

# 18.783 Elliptic Curves

## Lecture 4

Andrew Sutherland

September 16, 2025

# The function field of a curve

## Definition

Let  $C/k$  be a plane projective curve  $f(x, y, z) = 0$  with  $f \in k[x, y, z]$  nonconstant, homogeneous, and irreducible in  $\bar{k}[x, y, z]$ . The **function field**  $k(C)$  is the set of equivalence classes of rational functions  $g/h$  such that:

- (i)  $g$  and  $h$  are homogeneous polynomials in  $k[x, y, z]$  of the same degree;
- (ii)  $h$  is not divisible by  $f$ , equivalently,  $h$  is not an element of the ideal  $(f)$ ;
- (iii)  $g_1/h_1$  and  $g_2/h_2$  are considered equivalent whenever  $g_1h_2 - g_2h_1 \in (f)$ .

Addition:  $\frac{g_1}{h_1} + \frac{g_2}{h_2} = \frac{g_1h_2 + g_2h_1}{h_1h_2}$ ,    Multiplication  $\frac{g_1}{h_1} \cdot \frac{g_2}{h_2} = \frac{g_1g_2}{h_1h_2}$ ,    Inverse:  $(\frac{g}{h})^{-1} = \frac{h}{g}$ .

If  $g \in (f)$  then  $g/h = 0$  in  $k(C)$ , so we don't define  $(g/h)^{-1}$  in this case.

The field  $k(C)$  is a transcendental extension of  $k$  (of transcendence degree 1).

😎 Pro tips: • Don't confuse  $k(C)$  and  $C(k)$ . • Don't assume  $k[x, y, z]/(f)$  is a UFD.

## Evaluating functions in $k(C)$ at a point in $C(\bar{k})$

For  $g/h \in k(C)$  with  $\deg g = \deg h = d$  and any  $\lambda \in k^\times$  we have

$$\frac{g(\lambda x, \lambda y, \lambda z)}{h(\lambda x, \lambda y, \lambda z)} = \frac{\lambda^d g(x, y, z)}{\lambda^d h(x, y, z)} = \frac{g(x, y, z)}{h(x, y, z)} \quad \checkmark$$

For any  $P \in C(\bar{k})$  we have  $f(P) = 0$ , so if  $g_1/h_1 = g_2/h_2$  with  $h_1(P), h_2(P) \neq 0$ , then  $g_1(P)h_2(P) - g_2(P)h_1(P) = f(P) = 0$ , so  $(g_1/h_1)(P) = (g_2/h_2)(P)$ .  $\checkmark$

To evaluate  $\alpha \in k(C)$  at  $P \in C(\bar{k})$  we need to choose  $\alpha = g/h$  with  $h(P) \neq 0$ .

### Example

$f(x, y, z) = zy^2 - x^3 - z^2x$ ,  $P = (0 : 0 : 1)$ ,  $\alpha = 3xz/y^2$ . We have

$$\alpha(P) = \frac{3xz}{y^2}(0 : 0 : 1) = \frac{3xz^2}{x^3 + z^2x}(0 : 0 : 1) = \frac{3z^2}{x^2 + z^2}(0 : 0 : 1) = 3$$

# Rational maps

## Definition

We say that  $\alpha \in k(C)$  is **defined** at  $P \in C(\bar{k})$  if  $\alpha = g/h$  with  $h(P) \neq 0$ .

## Definition

Let  $C_1/k$  and  $C_2/k$  be projective plane curves. A **rational map**  $\phi: C_1 \rightarrow C_2$  is a triple  $(\phi_x : \phi_y : \phi_z) \in \mathbb{P}^2(k(C_1))$  such that for any  $P \in C_1(\bar{k})$  where  $\phi_x, \phi_y, \phi_z$  are defined and not all zero we have  $(\phi_x(P) : \phi_y(P) : \phi_z(P)) \in C_2(\bar{k})$ .

The rational map  $\phi$  is **defined** at  $P$  if there exists  $\lambda \in k(C_1)^\times$  such that  $\lambda\phi_x, \lambda\phi_y, \lambda\phi_z$  are defined and not all zero at  $P$ .

## Rational maps (alternative approach)

Let  $C_1 : f_1(x, y, z) = 0$  and  $C_2 : f_2(x, y, z) = 0$  be projective curves over  $k$ .  
If  $\psi_x, \psi_y, \psi_z \in k[x, y, z]$  are homogeneous of the same degree, not all in  $(f_1)$ ,  
and  $f_2(\psi_x, \psi_y, \psi_z) \in (f_1)$ , then at least one and possibly all of

$$(\psi_x/\psi_z : \psi_y/\psi_z : 1), \quad (\psi_x/\psi_y : 1 : \psi_z/\psi_y), \quad (1 : \psi_y/\psi_x : \psi_z/\psi_x)$$

is a rational map  $\psi : C_1 \rightarrow C_2$ . Call two such triples  $(\psi_x : \psi_y : \psi_z)$  and  $(\psi'_x : \psi'_y : \psi'_z)$  equivalent if  $\psi'_x\psi_y - \psi_x\psi'_y$  and  $\psi'_x\psi_z - \psi_x\psi'_z$  and  $\psi'_y\psi_z - \psi_y\psi'_z$  all lie in  $(f_1)$ .

This holds in particular when  $\psi'_* = \lambda\psi_*$  for some nonzero homogeneous  $\lambda \in k[x, y, z]$ , so we can always remove any common factor of  $\psi_x, \psi_y, \psi_z$ .

Equivalent triples define the same rational map, and every rational map can be defined this way: if  $\phi = (\frac{g_x}{h_x} : \frac{g_y}{h_y} : \frac{g_z}{h_z})$  then take  $\psi_x := g_x h_y h_z$ ,  $\psi_y := g_y h_x h_z$ ,  $\psi_z := g_z h_x h_y$ .

The rational map given by  $[\psi_x, \psi_y, \psi_z]$  is defined at  $P \in C_1(\bar{k})$  whenever any of  $\psi_x(P), \psi_y(P), \psi_z(P)$  is nonzero, in which case  $(\psi_x(P) : \psi_y(P) : \psi_z(P)) \in C_2(\bar{k})$ .

# Morphisms

## Definition

A **morphism** is a rational map  $\phi: C_1 \rightarrow C_2$  that is defined at every  $P \in C_1(\bar{k})$ .

## Theorem

*If  $C_1$  is a smooth projective curve then every rational map  $\phi: C_1 \rightarrow C_2$  is a morphism.*

(Because when  $C_1$  is smooth its coordinate ring  $k[C_1]$  is a **Dedekind domain**.)

## Theorem

*A morphism of projective curves is either surjective or constant.*

(Because projective varieties are **complete/proper**.)

Projective curves are **isomorphic** if there is an invertible morphism  $\phi: C_1 \rightarrow C_2$ .

We then have a bijection  $C_1(\bar{k}) \rightarrow C_2(\bar{k})$ , but this necessary condition is not sufficient!

# An equivalence of categories

Every surjective morphism of projective curves  $\phi: C_1 \rightarrow C_2$  induces an injective morphism  $\phi^*: k(C_2) \rightarrow k(C_1)$  of function fields defined by  $\alpha \mapsto \alpha \circ \phi$ .

## Theorem

*The categories of smooth projective curves over  $k$  with surjective morphisms and function fields of transcendence degree one over  $k$  are contravariantly equivalent via the functor  $C \mapsto k(C)$  and  $\phi \mapsto \phi^*$ .*

Every curve  $C$ , even singular affine curves, has a function field (for plane curves  $f(x, y) = 0$ ,  $k(C)$  is the fraction field of  $k[C] := k[x, y]/(f)$ ). The function field  $k(C)$  is categorically equivalent to a smooth projective curve  $\tilde{C}$ , the **desingularization** of  $C$ .

One can construct  $\tilde{C}$  from  $C$  geometrically (using blow ups), but its existence is categorical, and in many applications the function field is all that matters.

# Isogenies

Let  $E_1, E_2$  be elliptic curves over  $k$ , with distinguished points  $O_1, O_2$ .

## Definition

An **isogeny**  $\phi: E_1 \rightarrow E_2$  is a surjective morphism that is also a group homomorphism.

## Definition (apparently weaker but actually equivalent)

An **isogeny**  $\phi: E_1 \rightarrow E_2$  is a non-constant rational map with  $\phi(O_1) = O_2$ .

$E_1$  and  $E_2$  are **isomorphic** if there are isogenies  $\phi_1: E_1 \rightarrow E_2$  and  $\phi_2: E_2 \rightarrow E_1$  whose composition is the identity (the isogenies  $\phi_1$  and  $\phi_2$  are then called **isomorphisms**).

Morphisms  $\phi: E_1 \rightarrow E_1$  with  $\phi(O_1) = O_1$  are **endomorphisms**.

Note that  $E_1 \rightarrow O_1$  is an endomorphism, but it is **not an isogeny** (for us at least).

Endomorphisms that are isomorphisms are called **automorphisms**.

## Examples of isogenies and endomorphisms

- The negation map  $[-1]: P \mapsto -P$  defined by  $(x : y : z) \mapsto (x : -y : z)$  is an isogeny, an endomorphism, an isomorphism, and an automorphism.
- For any integer  $n$  the multiplication by  $n$  map  $[n]: P \mapsto nP$  is an endomorphism. It is an isogeny for  $n \neq 0$  and an automorphism for  $n = \pm 1$ .
- For  $E/\mathbb{F}_q$  we have the **Frobenius endomorphism**  $\pi_E: (x : y : z) \mapsto (x^q : y^q : z^q)$ . It induces a group isomorphism  $E(\overline{\mathbb{F}}_q) \rightarrow E(\overline{\mathbb{F}}_q)$ , but it is **not an isomorphism**.
- For  $E/\mathbb{F}_q$  of characteristic  $p$  the map  $\pi: (x : y : z) \mapsto (x^p : y^p : z^p)$  is an isogeny, but typically not an endomorphism. For  $E: y^2 = x^3 + Ax + B$  the image of  $\pi$  is the elliptic curve  $E^{(p)}: y^2 = x^3 + A^p x + B^p$ , which need not be isomorphic to  $E$ .

## The multiplication-by-2 map

Let  $E/k$  be defined by  $y^2 = x^3 + Ax + B$  and let  $\phi$  be the endomorphism  $P \mapsto 2P$ . The doubling formula for affine  $P = (x : y : 1) \in E(\bar{k})$  is given by

$$\phi_x(x, y) = m(x, y)^2 - 2x = \frac{(3x^2 + A)^2 - 8xy^2}{4y^2},$$

$$\phi_y(x, y) = m(x, y)(x - \phi_x(x, y)) - y = \frac{12xy^2(3x^2 + A) - (3x^2 + A)^3 - 8y^4}{8y^3},$$

with  $m(x, y) := (3x^2 + A)/(2y)$ . We then have  $\phi := (\psi_x/\psi_z : \psi_y/\psi_z : 1)$  with

$$\psi_x(x, y, z) = 2yz((3x^2 + Az^2)^2 - 8xy^2z),$$

$$\psi_y(x, y, z) = 12xy^2z(3x^2 + Az^2) - (3x^2 + Az^2)^3 - 8y^4z^2,$$

$$\psi_z(x, y, z) = 8y^3z^3.$$

How do we evaluate this morphism at the point  $O := (0 : 1 : 0)$ ? 🤖

## The multiplication-by-2 map

How do we evaluate this morphism at the point  $O := (0 : 1 : 0)$ ?

We can add any multiple of  $f(x, y, z) = y^2z - x^3 - Axz^2 - Bz^3$  to any of  $\psi_x, \psi_y, \psi_z$ ; this won't change the morphism  $\phi$ .

Replacing  $\psi_x$  by  $\psi_x + 18xyzf$  and  $\psi_y$  by  $\psi_y + (27f - 18y^2z)f$ , and simplifying yields

$$\psi_x(x, y, z) = 2y(xy^2 - 9Bxz^2 + A^2z^3 - 3Ax^2z),$$

$$\psi_y(x, y, z) = y^4 - 12y^2z(2Ax + 3Bz) - A^3z^4 + 27Bz(2x^3 + 2Axz^2 + Bz^3) + 9Ax^2(3x^2 + 2Az^2),$$

$$\psi_z(x, y, z) = 8y^3z.$$

Now  $\phi(O) = (\psi_x(0, 1, 0) : \psi_y(0, 1, 0) : \psi_z(0, 1, 0)) = (0 : 1 : 0) = O$ , as expected.

That wasn't particularly fun. 😞 But there is a way to completely avoid this! 😊

## A standard form for isogenies

### Lemma

Let  $E_1: y^2 = f_1(x)$  and  $E_2: y^2 = f_2(x)$  be elliptic curves over  $k$  and let  $\alpha: E_1 \rightarrow E_2$  be an isogeny. Then  $\alpha$  can be put in the affine *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  $u \perp v$  and  $s \perp t$ .

### Corollary

When  $\alpha: E_1 \rightarrow E_2$  is defined as above we necessarily have  $v^3 | t^2$  and  $t^2 | v^3 f_1$ .

It follows that  $v(x)$  and  $t(x)$  have the same set of roots in  $\bar{k}$ , and these roots are precisely the  $x$ -coordinates of the affine points in  $E_1(\bar{k})$  that lie in the kernel of  $\alpha$ . In particular,  $\ker \alpha$  is a finite subgroup of  $E_1(\bar{k})$ .

# Degree and separability

## Definition

Let  $\alpha(x, y) = \left( \frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y \right)$  be an isogeny in standard form.

The **degree** of  $\alpha$  is  $\deg \alpha := \max(\deg u, \deg v)$ .

We say that  $\alpha$  is **separable** if  $(u/v)'$  is nonzero, otherwise  $\alpha$  is **inseparable**.

## Definition (equivalent)

Let  $\alpha: E_1 \rightarrow E_2$  be an isogeny, let  $\alpha^*: k(E_2) \rightarrow k(E_1)$  be the corresponding embedding of function fields, and consider the field extension  $k(E_1)/\alpha^*(k(E_2))$ .

The **degree** of  $\alpha$  is the degree of the field extension  $k(E_1)/\alpha^*(k(E_2))$ .

We say that  $\alpha$  is **separable** if  $k(E_1)/\alpha^*(k(E_2))$  is separable, otherwise  $\alpha$  is **inseparable**.

## Examples

- The standard form of the negation map  $[-1]$  is  $[-1](x, y) = (x, -y)$ . It is separable and has degree 1.

- The standard form of the multiplication-by-2 map  $[2]$  is

$$[2](x, y) = \left( \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4(x^3 + Ax + B)}, \frac{x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - A^3 - 8B^2}{8(x^3 + Ax + B)^2} y \right).$$

It is separable and has degree 4.

- The standard form of the Frobenius endomorphism of  $E/\mathbb{F}_q$  is

$$\pi_E(x, y) = \left( x^q, (x^3 + Ax + B)^{(q-1)/2} y \right).$$

Note that we have used the curve equation to transform  $y^q$  (here  $q$  is odd). It is inseparable, because  $(x^q)' = qx^{q-1} = 0$ , and it has degree  $q$ .

MIT OpenCourseWare

<https://ocw.mit.edu>

18.783 / 18.7831 Elliptic Curves

Fall 2025

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