23 Divisors and the Weil pairing

In this lecture we address a completely new topic, the Weil pairing, which has many practical and theoretical applications. In order to define the Weil pairing we first need to expand our discussion of the function field of a curve from Lecture 4. This requires a few basic results from commutative algebra and algebraic geometry that we will not take the time to prove; almost everything we need is summarized in the first two chapters of Silverman's book [7], which I recommend reviewing if you have not seen this material before.

23.1 Valuations on the function field of a curve

Let C/k be a smooth projective curve defined by a homogeneous polynomial $f_C(x,y,z)=0$ that (as always) we assume is irreducible over $\bar{k}$.[1] For the sake of simplicity we assume throughout this section that k is a perfect field (every algebraic extension is separable).

In Lecture 4 we defined the *function field* $k(C)$ as the field of rational functions g/h, where $g,h\in k[x,y,z]$ are homogeneous polynomials of the same degree with $h\not\in(f_C)$, modulo the equivalence relation

$$\frac{g_1}{h_1}\sim\frac{g_2}{h_2}\qquad\Longleftrightarrow\qquad g_1h_2-g_2h_1\in(f_C).$$

Alternatively, we can view the function g/h as a rational map $(g:h)$ from C to $\mathbb{P}^1$. Our assumption that C is smooth implies that this rational map is actually a *morphism*, meaning that it is defined at every point $P\in C(\bar{k})$; this was stated as Theorem 4.15 and we will prove it below. This means that even though the rational map $(g_1:h_1):C\to\mathbb{P}^1$ associated to a particular representative g_1/h_1 of an element of $k(C)$ might not be defined at a point P (this occurs when $g_1(P)=h_1(P)=0$, since $(0:0)$ is not a point in $\mathbb{P}^1$), there is always an equivalent g_2/h_2 representing the same element of $k(C)$ that *is* defined at P.

Example 23.1. Consider the function x/z on the elliptic curve $E\colon y^2z=x^3+Axz^2+Bz^3$. We can evaluate the map $(x:z)$ at any affine point, but not at the point $(0:1:0)$, where we get $(0:0)$. But the maps

$$(x:z)\sim(x^3:x^2z)\sim(y^2z-Axz^2-Bz^3:x^2z)\sim(y^2-Axz-Bz^2:x^2)$$

all represent the same element of $k(E)$, and the last one sends $(0:1:0)$ to $(1:0)\in\mathbb{P}^1$, which is defined. Moreover, any other representative of the function x/z that is defined at $(0:1:0)$ will give the same value. Notice that the right-most map is also not defined everywhere, since it gives $(0:0)$ at the point $(0:\sqrt{B}:1)$. In general, there will typically not be a single representative for a function $f\in k(E)$ that can be used to evaluate the morphism $f\colon E\to\mathbb{P}^1$ at every point, even though the morphism is defined at every point.

Remark 23.2. It is often more convenient to write elements of the function field in affine form, just as we typically use the equation $y^2=x^3+Ax+B$ to refer to the projective curve defined by its homogenization; so we may write x instead of x/z, for example. In general, any time we refer to a function $r(x,y)$ as an element of $k(C)$ that is not a ratio

[1] Here we are assuming for simplicity that C is a plane curve (e.g. an elliptic curve in Weierstrass form). One can work more generally in $\mathbb{P}^n$ by replacing (f) with a homogeneous ideal I in $k[x_0,\ldots,x_n]$ whose zero locus is a smooth absolutely irreducible projective variety of dimension one in $\mathbb{P}^n$. Everything in this section applies to any smooth projective (geometrically integral) curve, we use plane curves only for the sake of concreteness.

Lecture by Andrew Sutherland

$g(x,y,z)/h(x,y,z)$ of two homogeneous polynomials g and h of the same degree, it should be understood that we mean the function one obtains by multiplying each term in the numerator and denominator of $r(x,y)$ by a suitable power of z to put it in the form g/h with g and h homogeneous polynomials of the same degree.

Definition 23.3. For any point $P \in C(\bar{k})$, we define the *local ring at* P (or the *ring of regular functions at* P) by

$$\mathcal{O}_P := \{f \in k(C) : f(P) \neq \infty\} \subseteq k(C),$$

where $\infty = (1:0) \in \mathbb{P}^1$. It is a principal ideal domain (PID) with a unique maximal ideal

$$\mathfrak{m}_P := \{f \in \mathcal{O}_P : f(P) = 0\}.$$

Any generator u_P for the principal ideal $\mathfrak{m}_P = (u_P)$ is called a *uniformizer* at P.

Definition 23.4. A *discrete valuation* on a field F is a surjective homomorphism $v\colon F^\times \to \mathbb{Z}$ that satisfies

$$v(x+y) \geq \min(v(x), v(y))$$

for all $x, y \in F^\times$ with $x + y \neq 0$ (one typically defines $v(0) = \infty$). If v is a discrete valuation on F, then the subring

$$R := \{x \in F : v(x) \geq 0\}$$

is a PID with the unique maximal ideal

$$\mathfrak{m} := \{x \in R : v(x) \geq 1\}.$$

Every nonzero ideal (x) of R is then of the form $\mathfrak{m}^n$, where $n = v(x)$. Any $u \in F$ with $v(u) = 1$ is a generator for $\mathfrak{m}$ and called a *uniformizer* for $\mathfrak{m}$.

Given a principal ideal domain R with a unique nonzero maximal ideal $\mathfrak{m} = (u)$, we can define a discrete valuation on its fraction field F via

$$v(x) := \min\{n \in \mathbb{Z} : u^{-n}x \in R\},$$

and we then have $R = \{x \in F : v(x) \geq 0\}$. Note that $v(x)$ does not depend on the choice of the uniformizer u. We call any such ring R a *discrete valuation ring* (DVR).

For the curve C/k, the local rings $\mathcal{O}_P$ are a family of DVRs that all have the same fraction field $k(C)$. We thus have a discrete valuation v_P for each point $P \in C(\bar{k})$ which we think of as measuring the "order of vanishing" of a function $f \in k(C)$ at P (one can formally expand f as a Laurent series in any uniformizer u_P for $\mathfrak{m}_P$, and the degree of the first nonzero term will be $v_P(f)$, just as with meromorphic functions over $\mathbb{C}$).

Remark 23.5. When k is not algebraically closed the function field $k(C)$ has many valuations that are not associated to rational points $P \in C(k)$. One can always work with $\bar{k}$-points as above (and in [7]), but a more natural approach is to work with *closed points*: $\mathrm{Gal}(\bar{k}/k)$-orbits in $C(\bar{k})$, which we also denote P (note that we have assumed k is a perfect field, so $\bar{k}/k$ is separable). Each closed point is a finite subset of $C(\bar{k})$ whose cardinality we denote $\deg P$; this is the same as the degree of the minimal extension of k over which all the points in P are defined (which is necessarily a finite Galois extension), and it is also the degree of the residue field $\mathcal{O}_P/\mathfrak{m}_P$ as an extension of k. Rational points (elements of $C(k)$) are closed points of degree one. Each closed point corresponds to a maximal ideal $\mathfrak{m}_P$ of the coordinate ring $k[C]$. Note that it still makes sense to "evaluate" a rational function $f \in k(C)$ at a closed point P; the result is a closed point $f(P)$ of $\mathbb{P}^1$ (because $f \in k(C)$ is, by definition, Galois invariant).

Now that we have valuations v_P and uniformizers u_P associated to each point P of a smooth projective curve we can easily prove Theorem 4.15, which was stated without proof.

Theorem 23.6. *Let C_1/k be a smooth projective curve and let $\phi\colon C_1 \to C_2$ be a rational map. Then ϕ is a morphism.*

Proof. Let $\phi = (\phi_0 : \cdots : \phi_m)$, let $P \in C_1(\bar{k})$ be any point, let u_P be a uniformizer at P, and let $n = \min_i v_P(\phi_i)$. Then

$$\phi = (u_P^{-n}\phi_0 : \cdots : u_P^{-n}\phi_m)$$

is defined at P because $v_P(u_P^{-n}\phi_i) \geq 0$ for all i and $v_P(u_P^{-n}\phi_i) = 0$ for at least one i. □

Remark 23.7. When C_1 is not smooth one can construct counterexamples to the theorem above. Smoothness guarantees that the local rings $\mathcal{O}_P$ are all DVRs, so that we have a valuation v_P to work with. Indeed, a curve is smooth if and only if all its local rings are DVRs; this gives an alternative criterion for smoothness that does not depend on the equation of the curve or even the dimension of the projective space in which it is embedded.

Example 23.8. For the function x on the elliptic curve $E\colon y^2 = x^3 + Ax + B$ we have

$$v_P(x) = \begin{cases} 0 & \text{if } P = (1 : * : *) \\ 1 & \text{if } P = (0 : \pm\sqrt{B} : 1) \quad (B \neq 0) \\ 2 & \text{if } P = (0 : 0 : 1) \qquad\quad (B = 0) \\ -2 & \text{if } P = (0 : 1 : 0) \end{cases}$$

For the function y we have

$$v_P(y) = \begin{cases} 0 & \text{if } P = (* : y_0 : 1) \qquad (y_0 \neq 0) \\ 1 & \text{if } P = (x_0 : 0 : 1) \qquad (x_0^3 + Ax_0 + B = 0) \\ -3 & \text{if } P = (0 : 1 : 0) \end{cases}$$

You may wonder how we computed these valuations. In particular, how do we know that $v_\infty(x) = -2$ and $v_\infty(y) = -3$? There are a couple of ways to see this. One is to use the fact that for any $f \in k(C)$ we always have $\sum_P v_P(f) = 0$ (see below), so every function in $k(C)$ has the same number of zeros and poles. Thus if we know all the zeros (and the order of vanishing at each) and there is only one pole, we know its order.

A more general approach is to consider the *degree* of the morphism $f\colon C \to \mathbb{P}^1$. For non-constant functions f this is defined as

$$\deg f := [k(C) : f^*(k(\mathbb{P}^1))]$$

where $f^*\colon k(\mathbb{P}^1) \to k(C)$ is the morphism of function fields that sends $g \in k(\mathbb{P}^1)$ to the function $g \circ f$ in $k(C)$; for $f \in k^\times$ the convention is to define $\deg f = 0$. In explicit examples it is often obvious what the degree is, it is the cardinality of the fibers $f^{-1}(P)$ for all but finitely many $P \in \mathbb{P}^1(\bar{k})$. In our example, the function x defines a morphism of degree two from E to $\mathbb{P}^1$, because if we pick an arbitrary point on $\mathbb{P}^1$ there will generically be two points on E that get mapped to it (points with the same x-coordinate). Any time this is not the case, we have a *ramified* point, and in the case of a zero or pole the degree of ramification is what determines its multiplicity.

Whenever we have $f(P) = Q \in \mathbb{P}^1(\bar{k})$ and the size of the preimage $f^{-1}(Q)$ is the same as the degree of f as a morphism (which happens for all but finitely many Q), no ramification occurs and if $Q = 0$ or $Q = \infty$ then f has a simple zero or pole at P. More generally, we have the following theorem, which says that so long as we count points with multiplicity, every fiber of the morphism $f\colon C \to \mathbb{P}^1$ has the same size, equal to the degree of f.

Theorem 23.9. *Let C be a smooth projective curve over an algebraically closed field k and let $f \in k(C)^\times$ be an element of its function field (viewed as a morphism $f\colon C \to \mathbb{P}^1$). For every point $Q \in \mathbb{P}^1(k)$ we have*

$$\deg f = \sum_{f(P)=Q} v_P(u_Q \circ f),$$

where $u_Q \in k(\mathbb{P}^1)$ denotes any uniformizer for $\mathfrak{m}_Q$.

Proof. This is a special case of Proposition 2.6 in [7]. □

If t is our coordinate for $\mathbb{P}^1$ (which we may view as taking values in $k \cup \{\infty\}$), then we can take $u_Q := t - Q$ to be a simple translation. Computing $v_P(u_Q \circ f)$ then amounts to re-interpreting the order of "vanishing" at P with the order of "Q-ing" at P.

Corollary 23.10. *Let C be a smooth projective curve over an algebraically closed field k. For every $f \in k(C)^\times$ we have*

$$\sum_{P \in C(k)} v_P(f) = 0,$$

and $v_P(f) = 0$ for all but finitely many P; we have $v_P(f) = 0$ for all P if and only if $f \in k^\times$.

Proof. We have $v_P(f) \neq 0$ only when $f(P) = 0$ or $f(P) = \infty$. Applying Theorem 23.9 to $Q = 0$ using the uniformizer $u_0 = t$ yields

$$\deg f = \sum_{f(P)=0} v_P(f),$$

and if we apply it to $Q = \infty$ with uniformizer $u_\infty = 1/t$ we have

$$\deg f = \sum_{f(P)=\infty} v_P(u_\infty \circ f) = \sum_{f(P)=\infty} -v_P(f),$$

which implies $\sum v_P(f) = 0$. The cardinalities of $f^{-1}(0)$ and $f^{-1}(\infty)$ are each bounded by $\deg f$, hence finite, so $v_P(f) \neq 0$ for only finitely many P, and these cardinalities can be zero if and only if $f \in k^\times$, since otherwise $\deg f \geq 1$. □

Remark 23.11. When working with closed points over a non-algebraically closed field the formula in Theorem 23.9 needs to be modified to account for the degrees of the points. We then have

$$\deg f \deg Q = \sum_{f(P)=Q} v_P(u_Q \circ f) \deg P,$$

which holds for any closed point Q of $\mathbb{P}^1/k$; the formula in Corollary 23.10 becomes

$$\sum v_P(f) \deg P = 0,$$

where the sum is over closed points P.

Example 23.12. Another way to compute valuations is to work directly from the definition using a uniformizer u_P. We did not do this in Example 23.8 because we hadn't yet determined uniformizers for the points on an elliptic curve. But from the example it is clear that we can take

$$u_P = \begin{cases} x - x(P) & \text{if } y(P) \neq 0 \text{ and } P \neq (0:1:0) \\ y & \text{if } y(P) = 0 \\ x/y & \text{if } P = (0:1:0) \end{cases}$$

Note that $v_P(x/y) = v_P(x) - v_P(y) = -2 - (-3) = 1$. To check that $v_\infty(y) = -3$ using the uniformizer u_∞, for example, it suffices to show that $1/y$ and u_∞^3 generate the same ideal in $\mathcal{O}_\infty$: the function $s := y^2/x^3 = y^2/(y^2 - Ax - B)$ is a unit in $\mathcal{O}_\infty$ and we have $1/y = su_\infty^3$.

23.2 The divisor class group of a curve

As in the previous section, we continue to assume that C is a smooth projective curve over a perfect field k, and in this subsection we will temporarily assume k is algebraically closed (but we may still write $\bar{k}$ to emphasize this in places where it is especially important).

Definition 23.13. To each point $P \in C(\bar{k})$ we associate a formal symbol $[P]$. The *divisor group* of C is the free abelian group on the set $\{[P] : P \in C(\bar{k})\}$, denoted $\operatorname{Div} C$. Its elements are called *divisors*. Each is a finite sum of the form

$$D = \sum_P n_P[P]$$

in which the n_P are integers (so $n_P = 0$ for all but finitely many P).

Remark 23.14. Some authors write P rather than $[P]$ and rely on context to make it clear which is meant, but when C is an elliptic curve this makes it very hard to know whether $P + Q$ is meant to denote $[P] + [Q]$ or $[P + Q]$ (these two divisors are equivalent in a sense to be defined, but they are not the same divisor). It is also common to use (P) rather than $[P]$, but this can cause confusion when similar symbols are used for divisor coefficients and elements of $k(C)$, so we will avoid this notation.

The integer n_P is the *valuation* of D at P, also denoted by $v_P(D) := n_P$. For each divisor D the finite set

$$\operatorname{supp}(D) := \{P : v_P(D) \neq 0\}$$

is its *support*, and the integer

$$\deg D := \sum_P v_P(D)$$

is its *degree*. The degree map $D \mapsto \deg D$ is a surjective homomorphism of abelian groups whose kernel is the subgroup $\operatorname{Div}^0 C$ of divisors of degree zero. Associated to each function $f \in k(C)^\times$ there is a divisor

$$\operatorname{div} f := \sum_P v_P(f)[P],$$

which is called a *principal divisor*. Because each $v_P \colon k(C)^\times \to \mathbb{Z}$ is a group homomorphism, we have $\operatorname{div} fg = \operatorname{div} f + \operatorname{div} g$, and the map

$$\operatorname{div} \colon k(C)^\times \to \operatorname{Div} C$$

is a group homomorphism whose image is the subgroup of Div C consisting of principal divisors, and whose kernel consists of the nonzero constant functions $k^\times$, by Corollary 23.10.

The quotient group

$$\operatorname{Pic} C := \operatorname{Div} C/\operatorname{div}(k(C)^\times)$$

is the *Picard group* of C. We also have a degree map

$$\deg\colon\ \operatorname{Pic} C \to \mathbb{Z}$$

on divisor classes, and its kernel is the *reduced Picard group*

$$\operatorname{Pic}^0 C := \operatorname{Div}^0 C/\operatorname{div}(k(C)^\times)$$

also known as the (degree zero) *divisor class group* of C. We then have an exact sequence

$$1 \longrightarrow k^\times \longrightarrow k(C)^\times \longrightarrow \operatorname{Div}^0 C \longrightarrow \operatorname{Pic}^0 C \longrightarrow 0.$$

When $k \neq \bar{k}$ one instead defines divisors as sums over closed points (each of which is a Galois orbit of $\bar{k}$-points). The degree of a divisor is then $\deg D := \sum_P v_P(D)\deg P$, and if we let $\operatorname{Gal}(\bar{k}/k)$ act on $\operatorname{Div} C$ by defining $\sigma([P]) := [\sigma(P)]$ for $\sigma \in \operatorname{Gal}(\bar{k}/k)$, then the $\operatorname{Gal}(\bar{k}/k)$-invariant elements of $\operatorname{Div} C_{\bar{k}}$ and $\operatorname{Div}^0 C_{\bar{k}}$ are precisely those that are sums of closed points. So long as $C(k) \neq \emptyset$ (necessarily true when C is an elliptic curve), the $\operatorname{Gal}(\bar{k}/k)$-invariant elements of $\operatorname{Pic}^0 C_{\bar{k}}$ will all be represented by $\operatorname{Gal}(\bar{k}/k)$-invariant elements of $\operatorname{Div}^0 C_{\bar{k}}$ and we obtain the same exact sequence as above whether we start over $\bar{k}$ and take $\operatorname{Gal}(\bar{k}/k)$-invariants of each term or simply work over k (using closed points) throughout. But this is not automatic! In general it is possible for a coset of $\operatorname{div}(\bar{k}(C)^\times)$ in $\operatorname{Div}^0 C_{\bar{k}}$ to be $\operatorname{Gal}(\bar{k}/k)$-invariant without being a coset of $\operatorname{div}(k(C)^\times)$.

Remark 23.15. The condition $C(k) \neq \emptyset$ ensuring that every k-rational divisor class is represented by a k-rational divisor is stronger than necessary, any k-rational divisor of degree 1 will suffice, and such a divisor might involve closed points of higher degree.

Of the various groups defined above, the divisor class group $\operatorname{Pic}^0 C$ is the one of greatest interest to us, because it is intimately related to the curve C. Provided $C(k) \neq \emptyset$, the divisor class group $\operatorname{Pic}^0 C$ is isomorphic to the *Jacobian* of the curve C. Although this is not at all obvious from the definition above, in addition to its structure as an abelian group, $\operatorname{Pic}^0 C$ can be given the structure of an algebraic variety, making it an *abelian variety.* When $C(k) \neq \emptyset$ this variety is canonically isomorphic to the Jacobian of C in the category of abelian varieties over k. The formal definition of these objects is outside the scope of this course, but the details do not matter to us, because when C is an elliptic curve E we already know exactly what its Jacobian is: it is the abelian variety E.

Definition 23.16. Let C/k be a smooth projective curve with a rational point $0 \in C(k)$. The *Abel-Jacobi map* is the map $C(k) \to \operatorname{Pic}^0 C$ defined by

$$P \mapsto [P] - [0].$$

Although we will not prove this here, for a curve C/k of genus g, over an algebraically closed field the Abel-Jacobi map is surjective if and only if $g \le 1$ and injective if and only if $g \ge 1$. As usual, genus $g = 1$ is the sweet spot, and we will prove in the next section that for smooth projective curves of genus 1 with a rational point (elliptic curves), the Abel-Jacobi map is an isomorphism.

23.3 The Jacobian of an elliptic curve

Definition 23.17. Let E/k be an elliptic curve with 0 as its distinguished point (for curves in Weierstrass form this is the projective point $(0:1:0)$, the point "at infinity"). For each pair of points $P,Q \in E(k)$ let $L_{P,Q} \in k(E)$ denote the function corresponding to the line $\overline{PQ}$, which we define as the tangent to the curve when $P = Q$. For example, if $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ are distinct affine points then the point-slope formula tells us that

$$L_{P,Q} = (y - y_1)(x_2 - x_1) - (x - x_1)(y_2 - y_1),$$

which has zeros at P, Q, and $-(P+Q)$ where it intersects the curve E, but here we are thinking of $L_{P,Q} \in k(E)$ as a map $E \to \mathbb{P}^1$ that we can evaluate at any point R on E. We now define

$$G_{P,Q} := \frac{L_{P,Q}}{L_{P+Q,-(P+Q)}}.$$

The motivation for this is that $G_{P,Q}$ effectively encodes our geometric definition of the group law on E: to add P and Q we construct the line $\overline{PQ}$, which intersects the curve E at a third point $-(P+Q)$, and we then compute $P+Q$ as the point on the line through 0 and $-(P+Q)$; in the formula for $G_{P,Q}$ above this is the line $L_{P+Q,-(P+Q)}$ in the denominator.

To see this more clearly, let us compute the principal divisors corresponding to the functions $L_{P,Q}$ and $G_{P,Q}$. By definition, the function $L_{P,Q}$ has zeros at the points P, Q and $-(P+Q)$ (possibly with multiplicity if any of these points coincide); it has no other zeros and no poles at any affine points, so it must have a triple point at the point at infinity. Thus

$$\operatorname{div} L_{P,Q} = [P] + [Q] + [-(P+Q)] - 3[0].$$

We can then compute

$$\begin{aligned} \operatorname{div} G_{P,Q} &= [P] + [Q] + [-(P+Q)] - 3[0] - ([P+Q] + [-(P+Q)] + [0] - 3[0]) \\ &= [P] + [Q] - [P+Q] - [0]. \end{aligned}$$

Since $\operatorname{div} G_{P,Q}$ is a principal divisor, it follows that $[P]+[Q]$ and $[P+Q]+[0]$ represent the same equivalence class in $\operatorname{Pic} E$; such divisors are said to be *linearly equivalent*, and we use

$$[P] + [Q] \sim [P+Q] + [0] \qquad (1)$$

to denote this relation.

Theorem 23.18. *Let E/k be an elliptic curve with distinguished point 0. The Abel-Jacobi map $E(k) \to \operatorname{Pic}^0 E$ defined by $P \mapsto [P] - [0]$ is a group isomorphism.*

Proof. By (1) we have

$$([P] - [0]) + ([Q] - [0]) \sim [P+Q] + [0] - 2[0] = [P+Q] - [0],$$

and clearly $[0] - [0] = 0$, so the Abel-Jacobi map is a group homomorphism.

To show surjectivity, let $D = \sum n_P[P]$ represent a divisor class in $\operatorname{Pic}^0 E$. By splitting D into separate sums with $n_P > 0$ and $n_P < 0$, we can write

$$D = \sum_{n_P > 0} n_P[P] - \sum_{n_P < 0} (-n_P)[P],$$

and by applying (1) repeatedly we obtain

$$D \sim \left[\sum_{n_P>0} n_P P\right] - \left[\sum_{n_P<0} (-n_P) P\right] + m[0],$$

for some integer m (note that the sums $\sum n_P P$ and $\sum(-n_P)P$ inside the brackets are sums of points in $E(k)$ that yield a single point in $E(k)$ in each case). Since D represents a class in $\operatorname{Pic}^0 E$, we have $\deg D = 0$, and computing degrees of both sides above yields

$$0 = 1 - 1 + m,$$

so $m = 0$. If we now let $Q = \sum_{n_P>0} n_P P$ and $R = \sum_{n_P<0}(-n_P)P$ then

$$D \sim [Q] - [R] = [Q] - [0] - ([R] - [0]) = [Q - R] - [0],$$

where we have used the fact that the Abel-Jacobi map is a group homomorphism to get the rightmost equality, which shows that D is in the image of the Abel-Jacobi map, which is thus surjective.

To show injectivity we need to show that the kernel of the Abel-Jacobi map is trivial, which amounts to showing that if $D = \sum n_P[P]$ is a principal divisor, then $\sum n_P P = 0$. As above, by applying (1) repeatedly we can obtain $D \sim [Q] - [R]$. By adding $G_{R,-Q}$ and negating, we obtain the principal divisor $[T] - [0]$, where $T = Q - R$.

We claim that $T = 0$, which implies $Q = R$ and therefore $\sum n_P P = 0$ as desired. Suppose not. Let $t \in k(E)^\times$ be a function with $\operatorname{div} t = [T] - [0]$ (in fact no such functions exist, we are supposing that $[T] - [0]$ is a principal divisor with $T \neq 0$ and this is going to lead to a contradiction). For any $f \in k(E)^\times - k^\times$, define

$$\tilde{f} := \prod_S (t - t(S))^{v_S(f)}$$

If f does not have a zero or pole at 0, then f and $\tilde{f}$ have the same divisor and f is a rational function of t. If f has a zero or pole at 0, we can replace f by $ft^{-v_0(f)}$, which does not have a zero or pole at 0, and we again find that f is a rational function of t. Thus every function in $k(E)$ is a rational function of t, so $k(E) = k(t)$. But $k(t) \simeq k(\mathbb{P}^1)$ and $\mathbb{P}^1$ has genus 0 while E has genus 1, a contradiction, so $T = 0$ as claimed. □

Corollary 23.19. *Let E/k be an elliptic curve and let $D = \sum_P n_P[P] \in \operatorname{Div}(E)$. Then D is a principal divisor if and only if $\sum n_P = 0$ and $\sum_P n_P P = 0$.*

Proof. It suffices to show that $D = \sum_P n_P[P] \in \operatorname{Div}^0(E)$ is principal if and only if $\sum_P n_P P = 0$. Let $\varphi\colon \operatorname{Pic}^0(E) \xrightarrow{\sim} E(\bar{k})$ denote the inverse of the Abel-Jacobi map. Then

$$D \sim 0 \iff \varphi(D) = 0 \iff \sum_P n_P \varphi([P]) = 0 \iff \sum_P n_P \varphi([P] - [0]) = 0 \iff \sum_P n_P P = 0,$$

where we have used $\sum_P n_P = 0$ to subtract $\sum_P n_P \varphi([0]) = 0$ in the third equivalence. □

23.4 Pullback maps

Let $\alpha\colon E \to E'$ be a separable isogeny of elliptic curves over k. Recall from Remark 4.32 that α induces a morphism of function fields

$$\begin{aligned} \alpha^*\colon k(E') &\to k(E) \\ f &\mapsto f \circ \alpha \end{aligned}$$

that allows us to view $k(E)$ as a separable field extension of $\alpha^*(k(E'))$ of degree equal to $\deg \alpha$. The isogeny α also induces a homomorphism of divisor groups defined by

$$\begin{aligned} \alpha^*\colon \operatorname{Div} E' &\to \operatorname{Div} E \\ [P] &\mapsto \sum_{\alpha(Q)=P} [Q], \end{aligned}$$

that is, given a divisor in $\operatorname{Div} E'$, replace each formal symbol corresponding to a point (or closed point) P with the sum of the formal symbols of each of its preimages under α. The two morphisms denoted α^* are compatible in that for every $f \in k(E')$ we have

$$\operatorname{div}(\alpha^*(f)) = \alpha^*(\operatorname{div} f).$$

Corollary 23.19 implies that α^* maps principal divisors to principal divisors, and it clearly maps divisors of degree 0 to divisors of degree 0, thus induces a homomorphism $\alpha^*\colon \operatorname{Pic}^0 E' \to \operatorname{Pic}^0 E$. When composed with the isomorphisms $E' \simeq \operatorname{Pic} E'$ and $\operatorname{Pic} E \simeq E$ given by the Abel-Jacobi maps, this yields the dual isogeny $\hat{\alpha}$. If $\beta\colon E' \to E''$ is another separable isogeny then $(\beta \circ \alpha)^* = \alpha^* \circ \beta^*$, consistent with $\widehat{\beta \circ \alpha} = \hat{\alpha} \circ \hat{\beta}$.

We also recall that each $P \in E(k)$ has an associated translation-by-P map τ_P that induces an automorphism τ_P^* of $k(E)$ defined by $f \mapsto f \circ \tau_P$. When α is separable and $E[\alpha] := \ker \alpha \subseteq E(k)$, each $P \in \ker \alpha$ induces an automorphism of $k(E)$ that fixes $\alpha^*(k(E'))$, making $k(E)/\alpha^*(k(E'))$ a Galois extension with Galois group $E[\alpha]^* = \{\tau_P^* : P \in \ker \alpha\}$. We may then view $\alpha^*(k(E'))$ as the fixed field of $k(E)$ under the action of $(\ker \alpha)^*$. It follows that the functions $g \in k(E)$ of the form $f \circ \alpha$ for some $f \in k(E')$ are precisely those for which $g \circ \tau_P = g$ for all $P \in E[\alpha]$.

We will apply these facts in the next section in the special case $E' = E$ with $\alpha \in \operatorname{End}(E)$ a multiplication-by-n map for some n not divisible by the characteristic of k.

Remark 23.20. When α is not necessarily separable the pullback map on divisors is defined by $[P] \mapsto \sum_{\alpha(Q)=P} e_\alpha(Q)[Q]$ where $e_\alpha(Q) := v_Q(\alpha^* u_P)$ is the *ramification index*, computed using a uniformizer u_P at $P = \alpha(Q)$. When α is separable we always have $e_\alpha(Q) = 1$.

23.5 The Weil pairing

Let E/k be an elliptic curve and let n be a positive integer not divisible by the characteristic of k. We will temporarily assume that $E[n] \subseteq E(k)$, which can be achieved by taking the base change of E to $k(E[n])$ if needed. For each $Q \in E[n]$ we define the divisor

$$D_Q := [n]^*([Q] - [0]) = \sum_{nQ'=Q} [Q'] - \sum_{nP=0} [P].$$

Note that our assumption $E[n] \subseteq E(k)$ ensures that D_Q is a k-rational divisor even if the Q' are not k-rational. For any $T \in E(\bar{k})$, if $nS_0 = T$ then

$$\sum_{nS=T} S = \sum_{R\in E[n]} (S_0 + R) = n^2 S_0 = nT,$$

and it follows that $\sum_{nQ'=Q} Q' = nQ = 0$ and $\sum_{P\in E[n]} P = 0$. Corollary 23.19 then implies that D_Q is a principal divisor, so there exists $g_Q \in k(E)^\times$ such that

$$\operatorname{div}(g_Q) = D_Q,$$

which is unique up to a scalar in $k^\times$. If we compose g_Q with a translation-by-P map τ_P for some $P \in E[n]$, this will not change its divisor, since the sums defining D_Q are both invariant under translation-by-P for any n-torsion point P. However, we may get a different element of $k(E)^\times$, which differs from g_Q by a scalar in $k^\times$. It is thus natural to consider the ratio

$$e_n(P, Q) := \frac{g_Q \circ \tau_P}{g_Q},$$

which does not depend on the choice of g_Q.

Warning 23.21. Some authors define $e_n(P, Q)$ as $\frac{g_P \circ \tau_Q}{g_P}$, reversing the roles of P and Q; see [8, §16] for example (but note that there is a typo in [8, Def. 16.2.1] which is corrected in [8, Eq.16.3]). By Theorem 23.23 below, this amounts to replacing $e_n(P, Q)$ with $e_n(Q, P) = e_n(P, Q)^{-1}$. Our definition matches the one used in Silverman [7].

Now consider $f_Q \in k(E)^\times$ with $\operatorname{div} f_Q = n[Q] - n[0]$ (via Corollary 23.19). We have

$$\operatorname{div}(f_Q \circ [n]) = n \sum_{nQ'=Q} [Q'] - n \sum_{nP=0} [P] = nD_Q = \operatorname{div}(g_Q^n)$$

and choose f_Q so $f_Q \circ [n] = g_Q^n$. It follows that $g_Q^n \in [n]^*(k(E))$ is invariant under composition with τ_P for all $P \in E[n]$, so $e_n(P, Q) = (g_Q \circ \tau_P)/g_Q \in k^\times$ is an nth root of unity.

Let $\mu_n \simeq \mathbb{Z}/n\mathbb{Z}$ denote the group of nth roots of unity in $\bar{k}^\times$. We now drop our assumption that $E[n] \subseteq E(k)$ and base change as required to define $e_n \colon E[n] \times E[n] \to \mu_n$.

Definition 23.22. Let E/k be an elliptic curve. For each $n \geq 1$ not divisible by the characteristic of k we define the *Weil pairing* to be the function $e_n \colon E[n] \times E[n] \to \mu_n$.

Theorem 23.23. *Let E/k be an elliptic curve and let m and n be positive integers not divisible by the characteristic of k. The Weil pairing satisfies the following properties.*

- *Bilinear: $e_n(P + Q, R) = e_n(P, R)e_n(Q, R)$ and $e_n(P, Q + R) = e_n(P, Q)e_n(P, R)$;*
- *Alternating: $e_n(P, P) = 1$ and $e_n(P, Q) = e_n(Q, P)^{-1}$;*
- *Nondegenerate: If $Q \neq 0$ then $e_n(P, Q) \neq 1$ for some $P \in E[n]$;*
- *Galois-equivariant: $e_n(P^\sigma, Q^\sigma) = e_n(P, Q)^\sigma$ for all $\sigma \in \operatorname{Gal}(\bar{k}/k)$;*
- *Compatibility: $e_{mn}(P, Q) = e_n(mP, Q)$ for all $P \in E[mn]$ and $Q \in E[n]$;*
- *Endomorphisms: $e_n(\phi(P), \phi(Q)) = e_n(P, Q)^{\deg \phi}$ for nonzero $\phi \in \operatorname{End}(E)$;*
- *Isogenies: $e_n(P, \hat{\alpha}(Q)) = e_n(\alpha(P), Q)$ for $\alpha \in \operatorname{Hom}(E, E')$, $P \in E[n]$, $Q \in E'[n]$;*
- *Surjective: for each $P \in E[n]$ we have $\{e_n(P, Q) : Q \in E[n]\} = \mu_r$, where $r := |P|$.*

Proof. We first note that our assumption that m and n are not divisible by the characteristic of k ensures the $\#E[m]=m^2$, $\#E[n]=n^2$, and $E[mn]=m^2n^2$, by Theorem 5.25.

Bilinear: We have

$$e_n(P+Q,R)=\frac{g_R\circ\tau_{P+Q}}{g_R}=\left(\frac{g_R\circ\tau_P}{g_R}\circ\tau_Q\right)\frac{g_R\circ\tau_Q}{g_R}=e_n(P,R)e_n(Q,R)$$

since the ratio $g_R\circ\tau_P/g_R$ lies in $\bar{k}^\times$ and is therefore invariant under composition. We now apply Corollary 23.19 to obtain $h\in\bar{k}(E)^\times$ with

$$\operatorname{div}h=[Q+R]-[Q]-[R]+[0]$$

so that $\operatorname{div}f_{Q+R}-\operatorname{div}f_Q-\operatorname{div}f_R=n[Q+R]-n[Q]-n[R]+n[0]=n\operatorname{div}h$. Then

$$\operatorname{div}\frac{g_{Q+R}}{g_Qg_R}=\frac{1}{n}\operatorname{div}\left(\frac{g_{Q+R}^n}{g_Q^ng_R^n}\right)=\frac{1}{n}\operatorname{div}\left(\frac{f_{Q+R}}{f_Qf_R}\circ[n]\right)=\operatorname{div}(h\circ[n]).$$

It follows that $g_{Q+R}/(g_Qg_R)$ is a scalar multiple of $h\circ[n]$, hence invariant under composition with τ_P for $P\in E[n]$, so $g_Qg_R(g_{Q+R}\circ\tau_P)=g_{Q+R}(g_Qg_R\circ\tau_P)$. We then have

$$\begin{aligned}e_n(P,Q+R)=\frac{g_{Q+R}\circ\tau_P}{g_{Q+R}}&=\left(\frac{g_Qg_R}{g_Qg_R}\right)\left(\frac{g_{Q+R}\circ\tau_P}{g_{Q+R}}\right)=\left(\frac{g_{Q+R}}{g_{Q+R}}\right)\left(\frac{g_Qg_R\circ\tau_P}{g_Qg_R}\right)\\&=\frac{g_Qg_R\circ\tau_P}{g_Qg_R}=\frac{g_Q\circ\tau_P}{g_Q}\frac{g_R\circ\tau_P}{g_R}=e_n(P,Q)e_n(P,R).\end{aligned}$$

Alternating: Bilinearity implies $e_n(P+Q,P+Q)=e_n(P,P)e_n(P,Q)e_n(Q,P)e_n(Q,Q)$, so it suffices to show $e_n(P,P)=1$ for $P\in E[n]$. Pick $R\in E[n^2]$ with $nR=P$ and let $F_P:=\prod_{i=0}^{n-1}(f_P\circ\tau_{iP})$ and $G_P=\prod_{i=0}^{n-1}(g_P\circ\tau_{iR})$ with $f_P\circ\tau_{iP}\circ[n]=g_P\circ\tau_{iR}$ so $F_P=G_P^n$. We then have

$$n\operatorname{div}G_P=\operatorname{div}F_P=\sum_{i=0}^{n-1}(n[P+iP]-n[0+iP])=n\sum_{i=1}^{n}[iP]-n\sum_{i=0}^{n-1}[iP]=0,$$

so $G_P\in\bar{k}^\times$ is constant. Therefore $G_P=G_P\circ\tau_R$, and

$$\prod_{i=0}^{n-1}g_P\circ\tau_{iR}=\prod_{i=0}^{n-1}g_P\circ\tau_{(i+1)R}$$

implies $g_P=g_P\circ\tau_{nR}=g_P\circ\tau_P$. Thus $e_n(P,P)=(g_P\circ\tau_P)/g_P=1$ as desired.

Nondegenerate: If $e_n(P,Q)=1$ for all $P\in E[n]$ then $g_Q\circ\tau_P=g_Q$ for all $P\in E[n]$. Since n is not divisible by the characteristic, the multiplication-by-n map is separable, and the field extension $\bar{k}(E)/[n]^*(\bar{k}(E))$ is Galois, with the Galois group $E[n]^*=\{\tau_P^*:P\in E[n]\}$. So g_Q lies in the fixed field $\bar{k}(E)^{E[n]^*}$, hence of the form $h\circ[n]$ for some $h\in\bar{k}(E)^\times$. We then have $(h\circ[n])^n=g_Q^n=f_Q\circ[n]$, which implies $f_Q=h^n$ and $n\operatorname{div}h=\operatorname{div}f_Q=n[Q]-n[0]$ implies $\operatorname{div}h=[Q]-[0]$. But then either $h\in\bar{k}^\times$, in which case $\operatorname{div}h=0$ and $Q=0$, or $\deg h=\sum_{h(R)=0}v_R(h)=1$, in which case h defines a map of degree one from E to $\mathbb{P}^1$. The latter is impossible, because $E\not\simeq\mathbb{P}^1$, so if $Q\neq 0$ then $e_n(P,Q)\neq 1$ for some $P\in E[n]$.

Galois equivariance: For any $\sigma\in\operatorname{Gal}(\bar{k}/k)$ and $P,Q\in E[n]$ we have

$$e_n(P^\sigma,Q^\sigma)=\frac{g_{Q^\sigma}\circ\tau_{P^\sigma}}{g_{Q^\sigma}}=\left(\frac{g_Q\circ\tau_P}{g_Q}\right)^\sigma=e_n(P,Q)^\sigma.$$

Compatibility: Let $P \in E[mn]$ and $Q \in E[n] \subseteq E[mn]$. Let us temporarily use the notation $g_{n,Q}, g_{mn,Q}$ and $f_{n,Q}, f_{mn,Q}$ to denote the functions g_Q and f_Q defined above to make the dependence on n explicit. We have

$$\operatorname{div}(g_{n,Q} \circ [m]) = [m]^* \operatorname{div} g_{n,Q} = [m]^*[n]^*([Q] - [0]) = [mn]^*([Q] - [0]) = \operatorname{div} g_{mn,Q}.$$

It follows that $g_{mn,Q} = \lambda(g_{n,Q} \circ [m])$ for some $\lambda \in \bar{k}^\times$, and this implies

$$e_{mn}(P,Q) = \frac{g_{mn,Q} \circ \tau_P}{g_{mn,Q}} = \frac{g_{n,Q} \circ [m] \circ \tau_P}{g_{n,Q} \circ [m]} = \frac{g_{n,Q} \circ \tau_{mP} \circ [m]}{g_{n,Q} \circ [m]} = e_n(mP,Q) \circ [m],$$

and $e_n(mP,Q) \circ [m] = e_n(mP,Q)$, since $e_n(mP,Q)$ is a constant function.

Endomorphisms: Let us fix a basis $E[n] = \langle R, S \rangle$. The action of any $\phi \in \operatorname{End}(E)$ on $E[n]$ is then described by a matrix $\gamma_\phi = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{M}_2(\mathbb{Z}/n\mathbb{Z})$ with $\deg \phi \equiv \det \gamma_\phi = (ad - bc) \bmod n$. For $P = uR + vS$ and $Q = wR + xS$ in $E[n]$, the alternating and bilinearity properties give

$$\begin{aligned} e_n(\phi(P), \phi(Q)) &= e_n((au+bv)R + (cu+dv)S, (aw+bx)R + (cw+dx)S) \\ &= e_n((au+bv)R, (cw+dx)S) e_n((cu+dv)S, (aw+bx)R) \\ &= e_n(R,S)^{(au+bv)(cw+dx) - (aw+bx)(cu+dv)} \\ &= e_n(R,S)^{(ad-bc)(ux-vw)} \\ &= e_n(uR, xS)^{\det \gamma_\phi} e_n(vS, wR)^{\det \gamma_\phi} \\ &= e_n(uR + vS, wR + xS)^{\deg \phi} \\ &= e_n(P,Q)^{\deg \phi} \end{aligned}$$

where we have used the fact that e_n has image in μ_n to apply equivalences modulo n.

Isogenies: We first note that it suffices to prove this for isogenies of prime degree, since if $\varphi = \psi \circ \phi$ then

$$e_n(P, \hat{\varphi}(Q)) = e_n(P, \hat{\phi}(\hat{\psi}(Q))) = e_n(\phi(P), \hat{\psi}(Q)) = e_n(\psi(\phi(P)), Q) = e_n(\varphi(P), Q)$$

follows once we know the claim holds for ψ and ϕ, and we can decompose any isogeny into a composition of isogenies of prime degree. So let ϕ be an isogeny of degree ℓ. If ℓ does not divide n then choose r so $\ell r \equiv 1 \bmod n$ and use endomorphism compatibility to obtain

$$e_n(P, \hat{\phi}(Q)) = e_n(P, \hat{\phi}(Q))^{\ell r} = e_n(\phi(P), \ell Q)^r = e_n(\phi(P), Q)^{\ell r} = e_n(\phi(P), Q).$$

If $n = \ell m$ we instead use

$$e_n(P, \hat{\phi}(Q)) = e_m(\ell P, \hat{\phi}(Q)) = e_m(P, \hat{\phi}(Q))^\ell = e_m(\phi(P), \ell Q) = e_n(\phi(P), Q).$$

Surjectivity: Fix any $P \in E[n]$. Bilinearity implies that $\{e_n(P,Q) : Q \in E[n]\}$ is a subgroup μ_m of μ_n. For all $Q \in E[n]$ we have

$$1 = e_n(P,Q)^m = e_n(mP, Q),$$

so by non-degeneracy, $mP = 0$ and m is a multiple of $r = |P|$. On the other hand, if $e_n(P,Q)$ has order m greater than r for any Q, then $e_n(rP,Q) = e_n(P,Q)^r \neq 1$, so $e_n(0,Q) \neq 1$, but $e_n(0,Q) = e_n(0,Q)e_n(Q,Q) = e_n(Q+0,Q) = e_n(Q,Q) = 1$, a contradiction. □

Corollary 23.24. *Let E/k be an elliptic curve and let n be a positive integer prime to the characteristic of k. If $E[n] \subseteq E(k)$ then $\mu_n \subseteq k^\times$. In particular, if $k = \mathbb{Q}$ then $E[n] \subseteq E(k)$ can occur only for $n \leq 2$, and if $k = \mathbb{F}_q$ then $E[n] \subseteq E(k)$ can occur only if $q \equiv 1 \bmod n$.*

Corollary 23.25. *Let E/k be an elliptic curve and let $P \in E(\bar{k})$ be a point of order n prime to the characteristic of k. For every $Q \in E[n]$ the order of $e_n(P,Q)$ in μ_n is the largest $m|n$ for which $E[m] \subseteq \langle P, Q\rangle$, equivalently, the least $m|n$ for which $mQ \in \langle P\rangle$. In particular, $e_n(P,Q) = 1$ if and only if $\langle P, Q\rangle$ is cyclic.*

Proof. Let us first suppose $m = n$, in which case $\langle P, Q\rangle = E[n] \simeq (\mathbb{Z}/n\mathbb{Z})^2$. By the surjectivity of $e_n \colon E[n] \times E[n] \to \mu_n$, we have $e_n(P, aP + bQ) = \zeta_n$ for some $a, b \in \mathbb{Z}$, and

$$\zeta_n = e_n(P, aP + bQ) = e_n(P,P)^a e_n(P,Q)^b = e_n(P,Q)^b$$

(by the bilinear and alternating properties of e_n), so $e_n(P,Q)$ generates $\mu_n = \langle \zeta_n\rangle \simeq \mathbb{Z}/n\mathbb{Z}$ and must have order n.

In the general case we have $mQ = aP$ with $0 \leq a < n$. The order of $aP = mQ$ is at most $r \coloneqq n/m$, so a is divisible by m, and if we put $c = -a/m$ then $\langle rP, Q + cP\rangle = E[m]$. By the case we have already proved, $e_m(rP, Q + cP)$ has order m, and therefore

$$e_n(P,Q) = e_n(P,Q)e_n(P,P)^c = e_n(P, Q + cP) = e_{mr}(P, Q + cP) = e_m(rP, Q + cP)$$

also has order m (the last equality follows from compatibility). □

The isogeny compatibility of the Weil pairing provides an easy proof of Lemma 6.11.

Corollary 23.26. *Let E_1, E_2 be elliptic curves over a field k. For all $\alpha, \beta \in \operatorname{Hom}(E_1, E_2)$ we have $\widehat{\alpha + \beta} = \hat{\alpha} + \hat{\beta}$.*

Proof. We will show $\phi := \widehat{\alpha + \beta} - \hat{\alpha} - \hat{\beta} = 0$. Suppose not. Choose n coprime to the characteristic of k with $n^2 > \deg \phi$ so $E_2[n] \not\subseteq \ker \phi$. For any $P \in E_1[n]$, $Q \in E_2[n]$ we have

$$\begin{aligned} e_n(P, \widehat{\alpha + \beta}(Q)) &= e_n((\alpha + \beta)(P), Q) \\ &= e_n(\alpha(P) + \beta(P), Q) \\ &= e_n(\alpha(P), Q)e_n(\beta(P), Q) \\ &= e_n(P, \hat{\alpha}(Q))e_n(P, \hat{\beta}(Q)) \\ &= e_n(P, \hat{\alpha}(Q) + \hat{\beta}(Q)), \end{aligned}$$

where the first and fourth equalities use isogeny compatibility. It follows that for every $P \in E_1[n]$ and $Q \in E_2[n]$ we have

$$e_n(P, \widehat{\alpha + \beta}(Q) - \hat{\alpha}(Q) - \hat{\beta}(Q)) = e_n(P, \phi(Q)) = 1,$$

and the non-degeneracy of e_n implies that this can only hold if $\phi(Q) = 0$ for all $Q \in E_2[n]$, which contradicts $E_2[n] \not\subseteq \ker \phi$. □

23.6 Computing the Weil pairing

For practical applications we want to be able to compute $e_n(P,Q)$ explicitly, in a computationally efficient manner. For this purpose we use the following sequence of functions proposed by Miller [5].

Definition 23.27. Let E/k be an elliptic curve and let $P \in E(k)$. For each integer n we recursively define the function $f_{n,P}$ via

$$f_{0,P} = f_{1,P} := 1, \qquad f_{n+1,P} := f_{n,P}G_{P,nP}, \qquad f_{-n,P} := (f_{n,P}G_{nP,-nP})^{-1},$$

where $G_{P,Q}$ is as in Definition 23.17.

We assume that the line functions $L_{P,Q}$ are all normalized (they will still be defined by an equation for the line $\overline{PQ}$); this implies that the functions $G_{P,Q}$ are also normalized, as are the functions $f_{n,P}$.

Lemma 23.28. *The functions $f_{n,P}$ satisfy the following properties:*

(i) $\operatorname{div} f_{n,P} = n[P] - (n-1)[0] - [nP]$;

(ii) $f_{m+n,P} = f_{m,P}f_{n,P}G_{mP,nP}$;

(iii) $f_{mn,P} = f_{m,P}^n f_{n,mP} = f_{n,P}^m f_{m,nP}$.

Proof. For (i) we proceed by induction on $n \ge 0$. For $n = 0, 1$ we have

$$\operatorname{div} f_{0,P} = 0 = 0[P] - (0-1)[0] - [0P] \quad \text{and} \quad \operatorname{div} f_{1,P} = 0 = 1[P] - (1-1)[0] - [1P],$$

and for $n > 1$ the inductive hypothesis yields

$$\begin{aligned}\operatorname{div} f_{n+1} &= \operatorname{div} f_{n,P} + \operatorname{div} G_{P,nP}\\ &= n[P] - (n-1)[0] - [nP] + [P] + [nP] - [P+nP] - [0]\\ &= (n+1)[P] - (n+1-1)[0] - [(n+1)P].\end{aligned}$$

We then note that

$$\begin{aligned}\operatorname{div} f_{-n,P} &= -\operatorname{div} f_{n,P} - \operatorname{div} G_{nP,-nP}\\ &= -n[P] + (n-1)[0] + [nP] - [nP] - [-nP] + [nP - nP] + [0]\\ &= -n[P] + (n-1)[0] - [-nP] + 2[0]\\ &= -n[P] - (-n-1)[0] - [-nP].\end{aligned}$$

which establishes (i) for all $n \in \mathbb{Z}$.

For (ii) we use (i) to compute

$$\begin{aligned}\operatorname{div} f_{m,P}f_{n,P}G_{mP,nP} &= (m+n)[P] - (m+n-2)[0] - [mP] - [nP]\\ &\qquad + [mP] + [nP] - [mP+nP] - [0]\\ &= (m+n)[P] - (m+n-1)[0] - [(m+n)P]\\ &= \operatorname{div} f_{m+n,P},\end{aligned}$$

and since these are all normalized functions, (ii) follows.

For (iii) we use (i) to compute

$$\begin{aligned}\operatorname{div} f_{m,P}^n f_{n,mP} &= n(m[P]-(m-1)[0]-[mP]) + n[mP]-(n-1)[0]-[mnP]\\ &= nm[P]-(nm-1)[0]-[mnP]\\ &= \operatorname{div} f_{mn,P}.\end{aligned}$$

which establishes the first equality in (iii), since these are normalized functions. The second equality is proved similarly. □

The key part of Lemma 23.28 is (ii), which allows us to efficiently compute $f_{n,P}$ using a double-and-add approach, or any generic exponentiation algorithm, in $O(\log n)$ steps. Lemma 23.28 allows us to reduce the computation of $f_{n,P}(Q)$ to computations of $G_{aP,bP}(Q)$, for various integers a and b. Computing $G_{aP,bP}(Q)$ involves evaluating the line functions $L_{aP,bP}$ and $L_{aP+bP,-(aP+bP)}$ at Q. Assuming we know the coordinates of the points aP and bP (which we will have computed in previous steps of an addition chain), this involves a single application of the group law on E to compute the coordinates of the point $aP+bP$ which we can then negate to compute $-(aP+bP)$ (for curves in short Weierstrass form, this means negating the y-coordinate), followed by $O(1)$ operations in k to evaluate the line functions at Q. Each group operation in $E(k)$ involves just $O(1)$ field operations, and we thus obtain the following corollary,

Corollary 23.29. *Let E/k be an elliptic curve and let n be a positive integer. For any $P,Q\in E(k)$ we can evaluate $f_{n,P}(Q)$ using $O(\log n)$ field operations in k.*

The following result allows us to use the Miller functions to efficiently compute the Weil pairing.

Theorem 23.30. *Let E/k be an elliptic curve with distinct points $P,Q\in E(k)[n]$, where $n\ge 1$ is prime to the characteristic of k. Then*

$$e_n(P,Q) = (-1)^n \frac{f_{n,Q}(P)}{f_{n,P}(Q)}.$$

Proof. This follows from [5, Prop. 8], since, as proved in [8, Prop. 16.1.1], the definition of $e_n(P,Q)$ used in [5] is equivalent to our definition of $e_n(Q,P)$ (the roles of P and Q are swapped in [8, Eq. 16.3] relative to our definition), and $e_n(P,Q)=e_n(Q,P)^{-1}$. □

Warning 23.31. The factor $(-1)^n$ is sometimes incorrectly omitted from this formula in the literature ([4, p. 387] is a notable example).

Note that the definition of $f_{n,P}$ does not require k to be algebraically closed, we just need to work over a field where P is defined, in which case all the points in the support of $\operatorname{div} f_{n,P}$ will be closed points of degree 1 and everything we have done over algebraically closed fields still applies. In particular, if P and Q are k-rational n-torsion points, then $e_n(P,Q)$ will be k-rational.

23.7 Applications of the Weil pairing

There are many applications of the Weil pairing, two of which you will have the opportunity to explore on Problem Set 13. These include an efficient algorithm to compute the structure of the group $E(\mathbb{F}_q)$, which was the original motivation of Miller's work in [5], and a method for transferring the discrete logarithm problem on an elliptic curve $E/\mathbb{F}_q$ to the multiplicative group of an extension of $\mathbb{F}_q$ containing μ_n, where n is the cardinality of the subgroup of $E(\mathbb{F}_q)$ in which one wishes to compute a discrete logarithm. In most cases the minimal extension of $\mathbb{F}_q$ containing μ_n will be impractically large, but when this is not the case it may be easier to solve the discrete logarithm problem in this extension of $\mathbb{F}_q$ rather than in $E(\mathbb{F}_q)$. The degree of this minimal extension is known as the *embedding degree*, which we discuss in the next section. For cryptographic applications that depend on the difficulty of the discrete logarithm problem, it is important that the embedding degree is not too small. On the other hand, if the embedding degree is not too large, one can then use pairings to efficiently implement cryptographic protocols that would otherwise be impractical.

This brings us to the notion of *pairing-based cryptography*, a topic that we unfortunately do not have time to address in any detail. But we will give one example to demonstrate its utility: a one round tripartite Diffie-Hellman key exchange, due to Joux [4]. For the sake of presentation we will describe it in terms of the Weil pairing, but in practice one uses the more efficient Tate pairing defined in §23.9 below.

We assume that Alice, Bob, and Carol all know an elliptic curve $E/\mathbb{F}_q$ and two independent n-torsion points P and Q in $E[n]$. They want to agree on a random secret, and they would like to do this with a single round of messaging that does not require any back-and-forth communication.

To begin the protocol, Alice, Bob, and Carol individually generate random integers a, b, and c, respectively. Alice then sends $P_A := aP$ and $Q_A := aQ$ to Bob and Carol, Bob sends $P_B := bP$ and $Q_B := bQ$ to Alice and Carol, and Carol sends $P_C := cP$ and $Q_C := cQ$ to Alice and Bob.

Alice then computes

$$e_n(P_B, Q_C)^a = e_n(bP, cQ)^a = e_n(P, Q)^{bca},$$

Bob computes

$$e_n(P_A, Q_C)^b = e_n(aP, cQ)^b = e_n(P, Q)^{acb},$$

and Carol computes

$$e_n(P_A, Q_B)^c = e_n(aP, bQ)^c = e_n(P, Q)^{abc}.$$

The common value $e_n(P, Q)^{abc} \in \mu_n$ is now known to Alice, Bob, and Carol. If one assumes that the discrete logarithm problem is hard, an eavesdropper cannot readily determine the values of a, b, or c, and if one further assumes that the computational Diffie-Hellman problem is hard, an eavesdropper cannot readily determine the shared secret $e_n(P, Q)^{abc}$. The *computational Diffie-Hellman problem* is to compute abP, given P, aP, and bP; this can clearly be solved efficiently if one can compute discrete logarithms efficiently, but the converse is not known.

23.8 Embedding degree

For practical applications one typically applies Miller's algorithm to n-torsion points of an elliptic curve $E/\mathbb{F}_q$, where $\mathbb{F}_q$ is a finite field and n is a prime dividing $\#E(\mathbb{F}_q)$. While we typically will not have $E[n] \subseteq E(\mathbb{F}_q)$ (indeed, $E(\mathbb{F}_q)$ will often be cyclic), we can always choose an n that divides $\#E(\mathbb{F}_q)$, in which case we at least have a cyclic subgroup of $E[n]$ of order n that lies in $E(\mathbb{F}_q)$ (assuming n is prime). The remaining points in $E[n]$ will then lie in a finite extension of $\mathbb{F}_q$; as indicated in the previous section, the degree of this extension is a key parameter.

Definition 23.32. Let E/K be an elliptic curve over a field K and let n be a positive integer. The *embedding degree* of E with respect to n is the degree of the minimal extension L/K for which $E[n] \subseteq E(L)$.

An easy lower bound on the embedding degree k arises from the fact that the Weil pairing $E[n] \times E[n] \to \mu_n$ is surjective. If $E[n] \subseteq E(\mathbb{F}_{q^k})$ then we must have $\mu_n \subseteq \mathbb{F}_{q^k}^\times$. The group $\mathbb{F}_{q^k}^\times$ is cyclic, so this is the same as requiring n to divide $q^k - 1$, equivalently, $q^k \equiv 1 \bmod n$. When $E(\mathbb{F}_q)$ contains a cyclic group of order n, this necessary condition is also sufficient.

Lemma 23.33. *Let $E/\mathbb{F}_q$ be an elliptic curve, let $n \perp q$ be a prime divisor of $\#E(\mathbb{F}_q)$, and let $\pi_n \in \operatorname{End}(E[n]) \simeq \operatorname{GL}_2(\mathbb{Z}/n\mathbb{Z})$ denote the restriction of the Frobenius endomorphism π_E to $E[n]$. Then either $E[n] \subseteq E(\mathbb{F}_q)$ or $E[n] \simeq \ker(\pi_n - 1) \oplus \ker(\pi_n - q)$, and the embedding degree of E with respect to n is the least integer $k > 0$ such that $q^k \equiv 1 \bmod n$.*

Proof. Let $t = \operatorname{tr} \pi_E$, so that $\#E(\mathbb{F}_q) = q+1-t$. Then $t \equiv q+1 \bmod n$ and the characteristic polynomial of π_E satisfies $x^2 - tx + q \equiv x^2 - (q+1)x + q \equiv (x-1)(x-q) \bmod n$. It follows that $(\pi_n - 1)(\pi_n - q) = 0$ in $\operatorname{End}(E[n])$. If $q \equiv 1 \bmod n$ then π_E acts trivially on $E[n]$ and $E[n] \subseteq E(\mathbb{F}_q)$; otherwise $\pi_n \in \operatorname{End}(E[n]) \simeq \operatorname{GL}_2(\mathbb{Z}/n\mathbb{Z})$ can be diagonalized and $E[n]$ can be decomposed as the sum of the distinct eigenspaces $\ker(\pi_n - 1)$ and $\ker(\pi_n - q)$ of π_n.

As observed above, the embedding degree e necessarily satisfies $q^e \equiv 1 \bmod n$, since $\mu_n \subseteq \mathbb{F}_{q^e}^\times$, so $e \geq k$. On the other hand, for $P \in \ker(\pi_n - 1)$ we have $P \in E(\mathbb{F}_q) \subseteq E(\mathbb{F}_{q^k})$, and for $P \in \ker(\pi_n - q)$ we have $\pi_n^k(P) = q^k P = P$ (since $q^k \equiv 1 \bmod n$), in which case P is fixed by π_E^k and lies in $E(\mathbb{F}_{q^k})$. It follows that $E[n] \subseteq E(\mathbb{F}_{q^k})$ and therefore $e \leq k$, so $e = k$ as claimed. □

Lemma 23.33 gives us an easy way to compute the embedding degree k when $n | \#E(\mathbb{F}_q)$. If we suppose E is chosen arbitrarily, we should expect q to be roughly equidistributed modulo n, and for most values of n this means it is likely that q is a primitive root modulo n, in which case we must have $k = n - 1$ (assuming n is prime). This is bad news for practical applications: if $k = n - 1$ it will take $\log_2(\#\mathbb{F}_{q^k}) = (n-1)\log_2 q \approx n \log n$ bits just to write down a typical n-torsion point, which is hopeless if n is of cryptographic size (say $n \approx 2^{256}$), since this will be more bits than there are atoms in the universe.

Practical applications of the Weil pairing are feasible only when k is small. It is possible to have k as small as 1 or 2 when E is supersingular (see Problem Set 12), but this is too small for cryptographic applications, as you will demonstrate on Problem Set 12, since one can transfer the discrete logarithm problem in $E(\mathbb{F}_q)$ to the discrete logarithm problem in $\mathbb{F}_{q^k}^\times$. Ideally one wants k to be around 10 or 20 to balance the difficulty of the discrete logarithm problems in $E(\mathbb{F}_q)$ and $\mathbb{F}_{q^k}^\times$; for $q \approx 2^{256}$ using $k = 12$ yields $\#\mathbb{F}_{q^k}^\times \approx 2^{3072}$, in which case the discrete logarithm problems have similar difficulty.

Elliptic curves with embedding degrees in this range are known as *pairing-friendly* curves. They are quite rare, far too rare to find by brute force search, but they can be constructed using the CM method. See [3] for an extensive survey of methods to compute suitable parameters q, n, k, D, where q and n are cryptographic size primes, k is small, $q^k \equiv 1 \bmod n$, and D is an imaginary quadratic discriminant with $|D|$ small enough so that the CM method can be used to construct an elliptic curve $E/\mathbb{F}_q$ so that n divides $\#E(\mathbb{F}_q)$.

23.9 Tate pairing

In most practical applications of pairings, rather than using the Weil pairing one instead uses the Tate pairing, or variations thereof, which can be computed much more efficiently.

Definition 23.34. Let $n > 2$ be an integer and let $E/\mathbb{F}_q$ be an elliptic curve over a finite field with embedding degree k with respect to n. The (modified) *Tate pairing* is the map $t_n\colon E[n] \times E[n] \to \mu_n$ defined by

$$t_n(P,Q) := \left(\frac{f_{n,P}(Q+T)}{f_{n,P}(T)}\right)^{(q^k-1)/n}$$

where $T \in E[n] - \{0, P, -Q, P-Q\}$.

The exponentiation by $(q^k-1)/n$ included in our definition of the Tate pairing means that if $P \in E[n]$ we can actually compute $t_n(P,Q)$ using any $Q \in E(\mathbb{F}_{q^k})$; the value of $t_n(P,Q)$ depends only on the image of $Q \in E(\mathbb{F}_{q^k})$ under the quotient map

$$E(\mathbb{F}_{q^k}) \to E(\mathbb{F}_{q^k})/nE(\mathbb{F}_{q^k}) \simeq E[n],$$

and we can view $Q \in E(\mathbb{F}_{q^k})$ as representing a coset of $nE(\mathbb{F}_{q^k})$ corresponding to an element of $E[n]$ (the Tate pairing is sometimes defined with this interpretation in mind).

Like the Weil pairing, the Tate pairing is a non-degenerate bilinear pairing that is surjective and Galois-equivariant. Unlike the Weil pairing, the Tate pairing is not alternating, and may have $t_n(P,P) \neq 1$; this is an advantage in many practical applications, because it means that the pairing may be non-trivial even when we restrict to points in a cyclic subgroup of $E[n]$, which is never true of the Weil pairing. Another advantage is that we only need to compute one Miller function $f_{n,P}$, rather than the two Miller functions $f_{n,P}$ and $f_{n,Q}$ required by the Weil pairing, and in the typical case where n is a prime dividing $\#E(\mathbb{F}_q)$, we can choose $P \in E(\mathbb{F}_q)$ to be rational, which greatly accelerates this computation.

In the practically interesting scenario where $n \perp q$ is a prime dividing $\#E(\mathbb{F}_q)$ and $k > 1$, Lemma 23.33 gives us a natural decomposition of $E[n] \simeq \ker(\pi_n - 1) \oplus \ker(\pi_n - q)$ into two cyclic subgroups of order n, the first of which is just $E(\mathbb{F}_q)[n]$. In many applications (and in many descriptions of the Tate pairing in the literature), one restricts the inputs of the Tate pairing to $P \in \ker(\pi_n - 1) = E(\mathbb{F}_q)[n]$ and $Q \in \ker(\pi_n - q) \subseteq E(\mathbb{F}_{q^k})$.

References

[1] Dan Boneh and Matthew Franklin, *Identity-based encryption from the Weil pairing*, SIAM J. Comput. **32** (2003), 586–615.

[2] Andreas Enge, *Elliptic curves and their applications to cryptography: An introduction*, Springer, 1999.

[3] David Freeman, Michael Scott, and Edlyn J. Teske, *A taxonomy of pairing-friendly elliptic curves*, J. Cryptology **23** (2010), 224-280.

[4] Antoine Joux, *A one round protocol for tripartite Diffie-Hellman*, Algorithmic Number Theory 4th International Symposium (ANTS IV), LNCS **1838** (2000), 385–394.

[5] Victor S. Miller, *The Weil pairing and its efficient calculation*, J. Cryptology **17** (2004), 235–261.

[6] Adi Shamir, *Identity based cryptosystems and signature schemes*, Advances in Cryptology – Proceedings of CRYPTO '84, LNCS **196** (1985), 47–53.

[7] Joseph H. Silverman, *The arithmetic of elliptic curves*, second edition, Springer, 2009.

[8] Katherine E. Stange, *Elliptic nets and elliptic curves*, PhD Thesis, Brown University, 2008.

[9] Lawrence C. Washington, *Elliptic curves: Number theory and cryptography*, second edition, Chapman and Hall/CRC, 2008.

MIT OpenCourseWare
https://ocw.mit.edu

18.783 / 18.7831 Elliptic Curves
Fall 2025

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