18.783 Elliptic Curves
Lecture 6

Andrew Sutherland

February 16, 2022

Lecture 5 recap

- Isogeny decomposition (in characteristic $p > 0$): $\alpha = \alpha_{\text{sep}} \circ \pi^n$ for some $n \geq 0$.
- The separable degree is $\deg_s \alpha := \deg \alpha_{\text{sep}}$, the inseparable degree is $\deg_i \alpha := p^n$.
- $\# \ker \varphi = \# E[\alpha] := \{P \in E(\bar{k}) : \alpha(P) = 0\} = \deg_s \alpha$.
- $\alpha = \beta \circ \gamma \Rightarrow \deg \alpha = \deg \beta \deg \gamma$ and $\deg_* \alpha = \deg_* \beta \deg_* \gamma$ for $* = s, i$.
- Every finite $G \leq E[\bar{k}]$ is the kernel of a separable isogeny that is unique up to isomorphism and can be explicitly constructed using Vélu's formulas.
- For $E\colon y^2 = x^3 + Ax + B$ the multiplication-by-n map can be written in the form

  $$[n](x, y) = \left(\frac{\phi_n(x)}{\psi_n^2(x)}, \frac{\omega_n(x, y)}{\psi_n^3(x, y)}\right),$$

  where $\phi_n, \omega_n, \psi_n \in \mathbb{Z}[x, y, A, B]$ are given by explicit recurrence relations.
- $\deg[n] = n^2$ and $[n]$ is separable if and only if $n \perp p$.

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 $n \perp p$.

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.

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

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

The group of homomorphisms between elliptic curves

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

Definition

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

Lemma

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

The group of homomorphisms between elliptic curves

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

Definition

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

Lemma

Let $\alpha, \beta \in \mathrm{Hom}(E_1, E_2)$. 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 $\alpha - \beta = 0$.

The group of homomorphisms between elliptic curves

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

Definition

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

Lemma

Let $\alpha, \beta \in \mathrm{Hom}(E_1, E_2)$. 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 $\alpha \in \mathrm{Hom}(E_1, E_2)$ we have $[n] \circ \alpha = n\alpha = \alpha \circ [n]$.

The group of homomorphisms between elliptic curves

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

Definition

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

Lemma

Let $\alpha, \beta \in \mathrm{Hom}(E_1, E_2)$. 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 $\alpha \in \mathrm{Hom}(E_1, E_2)$ 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
$([n] \circ \alpha)(P) = n\alpha(P) = \alpha(P) + \cdots + \alpha(P) = \alpha(P + \cdots P) = \alpha(nP) = (\alpha \circ [n])(P)$.

The cancellation law for isogenies

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

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

since these identities hold pointwise.

Lemma

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

$$\gamma \circ \alpha = \gamma \circ \beta \quad \Longrightarrow \quad \alpha = \beta,$$
$$\alpha \circ \delta = \beta \circ \delta \quad \Longrightarrow \quad \alpha = \beta.$$

The cancellation law for isogenies

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

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

since these identities hold pointwise.

Lemma

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

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

Proof: Isogenies are surjective, so $\alpha, \beta, \gamma, \delta$ and their compositions not zero maps.
Then $\gamma \circ \alpha = \gamma \circ \beta \Rightarrow \gamma \circ \alpha - \gamma \circ \beta = 0 \Rightarrow \gamma \circ (\alpha - \beta) = 0 \Rightarrow \alpha - \beta = 0 \Rightarrow \alpha = \beta$
and $\alpha \circ \delta = \beta \circ \delta \Rightarrow \alpha \circ \delta - \beta \circ \delta = 0 \Rightarrow (\alpha - \beta) \circ \delta = 0 \Rightarrow \alpha - \beta = 0 \Rightarrow \alpha = \beta$.

The dual isogeny

Definition

Let $\alpha\colon E_1 \to E_2$ 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,* $\hat{\hat{\alpha}} = \alpha$, *and for* $n \in \mathbb{Z}$ *we have* $\hat{[n]} = [n]$.

(2) *For any* $\alpha, \beta \in \operatorname{Hom}(E_1, E_2)$ *we have* $\widehat{\alpha+\beta} = \hat{\alpha} + \hat{\beta}$.

(3) *For any* $\alpha \in \operatorname{Hom}(E_2, E_3)$ *and* $\beta \in \operatorname{Hom}(E_1, E_2)$ *we have* $\widehat{\alpha\circ\beta} = \hat{\beta}\circ\hat{\alpha}$.

The dual isogeny

Definition

Let $\alpha\colon E_1 \to E_2$ 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,* $\hat{\hat\alpha} = \alpha$, *and for* $n \in \mathbb{Z}$ *we have* $\hat{[n]} = [n]$.
(2) *For any* $\alpha, \beta \in \operatorname{Hom}(E_1, E_2)$ *we have* $\widehat{\alpha + \beta} = \hat\alpha + \hat\beta$.
(3) *For any* $\alpha \in \operatorname{Hom}(E_2, E_3)$ *and* $\beta \in \operatorname{Hom}(E_1, E_2)$ *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) $(\hat\beta \circ \hat\alpha) \circ (\alpha \circ \beta) = \hat\beta \circ [\deg \alpha] \circ \beta = [\deg \alpha] \circ \hat\beta \circ \beta = [\deg \alpha] \circ [\deg \beta] = [\deg(\alpha \circ \beta)]$.

The endomorphism ring of an elliptic curve

Definition

$\mathrm{End}(E)$ is the ring with additive group is $\mathrm{Hom}(E, E)$ 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 $\mathrm{End}(E)$ has no zero divisors.

Lemma

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

The endomorphism ring of an elliptic curve

Definition

$\mathrm{End}(E)$ is the ring with additive group is $\mathrm{Hom}(E,E)$ 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 $\mathrm{End}(E)$ has no zero divisors.

Lemma

The map $n \mapsto [n]$ defines an injective ring homomorphism $\mathbb{Z} \mapsto \mathrm{End}(E)$ 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 $\mathrm{End}(E)$ we are thus free to replace $[n]$ with n (so $\alpha + n$ means $\alpha + [n]$, for example).

The trace of an an endomorphism

Lemma

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

The trace of an an endomorphism

Lemma

For any $\alpha \in \operatorname{End}(E)$ *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 $\alpha \in \operatorname{End}(E)$ is the integer $\operatorname{tr} \alpha = \alpha + \hat{\alpha}$.

Theorem

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

The trace of an an endomorphism

Lemma

For any $\alpha \in \mathrm{End}(E)$ *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 $\alpha \in \mathrm{End}(E)$ is the integer $\operatorname{tr}\alpha = \alpha + \hat{\alpha}$.

Theorem

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

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

Restricting endomorphisms to $E[n]$

Definition

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

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 $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$, 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 $\alpha \in \mathrm{End}(E)$ and let $n \geq 1$ be coprime to the characteristic. Then

$$\mathrm{tr}\,\alpha \equiv \mathrm{tr}\,\alpha_n \bmod n \qquad \textit{and} \qquad \deg\alpha \equiv \det\alpha_n \bmod n.$$