

18.783 Elliptic Curves

Lecture 6

Andrew Sutherland

March 9, 2021

The n -torsion subgroup of an elliptic curve

Theorem (Lecture 5)

The multiplication-by- n map $[n]$ has degree n^2 that is separable if and only if $n \perp p$.

Theorem

Let E/k be an elliptic curve over a field of characteristic p . For each prime ℓ we have

$$E[\ell^e] \simeq \begin{cases} \mathbb{Z}/\ell^e\mathbb{Z} \oplus \mathbb{Z}/\ell^e\mathbb{Z} & \text{if } \ell \neq p, \\ \mathbb{Z}/\ell^e\mathbb{Z} \text{ or } \{0\} & \text{if } \ell = p. \end{cases}$$

When $E[\ell] \simeq \{0\}$ we say that E is *supersingular*, otherwise E is *ordinary*.

Corollary

Every finite subgroup of $E(\bar{k})$ can be written as the sum of two (possibly trivial) cyclic groups with at most one of order divisible by p .

The group of homomorphisms between elliptic curves

Let E_1/k and E_2/k be elliptic curves.

Definition

$\text{Hom}(E_1, E_2)$ is the abelian group of morphisms $\alpha: E_1 \rightarrow E_2$ under pointwise addition. Note that $\alpha \in \text{Hom}(E_1, E_2)$ is defined over k (it is an arrow in the category of E/k).

Lemma

Let $\alpha, \beta \in \text{Hom}(E_1, E_2)$. If $\alpha(P) = \beta(P)$ for all $P \in E_1(\bar{k})$ then $\alpha = \beta$.

Proof: $\ker(\alpha - \beta) = E_1(\bar{k})$ is infinite so $\alpha - \beta = 0$.

Lemma

For all $n \in \mathbb{Z}$ and $\alpha \in \text{Hom}(E_1, E_2)$ we have $[n] \circ \alpha = n\alpha = \alpha \circ [n]$.

Proof: We have $([-1] \circ \alpha)(P) = -\alpha(P) = \alpha(-P) = (\alpha \circ [-1])(P)$ and $([n] \circ \alpha)(P) = n\alpha(P) = \alpha(P) + \dots + \alpha(P) = \alpha(P + \dots + P) = \alpha(nP) = (\alpha \circ [n])(P)$.

The cancellation law for isogenies

For $\delta \in \text{Hom}(E_0, E_1)$, $\alpha, \beta \in \text{Hom}(E_1, E_2)$ and $\gamma \in \text{Hom}(E_2, E_3)$ we have

$$(\alpha + \beta) \circ \gamma = \alpha \circ \gamma + \beta \circ \gamma \quad \text{and} \quad \delta \circ (\alpha + \beta) = \delta \circ \alpha + \delta \circ \beta$$

since these identities hold pointwise.

Lemma

Let $\delta: E_0 \rightarrow E_1$, $\alpha, \beta: E_1 \rightarrow E_2$, and $\gamma: E_2 \rightarrow E_3$ be isogenies. Then

$$\delta \circ \alpha = \delta \circ \beta \implies \alpha = \beta$$

$$\alpha \circ \gamma = \beta \circ \gamma \implies \alpha = \beta.$$

Proof: Isogenies are surjective, so $\alpha, \beta, \gamma, \delta$ and their compositions not zero maps.

Then $\delta \circ \alpha = \delta \circ \beta \Rightarrow \delta \circ \alpha - \delta \circ \beta = 0 \Rightarrow \delta \circ (\alpha - \beta) = 0 \Rightarrow \alpha - \beta = 0 \Rightarrow \alpha = \beta$

and $\alpha \circ \gamma = \beta \circ \gamma \Rightarrow \alpha \circ \gamma - \beta \circ \gamma = 0 \Rightarrow (\alpha - \beta) \circ \gamma = 0 \Rightarrow \alpha - \beta = 0 \Rightarrow \alpha = \beta.$

The dual isogeny

Definition

Let $\alpha: E_1 \rightarrow E_2$ be an isogeny of elliptic curves of degree n . The **dual isogeny** is the unique isogeny $\hat{\alpha}$ for which $\hat{\alpha} \circ \alpha = [n]$. We also define $[\hat{0}] := 0$.

Uniqueness follows from the cancellation law. Existence is nontrivial (see notes).

Lemma

- (1) If $\hat{\alpha} \circ \alpha = [n]$ then $\alpha \circ \hat{\alpha} = [n]$, that is, $\widehat{\hat{\alpha}} = \alpha$, and for $n \in \mathbb{Z}$ we have $[\hat{n}] = [n]$.
- (2) For any $\alpha, \beta \in \text{Hom}(E_1, E_2)$ we have $\widehat{\alpha + \beta} = \hat{\alpha} + \hat{\beta}$.
- (3) For any $\alpha \in \text{Hom}(E_2, E_3)$ and $\beta \in \text{Hom}(E_1, E_2)$ we have $\widehat{\alpha \circ \beta} = \hat{\beta} \circ \hat{\alpha}$.

Proof: (1) $(\alpha \circ \hat{\alpha}) \circ \alpha = \alpha \circ (\hat{\alpha} \circ \alpha) = \alpha \circ [n] = [n] \circ \alpha$, and $[n] \circ [n] = [n^2] = [\deg[n]]$.

(2) Deferred to Lecture 23.

(3) $(\hat{\beta} \circ \hat{\alpha}) \circ (\alpha \circ \beta) = \hat{\beta} \circ [\deg \alpha] \circ \beta = [\deg \alpha] \hat{\beta} \circ \beta = [\deg \alpha] \circ [\deg \beta] = [\deg(\alpha \circ \beta)]$.

The endomorphism ring of an elliptic curve

Definition

$\text{End}(E)$ is the ring with additive group is $\text{Hom}(E, E)$ and multiplication $\alpha\beta := \alpha \circ \beta$. The additive identity is $0 := [0]$ and the multiplicative identity is $1 := [1]$. The distributive laws are verified pointwise.

Note that $\alpha\beta \neq 0$ whenever $\alpha, \beta \neq 0$ (by surjectivity), so $\text{End}(E)$ has no zero divisors.

Lemma

The map $n \mapsto [n]$ defines an injective ring homomorphism $\mathbb{Z} \mapsto \text{End}(E)$ that agrees with scalar multiplication.

Proof: $[m + n] = [m] + [n]$, $[mn] = [m] \circ [n]$, and $m \neq 0 \Rightarrow [m] \neq 0$ (finite kernel), and we note that $([n]\alpha)(P) = [n](\alpha(P)) = n\alpha(P) = (n\alpha)(P)$ for all $P \in E(\bar{k})$.

In $\text{End}(E)$ we are thus free to replace $[n]$ with n (so $\alpha + n$ means $\alpha + [n]$, for example).

The trace of an endomorphism

Lemma

For any $\alpha \in \text{End}(E)$ we have $\alpha + \hat{\alpha} = 1 + \deg \alpha - \deg(1 - \alpha)$.

Proof: $\deg(1 - \alpha) = \widehat{(1 - \alpha)}(1 - \alpha) = (1 - \hat{\alpha})(1 - \alpha) = 1 - (\alpha + \hat{\alpha}) + \deg(\alpha)$.

Definition

The **trace** of $\alpha \in \text{End}(E)$ is the integer $\text{tr } \alpha = \alpha + \hat{\alpha}$.

Theorem

For all $\alpha \in \text{End}(E)$ both α and $\hat{\alpha}$ are solutions to $x^2 - (\text{tr } \alpha)x + \deg \alpha = 0$ in $\text{End}(E)$.

Proof: $\alpha^2 - (\text{tr } \alpha)\alpha + \deg \alpha = \alpha^2 - (\alpha + \hat{\alpha})\alpha + \hat{\alpha}\alpha = 0$ and similarly for $\hat{\alpha}$.

Restricting endomorphisms to $E[n]$

Definition

For any $\alpha \in \text{End}(E)$ its restriction to $E[n]$ is denoted $\alpha_n \in \text{End}(E[n])$.

Let $n \geq 1$ be coprime to the characteristic and let $E[n] \simeq \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z} = \langle P_1, P_2 \rangle$. Then we can view α_n as the matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$, where

$$\alpha(P_1) = aP_1 + bP_2$$

$$\alpha(P_2) = cP_1 + dP_2$$

The determinant and trace of this matrix do not depend on our choice of P_1 and P_2 .

Theorem

Let $\alpha \in \text{End}(E)$ and let $n \geq 1$ be coprime to the characteristic. Then

$$\text{tr } \alpha = \text{tr } \alpha_n \pmod{n} \quad \text{and} \quad \deg \alpha = \det \alpha_n \pmod{n}.$$

MIT OpenCourseWare

<https://ocw.mit.edu>

18.783 / 18.7831 Elliptic Curves

Spring 2021

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