6 Torsion subgroups and endomorphism rings

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

Having determined the degree and separability of the multiplication-by-n map $[n]$ in the previous lecture, we now want to determine the structure of its kernel, the n-torsion subgroup $E[n]$, 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 6.1. *Let E/k be an elliptic curve and let $p := \operatorname{char}(k)$. 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, and we may apply Theorem 5.8 to compute $\#E[\ell] = \#\ker[\ell] = \deg[\ell] = \ell^2$. 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 $E[\ell^e] \simeq \langle P_1 \rangle \oplus \cdots \oplus \langle P_r \rangle$ with each $P_i \in E(\bar{k})$ of order $\ell^{e_i} > 1$, then

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

and we must have $r = 2$; more generally, for 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 we have $\#E[\ell^e] = \#\ker[\ell^e] = \deg[\ell^e] = \ell^{2e}$ and $E[\ell^e]$ contains no elements of order greater than ℓ^e.

We now suppose $\ell = p$. We have $\deg[\ell] = \deg_s[\ell]\deg_i[\ell] = \ell^2$ with $\deg_i[\ell] > 1$, so $\deg_s[\ell]$ is either ℓ or 1, which means that $E[\ell]$ must be isomorphic to $\mathbb{Z}/\ell\mathbb{Z}$ or $\{0\}$. In the latter case we clearly have $E[\ell^e] = \{0\}$ and the theorem holds, so we assume $E[\ell] \simeq \mathbb{Z}/\ell\mathbb{Z}$. The group $E[\ell^e]$ must be cyclic (as argued above it has the same ℓ-rank as $E[\ell]$), so let $E[\ell^e] = \langle P_1 \rangle$ with P_1 of order ℓ^{e_1}. The isogeny $[\ell]: E \to E$ is surjective, so $\ell Q = P$ for some $Q \in E(\bar{k})$, and $P \neq 0$ implies Q has order ℓ^{e_1+1} and is not an element of $\langle P \rangle = E[\ell^e]$. This is possible only if $e_1 = e$, in which case $E[\ell^e] \simeq \mathbb{Z}/\ell^e\mathbb{Z}$ as desired. ∎

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 6.2. 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 6.3. 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 6.4. *Let E/k be an elliptic curve. Every finite subgroup of $E(\bar{k})$ can be written as the direct sum of two (possibly trivial) cyclic groups, at most one of which has order divisible by the characteristic of k. If $k = \mathbb{F}_q$ is a finite field of characteristic p 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 $p \nmid m$.

Lecture by Andrew Sutherland

Proof. Let T be a finite subgroup of $E(\bar{k})$. As a finite abelian group, T is the direct sum of its ℓ-sylow subgroups T_ℓ, each of which is a subgroup of $E[\ell^e]$ for some e, hence a product of at most two cyclic groups by Theorem 6.1, and we can write $T_\ell \simeq T_{\ell,1} \oplus T_{\ell,2}$ with $T_{\ell,1}$ and $T_{\ell,2}$ groups of ℓ-power order, with $T_{\ell,2}$ is trivial if $\ell = p$. The groups $T_1 \coloneqq \bigoplus_\ell T_{\ell,1}$ and $T_2 \coloneqq \bigoplus_\ell T_{\ell,2}$ are cyclic, with $p \nmid \#T_2$, and $T \simeq T_1 \oplus T_2$. □

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

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

where $|t| \leq 2\sqrt{q}$, but we first need to study the endomorphism ring of E.

6.2 Groups of homomorphisms

For any pair of elliptic curves E_1/k and E_2/k, the set $\operatorname{Hom}(E_1, E_2)$ 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 $\operatorname{Hom}_L(E_1, E_2)$ for the homomorphisms from E_1 to E_2 that are defined over L.[1]

The set $\operatorname{Hom}(E_1, E_2)$ forms an abelian group: for $\alpha, \beta \in \operatorname{Hom}(E_1, E_2)$ the sum $\alpha + \beta$ is defined pointwise via

$$(\alpha + \beta)(P) \coloneqq \alpha(P) + \beta(P),$$

and the zero morphism from E_1 to E_2 is the identity element of $\operatorname{Hom}(E_1, E_2)$. Because addition is defined pointwise, if $\alpha(P) = \beta(P)$ for all $P \in E_1(\bar{k})$ then $\alpha = \beta$ because $\alpha - \beta$ is the zero morphism; we can thus test equality in $\operatorname{Hom}(E_1, E_2)$ pointwise.

Proposition 6.5. *Let E_1, E_2 be elliptic curves over a field k. For all $n \in \mathbb{Z}$ and all $\alpha \in \operatorname{Hom}(E_1, E_2)$ we have*

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

where the map $[n]$ on the LHS is multiplication-by-n on E_2 and the map $[n]$ on the RHS is multiplication-by-n on E_1.

Proof. For any $P \in E(\bar{k})$ and $\alpha \in \operatorname{Hom}(E_1, E_2)$ we have

$$([-1] \circ \alpha)(P) = -\alpha(P) = \alpha(-P) = (\alpha \circ [-1])(P),$$

since α is a group homomorphism, thus the proposition holds for $n = -1$ (as noted above, we can check equality of morphisms pointwise). All sides of the equalities are multiplicative in n, so it suffices to consider the case $n \geq 0$, where we have

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

since α is a group homomorphism. The proposition follows. □

[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 $\operatorname{Hom}_L(E_1, E_2)$ is really shorthand for $\operatorname{Hom}(E_{1_L}, E_{2_L})$.

Provided α and n are nonzero, both $[n]$ and α are surjective, as is $n\alpha$, thus $n\alpha \neq 0$; recall that by Theorem 4.17, every morphism of projective curves is either surjective or constant, and for elliptic curves (whose morphisms must preserve the distinguished point) the only constant morphism is the zero map. It follows that $\operatorname{Hom}(E_1, E_2)$ is a torsion free abelian group (but $\operatorname{Hom}(E_1, E_2) = \{0\}$ is possible).

Composition of homomorphisms distributes with addition: for any $\delta \in \operatorname{Hom}(E_0, E_1)$, $\alpha, \beta \in \operatorname{Hom}(E_1, E_2)$ and $\gamma \in \operatorname{Hom}(E_2, E_3)$ we have

$$(\alpha + \beta) \circ \gamma = \alpha \circ \gamma + \beta \circ \gamma \qquad \text{and} \qquad \delta \circ (\alpha + \beta) = \delta \circ \alpha + \delta \circ \beta,$$

since these identities hold pointwise (because $\alpha, \beta, \gamma, \delta$ are group homomorphisms).

Lemma 6.6. *Let $\delta\colon E_0 \to E_1$, $\alpha, \beta\colon E_1 \to E_2$, and $\gamma\colon E_2 \to E_3$ be isogenies. Then*

$$\begin{aligned} \delta \circ \alpha = \delta \circ \beta \quad &\Longrightarrow \quad \alpha = \beta \\ \alpha \circ \gamma = \beta \circ \gamma \quad &\Longrightarrow \quad \alpha = \beta. \end{aligned}$$

Proof. Isogenies are surjective, so in particular, γ, δ are not zero morphisms. We have

$$\delta \circ \alpha = \delta \circ \beta \Rightarrow \delta \circ \alpha - \delta \circ \beta = 0 \Rightarrow \delta \circ (\alpha - \beta) = 0 \Rightarrow \alpha - \beta = 0 \Rightarrow \alpha = \beta$$
$$\alpha \circ \gamma = \beta \circ \gamma \Rightarrow \alpha \circ \gamma - \beta\gamma = 0 \Rightarrow (\alpha - \beta) \circ \gamma = 0 \Rightarrow \alpha - \beta = 0 \Rightarrow \alpha = \beta.$$

where the third arrow in both lines follows form the fact that a composition of morphisms is zero if and only if one of the morphisms in the composition is zero (because nonzero morphisms are surjective, as is their composition). □

6.3 The dual isogeny

To further develop our understanding of endomorphism rings (and isogenies in general) we now introduce the *dual isogeny*, whose existence is given by the following theorem. In the proof of the theorem we will appeal repeatedly to Theorem 5.11, which guarantees the existence of a separable isogeny with any given finite kernel, which is unique up to isomorphism. This implies that if $\alpha\colon E_1 \to E_2$ and $\alpha'\colon E_1 \to E_3$ are separable isogenies with the same kernel then there is an isomorphism $\iota\colon E_2 \to E_3$ such that $\alpha' = \iota \circ \alpha$. We will also make use of the fact that the kernel of an isogeny $\alpha\colon E_1 \to E_2$ of degree n is necessarily a subgroup of $E_1[n]$: by Theorem 5.8, $\#\ker\alpha = \deg_s \alpha$ is a divisor of $n = \deg\alpha$, so every $P \in \ker\alpha$ has order dividing n and is therefore an n-torsion point (satisfies $nP = 0$).

Theorem 6.7. *For any isogeny $\alpha\colon E_1 \to E_2$ of elliptic curves over a field k there exists a unique isogeny $\hat{\alpha}\colon E_2 \to E_1$ for which $\hat{\alpha} \circ \alpha = [n]$, where $n = \deg\alpha$.*

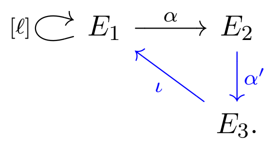
Proof. Uniqueness is immediate: if $\alpha_1 \circ \alpha = \alpha_2 \circ \alpha$ then $\alpha_1 = \alpha_2$ (by the cancellation law for composition of isogenies), so the equation $\hat{\alpha} \circ \alpha = [n]$ uniquely determines $\hat{\alpha}$.

To prove existence we proceed by induction on the number of prime factors of n, counted with multiplicity (recall from Corollary 5.12 that any isogeny can be written as a composition of isogenies of prime degree). Let p be the characteristic of the field k over which the elliptic curves E_1 and E_2 are defined.

If $n = 1$ has no prime factors then α is separable (other wise we would have $p \mid \deg\alpha$) and has trivial kernel, and the same is true of the identity map $[1]$. It follows from Theorem 5.11 that there is an isomorphism $\iota\colon E_2 \to E_1$ such that $\iota \circ \alpha = [1]$, and we can take $\hat{\alpha} = \iota$.

We now suppose $n = \ell$ is prime. There are three cases to consider:

Case 1 ($\ell \neq p$): In this case α and $[\ell]$ are both separable and $\alpha(E_1[\ell])$ is a subgroup of $E_2(\bar{k})$ of cardinality $\deg[\ell]/\deg\alpha = \ell^2/\ell = \ell$. Let $\alpha'\colon E_2 \to E_3$ be the separable isogeny with $\alpha(E[\ell])$ as its kernel. The isogenies $\alpha' \circ \alpha$ and $[\ell]$ both have kernel $E[\ell]$, so there is an isomorphism $\iota\colon E_3 \to E_1$ for which $\iota \circ \alpha' \circ \alpha = [\ell]$, by Theorem 5.11, as shown below.

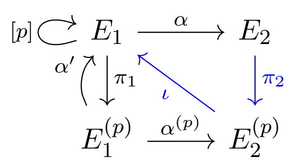


We now put $\hat{\alpha} := \iota \circ \alpha'$ to obtain $\hat{\alpha} \circ \alpha = [\ell]$ as desired.

Case 2 ($\ell = p$ and α separable): If α is separable then its kernel has order $\deg\alpha = p$ and we must have $\ker\alpha = E_1[p] \simeq \mathbb{Z}/p\mathbb{Z}$, by Theorem 6.1, and $\deg_s[p] = p$. Now $\deg[p] = p^2$, so by Corollary 5.4 we have $[p] = \alpha' \circ \pi_1$ for some separable isogeny $\alpha'\colon E_1^{(p)} \to E_1$ of degree p, where $\pi_1\colon E_1 \to E_1^{(p)}$ is the p-power Frobenius morphism.[2] We have $\pi_2 \circ \alpha = \alpha^{(p)} \circ \pi_1$, where $\alpha^{(p)}\colon E_1^{(p)} \to E_2^{(p)}$ is obtained by replacing each coefficient of α by its pth power, and

$$\ker(\alpha^{(p)} \circ \pi_1) = \ker(\pi_2 \circ \alpha) = \ker\alpha = \ker[p] = \ker(\alpha' \circ \pi_1),$$

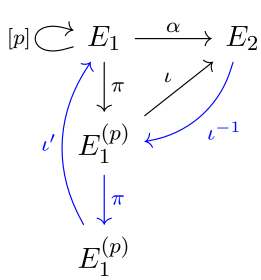
since the Frobenius morphisms π_1 and π_2 have trivial kernel, and it follows that $\alpha^{(p)}$ and α' are separable isogenies with the same kernel. There is thus an isomorphism $\iota\colon E_2^{(p)} \to E_1$ such that $\alpha' = \iota \circ \alpha^{(p)}$ (again by Theorem 5.11), as shown in the diagram below:

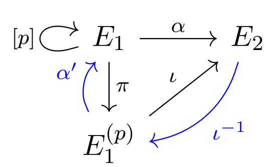


If we now put $\hat{\alpha} = \iota \circ \pi_2$ then

$$\hat{\alpha} \circ \alpha = \iota \circ \pi_2 \circ \alpha = \iota \circ \alpha^{(p)} \circ \pi_1 = \alpha' \circ \pi_1 = [p].$$

Case 3 ($\ell = p$ and α inseparable): In this case α must be purely inseparable, since its degree is prime, so $\alpha = \iota \circ \pi$ for some separable isogeny ι of degree $\deg_s\alpha = 1$, which must be an isomorphism. If $E[p] = \{0\}$ then $[p]$ is purely inseparable of degree p^2, so $[p] = \iota' \circ \pi^2$ for some isomorphism ι', and we may take $\hat{\alpha} = \iota' \circ \pi \circ \iota^{-1}$. If $E[p] \simeq \mathbb{Z}/p\mathbb{Z}$ then $[p] = \alpha' \circ \pi$ for some separable isogeny α' of degree p and we may take $\hat{\alpha} = \alpha' \circ \iota^{-1}$. The two cases are shown in the diagrams below.



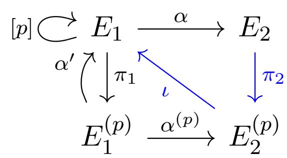


[2]If $E_1\colon y^2 = x^3 + A_1x + B_1$ then $E_1^{(p)}$ denotes the elliptic curve $E_1^{(p)}\colon y^2 = x^3 + A_1^p x + B_1^p$.

This completes the base case of our induction. If n is composite then we may decompose α into a sequence of isogenies of prime degree via Corollary 5.12. It follows that we can write $\alpha = \alpha_1 \circ \alpha_2$, where α_1, α_2 have degrees $n_1, n_2 < n$ with $n_1 n_2 = n$. Let $\hat{\alpha} = \hat{\alpha}_2 \circ \hat{\alpha}_1$, where the existence of $\hat{\alpha}_1$ and $\hat{\alpha}_2$ is given by the inductive hypothesis. Then

$$\hat{\alpha} \circ \alpha = (\hat{\alpha}_2 \circ \hat{\alpha}_1) \circ \alpha = \hat{\alpha}_2 \circ \hat{\alpha}_1 \circ \alpha_1 \circ \alpha_2 = \hat{\alpha}_2 \circ [n_1] \circ \alpha_2 = \hat{\alpha}_2 \circ \alpha_2 \circ [n_1] = [n_2] \circ [n_1] = [n],$$

where $[n_1] \circ \alpha_2 = \alpha_2 \circ [n_1]$ by Proposition 6.5.



□

Definition 6.8. The isogeny $\hat{\alpha}$ given by Theorem 6.7 is the *dual isogeny* of α.

Remark 6.9. One can define the dual isogeny for abelian varieties of any dimension, but in general 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) always are. This is yet another remarkable feature of elliptic curves.

As a matter of convenience we extend the notion of a dual isogeny to $\operatorname{Hom}(E_1, E_2)$ and $\operatorname{End}(E)$ by defining $\hat{0} = 0$, and we define $\deg 0 = 0$ so that $\hat{0} \circ 0 = [0]$ as in Theorem 6.7.

Lemma 6.10. *For an isogeny α of degree n we have $\alpha \circ \hat{\alpha} = [n]$, meaning that $\hat{\hat{\alpha}} = \alpha$. For any $n \in \mathbb{Z}$ the endomorphism $[n]$ is self-dual, that is, $\widehat{[n]} = [n]$.*

Proof. We have

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

Isogenies are nonzero, so we may cancel α on the right to obtain $\alpha \circ \hat{\alpha} = [n]$. The last statement follows from the fact that $[n] \circ [n] = [n^2] = [\deg n]$. □

Lemma 6.11. *For any $\alpha, \beta \in \operatorname{Hom}(E_1, E_2)$ 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. □

Lemma 6.12. *For any $\alpha \in \operatorname{Hom}(E_2, E_3)$ and $\beta \in \operatorname{Hom}(E_1, E_2)$ we have $\widehat{\alpha \circ \beta} = \hat{\beta} \circ \hat{\alpha}$.*

Proof. Let $m := \deg \alpha$ and $n := \deg \beta$. Then $\deg(\alpha \circ \beta) = mn$, by Corollary 5.10, and

$$(\hat{\beta} \circ \hat{\alpha}) \circ (\alpha \circ \beta) = \hat{\beta} \circ [m] \circ \beta = [m] \circ \hat{\beta} \circ \beta = [m] \circ [n] = [mn] = \deg(\alpha \circ \beta).$$

The lemma then follows from the definition of $\widehat{\alpha \circ \beta}$. □

6.4 Endomorphism rings

Definition 6.13. Let E/k be an elliptic curve. The endomorphism ring of E is the additive group $\mathrm{End}(E) := \mathrm{Hom}(E,E)$ with multiplication given by composition: $\alpha\beta := \alpha\circ\beta$.

Warning 6.14. Many 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

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

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, $\mathrm{Hom}(E,E)$ is torsion free, so the homomorphism $n\mapsto[n]$ 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. Proposition 6.5 implies that $\mathbb{Z}$ lies in the center of $\mathrm{End}(E)$, since $n\alpha = \alpha n$ for all $\alpha\in\mathrm{End}(E)$. As we shall see, the ring $\mathrm{End}(E)$ need not be commutative, in general, which makes the elements that lie in its center of interest.

When $k=\mathbb{F}_q$ is a finite field, the q-power Frobenius endomorphism π_E also lies in the center of $\mathrm{End}(E)$. This follows from the 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 6.15. 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 $[p]$ is necessarily the composition of $\pi^2 = \pi_E$ with an isomorphism. This isomorphism is typically $[\pm 1]$, in which case $\pi_E\in\mathbb{Z}$.

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 $\mathrm{End}(E)$ has no zero divisors, so the cancellation law holds (on both the left and the right).

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

Lemma 6.16. *For any endomorphism α we have $\alpha+\hat\alpha = 1+\deg\alpha-\deg(1-\alpha)$.*

Note that in the statement of this lemma, $1-\alpha$ denotes the endomorphism $[1]-\alpha$ and the integers $\deg\alpha$, and $\deg(1-\alpha)$ are viewed as elements of $\mathrm{End}(E)$ via the embedding $\mathbb{Z}\hookrightarrow\mathrm{End}(E)$ defined by $n\mapsto[n]$.

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

$$\deg(1-\alpha) = (\widehat{1-\alpha})(1-\alpha) = (\hat1-\hat\alpha)(1-\alpha) = (1-\hat\alpha)(1-\alpha) = 1-(\alpha+\hat\alpha)+\deg(\alpha),$$

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 integer $t\in\mathbb{Z}$.

Definition 6.17. The *trace* of an endomorphism α is the integer $\mathrm{tr}\,\alpha := \alpha+\hat\alpha$.

Note that for any $\alpha \in \operatorname{End}(E)$ we have $\operatorname{tr}\hat{\alpha} = \operatorname{tr}\alpha$, and $\deg\hat{\alpha} = \deg\alpha$. This implies that α and $\hat{\alpha}$ have the same characteristic polynomial.

Theorem 6.18. *Let α be an endomorphism of an elliptic curve. Both α and its dual $\hat{\alpha}$ are solutions to*

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

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

6.5 Endomorphism restrictions to $E[n]$

Let E/k be an elliptic curve with $\operatorname{char}(k) = p$ (possibly $p = 0$). For any $\alpha \in \operatorname{End}(E)$, 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 $E[n]$.

Provided n is not divisible by p, we have $E[n] \simeq \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ with rank 2, and we can pick a basis $\langle P_1, P_2\rangle$ for $E[n]$ as a $(\mathbb{Z}/n\mathbb{Z})$-module, so 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 — it suffices to pick any $P_1, P_2 \in E[n]$ that generate $E[n]$ as an abelian group. Having fixed a basis for $E[n]$, 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 determined by

$$\begin{aligned}\alpha(P_1) &= aP_1 + bP_2,\\ \alpha(P_2) &= cP_1 + dP_2.\end{aligned}$$

This matrix representation depends on our choice of basis but its conjugacy class does not; in particular the trace $\operatorname{tr}\alpha_n$ and determinant $\det\alpha_n$ are independent of our choice of basis.

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 $\ker(\alpha - \beta) > \deg(\alpha - \beta)$, which is impossible unless $\alpha - \beta = 0$, in which case $\alpha = \beta$. 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 6.19. *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 $n \ge 2\sqrt{m} + 1$ be an integer prime to the characteristic of k, and also relatively prime to the integers $\deg\alpha$ and $\deg\beta$. If $\alpha_n = \beta_n$ then $\alpha = \beta$.*

Proof. We shall make use of the following fact. 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 polynomials $u, v \in [x]$ can be uniquely determined using *Cauchy interpolation*; see [1, §5.8] for an efficient algorithm and a proof of its correctness. In particular, two rational functions with degrees bounded by N as above that agree on N distinct points must coincide.

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 v 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 u and v. For each $x_0 \in \bar{k}$ at most 2 points $P \in E(\bar{k})$ have x-coordinate x_0, so it suffices to know $\alpha(P)$ at $4\deg\alpha + 4$ affine points not in $\ker\alpha$.

For $n \ge 2\sqrt{m} + 1$ we have $n^2 \ge 4m + 4\sqrt{m} + 1$, and $E[n]$ contains $n^2 - 1 \ge 4\deg\alpha + 4$ affine points, none of which lie in $\ker\alpha$, since $\#\ker\alpha$ divides $\deg\alpha$ which is coprime to n. Thus 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 therefore infinite, and it follows that $\alpha = \pm\beta$.

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 $\alpha = \beta$. $\square$

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

Theorem 6.20. *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 $t_n I$ and $d_n I$, respectively. Let $\alpha_n = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$, and let $\delta_n = \det \alpha_n$. The fact that $\hat{\alpha}_n\alpha_n = d_n I \neq 0$ 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 plug the expression for $\hat{\alpha}_n$ 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.

If $a = d$ and $b = c = 0$ then 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 6.19. But then $\hat{\alpha} = \hat{m} = m = \alpha$, so $\operatorname{tr} \alpha = 2m \equiv \operatorname{tr} mI \equiv \operatorname{tr} \alpha_n \bmod n$ and $\deg \alpha = m^2 \equiv \det mI \equiv \det \alpha_n \bmod n$. $\square$

References

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