18.783 Elliptic Curves
Lecture 5

Andrew Sutherland

September 18, 2025

Isogenies (Lecture 4 recap)

Definition

An isogeny $\alpha\colon E \to E'$ is a surjective morphism that is also a group homomorphism, equivalently, a non-constant rational map that sends zero to zero.

Lemma

If E and E' are elliptic curves over k in short Weierstrass form then every isogeny $\alpha\colon E \to E'$ can be put in standard form

$$\alpha(x,y) = \left(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y\right),$$

where $u, v, s, t \in k[x]$ are polynomials with $u \perp v$, $s \perp t$.
The roots of both v and t are the x-coordinates of the affine points in $\ker\alpha$.
The degree of α is $\max(\deg u, \deg v)$, and α is separable if and only if $(u/v)' \neq 0$.

Separable and inseparable isogenies

Lemma

Let k be a field of characteristic p. For relatively prime $u, v \in k[x]$ we have

$$(u/v)' = 0 \quad \Longleftrightarrow \quad u' = v' = 0 \quad \Longleftrightarrow \quad u = f(x^p) \text{ and } v = g(x^p) \text{ with } f, g \in k[x]$$

Proof

(first $\Leftrightarrow$): $(u/v)' = (u'v - v'u)/v^2 = 0$ iff $u'v = v'u$, and $u \perp v$ implies $u|u'$, which is impossible unless $u' = 0$, and similarly for v.
(second $\Leftrightarrow$): If $u = \sum_n a_n x^n$ then $u' = \sum n a_n x^{n-1} = 0$ iff $n a_n = 0$ for n with $a_n \neq 0$, in which case $u = \sum_m a_{mp} x^{mp} = f(x^p)$ where $f = \sum_m a_m x^m$, and similarly for v. □

In characteristic zero the lemma says that $u' = v' = 0$ if and only if $\deg u = \deg v = 0$, but isogenies are non-constant morphisms, so this never happens.

Decomposing inseparable isogenies

Lemma

Let $\alpha\colon E \to E'$ be an inseparable isogeny over k with E and E' in short Weierstrass form. Then $\alpha(x,y) = (a(x^p), b(x^p)y^p)$ for some $a, b \in k(x)$.

Proof

This follows from the previous lemma, see Lemma 5.3 in the notes for details. □

Corollary

Isogenies of elliptic curves over a field of characteristic $p > 0$ can be decomposed as

$$\alpha = \alpha_{\text{sep}} \circ \pi^n,$$

for some separable α_{sep}, with $\pi\colon (x:y:z) \mapsto (x^p : y^p : z^p)$ and $n \geq 0$.
The separable degree is $\deg_s \alpha := \deg \alpha_{\text{sep}}$, the inseparable degree is $\deg_i \alpha := p^n$.

First isogeny-kernel theorem

Theorem

The order of the kernel of an isogeny is equal to its separable degree.

Proof

To the blackboard! □

Corollary

A purely inseparable isogeny has trivial kernel.

Corollary

In any composition of isogenies $\alpha = \beta \circ \gamma$ all degrees are multiplicative:

$$\deg \alpha = (\deg \beta)(\deg \gamma), \qquad \deg_s \alpha = (\deg_s \beta)(\deg_s \gamma), \qquad \deg_i \alpha = (\deg_i \beta)(\deg_i \gamma).$$

Second isogeny-kernel theorem

Definition

Let E/k be an elliptic curve. A subgroup G of $E(\bar{k})$ is defined over L/k if it is Galois stable, meaning $\sigma(G) = G$ for all $\sigma \in \mathrm{Gal}(\bar{k}/L)$.

Theorem

Let E/k be an elliptic curve and G a finite subgroup of $E(\bar{k})$ defined over k.
There is a separable isogeny $\alpha\colon E \to E'$ with kernel G.
The isogeny α and the elliptic curve E'/k are unique up to isomorphism.

Proof sketch

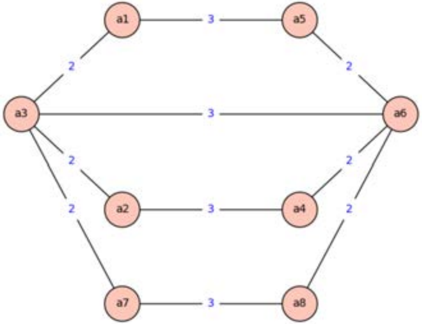
To the blackboard! □

Corollary

Isogenies of composite degree can be decomposed into isogenies of prime degree.

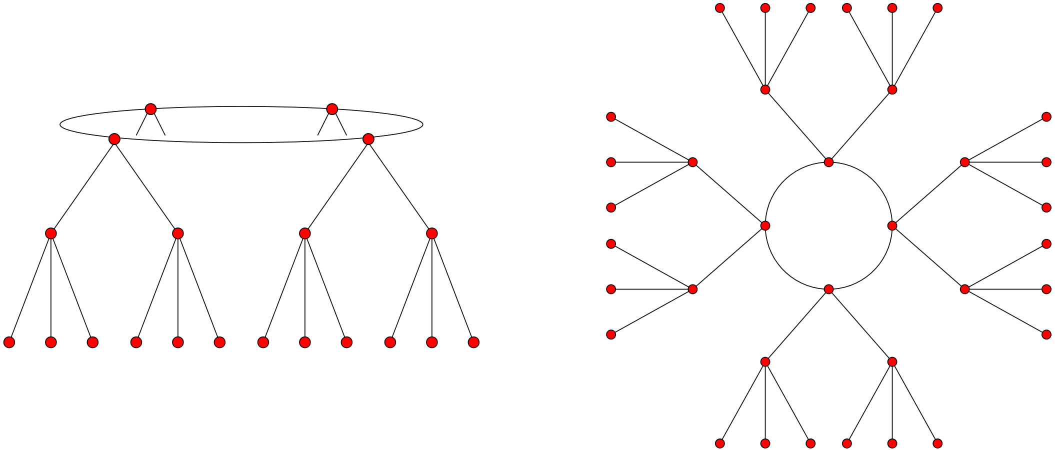
Isogeny graphs

$$\begin{pmatrix} 1 & 4 & 2 & 12 & 3 & 6 & 4 & 12 \\ 4 & 1 & 2 & 3 & 12 & 6 & 4 & 12 \\ 2 & 2 & 1 & 6 & 6 & 3 & 2 & 6 \\ 12 & 3 & 6 & 1 & 4 & 2 & 12 & 4 \\ 3 & 12 & 6 & 4 & 1 & 2 & 12 & 4 \\ 6 & 6 & 3 & 2 & 2 & 1 & 6 & 2 \\ 4 & 4 & 2 & 12 & 12 & 6 & 1 & 3 \\ 12 & 12 & 6 & 4 & 4 & 2 & 3 & 1 \end{pmatrix}$$



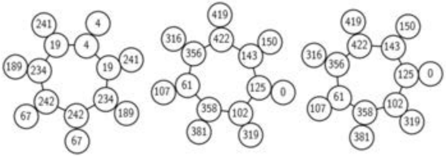
Isogeny class 30a in the L-functions and modular forms database.

Isogeny graphs

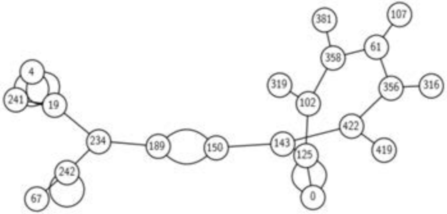


Side and top views of a 3-volcano over a finite field taken from *Isogeny volcanoes*.

Isogeny graphs



(a) The $\mathcal{G}_2(\mathbb{F}_p)$ *for* $p = 431$



(b) The spine $\mathcal{S} \subset \mathcal{G}_2(\overline{\mathbb{F}_p})$ *for* $p = 431$.

Figure 3.3: *Stacking, folding and attaching by an edge for* $\mathfrak{p} = 431$ *and* $\ell = 2$. *The leftmost component of* $\mathcal{G}_2(\mathbb{F}_p)$ *folds, the other two components stack, and the vertices* 189 *and* 150 *get attached by a double edge.*

Image taken from *Adventures in Supersingularland* by Sarah Arpin, Catalina Camacho-Navarro, Kristin Lauter, Joelle Lim, Kristina Nelson, Travis Scholl, and Jana Sotáková.

Isogeny graphs

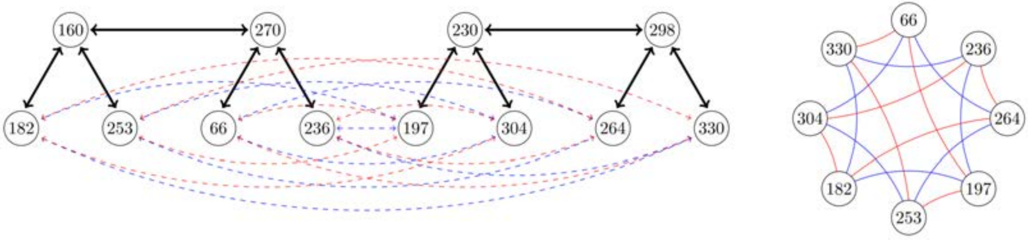


FIGURE 5. A whirlpool with two components.

Image taken from *Orienting supersingular isogeny graphs* by Leonardo Colò and David Kohel.

Constructing a separable isogeny from its kernel

Let E/k be an elliptic curve in Weierstrass form, and G a finite subgroup of $E(\bar{k})$.
Let $G_{\neq 0}$ denote the set of nonzero points in G, which are affine points $Q = (x_Q, y_Q)$.

For affine points $P = (x_P, y_P)$ in $E(\bar{k})$ not in G define

$$\alpha(x_P, y_P) := \left(x_P + \sum_{Q \in G_{\neq 0}} (x_{P+Q} - x_Q)\,,\; y_P + \sum_{Q \in G_{\neq 0}} (y_{P+Q} - y_Q) \right).$$

Here x_P and y_P are variables, x_Q and y_Q are elements of $\bar{k}$, and x_{P+Q} and y_{P+Q} are rational functions of x_P and y_P giving coordinates of $P+Q$ in terms of x_P and y_P.

For $P \notin G$ we have $\alpha(P) = \alpha(P+Q)$ if and only if $Q \in G$, so $\ker \alpha = G$.

Vélu's formula for constructing 2-isogenies

Theorem (Vélu)

Let $E\colon y^2 = x^3 + Ax + B$ be an elliptic curve over k and let $x_0 \in \bar{k}$ be a root of $x^3 + Ax + B$. Define $t := 3x_0^2 + A$ and $w := x_0 t$. The rational map

$$\alpha(x,y) := \left(\frac{x^2 - x_0 x + t}{x - x_0},\ \frac{(x - x_0)^2 - t}{(x - x_0)^2} y \right)$$

is a separable isogeny from E to $E'\colon y^2 = x^3 + A'x + B'$, where $A' := A - 5t$ and $B' := B - 7w$. The kernel of α is the group of order 2 generated by $(x_0, 0)$.

If $x_0 \in k$ then E' and α will be defined over k, but in general E' and α will be defined over $k(A', B')$ which might be a quadratic or cubic extension of k.

Vélu's formula for constructing cyclic isogenies of odd degree

Theorem (Vélu)

Let $E\colon y^2 = x^3 + Ax + B$ be an elliptic curve over k and let G be a finite subgroup of $E(\bar{k})$ of odd order. For each nonzero $Q = (x_Q, y_Q)$ in G define

$$t_Q := 3x_Q^2 + A, \qquad u_Q := 2y_Q^2, \qquad w_Q := u_Q + t_Q x_Q,$$

$$t := \sum_{Q \in G_{\neq 0}} t_Q, \qquad w := \sum_{Q \in G_{\neq 0}} w_Q, \qquad r(x) := x + \sum_{Q \in G_{\neq 0}} \left(\frac{t_Q}{x - x_Q} + \frac{u_Q}{(x - x_Q)^2} \right).$$

The rational map

$$\alpha(x, y) := \big(r(x),\, r'(x)y\big)$$

is a separable isogeny from E to $E'\colon y^2 = x^3 + A'x + B'$, where $A' := A - 5t$ and $B' := B - 7w$, with $\ker\alpha = G$. If G is defined over k then so are α and E'.

Jacobian coordinates

Let us now work in the weighted projective plane, where x, y, z have weights $2, 3, 1$. This means, for example, that x^3 and y^2 are monomials of the same degree.

The homogeneous equation for an elliptic curve E in short Weierstrass form is then

$$y^2 = x^3 + Axz^4 + Bz^6.$$

In general Weierstrass form we have

$$y^2 + a_1xyz + a_3yz^3 = x^3 + a_2x^2z^2 + a_4xz^4 + a_6z^6,$$

Pro tip 😎: a_i is the coefficient of the term containing z^i; this is why there is no a_5.

In Jacobian coordinates the formulas for the group law look more complicated, but the formula for z_3 becomes very simple: $z_3 = x_1z_2^2 - x_2z_1^2$ when adding distinct points $(x_1 : y_1 : z_1)$ and $(x_2 : y_2 : z_2)$ and $z_3 = 2y_1z_1$ when doubling $(x_1 : y_1 : z_1)$.

Division polynomials

If we apply the group law in Jacobian coordinates to an affine point $P = (x : y : 1)$ on $E\colon y^2 = x^3 + Ax + B$ we can compute the rational map (in affine coordinates):

$$nP = \left(\frac{\phi_n}{\psi_n^2}, \frac{\omega_n}{\psi_n^3} \right).$$

where ϕ_n, ω_n, ψ_n are polynomials in $\mathbb{Z}[x, y, A, B]$ with degree at most 1 in y (we can reduce modulo $(y^2 - x^3 - Ax - B)$ to ensure this).

The polynomials ϕ_n and ψ_n^2 have degree 0 in y, so we write them as $\phi_n(x)$ and $\psi_n^2(x)$. Exactly one of ω_n and ψ_n^3 has degree 1 in y, so nP is effectively in standard form.

Division polynomial recurrences

Definition

Let $E\colon y^2 = x^3 + Ax + B$ be an elliptic curve. Let $\psi_0 = 0$, and define $\psi_1, \psi_2, \psi_3, \psi_4$ as:

$$\begin{aligned}
\psi_1 &= 1, \\
\psi_2 &= 2y, \\
\psi_3 &= 3x^4 + 6Ax^2 + 12Bx - A^2, \\
\psi_4 &= 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - A^3 - 8B^2).
\end{aligned}$$

We then define ψ_n for $n > 4$ via the recurrences

$$\begin{aligned}
\psi_{2n+1} &= \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3, \\
\psi_{2n} &= \frac{1}{2y}\psi_n(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2).
\end{aligned}$$

We also define $\psi_{-n} := -\psi_n$ (and the recurrences work for negative integers as well).

Division polynomial recurrences

Definition

Having defined ψ_n for $E\colon y^2 = x^3 + Ax + B$ and all $n \in \mathbb{Z}$, we now define

$$\phi_n := x\psi_n^2 - \psi_{n+1}\psi_{n-1},$$
$$\omega_n := \frac{1}{4y}(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2),$$

and one finds that $\phi_n = \phi_{-n}$ and $\omega_n = \omega_{-n}$.

It is a somewhat tedious algebraic exercise to verify that these recursive definitions agree with the definitions given by applying the group law. See this Sage notebook.

We rarely use ϕ_n and ω_n, but need to know the degree and leading coefficient of ϕ_n to compute the degree and separability of the multiplication-by-n map.

Multiplication-by-n maps

Theorem

Let E/k be an elliptic curve defined by the equation $y^2 = x^3 + Ax + B$ and let n be a nonzero integer. The multiplication-by-n map is defined by the affine rational map

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

Lemma

The polynomial $\phi_n(x)$ is monic of degree n^2 and the polynomial $\psi_n^2(x)$ has leading coefficient n^2, degree $n^2 - 1$, and is coprime to $\phi_n(x)$.

Corollary

The multiplication-by-n map on E/k has degree n^2 and is separable if and only $p \nmid n$.

18.783 / 18.7831 Elliptic Curves
Fall 2025