24 Divisors and the Weil pairing

In this lecture we address a 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 (most of what we need it is summarized in the first two chapters of [5]).

24.1 Valuations on the function field of a curve

Let C/k be a smooth projective curve defined by a homogeneous polynomial $f(x,y,z)=0$ 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 $h\notin(f)$, modulo the equivalence relation

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

Alternatively, we can view the function g/h as a rational map $(g:h)$ from C to $\mathbb{P}^1$. The fact that C is a smooth curve 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 in Theorem 5.10 which we will prove below. This implies that although a particular choice of representative g_1/h_1 might not be defined at at point P (this occurs when $g_1(P)=h_1(P)=0$, since in this case $(g_1(P):h_1(P))$ does not define 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 at infinity $(0:1:0)$, where we get $(0:0)$. But the maps

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

all correspond to the same function in $k(E)$, and the last one sends $(0:1:0)$ to $(1:0)\in\mathbb{P}^1$, which is defined (and any other representative that is defined at $(0:1:0)$ must agree). We should note the 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 will often be no single representative in $k(x,y,z)$ of a function in $k(E)$ that is defined at every point, even though the function itself is.

[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 we will discuss in this section applies to any smooth projective (geometrically integral) curve.

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 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 by suitable powers of z to put it in the form g/h.

Definition 24.3. For any point $P \in C(k)$, we define the *local ring*

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

(here $\infty = (1 : 0) \in \mathbb{P}^1$).

Each local ring $\mathcal{O}_P$ is a principal ideal domain with a unique maximal ideal

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

(this follows from the fact that the coordinate ring $k[C]$ is a Dedekind domain, just like the ring of integers of a number field). Any generator u_P of $\mathfrak{m}_P$ is called a *uniformizer* at P.

Definition 24.4. A *discrete valuation* of a field F is a surjective homomorphism $v\colon F^\times \to \mathbb{Z}$ satisfying

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

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 principal ideal domain (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 $v(u) = 1$ is generates $\mathfrak{m}$ and is called a *uniformizer* for $\mathfrak{m}$.

Conversely, given a principal ideal domain R with a unique nonzero maximal ideal $\mathfrak{m} = (u)$, we can define a discrete valuation of 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 all discrete valuation rings with 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 $r \in k(C)$ at P (indeed, one can formally expand r as a Laurent series in any uniformizer u_P for m_P, and the degree of its least nonzero term will be $v_P(r)$, just as we did for 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 base change to $\bar{k}$ (which is effectively what is done in [5]), but a more general 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 (note: $\bar{k}$ is separable because we do assume k is perfect, even if it isn't algebraically closed). Each closed point is a finite subset of $C(\bar{k})$ whose cardinality we denote $\deg P$, this is equal to 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 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 $r \in k(C)$ at a closed point P; the result is a closed point $r(P)$ of $\mathbb{P}^1(k)$ (because $r \in k(C)$ is, by definition, Galois invariant). The point ∞ is always rational, so our definition of the local ring $\mathcal{O}_P$ still applies, and we get the same maximal ideal m_P.

Now that we understand the valuations v_P and uniformizers u_P associated to each point P of a smooth projective curve we can easily prove Theorem 5.11.

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

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

For the function y we have

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

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 $r \in k(C)$ we always have have $\sum_P v_P(r) = 0$ (see below), so every function in $k(C)$ has the same number of zeros and poles and if we know all the zeros (and their orders) and there is only one pole, then we know the order of the pole.

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

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

where $r^*\colon k(\mathbb{P}^1) \to k(C)$ is the morphism of function fields that sends $s \in k(\mathbb{P}_1)$ to the function $s \circ r$ in $k(C)$; for $r \in k^\times$ the convention is to define $\deg r = 0$. But 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. But whenever we have $r(P) = Q \in \mathbb{P}^1$ and the size of the preimage $r^{-1}(Q)$ is the same as the degree of r as a morphism (which happens for all but finitely many Q), then no ramification occurs and if $Q = 0$ or $Q = \infty$ then r 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 the correct multiplicity, every fiber of the morphism $r\colon C \to \mathbb{P}^1$ has the same size, equal to the degree of r.

Theorem 24.9. *Let C be a smooth projective curve over an algebraically closed field k and let $r \in k(C)^\times$ be an element of its function field (viewed as a morphism $r\colon C \to \mathbb{P}^1$). For every point $Q \in \mathbb{P}^1(k)$ we have*

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

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 [5]. □

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 $v_P(u_Q \circ r)$ 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 $r \in k(C)^\times$ we have*

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

and $v_P(r) = 0$ for all but finitely many P; moreover, $v_P(r) = 0$ for all P if and only if $r \in k^\times$.

Proof. We have $v_P(r) \neq 0$ only when $r(P) = 0$ or $r(P) = \infty$. Applying Theorem 24.9 to $Q = 0$ using the uniformizer $u_0 = t$ yields

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

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

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

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

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

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

which holds for any closed point Q of $\mathbb{P}^1/k$; the formula in Corollary 24.10 becomes

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

where the sum is over closed points P (note that $\deg 0 = \deg \infty = 1$).

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 assume 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

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

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

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

which is called a *principal* divisor. Because each $v_P\colon k(C) \to \mathbb{Z}$ 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 then $\deg D := \sum_P v_P(D) \deg P$.

Remark 24.15. There is a direct analogy between the Picard group of a curve C, and the ideal class group of a number field K. Both fields are the fraction field of a Dedekind domain: the coordinate ring $k[C]$ of the curve and the ring of integers $\mathcal{O}_K$ of the number field. In both cases we can consider the free abelian group over the set of nonzero prime ideals, in the case of the curve C, these are the maximal ideals m_P associated to each point. There is also a valuation associated to each prime ideal, in the case of $\mathcal{O}_K$, it is the exponent appearing in the factorization of an ideal into prime ideals. For the curve C we get the (additive) group of divisors, and for the number field K we get the (multiplicative) group of invertible fractional ideals. The principal ideals of $\mathcal{O}_K$ form a subgroup of the ideal group that corresponds to the subgroup of principal divisors in the divisor group, and the corresponding quotients are the ideal class group $\operatorname{cl}(\mathcal{O}_K)$ and the Picard group $\operatorname{Pic} C$; indeed the class group $\operatorname{cl}(\mathcal{O}_K)$ is written as $\operatorname{Pic} \mathcal{O}_K$ in some texts (and $\operatorname{Pic} C$ is written as $\operatorname{cl}(C)$ in others). You might think that the analogy breaks down because for functions $f \in k(C)$ we have sum $\sum_P v_P(f) = 0$ and this does not appear to be true for generators of principal ideals in $\mathcal{O}_K$, but in fact it is true if we include *all* the valuations of K not just that come from prime ideals of $\mathcal{O}_K$ (the others come from embeddings of K into $\mathbb{R}$ or $\mathbb{C}$).

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, $\operatorname{Pic}^0 C$ 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 $\mathrm{Pic}^0 C$ that is isomorphic to $\mathrm{Pic}^0 C$ 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 distinguish point 0 and the group law that makes it an abelian variety.

Definition 24.16. Let C/k be a smooth projective curve with a rational point $0 \in C(k)$; The *Abel-Jacobi map* is the map $C(k) \to \mathrm{Pic}^0 C$ 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 $g \leq 1$ and it is injective if and if only if $g \geq 1$. As usual $g = 1$ is the sweet spot, and we will prove in the next section that for curves of genus 1 with a rational point (i.e. elliptic curves), the Abel-Jacobi map is an isomorphism.

24.3 The Jacobian of an elliptic curve

Definition 24.17. 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 $P = Q$. So for example if $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ are distinct affine points we would have $L_{P,Q} = (y - y_1)(x_2 - x_1) - (x - x_1)(y_2 - y_1)$, which has zeros at P, Q, and $-(P + Q)$, but we are now thinking of it as map $E \to \mathbb{P}^1$ that we can evaluate at any point R on the curve E; note that $L_{P,Q}(R)$ will be nonzero except when $R \in \{P, Q, -(P + Q)\}$. Now define

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

The motivation for this definition is that $G_{P,Q}$ in some sense captures the geometric definition of the group law: 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 precisely 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), and 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

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

We can then compute

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

Since $\operatorname{div} G_{p,q}$ is a principal divisor, it follows that $[P]+[Q]$ and $[P+Q]+[0]$ are equivalent in $\operatorname{Pic}^0 E$. In order to keep things clear we will write

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

to denote this.

Theorem 24.18. *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

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

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 $\operatorname{Pic}^0 E$. Separating D into sums with $n_P>0$ and $n_P<0$, we can write

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

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. 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 $\sum n_P = 0$. 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 $[P]-[0]$, where $P=Q-R$. We can assume $P \neq 0$ (otherwise we are done). Let $t \in k(C)^\times$ be a function with $\operatorname{div} t = [P]-[0]$.

For any function $f \in k(C)^\times$, define

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

If f does not have a zero or pole at 0, then f and t have the same divisor and f is a rational function of t (note that $\operatorname{div} f - \operatorname{div} t = 0$ implies $f/t \in k^\times$). 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. □

24.4 The Weil pairing

Although we are ultimately interested in defining the Weil pairing as a function whose inputs are torsion points on an elliptic curve, in order to establish some of its properties it is convenient to work in greater generality. 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 24.19. 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 we note 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 24.20. 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 24.21. *Let C/k be a smooth projective curve and let $f, g \in k(C)^\times$ be functions whose divisors have disjoint support. Then*

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

Proof. See [5, Ex. 2.11]. □

Lemma 24.22. *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 nth root of unity in $k^\times$.*

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

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

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

To show that $e_n(D_1, D_2)$ is an nth root of unity, let f_1 and f_2 be the normalized functions with $\mathrm{div} f_1 = nD_1$ and $\mathrm{div} f_2 = nD_2$. We then have

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

Theorem 24.23. *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 $\mathrm{Pic}^0 C$. The Weil pairing $e_n \colon (\mathrm{Pic}^0 C)[n] \times (\mathrm{Pic}^0 C)[n] \to \mu_n$ has the following properties:*

- *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 $\mathrm{div} f_i = nD_i$. For bilinearity we 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

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

implies the alternating property. □

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

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 not divisible by 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 is assumed in our definition of e_n. But we can use (1) to translate them to equivalent divisors with disjoint support by picking some point T and replacing $[P] - [0]$ with $[P + T] - [T]$. In particular, this also allows us to compute $e_n(P, P)$, which by the alternating property must be equal to 1, since $e_n(P, P) = e_n(P, P)^{-1}$.

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 will use the following sequence of functions proposed by Miller [3].

Definition 24.24. 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 24.17.

We assume that the line functions $L_{P,Q}$ are all normalized (they just need to correspond to the lines $\overline{PQ}$, which remains true under after re-scaling). This implies that the functions $G_{P,Q}$ are also normalized, as are the functions $f_{n,P}$.

Lemma 24.25. *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

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

For the inductive step,

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

as desired, and also

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

which proves (i).

For (ii) we use (i) to compute

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

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

For (iii) we similarly use (i) to compute

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

and apply the same argument to conclude the first equality in (iii). The second equality is proved in the same way. □

The key part of Lemma 24.25 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. For practical applications it is generally never necessary to actual compute the functions $f_{n,P}$ explicitly, we only need to be able to evaluate them at points. Lemma 24.25 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 each $G_{aP,bP}(Q)$ boils down to evaluating the line functions $L_{aP,bP}$ and $L_{aP+bP,-(aP+bP)}$ at Q, which reduces to a group operation in $E(k)$ to compute the coordinates of the point $aP+bP$ and $O(1)$ operations in k. Since each group operation in $E(k)$ involves just a constant number of field operations, we obtain the following corollary,

Corollary 24.26. *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.*

Lemma 24.27. *Let n be a positive integer and let k be a field whose characteristic does not divide n. Let E/k be an elliptic curve with points $P, Q \in E(k)[n]$, and suppose $T \in E(k)$ is not equal to $-P$, Q, $Q-P$, or 0. Then*

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

Proof. We have $\operatorname{div} G_{P,T} = [P]+[T]-[P+T]-[0]$, so the divisors $[P]-[0]$ and $[P+T]-[T]$ are 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 $\operatorname{div} f_2 = n[Q] - n[0]$. If we let $\tau_{-T} \in k(C)^\times$ denote the normalized translation morphism $R \mapsto R - T$, then

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

and $f_{n,P} \circ \tau_{-T}$ is normalized, so $f_1 = f_{n,P} \circ \tau_{-T}$. 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

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

Corollary 24.28. *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 [3, Prop. 8]. □

Warning 24.29. The factor $(-1)^n$ is sometimes inadvertently omitted from this formula in the literature ([2, 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 24.23.

Theorem 24.30. *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 $e_n(P,Q+R) = e_n(P,R)e_n(Q,R)$;*
- *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 24.23. For non-degeneracy and compatibility, see [3, Prop. 7], or [5, Prop. III.8.1]. Galois equivariance follows immediately from the explicit formula for $e_n(P,Q)$ given by Corollary 24.28: 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 [6, 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 24.31. *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 24.32. *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 Practical applications of the Weil pairing

There are many practical 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 [3], and a method for transferring the discrete logarithm problem on an elliptic curve $E/\mathbb{F}_q$ to the multiplicative group of of a (typically much larger) extension of $\mathbb{F}_q$, namely, the extension $\mathbb{F}_{q^e}$ 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 enormous (with e exponential in $\log q$), but when this is not the case it may be easier to solve the discrete logarithm problem in $\mathbb{F}_{q^e}^\times$ rather than $E(\mathbb{F}_q)$.

The most important practical application is *pairing-based cryptography*, a topic that we unfortunately do not have time to address in any detail, but we will give a simple example: a one round tripartite Diffie-Hellman key exchange, due to Joux [2].

We assume Alice, Bob, and Carol, the three participants in the protocol all know an elliptic curve $E/\mathbb{F}_q$ and two independent n-torsion points P and Q in $E(\mathbb{F}_q)[n]$. They want to agree on a random secret, and they would like to do this with a single round of messaging; this means that each participant simultaneously broadcasts information to the two others, but no one one is allowed to hear from another participant before they decide what information to send.

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 both Bob and Carol, Bob sends $P_B := bP$ and $Q_B := bQ$ to both Alice and Carol, and Carol sends $P_C := cP$ and $Q_C := cQ$ to both Alice and Bob. Assuming that the discrete logarithm problem is hard, an eavesdropper cannot determine any of a, b, c from the knowledge of any of the broadcast points, even if they know P and Q (which we assume everyone knows).

Alice then computes

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

Bob similarly 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, and under the further assumption that the computational Diffie-Hellman problem[2] is hard, an eavesdropper cannot easily determine this value from the publicly broadcast information. It is not known whether the computational Diffie-Hellman problem is strictly as difficult as the discrete logarithm problem, but this is believed to be so.

This example was one of the early indications that pairings could be practically useful in cryptography, because it enabled protocols that no one previously knew how to implement efficiently. But the floodgates really opened with the seminal paper of Boneh and Franklin [1], which showed that identity-based cryptography could be efficiently realized using the Weil pairing (and variants thereof). The concept of identity-based cryptography was originally proposed much earlier [4], but it was only with the advent of protocols that use pairings on elliptic curves that an efficient realization of these ideas became possible.

References

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

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

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

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

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

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

[2] This is the problem of computing abP, given P, aP, and bP; this can clearly be solved efficiently given an oracle for the discrete logarithm problem, but the converse is not known.

18.783 Elliptic Curves

Spring 2015