24 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 5. 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 it is summarized in the first two chapters of Silverman's book [6], which I recommend reviewing if you have not seen this material before.

24.1 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] In order to simplify the presentation, we are going to assume in this section that $k = \bar{k}$ is algebraically closed, but we will note in remarks along the way how to handle non-algebraically closed (but still perfect) fields.

In Lecture 5 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 $h \notin (f_C)$, modulo the equivalence relation

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

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 5.10 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 particular representative g_1/h_1 of an element of $k(C)$ might not be defined at at 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 24.1. 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 $(0 : \sqrt{B} : 1)$. The moral is that there typically will not be a single representative for a function in $k(E)$ that is defined at every point, even though the function itself is defined everywhere.

Remark 24.2. 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

[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 $k[x_0, \dots k_n]$ 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.

general, any time we refer to a function $r(x,y)$ as an element of $k(C)$ that is not a ratio $g(x,y,z)/h(x,y,z)$ of two homogeneous polynomials g and h of the same degree, it should be understood that we mean the function one obtains by multiplying the numerator and denominator of $r(x,y)$ by suitable powers of z to put it in the form g/h with g and h homogeneous polynomials of the same degree.

Definition 24.3. For any point $P \in C(k)$, 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 nonzero 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 24.4. A *discrete valuation* on a field F is a surjective homomorphism $v\colon F^\times \to \mathbb{Z}$ that satisfies the inequality

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

for all $x, y \in F^\times$. If v is a discrete valuation on F, then the subring

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

is a PID with a unique nonzero 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 $u \in F$ for which $v(u) = 1$ generates $\mathfrak{m}$ and is 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 $P \in C(k)$ 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 m_P, and the degree of the first nonzero term will be $v_P(f)$, just as with meromorphic functions over $\mathbb{C}$).

Remark 24.5. When k is not algebraically closed the function field $k(C)$ has many valuations that are not associated to rational points $P \in C(k)$ and we need to account for these. One can always base change to $\bar{k}$ (which is effectively what is done in [6]), but a more flexible approach is to work with *closed points*: these are the orbits in $C(\bar{k})$ under the action of $\mathrm{Gal}(\bar{k}/k)$, which we also denote P (we do assume that k is a perfect field so that $\bar{k}/k$ is separable, otherwise one should replace $\bar{k}$ with the separable closure of k in $\bar{k}$). Each closed point is a finite subset of $C(\bar{k})$ whose cardinality we denote $\deg P$; this is 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 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 $\mathbb{P}^1(k)$ (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 5.10.

Theorem 24.6. *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 24.7. When C_1 is not smooth one can construct counter-examples to the theorem above. We used smoothness to guarantee that all of the local rings $\mathcal{O}_P$ are actually discrete valuation rings, 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 24.8. For the function x on the elliptic curve $E\colon y^2 = x^3 + Ax + B$ we have

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

For the function y we have

$$v_P(y) = \begin{cases} 0 & \text{if } P = (* : 1 : z) \qquad (z \neq 0) \\ 1 & \text{if } P = (x_i : 0 : 1) \\ -3 & \text{if } P = (0 : 1 : 0) \end{cases}$$

where x_i denotes one of the three (necessarily distinct) roots of $x^3 + Ax + B$.

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 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 $f\colon C \to \mathbb{P}^1$. Formally speaking, 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 $\deg f = 0$. But in explicit cases it is often obvious what the degree is. 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 must be dealing with a *ramified* point, and in the case of a zero or pole the degree of ramification is what determines its multiplicity.

Whenever we have $f(P) = Q \in \mathbb{P}^1$ 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, then 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 24.9. *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*

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

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

Proof. This is a special case of Proposition 2.6 in [6]. □

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 24.10. *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 24.9 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

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

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 24.11. When working with closed points over a non-algebraically closed field the formula in Theorem 24.9 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 24.10 becomes

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

where the sum is over closed points P.

Example 24.12. Another way to compute valuations is to work directly from the definition using, a uniformizer u_P. We did not do this in Example 24.8 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 $1/y = su_\infty^3$.

24.2 The divisor class group of a curve

As in the previous section, we continue to assume that C is a smooth projective curve over an algebraically closed field k.

Definition 24.13. To each point $P \in C(k)$ we associate a formal symbol $[P]$. The *divisor group* of C is the free abelian group on the set $\{[P] : P \in C(k)\}$, 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). 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 $\operatorname{Princ} C$ is a subgroup of $\operatorname{Div} C$, and whose kernel consists of the nonzero constant functions $k^\times$, by Corollary 24.10.

The quotient group

$$\operatorname{Pic} C := \operatorname{Div} C/\operatorname{Princ} C,$$

is the *divisor class group* or *Picard group* of C. Since $\operatorname{Princ} C$ lies in the kernel of the degree map $\deg\colon \operatorname{Div} C \to \mathbb{Z}$, we also have a degree map

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

on divisor classes, and its kernel is the group

$$\operatorname{Pic}^0 C := \operatorname{Div}^0 C/\operatorname{Princ} C$$

of divisor classes of degree zero. We then have an exact sequence

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

Remark 24.14. When k is not algebraically closed we instead define divisors as sums over closed points P and the degree of a divisor is defined as $\deg D := \sum_P v_P(D) \deg P$.

Of the many groups defined above, $\operatorname{Pic}^0 C$ is the one of greatest interest to us, because it is intimately related to the curve C. You might wonder why it doesn't have name shorter than "the group of divisor classes of degree zero". This is because it often goes by another name, the *Jacobian* of the curve C (at least when $C(k)$ is non-empty, which is certainly true under our assumption that k is algebraically closed). Although this is not at all obvious from the definition above, in addition to is structure as an abelian group, $\operatorname{Pic}^0 \mathbb{C}$ can also be given the structure of an algebraic variety, making it an *abelian variety*. In general, the construction of the Jacobian is quite complicated; strictly speaking it is an object separate from $\operatorname{Pic}^0 C$ that is isomorphic to $\operatorname{Pic}^0 C$ as an abelian group and geometrically characterized by a universal property that distinguishes it (up to a canonical isomorphism) within the category of abelian varieties in terms of the Abel-Jacobi map defined below. The details of this construction do not matter to us, because when C is an elliptic curve we already know exactly what its Jacobian looks like: it is the curve C together with the distinguished point 0 and the group law that makes it an abelian variety.

Definition 24.15. 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 the $g \le 1$ and injective if and if 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.

24.3 The Jacobian of an elliptic curve

Definition 24.16. 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 write

$$[P] + [Q] \sim [P + Q] + [0] \tag{1}$$

to denote this relation.

Theorem 24.17. *Let E/k be an elliptic curve the distinguished point 0. The Abel-Jacobi map $E \mapsto \operatorname{Pic}^0 E$ 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 now let $Q = \sum_{n_P>0} n_P P$ and $R = \sum_{n_P<0}(-n_P)P$ be the points in $E(k)$ obtained by computing the sums $\sum n_P P$ using the group law in $E(k)$, we have

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

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

$$\tilde{f} := \prod_Q (t - t(Q))^{v_Q(f)}$$

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 $S = 0$ as claimed. □

24.4 The Weil pairing

In this section we define the Weil pairing for torsion points in $\operatorname{Pic}^0 C$, where C/k is a smooth projective curve and k is algebraically closed field. In the next section we will specialize to elliptic curves and drop our assumption that k is algebraically closed.

Definition 24.18. Let C/k be a smooth projective curve, and let $f \in k(C)^\times$. For each divisor $D \in \operatorname{Div} C$ with support disjoint from $\operatorname{div} f$ we define

$$f(D) := \prod_P f(P)^{v_P(D)} \in k^\times,$$

which satisfies $f(D_1 + D_2) = f(D_1)f(D_2)$ for any D_1, D_2 with support disjoint from $\operatorname{div} f$.

We are now ready to define the Weil pairing. In order to do so it will be convenient to work with *normalized* functions. Recall that the kernel of the map $\operatorname{div}\colon k(C)^\times \to \operatorname{Div} C$ consists of the constant functions, so the divisor of a function $f \in k(C)^\times$ determines f only up to a scalar in $k^\times$. In order to pin down this scalar, let us fix a rational point $0 \in C(k)$, the same point used to define the Abel-Jacobi map, and fix a uniformizer u_0 at 0. We may then associate to each principal divisor $\operatorname{div} f$ the unique $f \in k(C)^\times$ for which

$$(u_0^{-v_0(f)} f)(0) = 1.$$

and call this the *normalized* function f with divisor $\operatorname{div} f$. The particular choice of the point 0 and the uniformizer u_0, does not matter, all that matters is that we scale all of our normalized functions consistently. The constant function 1 is normalized, and products and inverses of normalized functions are normalized, so if we restrict our attention to normalized functions we get an isomorphism between the multiplicative subgroup of $k(C)^\times$ consisting of normalized functions and the group $\operatorname{Princ} C$ of principal divisors.

Definition 24.19. Let n be a positive integer and let k be an algebraically closed field whose characteristic does not divide n. Let C/k be a smooth projective curve and let D_1, D_2 be divisors with disjoint support representing n-torsion elements of $\operatorname{Pic}^0 C$ (this means $D_1, D_2 \in \operatorname{Div}^0 C$ and $nD_1, nD_2 \in \operatorname{Princ} C$). Let $f_1, f_2 \in k(C)^\times$ be the unique normalized functions for which $nD_1 = \operatorname{div} f_1$ and $nD_2 = \operatorname{div} f_2$. We then define

$$e_n(D_1, D_2) := \frac{f_1(D_2)}{f_2(D_1)} \in k^\times.$$

For each integer n, the map $(D_1, D_2) \mapsto e_n(D_1, D_2)$ is called the *Weil pairing*.

The Weil pairing actually defines a map

$$e_n\colon (\operatorname{Pic}^0 C)[n] \times (\operatorname{Pic}^0 C)[n] \to \mu_n,$$

where μ_n denotes the group of nth roots of unity in $k^\times$ (which we continue to assume is algebraically closed). In order to prove this, we need the Weil reciprocity law.

Theorem 24.20. *Let C/k be a smooth projective curve and let $f, g \in k(C)^\times$ be functions whose divisors have disjoint support. Then*

$$f(\operatorname{div} g) = g(\operatorname{div} f).$$

Proof. See [6, Ex. 2.11]. □

Lemma 24.21. *The value of the Weil pairing $e_n(D_1, D_2) \in k^\times$ depends only on the divisor classes of D_1 and D_2 and is an element of $\mu_n \subseteq k^\times$.*

Proof. Let $g \in k(C)^\times$ be any normalized function for which $\operatorname{div} g$ and D_1 have disjoint support, and let f_1 and f_2 be the normalized functions with $\operatorname{div} f_1 = nD_1$ and $\operatorname{div} f_2 = nD_2$. Then $f_1 g^n$ is the normalized function for $n(D_1 + \operatorname{div} g)$, and we have

$$\begin{aligned} e_n(D_1 + \operatorname{div} g, D_2) &= \frac{f_1(D_2) g^n(D_2)}{f_2(D_1 + \operatorname{div} g)} = \frac{f_1(D_2) g^n(D_2)}{f_2(D_1) f_2(\operatorname{div} g))} \\ &= \frac{f_1(D_2) g^n(D_2)}{f_2(D_1) g(\operatorname{div} f_2)} = \frac{f_1(D_2) g^n(D_2)}{f_2(D_1) g(nD_2)} \\ &= \frac{f_1(D_2) g^n(D_2)}{f_2(D_1) g^n(D_2)} = \frac{f_1(D_2)}{f_2(D_1)} = e_n(D_1, D_2). \end{aligned}$$

If the supports of $\operatorname{div} g$ and D_2 are disjoint, we similarly have $e_n(D_1, D_2+\operatorname{div} g) = e_n(D_1, D_2)$; thus $e_n(D_1, D_2)$ depends only on the divisor classes of D_1 and D_2. We also have

$$e_n(D_1, D_2)^n = \frac{f_1(D_2)^n}{f_2(D_1)^n} = \frac{f_1(nD_2)}{f_2(nD_1)} = \frac{f_1(\operatorname{div} f_2)}{f_2(\operatorname{div} f_1)} = 1,$$

so $e_n(D_1, D_2) \in \mu_n$ as claimed. □

Theorem 24.22. *Let n be a positive integer, let k be an algebraically closed field whose characteristic does not divide n, and let C/k be a smooth projective curve. Let D_1, D_2, D_3 denote divisors with disjoint support that represent n-torsion elements of $\operatorname{Pic}^0 C$. The Weil pairing $e_n \colon (\operatorname{Pic}^0 C)[n] \times (\operatorname{Pic}^0 C)[n] \to \mu_n$ satisfies:*

- *Bilinear: $e_n(D_1 + D_2, D_3) = e_n(D_1, D_3)e_n(D_2, D_3)$;*
- *Alternating: $e_n(D_1, D_2) = e_n(D_2, D_1)^{-1}$.*

Note that the two properties together imply that e_n is bilinear in both variables.

Proof. For $i = 1, 2, 3$ let f_i be the normalized function with $\operatorname{div} f_i = nD_i$. We then have

$$e_n(D_1 + D_2, D_3) = \frac{f_1(D_3)f_2(D_3)}{f_3(D_1)f_3(D_2)} = e_n(D_1, D_3)e_n(D_2, D_3),$$

and

$$e_n(D_1, D_2)e_n(D_2, D_1) = \frac{f_1(D_2)}{f_2(D_1)}\frac{f_2(D_1)}{f_1(D_2)} = 1,$$

so the alternating property holds. □

The Weil pairing has many other important properties that hold in general, but to simplify their presentation (and proofs), we now specialize to the case of an elliptic curve C.

24.5 The Weil pairing on an elliptic curve

For an elliptic curve E/k, the isomorphism $E \xrightarrow{\sim} \operatorname{Pic}^0 E$ given by the Abel-Jacobi map $P \mapsto [P] - [0]$ allows us to view the Weil pairing as a map

$$e_n \colon E[n] \times E[n] \to \mu_n$$

defined on pairs of n-torsion points of E/k (for n prime to the characteristic of k). At first glance it might appear that we have a problem, since for $P, Q \in E[n]$ the divisors $[P] - [0]$ and $[Q] - [0]$ do not have disjoint support, which we assumed in our definition of e_n.

But note that we can always use (1) to translate these divisors them to linearly equivalent divisors with disjoint support by picking some point $T \neq 0, Q, -P, Q - P$ and replacing $[P] - [0]$ with the linearly equivalent divisor $[P + T] - [T]$; this does not change the element of $\operatorname{Pic}^0 E$ represented by $[P] - [0]$ nor does it change the value of the Weil pairing, by Lemma 24.21.

For practical applications we want to be able to compute $e_n(P, Q)$ explicitly, and in a computationally efficient manner. For this purpose we use the following sequence of functions proposed by Miller [4].

Definition 24.23. 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 24.16.

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 24.24. *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 $n \geq 0$. 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

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

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 24.24 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 24.24 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 24.25. *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 lemma allows us to use the Miller functions to compute the Weil pairing.

Lemma 24.26. *Let E/k be an elliptic curve, let n be a positive integer not divisible by the characteristic of k, and let $P, Q \in E(k)[n]$. For any point $T \notin \{0, Q, -P, Q - P\}$ on E we have*

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

Proof. We have $\operatorname{div} G_{P,T} = [P] + [T] - [P+T] - [0]$, so the divisors $[P] - [0]$ and $[P+T] - [T]$ are linearly equivalent, and the hypotheses ensure that the divisors $[P+T] - [T]$ and $[Q] - [0]$ have disjoint support. Let f_1 be the normalized function with $\operatorname{div} f_1 = n[P - T] - n[-T]$ and let f_2 be the normalized function with $\operatorname{div} f_2 = n[Q] - n[0]$. Let $\tau \in k(E)^\times$ denote the translation morphism $E \to E$ defined by $R \mapsto R - T$ (so plug $-T$ into the formula for point addition on E, treating the coordinates of the other point as variables, to obtain the coordinate functions of τ; note that τ is a morphism of smooth projective curves but not an isogeny of elliptic curves because it maps 0 to $-T$). Composing $f_{n,P}$ with τ yields a map $E \to \mathbb{P}^1$ corresponding to an element of $k(E)^\times$ that we then normalize. Composition with τ shifts all the zeros and poles of $f_{n,P}$ by $-T$, which means that each point in the corresponding divisor gets shifted by $-T$. Using part (i) of Lemma 24.24 we compute

$$\operatorname{div}(f_{n,P} \circ \tau) = n[P - T] - (n - 1)[-T] - [nP - T] = n[P - T] - n[-T] = \operatorname{div} f_1,$$

since $nP = 0$, and $f_{n,P} \circ \tau$ is normalized, so $f_1 = f_{n,P} \circ \tau$. We also have

$$\operatorname{div} f_{n,Q} = n[Q] - (n - 1)[0] - [nQ] = n([Q] - [0]) = \operatorname{div} f_2,$$

since $nQ = 0$, and $f_{n,Q}$ is normalized, so $f_{n,Q} = f_2$. Thus by definition

$$e_n(P, Q) = \frac{(f_{n,P} \circ \tau)([Q] - [0])}{f_{n,Q}([P + T] - [T])} = \frac{f_{n,P}(Q - T)/f_{n,P}(-T)}{f_{n,Q}(P + T)/f_{n,Q}(T)} = \frac{f_{n,Q}(T) f_{n,P}(Q - T))}{f_{n,P}(-T) f_{n,Q}(P + T)}. \quad \square$$

Corollary 24.27. *Let E/k be an elliptic curve with distinct points $P, Q \in E(k)[n]$, where $n > 1$ is prime to the characteristic of k. Then*

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

Proof. See [4, Prop. 8]. □

Warning 24.28. The factor $(-1)^n$ is sometimes inadvertently omitted from this formula in the literature ([3, p. 387], for 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, the lemma and the corollary imply that if P and Q are k-rational n-torsion points, then $e_n(P,Q)$ is also k-rational.

When working with elliptic curves E/k with k not algebraically closed, for any integer n not divisible by the characteristic of k, we define $e_n(P,Q)$ for arbitrary $P,Q \in E[n]$ by simply working with the base-change of E to the field $k(E[n])$, the minimal field over which the n-torsion points of E are all defined (which is necessarily a Galois extension of k).

The following theorem gives a more complete list of the properties of the Weil pairing than given in Theorem 24.22.

Theorem 24.29. *Let E/k be an elliptic curve and let m and n be positive integers prime to the characteristic of k. The Weil pairing $e_n\colon E[n] \times E[n] \to \mu_n$ 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 $e_n(P,Q) = e_n(Q,P)^{-1}$;*
- *Non-degenerate: If $P \neq 0$ then $e_n(P,Q) \neq 1$ for some $Q \in E[n]$;*
- *Compatibility: $e_{mn}(P,Q) = e_n(mP,Q)$ for all $P \in E[mn]$ and $Q \in E[n]$;*
- *Galois-equivariant: $e_n(P^\sigma,Q^\sigma) = e_n(P,Q)^\sigma$ for all $\sigma \in \operatorname{Gal}(\bar{k}/k)$;*
- *Endomorphisms: $e_n(\alpha(P),\alpha(Q)) = e_n(P,Q)^{\deg \alpha}$ for all $\alpha \in \operatorname{End}(E)$;*
- *Surjective: for each $P \in E[n]$ we have $\{e_n(P,Q) : Q \in E[n]\} = \mu_m$, where $m = |P|$.*

Proof. We already proved the bilinearity and alternating properties in Theorem 24.22. For non-degeneracy and compatibility, see [4, Prop. 7], or [6, Prop. III.8.1]. Galois equivariance follows immediately from the explicit formula for $e_n(P,Q)$ given by Corollary 24.27: the formulas for $f_{n,P}$ and $f_{n,Q}$ are algebraic expressions that depend only on the coefficients of E, which are fixed by σ, and the points P and Q, so $f_{n,P^\sigma}(Q^\sigma) = f_{n,P}(Q)^\sigma$ and similarly, $f_{n,Q^\sigma}(P^\sigma) = f_{n,Q}(P)^\sigma$. See [7, Thm. 11.7] for a proof of the endomorphism compatibility.

Surjectivity follows from non-degeneracy. 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 $|P|$. On the other hand, if $e_n(P,Q)$ has order m greater than $e = |P|$ for any Q, then $e_n(eP,Q) = e_n(0,Q) \neq 1$, which is a contradiction, because $e_n(0,Q) = e_n(0,Q)e_n(Q,Q) = e_n(Q+0,Q) = e_n(Q,Q) = 1$, by the alternating property. □

Corollary 24.30. *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 24.31. *Let E/k be an elliptic curve and let n be a positive integer prime to the characteristic of k. For any points $P, Q \in E[n]$ the order of $e_n(P,Q)$ is the largest m for which $E[m] \subseteq \langle P, Q\rangle$. In particular, $e_n(P,Q) = 1$ if and only if $\langle P, Q\rangle$ is cyclic.*

Proof. Assume without loss of generality that $|P| \geq |Q|$. For some integer c we have $\langle P, Q\rangle = \langle P, Q + cP\rangle$ with $|Q + cP| = m$. We then have

$$e_n(P, Q + cP) = e_n(P,Q)e_n(P,cP) = e_n(P,Q)e_n(P,P)^c = e_n(P,Q),$$

so without loss of generality we can assume Q has order m. Let $a > 0$ be the least integer for which aP has order m, so that $\langle aP, Q\rangle = E[m]$. By surjectivity, $e_n(aP,Q) = e_n(P,Q)^a$ has order m, so m divides the order of $e_n(P,Q)$. On the other hand,

$$1 = e_n(P,0) = e_n(P,mQ) = e_n(P,Q)^m,$$

so the order of $e_n(P,Q)$ divides m and the two are equal. □

24.6 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 [4], 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 [3]. 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 §24.8 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 μ_n either. 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.

24.7 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 $E[n]$ or 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 24.32. 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 $E[n] \subseteq \mathbb{F}_{q^k}$ 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 24.33. *Let $E/\mathbb{F}_q$ be an elliptic curve, let $n \perp q$ be a prime divisor of $\#E(\mathbb{F}_q)$, and let π_n denote the restriction of the Frobenius endomorphism π_E to $\mathrm{End}(E[n]) \simeq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. 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 $\mathrm{End}(E[n])$. If $q \equiv 1 \bmod n$ then π_E acts trivially on $E[n]$ and $E[n] \subseteq E(\mathbb{F}_q)$; otherwise $\pi_n \in \mathrm{End}(E[n]) \simeq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ 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 $\pi_n^k(P) = q^k(P) = P$, 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 24.33 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 must 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 difficultly of the discrete logarithm problems in $E(\mathbb{F}_q)$ and $\mathbb{F}_q^\times$; for $q \approx 2^{256}$ using $k = 12$ yields $\#\mathbb{F}_q^\times \approx 2^{3072}$, 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 [2] 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 $\#E(\mathbb{F}_q)$.

24.8 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 24.34. 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 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 24.33 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] D. Boneh and M. Franklin, *Identity-based encryption from the Weil pairing*, Siam Journal of Computing **32** (2003), 586–615.

[2] D. Freeman, M. Scott, and E.J. Teske, *A taxonomy of pairing-friendly elliptic curves*, J. Cryptology **23** (2010), 224-280.

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

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

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

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

[7] L.C. Washington, *Elliptic Curves: Number Theory and Cryptography*, second edition, Chapman and Hall/CRC, 2008.

18.783 Elliptic Curves
Spring 2017