Math 6170 C, Lecture on March 18, 2020

Yongchang Zhu

Plan

(1) Review of Chapter III § 4.

(2) Chapter III § 5. The Invariant Differential

(3) Chapter III § 6. The Dual Isogeny

III. § 4. Isogenies

Definition. Let E_1 and E_2 be elliptic curves. An **isogeny** between E_1 and E_2 is a morphism $\phi : E_1 \to E_2$ such that $\phi(O) = O$.

Let

$$\mathrm{Hom}(E_1, E_2) = \text{ the set of isgenies } \phi : E_1 \to E_2.$$

$\mathrm{Hom}(E_1, E_2)$ is a group under the addition law:

$$(\phi + \psi)(P) = \phi(P) + \psi(P).$$

$\mathrm{End}(E) = \mathrm{Hom}(E, E)$ has a ring structure with multiplication given by composition.

For m a positive integer, we define

$$[m] : E \to E, \ \ P \mapsto P + \cdots + P \ (m \text{ copies}).$$

We define $[0] : E \to E$ to be the constant map $P \mapsto O$.

For negative integer $-m$:

$$[-m] : E \to E, \ \ P \mapsto -[m]P = -(P + \cdots + P) \ \ (m \text{ copies}).$$

$$[m][n] = [mn], \ \ [m] + [n] = [m+n]$$

The group of isogenies $\mathrm{Hom}(E_1, E_2)$ is a torsion free $\mathbb{Z}$-module.

The endomorphism ring $\mathrm{Hom}(E)$ is an integral domain of characteristic 0 containing $\mathbb{Z}$ as a subring.

$\mathbb{Z} \to \mathrm{Hom}(E) = \mathrm{Hom}(E, E)$ is given by $n \mapsto [n]$.

Theorem III 4.8.

Let $\phi : E_1 \to E_2$ be an isogeny. Then

$$\phi(P + Q) = \phi(O) + \phi(Q)$$

for all $P, Q \in E$. That is, ϕ is a group homomorphism.

Let $\phi \in \mathrm{Hom}(E_1, E_2)$ be a non-constant isogeny, Then

$$|\mathrm{Ker}(\phi)| = \mathrm{deg}_s \phi$$

So $\mathrm{Ker}(\phi)$ is a finite group.

Theorem 4.10.

The map

$$\operatorname{Ker}\phi \to \operatorname{Aut}(\bar{K}(E_1)/\phi^*\bar{K}(E_2))$$

given by

$$P \mapsto \tau_P^*$$

is an isomorphism.

Corollary III 4.11.

Let

$$\phi : E_1 \to E_2, \quad \psi : E_1 \to E_3$$

be non-constant isogenies, and assume that ϕ is separable. If

$$\ker \phi \subset \ker \psi,$$

then there is unique isogeny

$$\lambda : E_2 \to E_3$$

such that $\psi = \lambda \circ \phi$

Proof. We have

$$\phi^* \bar{K}(E_2) \subset \bar{K}(E_1), \;\; \psi^* \bar{K}(E_3) \subset \bar{K}(E_1).$$

Because ϕ is separable, so the extension $\phi^* \bar{K}(E_2) \subset \bar{K}(E_1)$ is Galois, and

$$\phi^* \bar{K}(E_2) = \bar{K}(E_1)^{\ker \phi}.$$

$$\psi^* \bar{K}(E_3) \subset \bar{K}(E_1)^{\ker \psi} \subset \bar{K}(E_1)^{\ker \phi} = \phi^* \bar{K}(E_2)$$

So we have

$$\phi^* \bar{K}(E_3) \subset \phi^* \bar{K}(E_2) \subset \bar{K}(E_1)$$

The first inclusion gives the isogeny $\lambda : E_2 \to E_2$.

Proposition III 4.12.

Let E be an elliptic curve, and let Φ be a finite subgroup of E. Then there is a unique elliptic curve E' and a separable isogeny

$$\phi : E \to E'$$

such that

$$\ker \phi = \Phi.$$

Let E/K be an elliptic curve given by the usual Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Proposition III 1.5. The differential

$$\omega = \frac{dx}{2y + a_1x + a_3} \in \Omega_E$$

has neither zeros nor poles.

Proof.

We write

$$F(x,y) = y^2 + a_1xy + a_3y - (x^3 + a_2x^2 + a_4x + a_6)$$

The function field $\bar{K}(E)$ is

$$\mathrm{Frac}\,\bar{K}[x,y]/(F(x,y))$$

$$\omega = \frac{dx}{2y + a_1x + a_3} = \frac{dx}{F_y(x,y)} = \frac{dy}{-F_x(x,y)}.$$

Let $P = (x_0, y_0) \in E$, $\bar{K}[E]_P$ local ring at P, $M_p \subset \bar{K}[E]_P$ be the maximal ideal.

It is easy to see that the ideal M_p is generated by $x - x_0$ and $y - y_0$.

Proof (continued).

$$0 = F(x,y) = F(x_0,y_0) + F_x(x_0,y_0)(x-x_0) + F_y(x_0,y_0)(y-y_0) + \text{higher terms}$$

$$F_x(x_0,y_0)(x-x_0) + F_y(x_0,y_0)(y-y_0) + \text{higher terms} = 0$$

Case 1. $F_y(x_0,y_0) \neq 0$. The above equation implies that $\mathrm{ord}_P(y-y_0) \geq \mathrm{ord}_P(x-x_0)$ so $x-x_0$ is a uniformizer at P.
Case 2. $F_x(x_0,y_0) \neq 0$, then $y-y_0$ is a uniformizer at P.

Case 1.

$$\omega = \frac{dx}{F_y(x,y)} = \frac{d(x-x_0)}{F_y(x,y)}$$

We see that $\mathrm{ord}_P \omega = 0$.

Case 2.

$$\omega = \frac{dy}{-F_x(x,y)} = \frac{d(y-y_0)}{-F_x(x,y)}$$

We see that $\mathrm{ord}_P \omega = 0$.

The proof for $P = [0, 1, 0]$, use the fact that x/y is a uniformizer.

Proposition III 5.1

For ω as above, for every $Q \in E$,

$$\tau_Q^* \omega = \omega.$$

Proof.

$$\tau_Q^*\omega = f\omega$$

for some $f \in \bar{K}(E)^*$. Because τ_Q is an isomorphism,

$$\mathrm{div}(\tau_Q^*\omega) = 0.$$

On the other hand side, we have

$$\mathrm{div}(\tau_Q^*\omega) = \mathrm{div}(f\omega) = \mathrm{div}(f) + \mathrm{div}(\omega) = \mathrm{div}(f).$$

So $\mathrm{div}(f) = 0$, $f \in \bar{K}^*$. We call this constant a_Q.

The map $E \to \mathbb{A}(\bar{K})$ given by $Q \mapsto a_Q$ is a morphism, since E is projective, the map is a constant map, So $a_Q = a_O = 1$.

A non-zero differential on ω on E with $\mathrm{div}(\omega) = 0$ is called an **invariant differential**. It is unique up to a scalar multiple by $\bar{K}^*$.

An invariant differential is translation invariant, that is, $\tau_Q^*\omega = \omega$ for all $Q \in E$.

Theorem III 5.2. Let E, E' be elliptic curves, let ω be an invariant differential on E, and let $\phi, \psi : E' \to E$ be two isogenies. Then

$$(\phi + \psi)^* \omega = \phi^* \omega + \psi^* \omega$$

Corollary III 5.3.

Let ω be an invariant differential on an elliptic curve E. Let $m \in \mathbb{Z}$. Then

$$[m]^*\omega = m\omega$$

Recall that for a non-constant morphism $\phi : C_1 \to C_2$ of smooth curves, we have

$$\phi^* : \mathrm{Pic}^0(C_2) \to \mathrm{Pic}^0(C_1)$$

induced from

$$\phi^* : \mathrm{Div}(C_2) \to \mathrm{Div}(C_1)$$

$$\phi^*(Q) = \sum_{P \in \phi^{-1}(Q)} e_\phi(P)\,(P).$$

If $\phi : E_1 \to E_2$ is an non-constant isogeny, we have a group homomorphism

$$E_2 \xrightarrow{\kappa} \mathrm{Pic}^0(E_2) \xrightarrow{\phi^*} \mathrm{Pic}^0(E_1) \xrightarrow{\kappa^{-1}} E_1$$

The composition map turns out to be an isogeny.

Theorem III 6.1.

Let $\phi : E_1 \to E_2$ be a non-constant isogeny with $\deg \phi = m$.
(a) There exists a unique isogeny

$$\hat{\phi} : E_2 \to E_1$$

satisfying

$$\hat{\phi} \circ \phi = [m]$$

(b) as a group homomorphism, $\hat{\phi}$ equals to the composition

$$E_2 \xrightarrow{\kappa} \mathrm{Pic}^0(E_2) \xrightarrow{\phi^*} \mathrm{Pic}^0(E_1) \xrightarrow{\kappa^{-1}} E_1$$

Proof.

(a) Uniqueness is easy. Suppose that $\psi : E_2 \to E_3$ is another non-constant isogeny of degree n, and suppose both $\hat{\phi}$ and $\hat{\psi}$ exist. Then

$$(\hat{\phi} \circ \hat{\psi}) \circ (\psi \circ \phi) = \hat{\phi} \circ [n] \circ \phi = [n] \circ \hat{\phi} \circ \phi = [nm].$$

Since every isogeny can be decomposed as $\phi \circ \psi$, where ϕ is separable, ψ is a Frobenius morphism, it is enough to prove the existence for the following two cases

Case 1. ϕ is separable.

Case 2. ϕ is a Frobenius morphism.

Proof (continued).

Case 1. ϕ is separable. Since $\deg \phi = m$, so $|\ker \phi| = m$. So

$$\ker \phi \subset \ker[m].$$

By Corollary III 4.11,
there is an isogeny $\hat{\phi} : E_2 \to E_1$ such that

$$\hat{\phi} \circ \phi = [m].$$

Case 2 and (b) (omitted).

Let $\phi : E_1 \to E_2$ be a non-constant isogeny. The **dual isogeny** to ϕ is the isogeny $\hat{\phi} : E_2 \to E_1$ such that

$$\hat{\phi} \circ \phi = [\deg \phi]$$

We define the dual isogeny of [0] to be [0].

Theorem III 6.2.

Let $\phi : E_1 \to E_2$ be an isogeny.
(a) Let $m = \deg \phi$. Then

$$\hat{\phi} \circ \phi = [m] \quad \text{on } E_1$$

$$\phi \circ \hat{\phi} = [m] \quad \text{on } E_2$$

(b) Let $\lambda : E_2 \to E_23$ be an isogeny. Then

$$\widehat{\lambda \circ \phi} = \hat{\phi} \circ \hat{\lambda}$$

Theorem III 6.2 (continued).

(c) Let $\psi : E_1 \to E_2$ be an isogeny. Then

$$\widehat{\phi + \psi} = \hat{\phi} + \hat{\psi}$$

(d) For all $m \in \mathbb{Z}$,

$$\widehat{[m]} = [m], \quad \deg [m] = m^2$$

(e)

$$\deg \hat{\phi} = \deg \phi$$

(f)

$$\hat{\hat{\phi}} = \phi$$

End