We spent the last four lectures focusing how to efficiently compute the group operation for an elliptic curve E over a finite field $\mathbb{F}_q$. Let's take a moment to look at the bigger picture. Given $E/\mathbb{F}_p$ there are several questions we might ask:

1. How big is the set $E(\mathbb{F}_p)$?
2. What is the structure of $E(\mathbb{F}_p)$ as a finite abelian group?

A bit later in the course we will also consider the converse questions: is there a way to construct an elliptic curve $E/\mathbb{F}_q$ with a specified number of $\mathbb{F}_q$-rational points and/or a specified group structure. Coming up with efficiently computable answers to these questions is critical to practical applications of elliptic curves such as cryptography.

When studying a set of mathematical objects with a particular structure, the maps that preserve this structure often play a crucial role in the theory. This is certainly true in the case of elliptic curves, whose structure-preserving maps are called *isogenies*; a thorough understanding of isogenies will allow us to answer all of the questions above.

5.1 Introduction to isogenies

Elliptic curves have both an algebraic structure, as an abelian group, and a geometric structure, as an algebraic curve. In this respect elliptic curves are the simplest examples of an *abelian variety*: elliptic curves are precisely the abelian varieties of dimension 1. Homomorphism of abelian varieties are called isogenies, and they respect both the algebraic and the geometric structure.

Definition 5.1. Let E_1 and E_2 be elliptic curves defined over a field k. An *isogeny* is a rational map $\alpha\colon E_1 \to E_2$ that induces a group homomorphism from $E_1(\bar{k})$ to $E_2(\bar{k})$.

This definition is (apparently) stronger than what is typically used. A rational map between elliptic curves induces a group homomorphism if and only if it preserves the identity element (the distinguished point 0); see [1, Theorem III.4.8].[1] But we will not need to use this fact, and our equivalent definition emphasizes the key feature of an isgoeny.

The map that sends every point on E_1 to the point 0 on E_2 is the *zero isogeny*. Some authors require isogenies to be nonzero by definition, but we include the zero isogeny in our definition as a matter of convenience (as does Silverman; see [1, III.4]). For example, pointwise addition $(\alpha+\beta)(P) = \alpha(P)+\beta(P)$ makes the set $\hom(E_1, E_2)$ of isogenies from E_1 to E_2 an additive abelian group; the zero isogeny is the identity element of this group.

To complete our definition we need to say exactly what we mean by a *rational map*. To do this we first introduce the *function field* of a curve, a concept that plays a key role in the general theory of algebraic curves. As this is an introductory course that focuses exclusively on curves of genus 1, we will shall make only very limited use of function fields, but they do allow us make our definitions more precise.

Definition 5.2. Let C/k be a projective curve defined by $f(x,y,z) = 0$, where $f \in k[x,y,z]$ is irreducible in $\bar{k}[x,y,z]$. The *function field* of C consists of rational functions g/h such that the following hold:

[1] According to Wikipedia, the term isogeny means "equal origins".

(i) g and h are homogenous elements of $k[x, y, z]$ of the same degree.

(ii) h does not lie in the ideal (f).

(iii) the functions g_1/h_1 and g_2/h_2 are considerd equivalent whenever $g_1h_2 - g_2h_1 \in (f)$.

The function field of C is denoted $k(C)$, which should not to be confused with $C(k)$, the set of k-rational points on C. The fact that f is irreducible and $k[x, y, z]$ is a unique factorization domain (so every irreducible element is prime) makes it clear that $k(C)$ is, in fact, a field. The field $\bar{k}(C)$ is defined analogously, with $g, h \in \bar{k}[x, y, z]$.

This definition follows [1, Remark 2.9]. Alternatively, if C is defined by an affine equation $f(x, y) = 0$, one can define $k(C)$ as the fraction field of the ring $k[x, y]/(f)$. When homogenizing a rational function $r(x, y) = g(x, y)/h(x, y)$ one introduces powers of z so that both the numerator and denominator have the same degree. For example:

$$\frac{x^3 + y + 1}{x^2 + y^2} \qquad \longrightarrow \qquad \frac{x^3 + yz^2 + z^3}{x^2z + y^2z}.$$

The *degree* of the rational function r is thus $\max\{\deg g, \deg h\}$.

We can now define a rational map.

Definition 5.3. Let C_1 and C_2 be projective curves k. A *rational map* $\phi\colon C_1 \to C_2$ has the form $(\phi_x : \phi_y : \phi_z)$, with $\phi_x, \phi_y, \phi_z \in \bar{k}(C_1)$, such that for every point $P \in C_1(\bar{k})$ where ϕ_x, ϕ_y, and ϕ_z are all defined, the point $(\phi_x(P) : \phi_y(P) : \phi_z(P))$ lies in $C_2(\bar{k})$.

Note that $\phi = (\phi_x : \phi_y : \phi_z)$ is defined only up to scalar equivalence: for any $\lambda \in \bar{k}^*$ the triple $(\lambda\phi_x : \lambda\phi_y : \lambda\phi_z)$ defines exactly the same rational map ϕ. There may be points $P \in \mathbb{C}_1(\bar{k})$ where one of ϕ_x, ϕ_y, or ϕ_z is not defined, but in this case it may still be possible to evaluate the map ϕ at P after rescaling ϕ by an element of $\bar{k}(C)$.

Definition 5.4. A rational map $\phi\colon C_1 \to C_2$ is *defined* (or *regular*) at a point $P \in C_1(\bar{k})$ if there exists a function $g \in \bar{k}(C_1)$ such that $g\phi_x, g\phi_y, g\phi_z$ are all defined at P and at least one is nonzero at P. We use $g\phi$ to denote the map $(g\phi_x : g\phi_y : g\phi_z)$.

Definition 5.5. 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 5.6 (Silverman II.2.1)**.** *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, but we will not give it here; we will see some explicit examples of it shortly. 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. For elliptic curves we have a stronger notion of isomorphism, since we also require the corresponding abelian groups to be isomorphic; this means that the identity element must be preserved.

Definition 5.7. An *isomorphism* of elliptic curves is an invertible isogeny.

Finally, we note the special case of an isogeny $\alpha\colon E \to E$ from an elliptic curve to itself; this is called an *endomorphism*. The set of endomorphisms of E forms a ring $\mathrm{End}(E)$ in which multiplication corresponds to composition.

5.2 Examples of isogenies

We now give two important examples of isogenies. As these are our first real examples, and both are particularly relevant to the material that follows, we will work them out in gory detail (which we will happily suppress in the future).

5.2.1 The multiplication-by-2 map

Let E/k be the elliptic curve defined by $y^2 = x^3 + Ax + B$, and let α be the map that sends P to $2P$. This is obviously a group homomorphism, and it is also a rational map, as we now show. The formula for doubling an affine point $P = (x, y)$ on E is given by the rational functions

$$\begin{aligned}
\alpha_x(x,y) &= m^2 - 2x \\
&= \left(\frac{3x^2+A}{2y}\right)^2 - 2x \\
&= \frac{9x^4 + 6Ax^2 + A^2x - 8xy^2}{4y^2}, \\
\alpha_y(x,y) &= m(x - \alpha_x(x,y)) - y = m(3x - m^2) - y \\
&= \left(\frac{3x^2+A}{2y}\right)\left(3x - \left(\frac{3x^2+A}{2y}\right)^2\right) - y \\
&= \frac{(3x^2+A)12xy^2 - (3x^2+A)^3 - 8y^4}{8y^3},
\end{aligned}$$

where $m = \frac{3x^2+A}{2y}$ is the slope of the tangent line at P. We can further simplify these expressions using the curve equation $y^2 = x^3 + Ax + B$, but for the moment we won't.

The functions $\alpha_x(x, y)$ and $\alpha_y(x, y)$ are defined at all affine points $P = (x, y)$ except those with $y = 0$. In order to understand what is happening at these points, we need to switch to projective coordinates. We have

$$\begin{aligned}
\alpha_x(x,y,z) &= \frac{9x^4 + 6Ax^2z^2 + A^2xz^3 - 8xy^2z}{4y^2z^2}, \\
\alpha_y(x,y,z) &= \frac{(3x^2+Az^2)12xy^2z - (3x^2+Az^2)^3 - 8y^4z^2}{8y^3z^3}, \\
\alpha_z(x,y,z) &= 1.
\end{aligned}$$

The points where α_x and α_y are undefined are precisely the 2-torsion points of $E(\bar{k})$; these are the three affine points $(x_i : 0 : 1)$ corresponding to the three distinct roots x_i of the cubic $x^3 + Ax + B$, and the point at infinity $(0 : 1 : 0)$. We know that, as a group homomorphism, the isogeny α maps all these points to 0 (the point at infinity). But we would like to confirm that this is also true of α as a rational map. As noted earlier, the rational map α is actually a morphism (since E is smooth), so it is defined everywhere. We just need to find a suitable rational function g for each 2-torsion point P such that $g\alpha_x, g\alpha_y, g\alpha_z$ are all defined at P and not all zero.

For the three affine points $(x_i : 0 : 1)$ we let $g = \frac{y^3}{z^3}$. We then have

$$\begin{aligned} g\alpha_x(x,y,z) &= \frac{y(9x^4 + 6Ax^2z^2 + A^2xz^3 - 8xy^2z)}{4z^5}, \\ g\alpha_y(x,y,z) &= \frac{(3x^2 + Az^2)12xy^2z - (3x^2 + Az^2)^3 - 8y^4z^2}{8z^6}, \\ g\alpha_z(x,y,z) &= \frac{y^3}{z^3}. \end{aligned}$$

These functions are defined at every affine point, and we have $g\alpha_y(x_i, 0, 1) = -(3x_i^2 + A)^3$, which is nonzero because x_i cannot be a root of both $x^3 + Ax + B$ and its derivative $3x^2 + A$, since the cubic discriminant $4A^3 + 27B^2$ is nonzero. Moreover, we can see that $(g\alpha)(x_i, 0, 1)$ is the point at infinity $(0 : 1 : 0)$, as expected.

For the point at infinity $(0 : 1 : 0)$ we instead let $g = \frac{z}{y}$. We then have

$$\begin{aligned} g\alpha_x(x,y,z) &= \frac{9x^4 + 6Ax^2z^2 + A^2xz^3 - 8xy^2z}{4y^3z} \\ &= \frac{9x(y^2 - Axz - Bz^2) + 6Ax^2z + A^2xz^2 + 8xy^2}{4y^3}, \\ g\alpha_y(x,y,z) &= \frac{(3x^2 + Az^2)12xy^2z - (3x^2 + Az^2)^3 - 8y^4z^2}{8y^4z^2} \\ &= \frac{x^6 + 5Ax^4z^2 + 20Bx^3z^3 - 5A^2x^2z^4 - 4ABxz^5 - A^3z^6 - 8B^2z^6}{8y^4z^2} \\ &= \frac{y^4 - 2Axy^2z - 2By^2z^2 + 5Ax^4 + 20Bx^3z - 4A^2x^2z^2 - 2ABxz^3 - A^3z^4 - 7B^2z^4}{8y^4}, \\ g\alpha_z(x,y,z) &= \frac{z}{y}. \end{aligned}$$

Here we have used $x^3 = y^2z - Axz^2 - Bz^3$ to introduce additional factors of z in the numerator that we use to remove factors of z from the denominator after cancellation. All three functions are defined at $(0 : 1 : 0)$, and we have $(g\alpha)(0, 1, 0) = (0 : 1 : 0)$, as required.

5.2.2 The Frobenius endomorphism

Let $\mathbb{F}_p$ be a finite field of prime order p. The *Frobenius automorphism* $\pi\colon \overline{\mathbb{F}}_p \to \overline{\mathbb{F}}_p$ is the map $\pi(x) = x^p$. 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 $f(x_1, \ldots, x_k)$ is any rational function with coefficients in $\mathbb{F}_p$, then

$$f(x_1, \ldots, x_k)^p = f(x_1^p, \ldots, x_k^p).$$

Note that π acts trivially on $\mathbb{F}_p$, but not on any proper extension of $\mathbb{F}_p$.

Every power π^n of π is also a field automorphism; the fixed field of π^n is the finite field $\mathbb{F}_{p^n}$. For a finite field $\mathbb{F}_q = \mathbb{F}_{p^n}$ the map that sends x to x^q is also often denoted π and called the q-power Frobenius map to avoid confusion.

Definition 5.8. Let E be an elliptic curve over a finite field $\mathbb{F}_q$. The Frobenius endomorphism of E sends the point (x, y, z) to (x^q, y^q, z^q).

We will usually use π to denote both the q-power Frobenius automorphism of $\mathbb{F}_q$ and the Frobenius endomorphism of E (which is meant will be clear from context). It is clear that π is a rational map from E to itself, and that it is defined everywhere. If E is defined by $y^2 = x^3 + Ax + B$, then for any point $P = (x_0, y_0, z_0) \in E(\overline{\mathbb{F}}_q)$ we have

$$0 = (y_0^2 z - x_0^3 - Ax_0 z_0^2 - Bz_0^3)^q = (y_0^q)^2 z_0^q - (x_0^q)^3 - Ax_0^q (z_0^q)^2 - B(z_0^q)^3,$$

thus $\pi(P) \in E(\overline{\mathbb{F}}_q)$ (here we have used $A, B \in \mathbb{F}_q$ to apply $A^q = A$ and $B^q = B$). To see that π 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 facts holds regardless of the equation used to define E and the formulas for the group law (so this holds in characteristic 2 as well).

Remark 5.9. Even though Frobenius endomorphism acts bijectively on $E(\overline{\mathbb{F}}_q)$ (it has trivial kernel), as an *isogeny*, it is *not an isomorphism*: there is no rational map from E to E that acts as its inverse. This will become clearer once we have defined the *degree* of an isogeny; isomorphisms have degree 1, but the Frobenius endomorphism has degree q. The fact that the degree of the Frobenius endomorphism is larger than its kernel is a distinctive feature. As we shall see, such isogenies are *inseparable*, a term that we will define shortly.

5.3 A standard form for isogenies

To facilitate our work with isogenies, it is convenient to put them in a standard form. In order to do so, we shall assume that our elliptic curves are in short Weierstrass form $y^2 = x^3 + Ax + B$. Note that this immediately implies that we are not working over a field of characteristic 2.

Lemma 5.10. *Let E_1 and E_2 be elliptic curves over k in short Weierstrass form, and let α be a nonzero isogeny from E_1 to E_2. Then α can be defined by an affine map of the form*

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

where $u, v, s, t \in \bar{k}[x]$ 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 relatively prime. Since we are working over $\bar{k}$, this is equivalent to assuming that f and g have no common roots.

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

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

where $r_1(x, y) = \alpha_x(x, y, 1)/\alpha_z(x, y, 1)$ and $r_2(x, y) = \alpha_y(x, y, 1)/\alpha_z(x, y, 1)$. Using the curve equation $y^2 = x^3 + Ax + B$ for E_1 to eliminate factors of y^n with $n > 1$, we can write $r_1(x, y) = \frac{p_1(x)+p_2(x)y}{p_3(x)+p_4(x)y}$, with $p_1, p_2, p_3, p_4 \in \bar{k}[x]$. We then 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 remove all factors of y from the denominator and put $r_1(x, y)$ in the form

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

for some $q_1, q_2, q_3 \in \bar{k}[x]$. Recall that the inverse of an affine point (x, y) on a curve in short Weierstrass form is $(x, -y)$. Thus $\alpha(x, -y) = -\alpha(x, y)$, since α is a group homomorphism, and therefore

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

Thus $r_1(x, y) = r_1(x, -y)$, which implies that q_2 is the zero polynomial. After eliminating any common factors of q_1 and q_3, we obtain $r_1(x, y) = \frac{u(x)}{v(x)}$ for some $u, v \in \bar{k}[x]$ 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 $s, t \in \bar{k}[x]$ with $s \perp t$. □

We shall refer to the expression $\alpha(x, y) = \big(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y\big)$ given by Lemma 5.10 as the *standard form* of an isogeny $\alpha\colon E_1 \to E_2$. Note that this assumes that E_1 and E_2 are in short Weierstrass form. The fact that the rational functions $u(x)/v(x)$ and $s(x)/t(x)$ are in lowest terms as elements of $\bar{k}(x)$ implies that the polynomials u, v, s and t are uniquely determined up to a scalar multiple.

Lemma 5.11. *Let $\alpha(x, y) = \big(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y\big)$ be an isogeny from E_1 to E_2 in standard form. Then $v(x)$ and $t(x)$ have the same set of roots. Moreover, v^3 divides t^2.*

Proof. Let E_1 be defined by $y^2 = x^3 + A_1x + B_1$ and let E_2 be defined by $y^2 = x^3 + A_2x + B_2$. By substituting $\big(\frac{u}{v}, \frac{s}{t}y\big)$ for (x, y) in the equation for E_2 we obtain

$$\left(\frac{s}{t}y\right)^2 = \left(\frac{u}{v}\right)^3 + A_2\frac{u}{v} + B_2.$$

Using the equation for E_1 to eliminate y^2 yields

$$\frac{s^2(x^3 + A_1x + B_1)}{t^2} = \frac{u^3 + A_2uv^2 + B_2v^3}{v^3}.$$

Setting $f(x) = x^3 + A_1x + B_1$ and $w = (u^3 + A_2uv^2 + B_2v^3)$, clearing denominators gives

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

Note that $u \perp v$ implies $v \perp w$, since any common root of v and w must be a root of u. Since v^3 divides the LHS, v^3 must divide t^2, since $v \perp w$, and every root of v is a root of t. Conversely, any root x_0 of t is a double root of t^2w and hence a double root of v^3s^2f. We have $s \perp t$, so x_0 is not a root of s, and f has no double roots, since E_1 is not singular. Thus x_0 is a root of v, as is every root of t. □

Corollary 5.12. *Let $\alpha(x, y) = \big(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y\big)$ be an isogeny from E_1 to E_2 in standard form. The affine points (x_0, y_0) in the kernel of α are precisely those points for which $v(x_0) = 0$.*

Proof. If $v(x_0) \neq 0$, then $t(x_0) \neq 0$, and $\alpha(x_0, y_0) = \big(\frac{u(x_0)}{v(x_0)}, \frac{s(x_0)}{t(x_0)}y\big)$ is an affine point and therefore not 0 (the point at infinity), hence not in the kernel of α. Now let α_x and α_y be the homogenizations of $\frac{u(x)}{v(x)}$ and $\frac{s(x)}{t(x)}y$, so that α is the rational map $(\alpha_x : \alpha_y : 1)$. If $v(x_0) = 0$ and $y_0 \neq 0$, we normalize α by the homogenization g of $t(x)$ as a rational function (homogenize $t(x)$ and divide by a suitable power of z). The lemma implies that $(g\alpha)(x_0 : y_0 : 1) = (0 : 1 : 0)$; note that the y-coordinate is non-zero because x_0 cannot be a root of $s \perp t$ and $y_0 \neq 0$. If $v(x_0) = 0$ and $y_0 = 0$, then we let g be the homogenization of $t(x)y/(x - x_0)$. Note that x_0 cannot be a double root of the cubic in the equation for E_1, which we use to replace y^2 in $g\alpha_y$, and the lemma implies that $t(x)y/(x-x_0)$ is still a multiple of $v(x)$, so $g\alpha_x$ is defined at $(x_0 : y_0 : 1)$, and we again have $(g\alpha)(x_0 : y_0 : 1) = (0 : 1 : 0)$. □

The corollary implies that once we put an isogeny $\alpha\colon E_1 \to E_2$ in standard form, we know exactly what to do if 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 the messy process that we went through with the multiplication-by-2 map. The corollary also implies that the kernel of any nonzero isogeny is a *finite* subgroup of $E(\bar{k})$.

We now define two important invariants of an isogeny that can be determined from its standard form.

Definition 5.13. Let $\alpha(x,y) = \left(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y\right)$ be an isogeny from E_1 to E_2 in standard form. The *degree* of α is $\deg\alpha = \max\{\deg u, \deg v\}$. The isogeny α is *separable* if the derivative of $\frac{u}{v}$ is not the zero function, and otherwise it is *inseparable*.
We adopt the convention that the zero isogeny is an inseparable isogeny of degree 0.

As noted earlier, the polynomials u, v, s, and 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. The degree and separability of an isogeny can also be defined using function fields. If α is a nonzero iosgeny from E_1/k to E_2/k then there is an injection of function fields

$$\alpha^*\colon \bar{k}(E_2) \to \bar{k}(E_1)$$

that sends f to $f \circ \alpha$. The degree of α is then the degree of $\bar{k}(E_1)$ as an extension of the subfield $\alpha^*(\bar{k}(E_2))$, and α is separable or not according to whether this field extension is separable or not. This definition has the virtue of generality, but it is not always so easy to apply. Our definition is equivalent, but we won't prove this.

Let us now return to the two examples that we saw earlier. The standard form of the multiplication-by-2 isogeny is

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

and we can see at once that it has degree 4. One can easily check that it is a separable (note that we are not in characteristic 2). The standard form of the Frobenius endomorphism is

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

thus it has degree p, and it is inseparable, since $(x^p)' = px^{p-1} = 0$ in characteristic p.

5.4 Seperability

The Frobenius endomorphism is the canonical example of an inseparable isogeny. Such isogenies occur only in positive characteristic; over a field of characteristic zero every isogeny is separable. More generally, we have the following lemma.

Lemma 5.14. *Let u and v be relatively prime polynomials in $\bar{k}[x]$.*

$$\left(\frac{u}{v}\right)' = 0 \quad\iff\quad u' = v' = 0 \quad\iff\quad u = f(x^p) \text{ and } v = g(x^p),$$

where f and g are polynomials in $\bar{k}[x]$ and p is the characteristic of k.

Proof. If $\left(\frac{u}{v}\right)' = \frac{u'v - v'u}{v^2} = 0$ then $u'v = v'u$. The polynomials u and v have no common roots, therefore every root of u most be a root of u' (with at least the same multiplicity), but this is impossible unless $u' = 0$; similarly, we must have $v' = 0$. Conversely, if $u' = v' = 0$ then $u'v = v'u$.

Now let $u(x) = \sum_k a_k x^k$. Then $u'(x) = \sum k a_k x^{k-1} = 0$ implies $k a_k = 0$, which means that k must be a multiple of p for every nonzero a_k. Thus $u(x) = \sum_j a_{pj} x^{pj} = f(x^p)$. Similarly, $v'(x) = 0$ implies $v(x) = g(x^p)$ for some $g \in \bar{k}[x]$. Finally, if $u(x) = f(x^p)$ then $u'(x) = p x^{p-1} f'(x^p) = 0$, and similarly for $v(x)$. □

We now show that every inseparable isogeny arises as the composition of a separable isogeny with some power of the p-power Frobenius map π that sends (x, y, z) to (x^p, y^p, z^p).[2]

Lemma 5.15. *Let $\alpha\colon E_1 \to E_2$ be an inseparable isogeny. Then α can be written in the form $\alpha = (r_1(x^p), r_2(x^p)y^p)$ for some rational functions $r_1, r_2 \in \bar{k}(x)$.*

Proof. We begin with $\alpha(x, y) = \left(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y\right)$ in standard form, and assume that E_1 is defined by $y^2 = x^3 + A_1 x + B_1$ and E_2 is defined by $y^2 = x^3 + A_2 x + B_2$. It follows from Lemma 5.14 that $\frac{u(x)}{v(x)} = r_1(x^p)$ for some $r_1 \in \bar{k}(x)$; we only need to show that $\frac{s(x)}{t(x)}y$ can be put in the form $r_2(x^p)y^p$. As in the proof of Lemma 5.11, we obtain

$$v^3 s^2 f = t^2 w,$$

where $f(x) = x^3 + A_1 x + B$ and $w = u^3 + A_2 u v^2 + B_2 v^3$. Since α is inseparable, we have $u' = v' = 0$, hence $w' = 0$, and therefore $\left(\frac{w}{v^3}\right)' = \left(\frac{s^2 f}{t^2}\right)' = 0$. Thus $s^2(x) f(x) = g(x^p)$ and $t^2 = h(x^p)$, for some polynomials g and h. Every root of $g(x^p)$ has multiplicity p and f's roots are distinct, thus we may write $s^2 f = s_1^2 f^p$, where $s_1 = g_1(x^p)$ for some polynomial g_1 (here we have used the fact that p is odd). We then have

$$(s(x)y)^2 \equiv s(x)^2 f(x) = g_1^2(x^p) f(x)^p \equiv g_1^2(x^p) y^p,$$

where the equivalences are modulo the curve equation for E_1. Thus

$$\left(\frac{s(x)}{t(x)}y\right)^2 \equiv \left(\frac{g_1(x^p)}{h(x^p)}y^p\right)^2 = (r(x^p)y^p)^2,$$

where $r(x) = g_1(x)/h(x)$. It follows that $\frac{s(x)}{t(x)}y \equiv r_2(x^p)y^p$ with $r_2 = \pm r$, since two rational functions that agree up to sign at infinitely many points can differ only in sign. □

Corollary 5.16. *Let α be an inseparable isogeny over a field of characteristic p. Then*

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

for some separable isogeny α_{sep}, where π is the p-power Frobenius map $(x, y, z) \mapsto (x^p, y^p, z^p)$.

Proof. By the lemma, we may write $\alpha = (r_1(x^p), r_2(x^p)y^p)$ for some $r_1, r_2 \in \bar{k}(x)$. We then have $\alpha = \alpha_1 \circ \pi$, where $\alpha_1 = (r_1(x), r_2(x)y)$. If α_1 is inseparable we apply the same procedure to α_1 (recursively) and eventually obtain $\alpha = \alpha_n \circ \pi^n$ where α_n is a separable isogeny (this process must terminate, since $\deg \alpha$ is finite and the each step reduces the degree by a factor of p). We may then take $\alpha_{\text{sep}} = \alpha_n$. □

[2]Note that the p-power Frobenius π is not necessarily an endomorphism; if the curve $E/\mathbb{F}_q$ is not defined over $\mathbb{F}_p$ the image of E under π will be a different elliptic curve.

With $\alpha = \alpha_{\text{sep}} \circ \pi^n$ as in the corollary above, the degree of α_{sep} is called the *separable degree* of α; the *inseparable degree* of α is p^n. Note that the isogeny α_{sep} does not necessarily have the same domain as α, since the image of π^n is not necessarily the original curve E (but π^n will map E to E whenever E is defined over $\mathbb{F}_{p^n}$).

References

[1] J. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics **106**, second edition, Springer 2009.

[2] L. Washington, *Elliptic curves: number theory and cryptography*, second edition, Chapman & Hall/CRC, 2008 **50**, 50–59.

18.783 Elliptic Curves
Spring 2013