WEIL PAIRING

LALIT JAIN

1. Weil Reciprocity

This article will discuss the Weil Pairing as presented in [1]. Throughout the following we will adopt the notation in the reference given above. Our goal will be to equate the definition of the Weil Pairing given in exercise 3.16. with the definition give in section 8 of chapter 3.

One of the key tools we will use in our study of the Weil pairing is that of Weil reciprocity.

First we need to define the *tame pairing*:

Definition 1.1. Given an elliptic curve E, the tame pairing of $f, g \in \bar{K}(E)$ at point $P \in E$ is

$$\langle f, g\rangle_P = (-1)^{\mathsf{ord}_P f \mathsf{ord}_P g} \frac{f^{\mathsf{ord}_P g}(P)}{g^{\mathsf{ord}_P f}(P)}.$$

It is easy to see that the tame symbol satisfies the following properties

1. Unless f, g have a zero or pole at P, $\langle f, g\rangle_P = 1$.
2. If $\mathsf{ord}_P f = 0$ then $\langle f, g\rangle_P = f(P)^{\mathsf{ord}_P g}$.
3. Similarly if $\mathsf{ord}_P g = 0$ then $\langle f, g\rangle_P = g(P)^{-\mathsf{ord}_P f}$.

Theorem 1.2 (Strong Weil Reciprocity)**.** *Let E be an elliptic curve and let $f, g \in \bar{K}(E)$ then*

$$\prod_{R \in E} \langle f, g\rangle_R = 1.$$

The proof of this result is rather involved so we refer the reader to [2].

For a function $f \in \bar{K}(E)$ and a divisor $D = \sum n_p\,(P)$, such that f has no zeros or poles on the support of D define

$$f(D) = \prod_{P \in E} f(P)^{n_P}.$$

Then strong Weil reciprocity implies the following

Theorem 1.3 (Weak Weil Reciprocity)**.** *Let E be an elliptic curve and let $f, g \in \bar{K}(E)$ whose divisors have disjoint support. Then*

$$f(\mathit{div}(g)) = g(\mathit{div}(f))$$

Proof. By strong Weil reciprocity

$$\prod_{R \in E} \langle f, g\rangle_R = 1.$$

The terms in this product are 1 except when f or g has a pole. If f has a pole or zero at R then $\langle f, g\rangle_R = g(R)^{-\mathsf{ord}_R f}$ and if g has a pole or zero at R then $\langle f, g\rangle_R = f(R)^{\mathsf{ord}_R g}$ since the divisors of f and g have disjoint supports.

Thus we see that by taking the product over all points in E,

$$\prod_{R\in E} g(R)^{\mathsf{ord}_R f} = \prod_{R\in E} f(R)^{\mathsf{ord}_R g}.$$

Dividing by the left hand side yields the result. □

For an algebraiuc number theory analogy, Weil reciprocity is a statement about the decomposition of the norm map under extensions of valuations. Ask David about this....

2. Definition of Weil Pairing

In the following we will make extensive use of the following theorem:

Theorem 2.1. *Let E be an elliptic curve and $D = \sum n_p\,(P) \in Div(E)$. Then D is principal if and only if $\sum n_p = 0$ and $\sum [n_p]\,P = 0$.*

Given $P, Q \in E\,[m]$ choose degree zero divisors $D_p \sim (P) - (0)$ and $D_q \sim (Q) - (0)$ with disjoint support. By the theorem above we can find $f_p, f_q \in \bar{K}(E)$ such that $\mathsf{div}\,(f_p) = mD_p$ and similarly $\mathsf{div}\,(f_q) = mD_q$. Note that $\mathsf{div}\,(f_q)$ and $\mathsf{div}\,(f_p)$ have disjoint support.

Definition 2.2 (First Weil Pairing)**.** In the situation above let

$$e_m\,(P, Q) = \frac{f_P(D_q)}{f_P(D_p)}.$$

To see that this pairing is well defined choose another divisor of degree zero, $D \sim D_p$ which has disjoint support from D_Q. Then for some $f \in \bar{K}(E)$, $D = D_p + \mathsf{div}\,(f)$. In the construction of $e_m\,(P, Q)$ we need to construct a function f'_P such that $\mathsf{div}\,(f'_P) = mD$ so with some easy calculation we see that $\mathsf{div}\,(f'_P) = \mathsf{div}\,(f_P f^m)$. Thus up to scaling by a constant $f'_P = f^m f_P$ and

$$\begin{aligned}
\frac{f'_P(D_q)}{f_P(D)} &= \frac{f^m(D_q) f_P(D_q)}{f_Q(D)} \\
&= \frac{f(mD_q) f_P(D_q)}{f_Q(D_p + \mathsf{div}\,(f))} \\
&= \frac{f(\mathsf{div}\,(f_Q)) f_P(D_q)}{f_Q(D_p) f_Q(\mathsf{div}\,(f))} \\
&= \frac{f(\mathsf{div}\,(f_Q)) f_P(D_q)}{f_Q(D_p) f(\mathsf{div}\,(f_Q))} \\
&= \frac{f_P(D_q)}{f_Q(D_p)} \\
&= e_m\,(P, Q)
\end{aligned}$$

so we see $e_m\,(P, Q)$ is well defined due to weak Weil reciprocity. The constant appearing in $f'_P = f^m f_P$ does not matter since for any divisor of degree zero, $D = \sum n_p\,(P)$, and any constant c

$$\prod_{P\in E} c^{n_p} = 1.$$

The Weil pairing produces m-th roots of unity, indeed

$$\begin{aligned} e_m(P,Q)^m &= \frac{f_P(D_q)^m}{f_Q(D_p)^m} \\ &= \frac{f_P(mD_q)}{f_Q(mD_p)} \\ &= \frac{f_P(\mathsf{div}\,(f_Q))}{f_Q(\mathsf{div}\,(f_p))} \\ &= \frac{f_P(\mathsf{div}\,(f_Q))}{f_P(\mathsf{div}\,(f_Q))} \\ &= 1 \end{aligned}$$

where we have employed weak Weil reciprocity.

To justify the use of the word 'pairing' [1] shows that $e_m(P,Q)$ is bilinear, alternating, non-degenerate, Galois invariant, and compatible with multiplication by m maps.

We now give an alternate definition of the Weil pairing. Given $P \in E[m]$ by employing theorem above, we can find a function $f \in \bar{K}(E)$ with $\mathsf{div}\,(f) = m(P) - m(O)$ and a point P' such that $[m]P' = P$. Again employing theorem blah, we can find a function $g \in \bar{K}(E)$ so that

$$\mathsf{div}\,(g) = [m]^*(P) - [m]^*(O) = \sum_{R \in E[m]} (P' + R) - (R).$$

(This simplify follows from the definition of $[m]^*$.) Now

$$\begin{aligned} \mathsf{div}\,(f \circ [m]) &= \mathsf{div}\left([m]^* f\right) \\ &= [m]^*\,\mathsf{div}\,(f) \\ &= [m]^*\,(m(P) - m(O) \\ &= \mathsf{div}\,(g^m) \end{aligned}$$

so we can assume that up to a constant $f \circ [m] = g^m$.

Now given some other point $S \in E[m]$, for any point $X \in E$,

$$g(X+S)^m = f([m]X + [m]S) = f([m]X) = g(X)^m.$$

Since this is true for all X we see that we the following definition is well defined:

Definition 2.3 (Second Weil Pairing)**.** In the situation above let

$$\tilde{e}_m(P,Q) = \frac{g(X+P)}{g(X)}.$$

Note that the dependence on Q came from g, also even though g was defined relative to $f \circ [m]$ up to a constant, that constant is irrelevant due to the quotient.

3. Equivalence of First and Second Weil Pairing

To prove the equivalence of the first and second definitions of Weil pairing we will make heavy use of theorem 1.2. In particular we will demonstrate the following:

Theorem 3.1. *Given an elliptic curve E and $P, Q \in E[m]$,*

$$\tilde{e}_m(P,Q) = (-1)^m e_m(P,Q).$$

In [1], the factor of $(-1)^m$ is missing. Exercise 3. 16 also suggests that there is a proof of the result using weak Weil reciprocity. We were unable to find such a proof, thus an argument using strong Weil reciprocity which is presented in [2] is given. However an erroneous proof (possibly modifiable to prove the theorem?) of the result is also given.

Now to the races.

Proof of Theorem 1. First we will show that

$$\tilde{e}_m\left(P,Q\right) = (-1)^m \frac{f_P(Q)}{f_Q(P)}\frac{f_Q(O)}{f_P(0)}.$$

Let g_P be the function such that

$$\mathsf{div}\left(g_P\right) = \left[m\right]^*\left(P\right) - \left[m\right]^*\left(O\right)$$

respectively we construct g_Q for Q. Let h be the function such that

$$\mathsf{div}\left(h\right) = \left(m-1\right)\left(Q'\right) + \left(Q'-Q\right) - m\left(O\right)$$

where $\left[m\right]Q' = Q$. Recall that $g_P^m = f_P \circ \left[m\right]$ and $g_Q^m = f_Q \circ \left[m\right]$.

By strong Weil reciprocity

$$\prod_{R\in E}\langle g_P, h\rangle_R = 1.$$

However by the properties of the tame symbol given above the only nontrivial contributions to this product come from zeros and poles of g_P and h namely $Q', Q'-Q$ and $R, P'-R$ where $\left[m\right]P' = P$ and R varies over all elements of $E\left[m\right]$. Again using the properties of the tame symbol we can immediately see,

$$\langle g_P, h\rangle_{Q'} = g_P^{m-1}(Q')$$

and

$$\langle g_P, h\rangle_{Q'-Q} = g_P(Q'-Q).$$

Thus

$$\begin{aligned}\langle g_P, h\rangle_{Q'}\langle g_P, h\rangle_{Q'-Q} &= g_P(Q'-Q)g_P^{m-1}(Q') \\ &= \frac{g_P(Q'-Q)}{g_P(Q')}g_P^m(Q') \\ &= \frac{f_P(Q)}{\tilde{e}_m\left(P,Q\right)}\end{aligned}$$

where we have used $X = Q'+Q$ in the second definition of the Weil pairing.

To proceed we analyze the function

$$\Omega(X) = \prod_{R\in E[m]} h(R+X).$$

Firstly note that

$$\begin{aligned}
\mathsf{div}\,(\Omega) &= \sum_{R\in E[m]} \tau_R^*(\mathsf{div}\,(h)) \\
&= \sum_{R\in E[m]} \tau_R^*((m-1)\,(Q') + (Q'-Q) - m\,(O)) \\
&= \sum_{R\in E[m]} (m-1)\,(Q'-R) + (Q'-Q-R) - m\,(-R) \\
&= \sum_{R\in E[m]} m\,(Q'+R) - m\,(R) \\
&= \mathsf{div}\,(g_Q) = \mathsf{div}\,(f_Q \circ [m])\,.
\end{aligned}$$

To go from step 3 to step 4 we used the fact that $Q'-R$ and $Q'-Q-R$ range over the same sets as R ranges over $E\,[m]$. Thus we can see (again up to a constant that is ignorable) $\Omega = g_Q^m = f_Q \circ [m]$. By using the properties of the tame symbol we are now in a position where we can consider the zeros and poles of g_P.

$$\begin{aligned}
\prod_{R zero of g_P} \langle g_P, h\rangle_S &= \prod_{R\in E[m]} \frac{1}{h(P'+T)} \\
&= \frac{1}{\Omega(P')} = \frac{1}{f_Q(P)}
\end{aligned}$$

$$\begin{aligned}
\prod_{R pole of g_P} \langle g_P, h\rangle_S &= \left(\prod_{R\in E[m]\setminus O} h(T)\right) \langle g_P, h\rangle_O \\
&= \left(\prod_{R\in E[m]\setminus O} h(T)\right) (-1)^m \frac{g_P^{-m}(0)}{h^{-1}(P)} \\
&= H(0)(-1)^m g_P^{-m}(0) \\
&= (-1)^m \frac{f_Q(O)}{f_P(O)}.
\end{aligned}$$

Combining this all together gives that,

$$\begin{aligned}
1 &= \langle g_P, h\rangle_{Q'} \langle g_P, h\rangle_{Q'-Q} \prod_{R\in E} \langle g_P, h\rangle_R \prod_{R \text{ zero of } g_P} \langle g_P, h\rangle_S \\
&= \prod_{R \text{ pole of } g_P} \langle g_P, h\rangle_S \\
&= \frac{f_P(Q)}{\tilde{e}_m\,(P,Q)} \frac{1}{f_Q(P)} (-1)^m \frac{f_Q(O)}{f_P(O)}.
\end{aligned}$$

To finish proving the theorem we need the following result:

Lemma 3.2. *For $T \in E\,[m]$*

$$e_m\,(P,Q) = \frac{f_P(Q-T)f_Q(T)}{f_Q(P+T)f_P(-T)}$$

Proof. It suffices to note that $(P)-(O) \sim (P+T)-(T)$. Then $(Q)-(O)$ is disjoint from $(P+T)-(T)$ and if f_1 is such that $\mathsf{div}\,(f_1) = m((P+T)-(T))$ then

$$e_m\,(P,Q) = \frac{f_1(Q)f_Q(T)}{f_Q(P+T)f_P(O)}$$

however $\mathsf{div}\,(f_1) = \mathsf{div}\,(f_1 \circ \tau_T)$ from which the result follows. □

So for fixed $P, Q \in E\,[m]$

$$F(T) = \frac{f_P(Q-T)f_Q(T)}{f_Q(P+T)f_P(-T)}$$

is constant for all but finitely many $T \in E$. In particular F is simply a rational function, thus if char $K = 0$ we see that as $T \to O$, $F(T) \to F(O)$ and in particular

$$e_m\,(P,Q) = \frac{f_P(Q)f_Q(O)}{f_Q(P)f_P(O)}.$$

From this we see that the result follows. If char $K \neq 0$ then we have to make use of the formal group of the Elliptic curve. A proof using the Tate curve should also be possible, however we simply refer the reader to [3].

□

To conclude we will outline a possible erroneous proof of exercise 3.16 in [1]. Let g_P and h be defined as in the above proof. If we erroneously assume that we can apply weak Weil reciprocity ($\mathsf{div}\,(g_P)$ and $\mathsf{div}\,(h)$ do not have disjoint divisors) then

$$g_P(Q')^{m-1}g_P(Q'-Q)g_P(O)^{-m} = \prod_{R \in mgp} h(R+P')h(R)^{-1}.$$

These are quantities which have been computed above, so substituting gives

$$\tilde{e}_m\,(P,Q) = \frac{f_P(Q)f_Q(O)}{f_Q(P)f_P(O)} = e_m\,(P,Q,.)$$

There might be a way to alter this proof by considering the divisor of $\tau_T \circ g_P$ by some $T \in E\,[m]$ which has disjoint support from $\mathsf{div}\,(h)$. However the computations become rather complicated and careful consideration of the norm map is required. However it is an avenue for further exploration.

References

[1] Joseph H. Silverman. The Arithmetic of Elliptic Curves.

[2] Leonard Charlap and Raymond Coley. An Elementary Introduction to Elliptic Curves, II. http://www.idaccr.org/reports/er34.ps, July 1990.

[3] Miller, Victor S. The Weil pairing, and its efficient calculation. J. Cryptology 17 (2004), no. 4, 235–261.