Math 6170 C, Lecture on April 15, 2020

Yongchang Zhu

Plan

(1). VI. §2. Elliptic Functions (Review)

(2). VI. §3. Constructions of Elliptic Functions (Continued).

(3). VI. §4. Maps – Analytic and Algebraic.

(4). VIII. §1. The Weak Mordell-Weil Theorem.

A **lattice** in $\mathbb{C}$ is a free $\mathbb{Z}$-submodule $\Lambda \subset \mathbb{C}$ of rank two such that a basis of Λ is $\mathbb{R}$-linearly independent.

A lattice can be written as

$$\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$$

where ω_1 and ω_2 are $\mathbb{R}$-linear independent.

Definition. An **elliptic function** (relative to the lattice Λ) is a meromorphic function $f(z)$ on $\mathbb{C}$ such that

$$f(z+\omega) = f(z)$$

for all $\omega \in \Lambda$ and all $z \in \mathbb{C}$.

Constant functions are elliptic functions relative to any lattice.

We denote the space of elliptic functions for Λ by

$$\mathbb{C}(\Lambda).$$

$\mathbb{C}(\Lambda)$ is a field.

Definition. Let $\Lambda \subset \mathbb{C}$ be a lattice, a **fundamental parallelogram** is a set of the form

$$D = \{a + t_1\omega_1 + t_2\omega_2 \mid 0 \leq t_1, t_2 < 1\}$$

where ω_1, ω_2 is a $\mathbb{Z}$-basis for Λ and $a \in \mathbb{C}$.

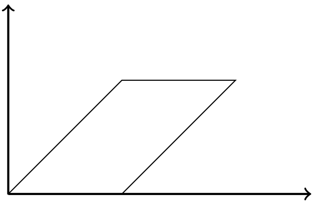

Figure: The domain $D = \{t_1 + t_2(1+i) \,|\, 0 \leq t_1, t_2 \leq 1\}$.

Theorem VI 2.2.

Let $f \in \mathbb{C}(\Lambda), f \neq 0$, then

(a) $\sum_{w \in \mathbb{C}/\Lambda} \mathrm{res}_w(f) = 0$

(b) $\sum_{w \in \mathbb{C}/\Lambda} \mathrm{ord}_w(f) = 0$

(c) $\sum_{w \in \mathbb{C}/\Lambda} \mathrm{ord}_w(f)\, w \in \Lambda$.

We define $\mathrm{Div}(\mathbb{C}/\Lambda)$ to the formal $\mathbb{Z}$-linear combination of points in $\mathbb{C}/\Lambda$. So an element in $\mathrm{Div}(\mathbb{C}/\Lambda)$ looks like

$$k_1[w_1] + \cdots + k_n[w_n], \quad k_i \in \mathbb{Z}, \ \ w_i \in \mathbb{C}/\Lambda.$$

We have $\deg : \mathrm{Div}(\mathbb{C}/\Lambda) \to \mathbb{Z}$,

$$\deg(k_1[w_1] + \cdots + k_n[w_n]) = k_1 + \cdots + k_n.$$

We write $\mathrm{Div}_0(\mathbb{C}/\Lambda)$ for $\mathrm{Ker}(\deg)$.

We have a group homomorphism

$$\mathrm{div}: \mathbb{C}(\Lambda)^* \to \mathrm{Div}(\mathbb{C}/\Lambda)$$

$$\mathrm{div}(f) = \sum_{w \in \mathbb{C}/\Lambda} \mathrm{ord}_w(f)[w]$$

(b) in Theorem VI 2.2. implies that $\deg(\mathrm{div}(f)) = 0$

(c) in Theorem VI 2.2. implies that the composition

$$\mathbb{C}(\Lambda)^* \to \mathrm{Div}(\mathbb{C}/\Lambda) \to \mathbb{C}/\Lambda$$

is 0, where the 2nd arrow is

$$S : k_1[w_1] + \cdots + k_n[w_n] \mapsto k_1 w_1 + \cdots + k_n w_n.$$

So we have

$$\mathrm{div}(\mathbb{C}(\Lambda)^*) \subset \mathrm{Div}_0(\mathbb{C}/\Lambda) \cap \mathrm{Ker}(S)$$

We have (Proposition 3.4)

$$\mathrm{div}(\mathbb{C}(\Lambda)^*) = \mathrm{Div}_0(\mathbb{C}/\Lambda) \cap \mathrm{Ker}(S)$$

See also my notes for Math 4991 for a proof using theta functions.

The Weierstrass elliptic function $\wp(z)$ for a lattice Λ is defined as

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

$\wp(z) \in \mathbb{C}(\Lambda)$.

Theorem.

$$\left(\wp'(z)\right)^2 = 4\left(\wp(z)\right)^3 - g_2\wp(z) - g_3 \tag{1}$$

where

$$g_2 = 60 \sum_{\omega\in\Lambda\setminus\{0\}} \frac{1}{\omega^4}$$

and

$$g_3 = 140 \sum_{\omega\in\Lambda\setminus\{0\}} \frac{1}{\omega^6}.$$

Lemma. (1) $\wp(z)$ is an even function, i.e., $\wp(-z) = \wp(z)$.

(2) For every $c \in \mathbb{C}$, the equation $\wp(z) = c$ has exactly two solutions modulo Λ.

Proof of Lemma. (1)

$$
\begin{aligned}
\wp(-z) &= \frac{1}{(-z)^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left(\frac{1}{(-z-\omega)^2} - \frac{1}{\omega^2} \right) \\
&= \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left(\frac{1}{(z+\omega)^2} - \frac{1}{\omega^2} \right) \\
&= \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left(\frac{1}{(z-((-\omega))^2} - \frac{1}{(-\omega)^2} \right) \\
&= \wp(z)
\end{aligned}
$$

Proof of Lemma (continued).

$f(z) \overset{\text{def}}{=} \wp(z) - c \in \mathbb{C}(\Lambda)$, by Theorem (b) Theorem VI 2.2.

$$\sum_{w \in \mathbb{C}/\Lambda} \mathrm{ord}_w(f) = 0$$

$f(z)$ has only one pole $z = 0$ modulo Λ and we have $\mathrm{ord}_0 f(z) = -2$, there exists $a \in \mathbb{C}$ with $f(a) = 0$. If $a = -a$ modulo Λ, then $\mathrm{ord}_a f \geq 2$, so

$$\mathrm{ord}_a f = 2$$

and there are on other zeros.

If $a \neq -a$ modulo Λ, a and $-a$ are all the zeros of f modulo Λ, and

$$\mathrm{ord}_a f = \mathrm{ord}_{-a} f = 1.$$

Theorem.

The field $\mathbb{C}(\Lambda)$ is generated by $\wp(z)$ and $\wp'(z)$ over $\mathbb{C}$ subject to the relation

$$\left(\wp'(z)\right)^2 = 4\left(\wp(z)\right)^3 - g_2\wp(z) - g_3$$

where

$$g_2 = 60 \sum_{\omega\in\Lambda\setminus\{0\}} \frac{1}{\omega^4}$$

$$g_3 = 140 \sum_{\omega\in\Lambda\setminus\{0\}} \frac{1}{\omega^6}.$$

Proposition VI. 3.6.

Let g_2, g_3 be the quantities associated to a lattice $\Lambda \subset \mathbb{C}$,

(a) The polynomial $f(x) = 4x^3 - g_2 x - g_3$ has distinct roots. Its discriminant

$$\Delta(\Lambda) = g_2^3 - 27g_3^2 \neq 0.$$

(b) Let $E/\mathbb{C}$ be the elliptic curve

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

The map

$$\phi : \mathbb{C}/\Lambda \to E \subset \mathbb{P}^2(\mathbb{C}), \quad z \mapsto [\wp(z), \wp'(z), 1]$$

is an isomorphism of complex Lie groups.

Proof of (a). Note that $\wp'(z)$ is an odd function. Let ω_1, ω_2 be a basis of Λ, let $\omega_3 = \omega_1 + \omega_2$. Then $\frac{\omega_i}{2}$ $(i = 1, 2, 3)$ are the non-zero 2 torsion points of $\mathbb{C}/\Lambda$. We have

$$\wp'(\frac{\omega_i}{2}) = -\wp'(-\frac{\omega_i}{2}) = -\wp'(\frac{\omega_i}{2})$$

so $\wp'(\frac{\omega_i}{2}) = 0$. So

$$4\wp(\frac{\omega_i}{2})^3 - g_2\,\wp(\frac{\omega_i}{2}) - g_3 = 0$$

$\wp(\frac{\omega_i}{2})$ are zeros of $4x^3 - g_2 x - g_3$. These three zeros are distinct. So $\Delta \neq 0$.

(b). First we note that $\phi(0) = [0, 1, 0] = O$. There are no other points that maps to O under ϕ. For arbitrary $[a, b, 1] \in E$, we can find $z \in \mathbb{C}$ such that $\wp(z) = a$, then $\wp(-z) = a$, then $b = \wp'(z)$ or $\wp'(-z)$. Suppose $b = \wp'(z)$, then

$$\phi(z) = [a, b, 1].$$

We see ϕ is surjective.

(to be continued)

To prove ϕ is a group homomorphism, we need to use the fact that there is $f \in \mathbb{C}(\Lambda)^*$ such that

$$\operatorname{div}(f) = [z_1 + z_2] - [z_1] - [z_2] + [0]$$

We regard $f \in \mathbb{C}(E)$, its divisor in $\operatorname{Div}(E)$ is

$$[\phi(z_1 + z_2)] - [\phi(z_1)] - [\phi(z_2)] + [O]$$

This implies

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

so ϕ is a group homomorphism.

In the above proof, we need the fact that

$$\operatorname{ord}_w(f) = \operatorname{ord}_{\phi(w)}(f)$$

This follows the definition of $\operatorname{ord}_{\phi(w)}(f)$.

For lattices Λ_1, Λ_2, we have Riemann surfaces $\mathbb{C}/\Lambda_1$, $\mathbb{C}/\Lambda_2$. and the corresponding elliptic curves E_1 and E_2
The main result of this section is the following 3 sets are in one-to-one correspondence:

$$Hom_{an}(\mathbb{C}/\Lambda_1, \mathbb{C}/\Lambda_2) = \{\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2 \mid \phi \text{ is holomorphic } \phi(0) = 0\}$$

$$Hom(E_1, E_2)$$

$$\{\alpha \in \mathbb{C} \mid \alpha\Lambda_1 \subset \Lambda_2\}$$

Given $\alpha \in \mathbb{C}$ satisfying $\alpha\Lambda_1 \subset \Lambda_2$, we have

$$\phi_\alpha : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$$

given by

$$\phi_\alpha(z) = \alpha z$$

Given a non-constant $\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ in the first set, it induces a field extension

$$\phi^* : \mathbb{C}(\Lambda_2) \to \mathbb{C}(\Lambda_1)$$

because

$$\mathbb{C}(\Lambda_i) = \mathbb{C}(E_i)$$

we have

$$\phi^* : \mathbb{C}(E_2) \to \mathbb{C}(E_1)$$

it induces $E_1 \to E_2$.

$\mathbb{C}/\Lambda_1$ and $\mathbb{C}/\Lambda_2$ are isomorphic as Riemann surfaces iff they are equivalent as elliptic curves over $\mathbb{C}$ iff there exists $\alpha \in \mathbb{C}^*$ such that

$$\alpha\Lambda_1 = \Lambda_2.$$

Two lattices Λ_1, Λ_2 are equivalent if there exists $\alpha \in \mathbb{C}^*$ such that

$$\alpha\Lambda_1 = \Lambda_2.$$

VI. §5. Uniformization.

The main result is every elliptic curve over $\mathbb{C}$ corresponds a unique equivalence class of lattices.

We will skip Chapter VII.

A number field is a field K of characteristic zero such that $[K : \mathbb{Q}] < \infty$.

Two types of global fields:
(1) Characteristic zero global fields = number fields.

(2) positive characteristic global fields: finitely generated field F over $k_p = \mathbb{Z}/p\mathbb{Z}$ such that

$$\operatorname{tr}\deg(F/k_p) = 1.$$

They are function fields of curves over k_p.

Main Theorem (Mordell-Weil Theorem). Let E be an elliptic curve over a number field K, then $E(K)$ is finitely generated.

So

$$E(K) \simeq E_{\mathrm{tors}}(K) \times \mathbb{Z}^r$$

Theorem VIII 1.1. (Weak Mordell-Weil Theorem). Let E be elliptic curve over a number field K, and m is a positive integer. Then

$$E(K)/mE(k)$$

is a finite group.

Lemma 1.1.1. Let L/K be a finite Galois extension. If $E(L)/mE(L)$ is finite, then $E(K)/mE(K)$ is also finite.

Proof. Let Φ be the kernel of the obvious map

$$E(K)/mE(K) \to E(L)/mE(L)$$

Thus

$$\Phi = (E(K) \cap mE(L))/mE(K).$$

For $P \in E(K) \cap mE(L)$, we choose $Q_P \in E(L)$ such that

$$mQ_P = P$$

We define a map

$$\lambda_P : G_{L/K} \to E(m), \;\; \lambda_P(\sigma) = Q_P^{\sigma} - Q_P$$

λ_P depends on the choice of Q_P.

$$m(Q_P^\sigma - Q_P) = (mQ_P)^\sigma - mQ_P = P^\sigma - P = 0.$$

Suppose now that $\lambda_P = \lambda_{P'}$ for two points $P, P' \in E(K) \cap mE(L)$. Then

$$(Q_P - Q_{P'})^\sigma = Q_P - Q_{P'} \text{ for all } \sigma \in G_{L/K}.$$

so $Q_P - Q_{P'} \in E(K)$. Therefore,

$$P - P' = m(Q_P - Q_{P'}) \in m\,E(K).$$

Choose a set $R \subset E(K) \cap mE(L)$, which is a set of representative $E(K) \cap mE(L)/mE(K)$,
For each $P \in R$, we choose Q_P so we have map $\lambda_P : G_{L/K} \to E[m]$,
The map

$$R \to Map(G_{L/K} \to E[m]), \quad P \mapsto \lambda_P$$

is 1-1. Since $Map(G_{L/K} \to E[m])$ is a finite set, so R is a finite set, thus $E(K) \cap mE(L)/mE(K)$ is a finite set.

Now the result follows from the exact sequence

$$0 \to E(K) \cap mE(L)/mE(K) \to E(K)/mE(K) \to E(L)/mE(L)$$

End