

5 Isogenies

In almost every branch of mathematics, when considering a category of mathematical objects with a particular structure, the maps between objects that preserve this structure (morphisms) play a crucial role. For groups and rings we have homomorphisms, for vector spaces we have linear transformations, and for topological spaces we have continuous functions. For elliptic curves (and more generally, abelian varieties), the structure-preserving maps are called *isogenies*.¹

5.1 Morphisms of projective curves

As abelian varieties, elliptic curves have both an algebraic structure (as an abelian group), and a geometric structure (as a smooth projective curve). We are all familiar with morphisms of groups (these are group homomorphisms), but we have not formally defined a morphism of projective curves. To do so we need to define a few notions from algebraic geometry. Since algebraic geometry is not a prerequisite for this course, we will take a brief detour to define the terms we need. To keep things as simple and concrete as possible, we will focus on plane projective curves with a few remarks along the way about how to generalize these definitions for those who are interested (those who are not can safely ignore the remarks). As usual, we use \bar{k} to denote a fixed algebraic closure of our base field k that contains any and all algebraic extensions of k that we may consider.

Definition 5.1. Let C/k be a plane projective curve $f(x, y, z) = 0$ with $f \in k[x, y, z]$ irreducible in $\bar{k}[x, y, z]$. The *function field* $k(C)$ consists of rational functions g/h , where

- (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 $g_1h_2 - g_2h_1 \in (f)$.

If L is any algebraic extension of k (including $L = \bar{k}$), the function field $L(C)$ is similarly defined with $g, h \in L[x, y, z]$.

Remark 5.2. The function field $k(X)$ of an (irreducible) projective variety X/k given by homogeneous polynomials $f_1, \dots, f_m \in k[x_0, \dots, x_n]$ is defined similarly, just replace the ideal (f) with the ideal (f_1, \dots, f_m) .

Be sure not to confuse the notation $k(C)$ with $C(k)$; the latter denotes the set of k -rational points on C , not its function field.

We claim that $k(C)$ is a ring under addition and multiplication of rational functions. To see this, first note that if $h_1, h_2 \notin (f)$ then $h_1h_2 \notin (f)$ because f is irreducible and $k[x, y, z]$ is a unique factorization domain (in particular, (f) is a prime ideal). Thus for any $g_1/h_1, g_2/h_2 \in k(C)$ we have

$$\frac{g_1}{h_1} + \frac{g_2}{h_2} = \frac{g_1h_2 + g_2h_1}{h_1h_2} \in k(C) \quad \text{and} \quad \frac{g_1}{h_1} \cdot \frac{g_2}{h_2} = \frac{g_1g_2}{h_1h_2} \in k(C).$$

We can compute the inverse of g/h as h/g except when $g \in (f)$, but in this case g/h is equivalent to $0/1 = 0$, since $g \cdot 1 - 0 \cdot h = g \in (f)$; thus every nonzero element of $k(C)$ is

¹The word *isogeny* literally means "equal origins". It comes from biology, where the terms *isogenous*, *isogenic*, and *isogenetic* refer to different tissues derived from the same progenitor cell. The prefix "iso" means equal and the root "gene" means origin (as in the word *genesis*).

invertible, hence the ring $k(C)$ is a field. The field $k(C)$ contains k as a subfield (take g and h with degree 0), but it is not an algebraic extension of k , it is transcendental; indeed, it has transcendence degree 1, consistent with the fact that C is a projective variety of dimension 1 (this is one way to define the dimension of an algebraic variety).

The fact that g and h have the same degree allows us to meaningfully assign a value to the function g/h at a projective point $P = (x : y : z)$ on C , so long as $h(P) \neq 0$, since

- (a) we get the same result for any projectively equivalent $P = (\lambda x : \lambda y : \lambda z)$ with $\lambda \in k^\times$, because g and h are homogeneous of the same degree (say d):

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

- (b) if g_1/h_1 and g_2/h_2 are equivalent with $h_1(P), h_2(P) \neq 0$, then $g_1(P)h_2(P) - g_2(P)h_1(P)$ is a multiple of $f(P) = 0$, so $(g_1/h_1)(P) = (g_2/h_2)(P)$.

Thus assuming the denominators involved are all nonzero, the value of $\alpha(P)$ does not depend on how we choose to represent either α or P . If $\alpha = g_1/h_1$ with $h_1(P) = 0$, it may happen that g_1/h_1 is equivalent to some g_2/h_2 with $h_2(P) \neq 0$. This is a slightly subtle point. It may not be immediately obvious whether or not such a g_2/h_2 exists, since it depends on equivalence modulo f ; in general there may be no canonical way to write g/h in "simplest terms", because the ring $k[x, y, z]/(f)$ is typically *not* a unique factorization domain.

Example 5.3. Suppose C/k is defined by $f(x, y, z) = zy^2 - x^3 - z^2x = 0$, and consider the point $P = (0 : 0 : 1) \in C(k)$. We can't evaluate $\alpha = 3xz/y^2 \in k(C)$ at P as written since its denominator vanishes at P , but we can use the equivalence relation in $k(C)$ to write

$$\alpha = \frac{3xz}{y^2} = \frac{3xz^2}{x^3 + z^2x} = \frac{3z^2}{x^2 + z^2},$$

and we then see that $\alpha(P) = 3$.

Definition 5.4. Let C/k be a projective curve with $\alpha \in k(C)$. We say that α is *defined* (or *regular*) at a point $P \in C(\bar{k})$ if α can be represented as g/h for some $g, h \in k[x, y, z]$ with $h(P) \neq 0$.

Remark 5.5. If C is the projective closure of an affine curve $f(x, y) = 0$, one can equivalently define $k(C)$ as the fraction field of $k[x, y]/(f)$; this ring is known as the *coordinate ring* of C , denoted $k[C]$, and it is an integral domain provided that (f) is a prime ideal (which holds in our setting because we assume f is irreducible). In this case one needs to homogenize rational functions $r(x, y) = g(x, y)/h(x, y)$ in order to view them as functions defined on projective space. This is done by introducing powers of z so that the numerator and denominator are homogeneous polynomials of the same degree. The same remark applies to (irreducible) varieties of higher dimension.

We can now formally define a *rational map* of projective curves. Recall that for any field F , including $F = k(C)$, we use $\mathbb{P}^2(F)$ to denote the set of projective triples $(x : y : z)$ with $x, y, z \in F$ not all zero, with the equivalence relation $(x : y : z) \sim (\lambda x : \lambda y : \lambda z)$ for all $\lambda \in F^\times$.

Definition 5.6. Let C_1 and C_2 be plane projective curves defined over k . A *rational map* $\phi: C_1 \rightarrow C_2$ is a projective triple $(\phi_x : \phi_y : \phi_z) \in \mathbb{P}^2(k(C))$, such that for every point $P \in C_1(\bar{k})$ where $\phi_x(P), \phi_y(P), \phi_z(P)$ are defined and not all zero, the projective point $(\phi_x(P) : \phi_y(P) : \phi_z(P))$ lies in $C_2(\bar{k})$. The map C_1 is *defined* (or *regular*) at P if there exists $\lambda \in k(C)^\times$ such that $\lambda\phi_x, \lambda\phi_y, \lambda\phi_z$ are all defined at P and not all zero at P .

Remark 5.7. This definition generalizes to projective varieties in \mathbb{P}^n in the obvious way.

We should note that a rational map is not simply a function from $C_1(k)$ to $C_2(k)$ defined by rational functions, for two reasons. First, it might not be defined everywhere (although for smooth projective curves this does not happen, by Theorem 5.10 below). Second, it is required to map $C_1(\bar{k})$ to $C_2(\bar{k})$, which does not automatically hold for every rational map that carries $C_1(k)$ to $C_2(k)$; indeed, in general $C_1(k)$ could be the empty set (if C_1 is an elliptic curve then $C_1(k)$ is nonempty, but it could contain just a single point).

Remark 5.8. This is a general feature of classical algebraic geometry. In order for the definitions to work properly, one must consider the situation over an algebraic closure; an alternative approach is to use schemes, but we will not use schemes in this course.

It is important to remember that a rational map $\phi = (\phi_x : \phi_y : \phi_z)$ is defined only up to scalar equivalence by functions in $k(C)^\times$. There may be points $P \in C_1(\bar{k})$ where one of $\phi_x(P), \phi_y(P), \phi_z(P)$ is not defined or all three are zero, but it may still be possible to evaluate $\phi(P)$ after rescaling by $\lambda \in k(C)^\times$; we will see an example of this shortly.

The value of $\phi(P)$ is unchanged if we clear denominators in $(\phi_x : \phi_y : \phi_z)$ by multiplying through by an appropriate homogeneous polynomial (note: this is not the same as rescaling by an element of $\lambda \in K(C)^\times$). This yields a triple $(\psi_x : \psi_y : \psi_z)$ of homogeneous polynomials of equal degree that we view as a representing any of the three equivalent rational maps

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

all of which are equivalent to ϕ . We then have $\phi(P) = (\psi_x(P) : \psi_y(P) : \psi_z(P))$ whenever any of ψ_x, ψ_y, ψ_z is nonzero at P . Of course it can still happen that ψ_x, ψ_y, ψ_z all vanish at P , in which case we might need to look for an equivalent tuple of homogeneous polynomials that represents ϕ , but with this representation at least ψ_x, ψ_y, ψ_z are always defined at P .

Definition 5.9. A rational map that is defined everywhere is called a *morphism*.

For elliptic curves, distinguishing rational maps from morphisms is unnecessary; every rational map between elliptic curves is a morphism. More generally, we have the following.

Theorem 5.10. *If C_1 is a smooth projective curve then every rational map from C_1 to a projective curve C_2 is a morphism.*

The proof of this theorem is straight-forward (see [2, II.2.1]), but requires some commutative algebra that we don't want to introduce here.²

Remark 5.11. Theorem 5.10 is specific to smooth curves, it is not true more generally.

²The key point is that the coordinate ring of a smooth curve is a Dedekind domain. Thus its localization at every point P is a DVR, and after choosing a uniformizer we can rescale any rational map ϕ by a suitable λ (which will typically vary with P) so that all the components of ϕ have non-negative valuation at P and at least one has valuation zero and is therefore nonvanishing at P .

Two projective curves C_1 and C_2 are *isomorphic* if they are related by an invertible morphism ϕ ; this means that there is a morphism ϕ^{-1} such that $\phi^{-1} \circ \phi$ and $\phi \circ \phi^{-1}$ are the identity maps on $C_1(\bar{k})$ and $C_2(\bar{k})$, respectively. An isomorphism $\phi: C_1 \rightarrow C_2$ is necessarily a morphism that defines a bijection from $C_1(\bar{k})$ to $C_2(\bar{k})$, but the converse is not true, in general, because the inverse map of sets from $C_2(\bar{k})$ to $C_1(\bar{k})$ might not be a morphism (because it can't be defined by rational functions); we will see an example of this shortly.

Before leaving the topic of morphisms of curves, we note one more useful fact.

Theorem 5.12. *A morphism of projective curves is either surjective or constant.*

This theorem is a consequence of the fact that projective varieties are *complete* (or *proper*), which implies that the image of a morphism of projective varieties is itself a projective variety. This is a standard result that is proved in most of algebraic geometry textbooks, such as [1, II.4.9], for example. In the case of projective curves the image of a morphism $\phi: C_1 \rightarrow C_2$ of curves either has dimension 1, in which case ϕ is surjective (our curves are irreducible, by definition, and therefore cannot properly contain another curve), or dimension 0, in which case the image is a single point and ϕ is constant.

5.2 Isogenies of elliptic curves

We can now define the structure preserving maps between elliptic curves that will play a key role in this course.

Definition 5.13. An *isogeny* $\phi: E_1 \rightarrow E_2$ of elliptic curves defined over k is a surjective morphism of curves that induces a group homomorphism $E_1(\bar{k}) \rightarrow E_2(\bar{k})$. The elliptic curves E_1 and E_2 are then said to be *isogenous*.

Remark 5.14. Unless otherwise stated, we assume that the isogeny ϕ is itself defined over k (meaning that it can be represented by a rational map whose coefficients lie in k). In general, if L/k is an algebraic extension, we say that two elliptic curves defined over k are "isogenous over L " if they are related by an isogeny that is defined over L . Strictly speaking, in this situation we are really referring to the "base change" of the elliptic curves to L (same equations, different field of definition), but we won't be pedantic about this.

This definition is stronger than is actually necessary, for three reasons. First, any morphism of abelian varieties that preserves the identity element (the distinguished point that is the zero element of the group) induces a group homomorphism; we won't bother to prove this (see [2, Theorem III.4.8] for a proof), since for all the isogenies we are interested in it will be obvious that they are group homomorphisms. Second, by Theorem 5.12, any non-constant morphism of curves is surjective, and third, by Theorem 5.10, a rational map whose domain is a smooth projective curve is automatically a morphism. This leads to the following equivalent definition which is commonly used.

Definition 5.15. An *isogeny* $\phi: E_1 \rightarrow E_2$ of elliptic curves defined over k is a non-constant rational map that sends the distinguished point of E_1 to the distinguished point of E_2 .

Warning 5.16. Under our definitions the zero morphism, which maps every point on E_1 to the zero point of E_2 , is *not* an isogeny. This follows the standard convention for general abelian varieties which requires isogenies to preserve dimension (so they must be surjective and have finite kernel). In the case of elliptic curves this convention is not always followed (notably, Silverman [2, III.4] includes the zero morphism in his definition of an isogeny), but

it simplifies the statement of many theorems and is consistent with the more general usage you may see in later courses, so we will use it (we will still have occasion to refer to the zero morphism, we just won't call it an isogeny).

Definition 5.17. Elliptic curves E_1 and E_2 defined over a field k are *isomorphic* if there exist isogenies $\phi_1: E_1 \rightarrow E_2$ and $\phi_2: E_2 \rightarrow E_1$ whose composition is the identity; the isogenies ϕ_1 and ϕ_2 are then *isomorphisms*.

Definition 5.18. A morphism from an elliptic curve E/k to itself that fixes the distinguished point is called an *endomorphism*. An endomorphism that is also an isomorphism is an *automorphism*.

Except for the zero morphism, every endomorphism is an isogeny. As we shall see in the next lecture, the endomorphisms of an elliptic curve have a natural ring structure.

5.3 Examples of isogenies

We now give three examples of isogenies that are endomorphisms of an elliptic curve E/k defined by a short Weierstrass equation $y^2 = x^3 + Ax + b$ (we assume $\text{char}(k) \neq 2, 3$).

5.3.1 The negation map

In projective coordinates the map $P \mapsto -P$ is given by

$$(x : y : z) \mapsto (x : -y : z),$$

which is evidently a rational map. It is defined at every projective point, and in particular, at every $P \in E(\bar{k})$, so it is a morphism (as it must be, since it is a rational map defined on a smooth curve). It fixes $0 = (0 : 1 : 0)$ and is not constant, thus it is an isogeny. It is also an endomorphism, since it is a morphism from E to E that fixes 0 , and moreover an isomorphism (it is its own inverse), and therefore an automorphism.

5.3.2 The multiplication-by-2 map

Let E/k be the elliptic curve defined by $y^2 = x^3 + Ax + B$, and let $\phi: E \rightarrow E$ be defined by $P \mapsto 2P$. This is obviously a non-trivial group homomorphism (at least over \bar{k}), and we will now show that it is a morphism of projective curves. Recall that the formula for doubling an affine point $P = (x, y)$ on E is given by the rational functions

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

where $m(x, y) := (3x^2 + A)/(2y)$ is the slope of the tangent line at P . Homogenizing these and clearing denominators yields the rational map $\phi := (\psi_x/\psi_z : \psi_y/\psi_z : 1)$, where

$$\begin{aligned} \psi_x(x, y, z) &= 2yz((3x^2 + Az^2)^2 - 8xy^2z), \\ \psi_y(x, y, z) &= 12xy^2z(3x^2 + Az^2) - (3x^2 + Az^2)^3 - 8y^4z^2, \\ \psi_z(x, y, z) &= 8y^3z^3. \end{aligned}$$

If $y = 0$ then $3x^2 + Az^2 \neq 0$ (because $y^2z = x^3 + Axz^2 + Bz^3$ is non-singular), and it follows that the only point in $E(\bar{k})$ where ψ_x, ψ_y, ψ_z simultaneously vanish is the point $0 = (0 : 1 : 0)$. As a rational map of smooth projective curves, we know that ϕ is a morphism, hence defined everywhere, so there must be an alternative representation of ϕ that we can evaluate at the point 0 . Now in fact we know *a priori* that $\phi(0)$ must be 0 , since $2 \cdot 0 = 0$ but let's verify this explicitly.

In projective coordinates the curve equation is $f(x, y, z) := y^2z - x^3 - Axz^2 - Bz^3 = 0$. We are free to add any multiple of f in $k[x, y, z]$ of the correct degree (in this case 6) to any of ψ_x, ψ_y, ψ_z without changing the rational function ϕ they define. Let us replace ψ_x with $\psi_x + 18xyzf$ and ψ_y with $\psi_y + (27f - 18y^2z)f$, and remove the common factor z^2 to obtain

$$\begin{aligned}\psi_x(x, y, z) &= 2y(xy^2 - 9Bxz^2 + A^2z^3 - 3Ax^2z), \\ \psi_y(x, y, z) &= y^4 - 12y^2z(2Ax + 3Bz) - A^3z^4 \\ &\quad + 27Bz(2x^3 + 2Axz^2 + Bz^3) + 9Ax^2(3x^2 + 2Az^2), \\ \psi_z(x, y, z) &= 8y^3z.\end{aligned}$$

This is another representation of the rational map ϕ , and we can use this representation of ϕ to evaluate $\phi(0) = (\psi_x(0, 1, 0) : \psi_y(0, 1, 0) : \psi_z(0, 1, 0)) = (0 : 1 : 0) = 0$, as expected.

Having seen how messy things can get even with the relatively simply isogeny $P \mapsto 2P$, in the future we will be happy to omit such verifications and rely on the fact that if we have a rational map that we know represents an isogeny ϕ , then $\phi(0) = 0$ must hold. For elliptic curves in Weierstrass form, this means we only have to worry about evaluating isogenies at affine points, which allows us to simplify the equations by fixing $z = 1$.

5.3.3 The Frobenius endomorphism

Let \mathbb{F}_p be a finite field of prime order p . The *Frobenius automorphism* $\pi: \bar{\mathbb{F}}_p \rightarrow \bar{\mathbb{F}}_p$ is the map $x \mapsto x^p$. It is easy to check that π is a field automorphism: $0^p = 0$, $1^p = 1$, $(-a)^p = -a^p$, $(a^{-1})^p = (a^p)^{-1}$, $(ab)^p = a^p b^p$, and $(a + b)^p = \sum \binom{p}{k} a^k b^{p-k} = a^p + b^p$. If $f(x_1, \dots, x_k)$ is any rational function with coefficients in \mathbb{F}_p , then

$$f(x_1, \dots, x_k)^p = f(x_1^p, \dots, x_k^p),$$

since the coefficients of f are all fixed by π , which acts trivially on \mathbb{F}_p .

Every power π^n of π is also an automorphism of $\bar{\mathbb{F}}_p$; the fixed field of π^n is the finite field \mathbb{F}_{p^n} with p^n elements. For a finite field $\mathbb{F}_q = \mathbb{F}_{p^n}$ the map $x \mapsto x^q$ is called the *q-power Frobenius map*, which we may denote by π_q .

Definition 5.19. Let E be an elliptic curve over a finite field \mathbb{F}_q . The *Frobenius endomorphism* of E is the map $\pi_E: (x : y : z) \mapsto (x^q : y^q : z^q)$.

To see that this defines a morphism from E to E , for any point $P = (x, y, z) \in E(\bar{\mathbb{F}}_q)$, if we raise both sides of the curve equation

$$y^2z = x^3 + Axz^2 + Bz^3$$

to the q th power, we get

$$\begin{aligned}(y^2z)^q &= (x^3 + Axz^2 + Bz^3)^q \\ (y^q)^2 z^q &= (x^q)^3 + Ax^q (z^q)^2 + B(z^q)^3,\end{aligned}$$

thus $(x^q : y^q : z^q) \in E(\overline{\mathbb{F}}_q)$; we have $A^q = A$ and $B^q = B$ because $A, B \in \mathbb{F}_q$. Note that if $q \neq p$ and use the p -power Frobenius we still get a point on an elliptic curve, namely $y^2 = x^3 + A^p x + B^p$, but this curve is not the same as E (or even isomorphic to E).

To see that π_E is also a group homomorphism, note that the group law on E is defined by rational functions whose coefficients lie in \mathbb{F}_q ; these coefficients are invariant under the q -power map, so $\pi_E(P + Q) = \pi_E(P) + \pi_E(Q)$ for all $P, Q \in E(\overline{\mathbb{F}}_q)$.

These facts holds regardless of the equation used to define E and the formulas for the group law, including curves defined by a general Weierstrass equation (which is needed in characteristic 2 and 3).

Remark 5.20. The Frobenius endomorphism induces a group isomorphism from $E(\overline{\mathbb{F}}_q)$ to $E(\overline{\mathbb{F}}_q)$, since over the algebraic closure we can take q th roots of coordinates of points, and doing so still fixes elements of \mathbb{F}_q (in other words, the inverse of π_q in $\text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ also commutes with the group operation). But as an *isogeny* the Frobenius endomorphism is *not* an isomorphism because there is no rational map from $E \rightarrow E$ that acts as its inverse (why this is so will become obvious in later lectures).

5.4 A standard form for isogenies

To facilitate our work with isogenies, it will be convenient to put them in a standard form. In order to do so we will assume throughout that we are working with elliptic curves in short Weierstrass form $y^2 = x^3 + Ax + B$. Implicit in this assumption is that our elliptic curves are defined over a field k whose characteristic is not 2 or 3.³

Lemma 5.21. *Let E_1 and E_2 be elliptic curves over k in short Weierstrass form, and let $\alpha: E_1 \rightarrow E_2$ be an isogeny. Then α can be defined by an affine rational map of the 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 in x with $u \perp v$ and $s \perp t$.

The notation $f \perp g$ indicates that the polynomials f and g are coprime in $k[x]$ (equivalently, they have no common roots in \overline{k}).

Proof. Suppose α is defined by the rational map $(\alpha_x : \alpha_y : \alpha_z)$. Then for any affine point $(x : y : 1) \in E_1(\overline{k})$ we can write

$$\alpha(x, y) = (r_1(x, y), r_2(x, y)),$$

with $r_1(x, y) := \alpha_x(x, y, 1)/\alpha_z(x, y, 1)$ and $r_2(x, y) := \alpha_y(x, y, 1)/\alpha_z(x, y, 1)$. By repeatedly using the curve equation $y^2 = x^3 + Ax + B$ for E_1 to replace y^2 with a polynomial in x , we can assume that both r_1 and r_2 have degree at most 1 in y . We then have

$$r_1(x, y) = \frac{p_1(x) + p_2(x)y}{p_3(x) + p_4(x)y},$$

³In fact everything in this section works without modification for elliptic curves of the form $y^2 = f(x)$, even if the quadratic term of $f(x)$ is nonzero, so we only need to assume the characteristic is not 2.

for some $p_1, p_2, p_3, p_4 \in k[x]$. We now multiply the numerator and denominator of $r_1(x, y)$ by $p_3(x) - p_4(x)y$, and use the curve equation for E_1 to replace y^2 in the denominator with a polynomial in x , putting r_1 in the form

$$r_1(x, y) = \frac{q_1(x) + q_2(x)y}{q_3(x)},$$

for some $q_1, q_2, q_3 \in k[x]$.

We now use the fact that α is a group homomorphism and must therefore satisfy $\alpha(-P) = -\alpha(P)$ for any $P \in E_1(\bar{k})$. Recall that the inverse of an affine point (x, y) on a curve in short Weierstrass form is $(x, -y)$. Thus $\alpha(x, -y) = -\alpha(x, y)$ and we have

$$(r_1(x, -y), r_2(x, -y)) = (r_1(x, y), -r_2(x, y))$$

Thus $r_1(x, y) = r_1(x, -y)$, and this implies that q_2 is the zero polynomial. After eliminating any common factors from q_1 and q_3 , we obtain $r_1(x, y) = \frac{u(x)}{v(x)}$ for some $u, v \in k[x]$ with $u \perp v$, as desired. The argument for $r_2(x, y)$ is similar, except now we use $r_2(x, -y) = -r_2(x, y)$ to show that q_1 must be zero, yielding $r_2(x, y) = \frac{s(x)}{t(x)}y$ for some $s, t \in k[x]$ with $s \perp t$. \square

We shall refer to the expression $\alpha(x, y) = (\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y)$ given by Lemma 5.21 as the *standard form* of an isogeny $\alpha: E_1 \rightarrow E_2$. The fact that the rational functions $u(x)/v(x)$ and $s(x)/t(x)$ are in lowest terms implies that the polynomials u, v, s and t are uniquely determined up to a scalar in k^\times .

Lemma 5.22. *Let $E_1: y^2 = f_1(x)$ and $E_2: y^2 = f_2(x)$ be elliptic curves over k and let $\alpha(x, y) = (\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y)$ be an isogeny from E_1 to E_2 in standard form. Then v^3 divides t^2 and t^2 divides $v^3 f_1$. Moreover, $v(x)$ and $t(x)$ have the same set of roots in \bar{k} .*

Proof. Substituting $(\frac{u}{v}, \frac{s}{t}y)$ for (x, y) in the equation for E_2 gives $((s/t)y)^2 = f_2(u/v)$, and using the equation for E_1 to replace y^2 with $f_2(x)$ yields

$$(s/t)^2 f_1 = (u/v)^3 + A_2(u/v) + B_2$$

as an identity involving polynomials $f_1, s, t, u, v \in k[x]$. If we put $w = u^3 + A_2 uv^2 + B_2 v^3$ and clear denominators we obtain

$$v^3 s^2 f_1 = t^2 w. \tag{1}$$

Note that $u \perp v$ implies $v \perp w$, since any common factor of v and w must divide u . It follows that $v^3 | t^2$ and $t^2 | v^3 f_1$. This implies that v and t have the same roots in \bar{k} : every root of v is clearly a root of t (since $v^3 | t^2$), and every root x_0 of t is a double root of $t^2 | v^3 f_1$, and since f_1 has no double roots (because E_1 is not singular), x_0 must be a root of t (and possibly also a root of f_1). \square

Corollary 5.23. *Let $\alpha(x, y) = (\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y)$ be an isogeny $E_1 \rightarrow E_2$ in standard form. The affine points $(x_0 : y_0 : 1) \in E_1(\bar{k})$ in the kernel of α are precisely those for which $v(x_0) = 0$.*

Proof. If $v(x_0) \neq 0$, then $t(x_0) \neq 0$, and $\alpha(x_0, y_0) = (\frac{u(x_0)}{v(x_0)}, \frac{s(x_0)}{t(x_0)}y)$ is an affine point and therefore not 0 (the point at infinity), hence not in the kernel of α .

By homogenizing and putting α into projective form, we can write α as

$$\alpha = (ut : vsy : vt),$$

where ut, vsy , and vt are now homogeneous polynomials of equal degree ($s, t, u, v \in k[x, z]$).

Suppose $y_0 \neq 0$. By the previous lemma, if $v(x_0, 1) = 0$, then $t(x_0, 1) = 0$, and since $v^3|t^2$, the multiplicity of $(x_0, 1)$ as a root of t is strictly greater than its multiplicity as a root of v . This implies that, working over \bar{k} , we can renormalize α by dividing by a suitable power of $x - x_0z$ so that α_y does not vanish at $(x_0 : y_0 : 1)$ but α_x and α_z both do. Then $\alpha(x_0 : y_0 : 1) = (0 : 1 : 0) = 0$, and $(x_0 : y_0 : 1)$ lies in the kernel of α as claimed.

If $y_0 = 0$, then x_0 is a root of the cubic $f(x)$ in the equation $y^2 = f_1(x)$ for E_1 , and it is not a double root, since E_1 is not singular. In this case we renormalize α by multiplying by yz and then replacing y^2z with $f_1(x, z)$. Because $(x_0, 1)$ only has multiplicity 1 as a root of $f_1(x, z)$, its multiplicity as a root of vf_1 is no greater than its multiplicity as a root of t (here again we use $v^3|t^2$), and we can again renormalize α by dividing by a suitable power of $x - x_0z$ so that α_y does not vanish at $(x_0 : y_0 : 1)$, but α_x and α_z do (since they are now both divisible by $y_0 = 0$). Thus $(x_0 : y_0 : 1)$ is again in the kernel of α . \square

The corollary implies that if we have an isogeny $\alpha: E_1 \rightarrow E_2$ in standard form, we know exactly what to do if whenever we get a zero in the denominator when we try to compute $\alpha(P)$: we must have $\alpha(P) = 0$. This allows us to avoid in all cases the messy process that we went through earlier with the multiplication-by-2 map. We also obtain the following.

Corollary 5.24. *Let $\alpha: E_1 \rightarrow E_2$ be an isogeny of elliptic curves defined over a field k . The kernel of α is a finite subgroup of $E_1(\bar{k})$*

This corollary is true in general, but we will prove it under the assumption that we can put the isogeny α in our standard form (so $\text{char}(k) \neq 2$).

Proof. If we put α in standard form $(\frac{u}{v}, \frac{s}{t}y)$ then the polynomial $v(x)$ has at most $\deg v$ distinct roots in \bar{k} , each of which can occur as the x -coordinate of at most two points on the elliptic curve E_1 . \square

Remark 5.25. Note that this corollary would not be true if we included the zero morphism in our definition of an isogeny.

One can also use the standard form of an isogeny $\alpha: E_1 \rightarrow E_2$ to show that α is surjective as a map from $E_1(\bar{k})$ to $E_2(\bar{k})$; see [3, Thm. 2.22].⁴ But we already know that this applies to any non-constant morphism of curves (and even included surjectivity in our original definition of an isogeny), so we won't bother to prove this.

5.5 Degree and separability

We now define two important invariants of an isogeny that can be easily determined when it is in standard form.

Definition 5.26. Let $\alpha(x, y) = (\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y)$ be an isogeny in standard form. The *degree* of α is $\deg \alpha := \max\{\deg u, \deg v\}$, and we say that α is *separable* if the derivative of $\frac{u(x)}{v(x)}$ is nonzero; otherwise we say that α is *inseparable*.

As noted earlier, the polynomials u, v, s, t are uniquely determined up to a scalar factor, so the degree and separability of α are intrinsic properties that do not depend on its representation as a rational map.

⁴The theorem in [3] assumes that α is an endomorphism but the proof works for any isogeny.

Remark 5.27. The degree and separability of an isogeny can be defined in a way that is more obviously intrinsic using function fields. If $\alpha: E_1 \rightarrow E_k$ is an isogeny of elliptic curves defined over k then it induces an injection of function fields

$$\alpha^*: k(E_2) \rightarrow k(E_1)$$

that sends f to $f \circ \alpha$ (notice the direction of this map; the categorical equivalence between smooth projective curves and their function fields is contravariant). The degree of α is then the degree of $k(E_1)$ as an extension of the subfield $\alpha^*(k(E_2))$; this degree is finite because both are finite extensions of a purely transcendental extension of k . The isogeny α is then said to be separable if this field extension is separable (and is inseparable otherwise). This approach has the virtue of generality, but it is not as easy to apply explicitly. Our definition is equivalent, but we won't prove this.

Let us now return to the three examples that we saw earlier.

- The standard form of the negation map is $\alpha(x, y) = (x, -y)$. It is separable and has degree 1.
- The standard form of the multiplication-by-2 isogeny is

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

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 (and q is odd because we are not in characteristic 2). It is inseparable, because $(x^q)' = qx^{q-1} = 0$ in \mathbb{F}_q (since q must be a multiple of the characteristic p), and it has degree q .

References

- [1] Robin Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics **52**, Springer 1977.
- [2] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics **106**, second edition, Springer 2009.
- [3] Lawrence C. Washington, *Elliptic curves: Number theory and cryptography*, second edition, Chapman and Hall/CRC, 2008.

MIT OpenCourseWare
<https://ocw.mit.edu>

18.783 Elliptic Curves
Spring 2017

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