

Weil Pairing - study

arnaucube

August 2022

Abstract

Notes taken from [Matan Prasma](#) math seminars and also while reading about Bilinear Pairings. Usually while reading papers and books I take handwritten notes, this document contains some of them re-written to *LaTeX*.

The notes are not complete, don't include all the steps neither all the proofs. I use these notes to revisit the concepts after some time of reading the topic.

Contents

1	Rational functions	1
1.1	Zeros, poles, uniformizers and multiplicities	2
2	Divisors	3
3	Weil reciprocity	4
4	Generic Weil Pairing	5
5	Properties	6
6	Exercises	6

1 Rational functions

Let E/\mathbb{k} be an elliptic curve defined by: $y^2 = x^3 + Ax + B$.

set of polynomials over E : $\mathbb{k}[E] := \mathbb{k}[x, y]/(y^2 - x^3 - Ax - B = 0)$
we can replace y^2 in the polynomial $f \in \mathbb{k}[E]$ with $x^3 + Ax + B$

canonical form: $f(x, y) = v(x) + yw(x)$ for $v, w \in \mathbb{k}[x]$

conjugate: $\bar{f} = v(x) - yw(x)$

norm: $N_f = f \cdot \bar{f} = v(x)^2 - y^2 w(x)^2 = v(x)^2 - (x^3 + Ax + B)w(x)^2 \in \mathbb{K}[x] \subset \mathbb{K}[E]$

we can see that $N_{fg} = N_f \cdot N_g$

set of rational functions over E : $\mathbb{K}(E) := \mathbb{K}[E] \times \mathbb{K}[E] / \sim$

For $r \in \mathbb{K}(E)$ and a finite point $P \in E(\mathbb{K})$, r is *finite* at P iff

$$\exists r = \frac{f}{g} \text{ with } f, g \in \mathbb{K}[E], \text{ s.t. } g(P) \neq 0$$

We define $r(P) = \frac{f(P)}{g(P)}$. Otherwise, $r(P) = \infty$.

Remark: $r = \frac{f}{g} \in \mathbb{K}(E)$, $r = \frac{f}{g} = \frac{f \cdot \bar{g}}{g \cdot \bar{g}} = \frac{f \bar{g}}{N_g}$, thus

$$r(x, y) = \frac{(f \bar{g})(x, y)}{N_g(x, y)} = \underbrace{\frac{v(x)}{N_g(x)} + y \frac{w(x)}{N_g(x)}}_{\text{canonical form of } r(x, y)}$$

degree of f : Let $f \in \mathbb{K}[E]$, in canonical form: $f(x, y) = v(x) + yw(x)$,

$$\deg(f) := \max\{2 \cdot \deg_x(v), 3 + 2 \cdot \deg_x(w)\}$$

For $f, g \in \mathbb{K}[E]$:

- i. $\deg(f) = \deg_x(N_f)$
- ii. $\deg(f \cdot g) = \deg(f) + \deg(g)$

Def 1.1. Let $r = \frac{f}{g} \in \mathbb{K}(E)$

- i. if $\deg(f) < \deg(g)$: $r(0) = 0$
- ii. if $\deg(f) > \deg(g)$: r is not finite at 0
- iii. if $\deg(f) = \deg(g)$ with $\deg(f)$ even:
 f 's canonical form leading terms ax^d
 g 's canonical form leading terms bx^d
 $a, b \in \mathbb{K}^\times$, $d = \frac{\deg(f)}{2}$, set $r(0) = \frac{a}{b}$
- iv. if $\deg(f) = \deg(g)$ with $\deg(f)$ odd
 f 's canonical form leading terms ax^d
 g 's canonical form leading terms bx^d
 $a, b \in \mathbb{K}^\times$, $\deg(f) = \deg(g) = 3 + 2d$, set $r(0) = \frac{a}{b}$

1.1 Zeros, poles, uniformizers and multiplicities

$r \in \mathbb{K}(E)$ has a *zero* in $P \in E$ if $r(P) = 0$

$r \in \mathbb{K}(E)$ has a *pole* in $P \in E$ if $r(P)$ is not finite.

uniformizer: Let $P \in E$, uniformizer: rational function $u \in \mathbb{k}(E)$ with $u(P) = 0$ if $\forall r \in \mathbb{k}(E) \setminus \{0\}$, $\exists d \in \mathbb{Z}$, $s \in \mathbb{k}(E)$ finite at P with $s(P) \neq 0$ s.t.

$$r = u^d \cdot s$$

order: Let $P \in E(\mathbb{k})$, let $u \in \mathbb{k}(E)$ be a uniformizer at P . For $r \in \mathbb{k}(E) \setminus \{0\}$ being a rational function with $r = u^d \cdot s$ with $s(P) \neq 0, \infty$, we say that r has order d at P ($\text{ord}_P(r) = d$).

multiplicity: *multiplicity of a zero* of r is the order of r at that point, *multiplicity of a pole* of r is the order of r at that point.

if $P \in E(\mathbb{k})$ is neither a zero or pole of r , then $\text{ord}_P(r) = 0$ ($= d$, $r = u^0 s$).

Multiplicities, from the book "Elliptic Tales" (p.69), to provide intuition

Factorization into *linear factors*: $p(x) = c \cdot (x - a_1) \cdots (x - a_d)$

d : degree of $p(x)$, $a_i \in \mathbb{k}$

Solutions to $p(x) = 0$ are $x = a_1, \dots, a_d$ (some a_i can be repeated)

eg.: $p(x) = (x - 1)(x - 1)(x - 3)$, solutions to $p(x) = 0$: 1, 1, 3

$x = 1$ is a solution to $p(x) = 0$ of *multiplicity 2*.

The total number of solutions (counted with multiplicity) is d , the degree of the polynomial whose roots we are finding.

2 Divisors

Def 2.1. Divisor

$$D = \sum_{P \in E(\mathbb{k})} n_P \cdot [P]$$

Def 2.2. Degree & Sum

$$\deg(D) = \sum_{P \in E(\mathbb{k})} n_P$$

$$\text{sum}(D) = \sum_{P \in E(\mathbb{k})} n_P \cdot P$$

The set of all divisors on E forms a group: for $D = \sum_{P \in E(\mathbb{k})} n_P [P]$ and $D' = \sum_{P \in E(\mathbb{k})} m_P [P]$,

$$D + D' = \sum_{P \in E(\mathbb{k})} (n_P + m_P) [P]$$

Def 2.3. Associated divisor

$$\text{div}(r) = \sum_{P \in E(\mathbb{k})} \text{ord}_P(r) [P]$$

Observe that

$$\operatorname{div}(rs) = \operatorname{div}(r) + \operatorname{div}(s)$$

$$\operatorname{div}\left(\frac{r}{s}\right) = \operatorname{div}(r) - \operatorname{div}(s)$$

Observe that

$$\sum_{P \in E(\mathbb{k})} \operatorname{ord}_P(r) \cdot P = 0$$

Def 2.4. Support of a divisor

$$\sum_P n_P [P], \quad \forall P \in E(\mathbb{k}) \text{ s.t. } n_P \neq 0$$

Def 2.5. Principal divisor iff

$$\deg(D) = 0$$

$$\operatorname{sum}(D) = 0$$

$D \sim D'$ iff $D - D'$ is principal.

Def 2.6. Evaluation of a rational function (function r evaluated at D)

$$r(D) = \prod r(P)^{n_P}$$

3 Weil reciprocity

Thm 3.1. (Weil reciprocity) Let E/\mathbb{k} be an e.c. over an algebraically closed field. If $r, s \in \mathbb{k} \setminus \{0\}$ are rational functions whose divisors have disjoint support, then

$$r(\operatorname{div}(s)) = s(\operatorname{div}(r))$$

Proof. (todo)

Example

$$p(x) = x^2 - 1, \quad q(x) = \frac{x}{x-2}$$

$$\operatorname{div}(p) = 1 \cdot [1] + 1 \cdot [-1] - 2 \cdot [\infty]$$

$$\operatorname{div}(q) = 1 \cdot [0] - 1 \cdot [2]$$

(they have disjoint support)

$$p(\operatorname{div}(q)) = p(0)^1 \cdot p(2)^{-1} = (0^2 - 1)^1 \cdot (2^2 - 1)^{-1} = \frac{-1}{3}$$

$$\begin{aligned} q(\operatorname{div}(p)) &= q(1)^1 \cdot q(-1)^1 - q(\infty)^2 \\ &= \left(\frac{1}{1-2}\right)^1 \cdot \left(\frac{-1}{-1-2}\right)^1 \cdot \left(\frac{\infty}{\infty-2}\right)^2 = \frac{-1}{3} \end{aligned}$$

so, $p(\operatorname{div}(q)) = q(\operatorname{div}(p))$.

4 Generic Weil Pairing

Let $E(\mathbb{k})$, with \mathbb{k} of char p , n s.t. $p \nmid n$.

\mathbb{k} large enough: $E(\mathbb{k})[n] = E(\overline{\mathbb{k}}) = \mathbb{Z}_n \oplus \mathbb{Z}_n$ (with n^2 elements).

For $P, Q \in E[n]$,

$$D_P \sim [P] - [0]$$

$$D_Q \sim [Q] - [0]$$

We need them to have disjoint support:

$$D_P \sim [P] - [0]$$

$$D'_Q \sim [Q + T] - [T]$$

$$\Delta D = D_Q - D'_Q = [Q] - [0] - [Q + T] + [T]$$

Note that nD_P and nD_Q are principal. Proof:

$$nD_P = n[P] - n[O]$$

$$\deg(nD_P) = n - n = 0$$

$$\text{sum}(nD_P) = nP - nO = 0$$

($nP = 0$ bcs. P is n -torsion)

Since nD_P , nD_Q are principal, we know that f_P , f_Q exist.

Take

$$f_P : \text{div}(f_P) = nD_P$$

$$f_Q : \text{div}(f_Q) = nD_Q$$

We define

$$e_n(P, Q) = \frac{f_P(D_Q)}{f_Q(D_P)}$$

Remind: evaluation of a rational function over a divisor D :

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

$$r(D) = \prod r(P)^{n_P}$$

If $D_P = [P + S] - [S]$, $D_Q = [Q - T] - [T]$ what is $e_n(P, Q)$?

$$f_P(D_Q) = f_P(Q + T)^1 \cdot f_P(T)^{-1}$$

$$f_Q(D_P) = f_Q(P + S)^1 \cdot f_Q(S)^{-1}$$

$$e_n(P, Q) = \frac{f_P(Q + T)}{f_P(T)} / \frac{f_Q(P + S)}{f_Q(S)}$$

with $S \neq \{O, P, -Q, P - Q\}$.

5 Properties

- i. $e_n(P, Q)^n = 1 \ \forall P, Q \in E[n]$
 $(\Rightarrow e_n(P, Q)$ is a n^{th} root of unity)

- ii. Bilinearity

$$e_n(P_1 + P_2, Q) = e_n(P_1, Q) \cdot e_n(P_2, Q)$$

$$e_n(P, Q_1 + Q_2) = e_n(P, Q_1) \cdot e_n(P, Q_2)$$

proof: recall that $e_n(P, Q) = \frac{g(S+P)}{g(S)}$, then,

$$\begin{aligned} e_n(P_1, Q) \cdot e_n(P_2, Q) &= \frac{g(P_1 + S)}{g(S)} \cdot \frac{g(P_2 + P_1 + S)}{g(P_1 + S)} \\ &\text{(replace } S \text{ by } S + P_1) \\ &= \frac{g(P_2 + P_1 + S)}{g(S)} = e_n(P_1 + P_2, Q) \end{aligned}$$

- iii. Alternating

$$e_n(P, P) = 1 \ \forall P \in E[n]$$

- iv. Nondegenerate

$$\text{if } e_n(P, Q) = 1 \ \forall Q \in E[n], \text{ then } P = 0$$

6 Exercises

An Introduction to Mathematical Cryptography, 2nd Edition - Section 6.8. Bilinear pairings on elliptic curves

6.29. $\text{div}(R(x) \cdot S(x)) = \text{div}(R(x)) + \text{div}(S(x))$, where $R(x), S(x)$ are rational functions.

proof:

Norm of f : $N_f = f \cdot \bar{f}$, and we know that $N_{fg} = N_f \cdot N_g \ \forall \mathbb{k}[E]$, then

$$\deg(f) = \deg_x(N_f)$$

and

$$\deg(f \cdot g) = \deg(f) + \deg(g)$$

Proof:

$$\begin{aligned} \deg(f \cdot g) &= \deg_x(N_{fg}) = \deg_x(N_f \cdot N_g) \\ &= \deg_x(N_f) + \deg_x(N_g) = \deg(f) + \deg(g) \end{aligned}$$

So, $\forall P \in E(\mathbb{k}), \text{ord}_P(rs) = \text{ord}_P(r) + \text{ord}_P(s)$.

As $\text{div}(r) = \sum_{P \in E(\mathbb{k})} \text{ord}_P(r)[P]$, $\text{div}(s) = \sum \text{ord}_P(s)[P]$.

So,

$$\begin{aligned} \operatorname{div}(rs) &= \sum \operatorname{ord}_P(rs)[P] \\ &= \sum \operatorname{ord}_P(r)[P] + \sum \operatorname{ord}_P(s)[P] = \operatorname{div}(r) + \operatorname{div}(s) \end{aligned}$$

6.31.

$$e_m(P, Q) = e_m(Q, P)^{-1} \forall P, Q \in E[m]$$

Proof: We know that $e_m(P, P) = 1$, so:

$$1 = e_m(P + Q, P + Q) = e_m(P, P) \cdot e_m(P, Q) \cdot e_m(Q, P) \cdot e_m(Q, Q)$$

and we know that $e_m(P, P) = 1$, then we have:

$$\begin{aligned} 1 &= e_m(P, Q) \cdot e_m(Q, P) \\ \implies e_m(P, Q) &= e_m(Q, P)^{-1} \end{aligned}$$