mathbb{Z} \\ (m,n) \neq (0,0)}} \frac{1}{(m+n\tau)^k}.$$

satisfies $G_k(\tau+1) = G_k(\tau)$ and $G_k(-1/\tau) = \tau^k G_k(\tau)$, making it a modular form.

Remark

If k is odd then $G_k(L) = 0$ for every lattice L in $\mathbb{C}$; we are only interested in even k.

The Weierstrass $\wp$-function

Definition

The Weierstrass $\wp$-function of a lattice L in $\mathbb{C}$ is defined by

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

Theorem

The function $\wp(z; L)$ is holomorphic at every $z_0 \notin L$ and meromorphic on $\mathbb{C}$, with a double pole at each $\omega \in L$. Its derivative $\wp'(z; L)$ has a triple pole at each $\omega \in L$.

Proof: To the board!

Corollary

$\wp$ is an even elliptic function of order 2 and $\wp'$ is an odd elliptic function of order 3.

Proof: To the board!

The Weierstrass $\wp$-function

Lemma

The Laurent series expansion of $\wp(z) = \wp(z; L)$ at $z = 0$ is

$$\wp(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty} (2n+1) G_{2n+2}(L) z^{2n},$$

where $G_k(L)$ denotes the Eisenstein series of weight k.

Proof: To the board!

Theorem

The function $\wp(z) = \wp(z; L)$ satisfies the differential equation

$$\wp'(z)^2 = 4\wp(z)^3 - g_2(L)\wp(z) - g_3(L),$$

where $g_2(L) := 60G_4(L)$ and $g_3(L) := 140G_6(L)$.

Proof: To the board!

Elliptic curves from lattices

If we put $x := \wp(z)$ and $y := \wp'(z)$, the differential equation for $\wp$ looks like

$$E_L\colon y^2 = 4x^3 - g_2(L)x - g_3(L).$$

which is an elliptic curve over $\mathbb{C}$ if it is nonsingular. If the partial derivatives of $zy^2 = 4x^3 - g_2(L)xz^2 - g_3(L)z^3$ simultaneously vanish at $(x_0 : y_0 : z_0) \neq 0$ then

$$12x_0^2 - g_2(L)z_0^2 = 0, \qquad 2z_0y_0 = 0, \qquad y_0^2 + 2g_2(L)x_0z_0 + 3g_3(L)z_0^2 = 0.$$

We cannot have $z_0 = 0$, since this would force $x_0 = y_0 = 0$, so we may assume $z_0 = 1$. Then $y_0 = 0$, and $x_0 = -3g_3(L)/(2g_2(L))$, and $g_2(L)^3 - 27g_3(L)^2 = 0$. Thus if

$$\Delta(L) := g_2(L)^3 - 27g_3(L)^2$$

is nonzero, E_L is an elliptic curve over $\mathbb{C}$.

Elliptic curves from lattices

Lemma

Let L be a lattice in $\mathbb{C}$. Then $z \notin L$ is a zero of $\wp'(z; L)$ if and only if $2z \in L$.

Proof: To the board!

Corollary

For every lattice L in $\mathbb{C}$, the discriminant $\Delta(L)$ is nonzero.

Proof: To the board!

Thus every lattice L in $\mathbb{C}$ gives rise to an elliptic curve $E_L/\mathbb{C}$, and the map

$$\begin{aligned} \Phi \colon \mathbb{C}/L &\to E_L(\mathbb{C}) \\ z &\mapsto (\wp(z), \wp'(z)) \end{aligned}$$

sends points on $\mathbb{C}/L$ to points on the elliptic curve E_L.