7 Endomorphism rings

7.1 The n-torsion subgroup $E[n]$

Now that we know the degree of the multiplication-by-n map, we can determine the structure of $E[n]$ as a finite abelian group. Recall that any finite abelian group G can be written as a direct sum of cyclic groups of prime power order (unique up to ordering). Since $\#E[n]$ always divides $\deg[n] = n^2$, to determine the structure of $E[n]$ it suffices to determine the structure of $E[\ell^e]$ for each prime power ℓ^e dividing n.

Theorem 7.1. *Let E/k be an elliptic curve and let $p = \mathrm{char}(k)$. For each prime ℓ:*

$$E[\ell^e] \simeq \begin{cases} \mathbb{Z}/\ell^e\mathbb{Z} \oplus \mathbb{Z}/\ell^e\mathbb{Z} & \text{if } \ell \neq p, \\ \mathbb{Z}/\ell^e\mathbb{Z} \text{ or } \{0\} & \text{if } \ell = p. \end{cases}$$

Proof. We first suppose $\ell \neq p$. The multiplication-by-ℓ map $[\ell]$ is then separable of degree ℓ^2, so $E[\ell] = \ker[\ell]$ has order ℓ^2. Every nonzero element of $E[\ell]$ has order ℓ, so we must have $E[\ell] \simeq \mathbb{Z}/\ell\mathbb{Z} \oplus \mathbb{Z}/\ell\mathbb{Z}$. If $E[\ell^e] \simeq \langle P_1\rangle \otimes \cdots \langle P_r\rangle$ with $P_i \in E(\bar{k})$ of order $\ell^{e_i} > 1$, then

$$E[\ell] \simeq \langle \ell^{e_1-1}P\rangle \cdots \langle \ell^{e_r-1}P\rangle \simeq (\mathbb{Z}/\ell\mathbb{Z})^r,$$

thus $r = 2$ (this argument applies to any abelian group G: the ℓ-rank r of $G[\ell^e]$ is the same as the ℓ-rank of $G[\ell]$). It follows that $E[\ell^e] \simeq \mathbb{Z}/\ell^e\mathbb{Z} \oplus \mathbb{Z}/\ell^e\mathbb{Z}$, since $E[\ell^e]$ has order ℓ^{2e} and contains no elements of order greater than ℓ^e.

We now suppose $\ell = p$. Then $[\ell]$ is inseparable and its kernel $E[\ell]$ has order strictly less than $\deg[\ell] = \ell^2$. Since $E[\ell]$ is a ℓ-group of order less than ℓ^2, it must be isomorphic to either $\mathbb{Z}/\ell\mathbb{Z}$ or $\{0\}$. In the latter case we clearly have $E[\ell^e] = \{0\}$ and the theorem holds, so we now assume $E[\ell] \simeq \mathbb{Z}/\ell\mathbb{Z}$. If $E[\ell] = \langle P\rangle$ with $P \in E(\bar{k})$ a point of order ℓ, then since the isogeny $[\ell] : E \to E$ is surjective, there is a point $Q \in E(\bar{k})$ for which $\ell Q = P$, and the point Q then has order ℓ^2. Iterating this argument shows that $E[\ell^e]$ contains a point of order ℓ^e, and by the argument above it has ℓ-rank 1, so we must have $E[\ell^e] \simeq \mathbb{Z}/\ell^e\mathbb{Z}$. □

The two possibilities for $E[p]$ admitted by the theorem lead to the following definitions. We do not need this terminology today, but it will be important in the weeks that follow.

Definition 7.2. Let E be an elliptic curve defined over a field of characteristic $p > 0$. If $E[p] \simeq \mathbb{Z}/p\mathbb{Z}$ then E is said to be *ordinary*, and if $E[p] \simeq \{0\}$, we say that E is *supersingular*.

Remark 7.3. The term "supersingular" is unrelated to the term "singular" (recall that an elliptic curve is nonsingular by definition). Supersingular refers to the fact that such elliptic curves are exceptional.

Corollary 7.4. *Let E/k be an elliptic curve. Every finite subgroup of $E(\bar{k})$ is the direct sum of at most two cyclic groups, at most one of which has order divisible by the characteristic p of k. In particular, when $k = \mathbb{F}_q$ is a finite field we have*

$$E(\mathbb{F}_q) \simeq \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$$

for some positive integers m, n with $m|n$ and $p \nmid m$.

Proof. Let p be the characteristic of k, and let T be a finite subgroup of $E(\bar{k})$ of order n. If $p \nmid n$, then $T \subseteq E[n] \simeq \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ can clearly be written as a sum of two cyclic groups. Otherwise we may write $T \simeq G \oplus H$ where H is the p-Sylow subgroup of T, and we have $G \subseteq E[m] \simeq \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$, where $m = |G|$ is prime to p and H has p-rank at most 1. It follows that T can always be written as a sum of at most two cyclic groups, at most one of which has order divisible by p. □

Now that we know what the structure of $E(\mathbb{F}_q)$ looks like, our next goal is to bound its cardinality. We will prove Hasse's Theorem, which states that

$$\#E(\mathbb{F}_q) = q + 1 - t,$$

where $|t| \leq 2\sqrt{q}$. To do this we need to introduce the endomorphism ring of E.

7.2 Endomorphism rings

For any pair of elliptic curves E_1/k and E_2/k, the set $\hom(E_1, E_2)$ of homomorphisms from E_1 to E_2 (defined over k) consists of all morphisms of curves $E_1 \to E_2$ that are also group homomorphisms $E_1(\bar{k}) \to E_2(\bar{k})$; since a morphism of curves is either surjective or constant, this is just the set of all isogenies from E_1 to E_2 plus the zero morphism. For any algebraic extension L/k, we write $\hom_L(E_1, E_2)$ for the homomorphisms from E_1 to E_2 that are defined over L.[1]

The set $\hom(E_1, E_2)$ forms an abelian group under addition, where the sum $\alpha + \beta$ is defined by

$$(\alpha + \beta)(P) := \alpha(P) + \beta(P),$$

and the zero morphism is the identity. For any $\alpha \in \hom(E_1, E_2)$ we have

$$\alpha + \cdots + \alpha = n\alpha = [n] \circ \alpha,$$

where $[n]$ is the multiplication-by-n map on E_1. Provided α and n are nonzero, both $[n]$ and α are surjective, as is $n\alpha$, thus $n\alpha \neq 0$. It follows that $\hom(E_1, E_2)$ is torsion free (but $\hom(E_1, E_2) = \{0\}$ is possible).

Definition 7.5. Let E/k be an elliptic curve. The endomorphism ring of E is the additive group $\mathrm{End}(E) := \hom(E, E)$ with multiplication defined by composition (so $\alpha\beta = \alpha \circ \beta$).

Warning 7.6. Some authors use $\mathrm{End}(E)$ to mean $\mathrm{End}_{\bar{k}}(E)$ rather than $\mathrm{End}_k(E)$.

To verify that $\mathrm{End}(E)$ is in fact a ring, note that it has a multiplicative identity $1 = [1]$ (the identity morphism), and for all $\alpha, \beta, \gamma \in \mathrm{End}(E)$ and $P \in E(\bar{k})$ we have

$$\begin{aligned}((\alpha + \beta)\gamma)(P) &= (\alpha + \beta)(\gamma(P)) = \alpha(\gamma(P)) + \beta(\gamma(P)) = (\alpha\gamma + \beta\gamma)(P)\\ (\gamma(\alpha + \beta))(P) &= \gamma(\alpha(P) + \beta(P)) = \gamma(\alpha(P)) + \gamma(\beta(P)) = (\gamma\alpha + \gamma\beta)(P),\end{aligned}$$

where we used the fact that γ is a group homomorphism to get the second identity.

For every integer n the multiplication-by-n map $[n]$ lies in $\mathrm{End}(E)$, and the map $n \mapsto [n]$ defines an ring homomorphism $\mathbb{Z} \to \mathrm{End}(E)$, since $[0] = 0, [1] = 1$, $[m] + [n] = [m + n]$ and $[m][n] = [mn]$. As noted above, $\hom(E, E)$ is torsion free, so the homomorphism

[1] Technically speaking, these homomorphisms are defined on the base changes E_{1_L} and E_{2_L} of E_1 and E_2 to L, so $\hom_L(E_1, E_2)$ is really shorthand for $\hom(E_{1_L}, E_{2_L})$.

$n \mapsto [n]$ is injective and may regard $\mathbb{Z}$ as a subring of $\mathrm{End}(E)$; we will thus feel free to write n rather than $[n]$ when it is convenient to do so. Note that this immediately implies that the multiplication-by-n maps commute with every element of $\mathrm{End}(E)$. Indeed, for any $\alpha \in \mathrm{End}(E)$ and $P \in E(\bar{k})$ we have

$$(\alpha \circ [n])(P) = \alpha(nP) = \alpha(P + \cdots + P) = \alpha(P) + \cdots + \alpha(P) = n\alpha(P) = ([n] \circ \alpha)(P).$$

When $k = \mathbb{F}_q$ is a finite field, the q-power Frobenius endomorphism π_E also commutes with every element of $\mathrm{End}(E)$. This follows from the basic fact that for any rational function $r \in \mathbb{F}_q(x_1, \ldots, x_n)$ we have $r(x_1, \ldots, x_n)^q = r(x_1^q, \ldots, x_n^q)$, and we can apply this to the rational maps defining any $\alpha \in \mathrm{End}(E)$. Thus the subring $\mathbb{Z}[\pi_E]$ generated by π_E lies in the center of $\mathrm{End}(E)$.

Remark 7.7. It can happen that $\mathbb{Z}[\pi_E] = \mathbb{Z}$. For example, when $E[p] = \{0\}$ and $q = p^2$ the multiplication-by-p map $[p]$ is purely inseparable and we must have $[p] = \pi^2 = \pi_E$.

For any nonzero $\alpha, \beta \in \mathrm{End}(E)$, the product $\alpha\beta = \alpha \circ \beta$ is surjective, since α and β are both surjective; in particular, $\alpha\beta$ is not the zero morphism. It follows that $\mathrm{End}(E)$ is has no zero divisors, so the cancellation law holds (on both the left and the right, a fact we will freely use in what follows).

7.3 The dual isogeny

In order to develop a deeper understanding of the structure of the endomorphism ring $\mathrm{End}(E)$ we want to introduce the *dual isogeny*. But first let us record the following lemma.

Lemma 7.8. *Let $\alpha = \alpha_1 \circ \alpha_2$ be an isogeny. Then $\deg \alpha = (\deg \alpha_1)(\deg \alpha_2)$.*

Proof. It is clear that

$$\#(\ker \alpha) = \#(\ker \alpha_1)\#(\ker \alpha_2),$$

since these are surjective group homomorphisms. It follows that $\deg_s \alpha = (\deg_s \alpha_1)(\deg_s \alpha_2)$. It is also clear that composing any isogeny with a purely inseparable isogeny of degree q multiplies the degree by q: both $u(x^q)/v(x^q)$ and $(u(x)/v(x))^q$ have degree $q \deg(u/v)$ as rational functions (max degree of numerator and denominator). The lemma follows. □

Corollary 7.9. *For any isogeny $\alpha = \alpha_1 \circ \alpha_2$ we have $\deg_s \alpha = (\deg_s \alpha_1)(\deg_s \alpha_2)$ and $\deg_i \alpha = (\deg_i \alpha_1)(\deg_i \alpha_2)$.*

Proof. This follows from the fact that $\deg \beta = (\deg_s \beta)(\deg_i \beta)$ for any isogeny β. □

Theorem 7.10. *For any isogeny $\alpha\colon E_1 \to E_2$ there exists a unique isogeny $\hat{\alpha}\colon E_2 \to E_1$ for which $\hat{\alpha} \circ \alpha = [n]$, where $n = \deg \alpha$.*

Proof. We proceed by induction on the number of prime factors of n. If $n = 1$ then α is an isomorphism and $\hat{\alpha}$ is just the inverse isomorphism. If α has prime degree ℓ different from that characteristic of the field we are working in, then α is separable and $\alpha(E_1[\ell])$ is a subgroup of $E_2(\bar{k})$ of cardinality $\ell^2/\ell = \ell$. If we let $\alpha'\colon E_2 \to E_3$ be the separable isogeny with $\alpha(E[\ell])$ as its kernel (applying Theorem 6.8), then the kernel of $\alpha' \circ \alpha$ is $E[\ell]$ and since $[n]\colon E_1 \to E_1$ is a separable isogeny with the same kernel, there is an isomorphism $\iota\colon E_3 \to E_1$ for which $\iota \circ \alpha' \circ \alpha = [n]$ and we may take $\hat{\alpha} = \iota \circ \alpha$.

If α has prime degree p equal to the characteristic of k, there are two cases.

Case 1: If α is separable then we must have $\ker\alpha = E[p] \simeq \mathbb{Z}/p\mathbb{Z}$, and since $\deg[p] = p^2$ and $\deg_s[p] = p$, we have $[p] = \pi\circ\alpha'$ for some separable isogeny α' of degree p, where π denotes the p-power Frobenius morphism (see Remark 6.5). Since α and α' are separable isogenies with the same kernel $E[p]$, we can write $\alpha' = \iota\circ\alpha$ for some isomorphism ι; we then have $\hat\alpha = \pi\circ\iota$.
Case 2: If α is inseparable then we must have $\alpha = \pi$. If $E[p] = \{0\}$ then $[p]$ is purely inseparable of degree p^2, so $[p] = \pi^2$ and $\hat\alpha = \pi$. If $E[p] \simeq \mathbb{Z}/p\mathbb{Z}$ then $[p] = \alpha'\circ\pi$ for some separable isogeny α' of degree p and $\hat\alpha = \alpha'$.

If n is composite then we may decompose α into a sequence of isogenies of prime degree (see Corollary 6.9). In particular we can write $\alpha = \alpha_1\circ\alpha_2$, where α_1, α_2 have degrees $n_1, n_2 < n$ with $n_1 n_2 = n$. We now claim that

$$\hat\alpha_2\circ\hat\alpha_1\circ\alpha = [n],$$

and therefore $\hat\alpha = \hat\alpha_2\circ\hat\alpha_1$. Indeed, we have

$$(\hat\alpha_2\circ\hat\alpha_1)\circ\alpha = \hat\alpha_2\circ\hat\alpha_1\circ\alpha_1\circ\alpha_2 = \hat\alpha_2\circ[n_1]\circ\alpha_2 = \hat\alpha_2\circ\alpha_2\circ[n_1] = [n_2]\circ[n_1] = [n],$$

where $\alpha_2\circ[n_1] = \alpha_2\circ[n_1]$ because for any $P\in E(\bar k)$ we have

$$(\alpha_2\circ[n_1])(P) = \alpha_2(n_1P) = \alpha_2(P+\cdots+P) = \alpha_2(P)+\cdots+\alpha_2(P) = n_1\alpha_2(P) = ([n_1]\circ\alpha_2)(P),$$

since α is a group homomorphism (note that above we have used $[n_1]$ and $[n_2]$ to generically denote multiplication maps on possibly different elliptic curves in the argument above). □

Definition 7.11. The isogeny $\hat\alpha$ given by the theorem is the *dual isogeny* of α.

Remark 7.12. There is a general notion of a dual isogeny for abelian varieties of any dimension. If we have an isogeny of abelian varieties $\alpha\colon A_1\to A_2$ then the dual isogeny

$$\hat\alpha\colon \hat A_2\to\hat A_1,$$

is actually an isogeny between the *dual abelian varieties* $\hat A_2$ and $\hat A_1$. We won't give a definition of the dual abelian variety here, but the key point is that in general, abelian varieties are not isomorphic to their duals. But abelian varieties of dimension one (elliptic curves) are self-dual. This is yet another remarkable feature of elliptic curves.

As a matter of convenience we extend the notion of a dual isogeny to $\hom(E_1,E_2)$ and $\mathrm{End}(E)$ by defining $\hat 0 = 0$, and define $\deg 0 = 0$, which we note is consistent with $\hat 0\circ 0 = [0]$ and the fact that degrees are multiplicative.

Lemma 7.13. *For an isogeny α of degree n we have $\deg\hat\alpha = \deg\alpha = n$ and*

$$\alpha\circ\hat\alpha = \hat\alpha\circ\alpha = [n].$$

Thus $\hat{\hat\alpha} = \alpha$. For any integer n the endomorphism $[n]$ is self-dual.

Proof. The first statement follows from $(\deg\hat\alpha)(\deg\alpha) = \deg[n]$. We now note that

$$(\alpha\circ\hat\alpha)\circ\alpha = \alpha\circ(\hat\alpha\circ\alpha) = \alpha\circ[n] = [n]\circ\alpha,$$

and therefore $\alpha\circ\hat\alpha = [n]$; since the isogenies involved are all surjective, it follows that we can cancel α on the LHS and RHS to obtain $\alpha\circ\hat\alpha = [n]$. The last statement follows from the fact that $[n]\circ[n] = [n^2] = [\deg n]$. □

The one other fact we need about dual isogenies is the following.

Lemma 7.14. *For any $\alpha, \beta \in \hom(E_1, E_2)$ we have $\widehat{\alpha+\beta} = \hat{\alpha} + \hat{\beta}$.*

Proof. We will defer the proof of this lemma — the nicest proof uses the Weil pairing, which we will see later in the course. □

We now return to the setting of the endomorphism ring $\mathrm{End}(E)$ of an elliptic curve E/k.

Lemma 7.15. *For any endomorphism α we have $\alpha + \hat{\alpha} = 1 + \deg\alpha - \deg(1-\alpha)$.*

Note that in the statement of this lemma, the integers $\deg\alpha$, and $\deg(1-\alpha)$ on the RHS are to be interpreted as elements of $\mathrm{End}(E)$ via the embedding $n \mapsto [n]$.

Proof. For any $\alpha \in \mathrm{End}(E)$ (including $\alpha = 0$) we have

$$\deg(1-\alpha) = \widehat{1-\alpha}(1-\alpha) = (\hat{1} - \hat{\alpha})(1-\alpha) = (1-\hat{\alpha})(1-\alpha) = 1 - (\alpha + \hat{\alpha}) + \deg(\alpha),$$

and therefore $\alpha + \hat{\alpha} = 1 + \deg\alpha - \deg(1-\alpha)$. □

A key consequence of the lemma is that $\alpha + \hat{\alpha}$ is always a multiplication-by-t map for some $t \in \mathbb{Z}$.

Definition 7.16. The *trace* of an endomorphism α is the integer $\mathrm{tr}\,\alpha := \alpha + \hat{\alpha}$.

Note that for any $\alpha \in \mathrm{End}(E)$ we have $\mathrm{tr}\,\hat{\alpha} = \mathrm{tr}\,\alpha$, and $\deg\hat{\alpha} = \deg\alpha$.

7.4 Endomorphism restrictions to $E[n]$

Let E be an elliptic curve over a field of charcteristic p (possibly $p = 0$). For any $\alpha \in \mathrm{End}(E)$, we may consider the restriction α_n of α to the n-torsion subgroup $E[n]$. Since α is a group homomorphism, it maps n-torsion points to n-torsion points, so α_n is an endomorphism of the abelian group $E[n]$, which we may view as a $(\mathbb{Z}/n\mathbb{Z})$-module.

When n is not divisible by p we have $E[n] \simeq \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$, and we can pick a basis (P_1, P_2) for $E[n]$ as a $(\mathbb{Z}/n\mathbb{Z})$-module. This just means that every element of $E[n]$ can be written uniquely as a $(\mathbb{Z}/n\mathbb{Z})$-linear combination of P_1 and P_2 — if suffices to pick any $P_1, P_2 \in E[n]$ that generate $E[n]$ as an abelian group. We may represent α_n as a 2×2 matrix $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$, where $a, b, c, d \in \mathbb{Z}/n\mathbb{Z}$ are uniquely determined by

$$\alpha(P_1) = aP_1 + bP_2,$$
$$\alpha(P_2) = cP_1 + dP_2.$$

Note that this matrix representation depends on our choice of basis, but matrix invariants such as the trace $\mathrm{tr}\,\alpha_n$ and the determinant $\det\alpha_n$ are independent of this choice.

A standard technique for proving that two endomorphisms α and β are equal is to prove that $\alpha_n = \beta_n$ for some sufficiently large n. If n^2 is larger than the degree of $\alpha - \beta$, then $\alpha_n = \beta_n$ implies that the kernel of $\alpha - \beta$ is infinite and therefore $\alpha - \beta = 0$ (since 0 is the only endomorphism with infinite kernel) and $\alpha = \beta$. To handle situations where we don't know the degree of $\alpha - \beta$, or don't even know exactly what β is (maybe we just know β_n), we need a more refined result.

Lemma 7.17. *Let α and β be endomorphisms of an elliptic curve E/k and let m be the maximum of $\deg\alpha$ and $\deg\beta$. Let $n \geq 2\sqrt{m}+1$ be an integer that is prime to the characteristic of k, and also prime to $\deg\alpha$ and $\deg\beta$. If $\alpha_n = \beta_n$ then $\alpha = \beta$.*

Proof. We shall make use of the following fact that we won't prove here. Let $r(x) = u(x)/v(x)$ be a rational function in $k(x)$ with $u \perp v$ and v monic. Suppose that we know the value of $r(x_i)$ for N distinct values $x_1, \ldots, x_N$ for which $v(x_i) \neq 0$. Provided that $N > 2\max\{\deg u, \deg v\} + 1$, the coefficients of u and v can be uniquely determined using *Cauchy interpolation*; see [1, §5.8] for an efficient algorithm and a proof of its correctness.

Now let $\alpha(x,y) = \left(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y\right)$ be in standard form, with $u \perp v$, and let us normalize u and v so that v is monic. If we know the value of $\alpha(P)$ at $2\deg\alpha+2$ affine points $P \notin \ker\alpha$ with distinct x-coordinates, then we can uniquely determine the coefficients of u and v. Since at most 2 points $P \in E(\bar{k})$ can share the same x-coordinate, it suffices to know $\alpha(P)$ at $4\deg\alpha + 4$ affine points not in $\ker\alpha$.

For $n \geq 2\sqrt{m}+1$ we have $n^2 \geq 4m + 4\sqrt{m} + 1$, and $E[n]$ contains $n^2 - 1 \geq 4\deg\alpha + 4$ affine points, none of which lie in $\ker\alpha$, since $\#\ker\alpha$ divides $\deg\alpha$ which is prime to n. Thus knowing α_n uniquely determines the x-coordinate of $\alpha(P)$ for all $P \in E(\bar{k})$. The same argument applies to β_n and β, hence $\alpha(P) = \pm\beta(P)$ for all $P \in E(\bar{k})$. The kernel of at least one of $\alpha+\beta$ and $\alpha-\beta$ is then infinite, hence $\alpha = \pm\beta$.

We have $n^2 > 4\deg\alpha \geq 4$, which implies that $\alpha(P)$ cannot lie in $E[2]$ for all $P \in E[n]$ (since $\#E[2] = 4$). Therefore $\alpha(P) \neq -\alpha(P)$ for some $P \in E[n]$, and for this P we have $\alpha(P) \neq -\alpha(P) = -\alpha_n(P) = -\beta_n(P) = -\beta(P)$, so $\alpha \neq -\beta$ and we must have $\alpha = \beta$. □

Theorem 7.18. *Let α be an endomorphism of an elliptic curve. Both α and its dual $\hat{\alpha}$ are roots of the characteristic polynomial*

$$\lambda^2 - (\operatorname{tr}\alpha)\lambda + \deg\alpha = 0.$$

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

The following theorem provides the key connection between endomorphisms and their restrictions to $E[n]$.

Theorem 7.19. *Let α be an endomorphism of an elliptic curve E/k and let n be a positive integer prime to the characteristic of k. Then*

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

Proof. We will just prove the theorem for odd n prime to $\deg\alpha$ such that $n \geq 2\sqrt{\deg\alpha}+1$, which is more than enough to prove Hasse's theorem. The general proof relies on properties of the Weil pairing that we will see later in the course.

We note that the theorem holds for $\alpha = 0$, so we assume $\alpha \neq 0$. Let n be as above and let $t_n = \operatorname{tr}\alpha \bmod n$ and $d_n = \deg\alpha \bmod n$. Since α and $\hat{\alpha}$ both satisfy $\lambda^2 - (\operatorname{tr}\alpha)\lambda + \deg\alpha = 0$, both α_n and $\hat{\alpha}_n$ must satisfy $\lambda^2 - t_n\lambda + d_n = 0$. It follows that $\alpha_n + \hat{\alpha}_n$ and $\alpha_n\hat{\alpha}_n$ are the scalar matrices t_nI and d_nI, respectively. Let $\alpha_n = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$, and let $\delta_n = \det\alpha_n$. The fact that $\hat{\alpha}_n\alpha_n = d_nI \neq 0$ with d_n prime to n implies that α_n is invertible, and we have

$$\hat{\alpha}_n = d_n\alpha_n^{-1} = \frac{d_n}{\det\alpha_n}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

If we put $\epsilon := d_n/\det \alpha_n$ and substitute the above expression for $\hat{\alpha}$ into $\alpha_n + \hat{\alpha}_n = t_n I$, we get

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \epsilon \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \begin{bmatrix} t_n & 0 \\ 0 & t_n \end{bmatrix}.$$

Thus $a + \epsilon d = t_n$, $b - \epsilon b = 0$, $c - \epsilon c = 0$, and $d + \epsilon a = t_n$. Unless $a = d$ and $b = c = 0$, we must have $\epsilon = 1$, in which case $d_n = \det \alpha_n$ and $t_n = a + d = \operatorname{tr} \alpha_n$ as desired.

Otherwise α_n is a scalar matrix. Let m be the unique integer with absolute value less than $n/2$ such that $\alpha_n = m_n$, where m_n is the restriction of the multiplication-by-m map to $E[n]$. We then have $\deg m = m^2$ and $n \geq 2\sqrt{\deg m} + 1$. Since we also have $n \geq 2\sqrt{\deg \alpha} + 1$ we must have $\alpha = m$, by Lemma 7.17. But then $\hat{\alpha} = \hat{m} = m = \alpha$ and we have $\operatorname{tr} \alpha = 2m \equiv \operatorname{tr} mI \equiv \operatorname{tr} \alpha_n \bmod n$ and $\deg \alpha = m^2 \equiv \det mI \equiv \det \alpha_n \bmod n$. □

7.5 Separable and inseparable endomorphisms

Recall that the Frobenius endomorphism π_E is inseparable. In order to prove Hasse's theorem we will need to know that $\pi_E - 1$ is actually separable. This follows from a much more general result: adding a separable isogeny to an inseparable isogeny always yields a separable isogeny.

Lemma 7.20. *Let α and β be isogenies from E_1 to E_2, with α inseparable. Then $\alpha + \beta$ is inseparable if and only if β is inseparable.*

Proof. If β is inseparable then we can write $\alpha = \alpha_{\text{sep}} \circ \pi^m$ and $\beta = \beta_{\text{sep}} \circ \pi^n$, where π is the p-power Frobenius map and $m, n > 0$. We then have

$$\alpha + \beta = \alpha_{\text{sep}} \circ \pi^m + \beta_{\text{sep}} \circ \pi^n = (\alpha_{\text{sep}} \circ \pi^{m-1} + \beta_{\text{sep}} \circ \pi^{n-1}) \circ \pi,$$

which is inseparable (any composition involving an inseparable isogeny is inseparable).

If $\alpha + \beta$ is inseparable, then so is $-(\alpha + \beta)$, and $\alpha - (\alpha + \beta) = \beta$ is a sum of inseparable isogenies, which we have just shown is inseparable. □

Remark 7.21. Since the composition of an inseperable isogeny with any isogeny is always inseparable, the lemma implies that the set of inseparable endomorphisms in the ring $\operatorname{End}(E)$ form an ideal (provided we view 0 as inseparable, which we do).

References

[1] Joachim von zur Gathen and Jürgen Garhard, *Modern Computer Algebra*, third edition, Cambridge University Press, 2013.

18.783 Elliptic Curves

Spring 2015