Goal: To define Weil Pairing and discuss its properties

Recall: C/K

Divisor is a formal sum $\sum_{P \in C} n_P P$, $P \in C$

Principal divisor i.e divisor of the form $\mathrm{div}(f)$ for some $f \in \bar{K}(C)$

$$\left\{ \begin{array}{c} \text{Set of all} \\ \text{principal divisors} \end{array} \right\} \subseteq \left\{ \begin{array}{c} \text{Set of all degree zero} \\ \text{divisors} \end{array} \right\} \subsetneq \left\{ \begin{array}{c} \text{Set of all} \\ \text{divisors} \end{array} \right\}$$

$\neq$

Let $\mathcal{E}$ be an elliptic curve defined over K.

Define: $$\mathrm{Pic}^0(\mathcal{E}) = \frac{\{\text{Group of all degree 0 divisors on } \mathcal{E}\}}{\{\text{Group of all Principal divisors}\}}$$

Thm: $\quad \mathrm{Pic}^0(E) \cong E$

$D \in \mathrm{Pic}^0(E)$

$D \sim (P) - (O) \quad \left(\exists\, P \in E \text{ s.t. } D \sim (P) - (O) \right)$

point at infinity

$\sigma : D \longmapsto P$

Observation: D degree 0

D is principal $\iff \sum [n_P] P = O$

$D = \sum n_P P$

D is principal $\iff D \sim 0$
degree 0

$\iff \sigma(D) = O$

$\iff \sigma\left(\sum n_P P\right) = O$

$\iff \sigma\left(\sum n_P P - \left(\sum n_P\right) O\right) = O$

$\iff \sigma\left(\sum n_P (P - O)\right) = O$

$\iff \sum n_P\, \sigma(P - O) = O$

$\iff \sum n_P P = \mathcal{O}$

Setup: E/K Elliptic curve defined over K

N N is coprime to char(K)

$$E[N] = \{P \in E(\bar{K}) \mid NP = \mathcal{O}\}$$

N-torsion points

Weil pairing is a function $e_N : E[N] \times E[N] \to \mu_N$

Recipe: Let $Q \in E[N]$.

$$\operatorname{div}(f) = NQ - N\mathcal{O}$$

($NQ - N\mathcal{O}$ is principal, hence there exists a function f s.t. $\operatorname{div}(f) = NQ - N\mathcal{O}$)

Let Q' be s.t $NQ' = Q$.

Using Q' we will construct another divisor.

$$\sum_{R \in E[N]} (Q'+R) - (R)$$, this is a degree 0 divisor

$$\# E[N] = N^2$$

$$N^2 Q' = N(NQ') = NQ = 0$$

$\rightarrow$ this is also a principal divisor.

So, there exists a function g s.t

$$\operatorname{div}(g) = \sum_{R \in E[N]} (Q'+R) - R$$

Some more observations

$$\begin{aligned} \operatorname{div}(g^N) &= N \operatorname{div}(g) \\ &= \sum_{R \in E[N]} N(Q'+R) - N(R) \end{aligned}$$

$$\begin{aligned} [N] : E &\to E \\ P &\mapsto NP \end{aligned}$$

$\mathrm{div}(f \circ [N])$

$$f \circ [N](X) = f(NX)$$

$$\mathrm{div}(f) = NQ - N\mathcal{O}$$

$$NX = Q$$

$$[N(Q' + R) = NQ' + NR = Q]$$

$$\mathrm{div}(f \circ [N]) = N\Big(\sum_{R \in E[N]} (Q' + R) - (R)\Big)$$

$$\Rightarrow \quad \mathrm{div}(f \circ [N]) = \mathrm{div}(g^N)$$

$$\Rightarrow \quad f \circ [N] = g^N \quad \text{(up to a constant)}$$

By adjusting f with this constant, assume

$$f_Q \circ [N] = g_Q^N$$

Let $P \in E[N]$, then for any $X \in E$

$$g_Q(X+P)^N = f_Q \circ [N](X+P)$$

$$= f_Q(NX + NP)$$

$$= f_Q(NX)$$

$$= f_Q \circ [N](X) = g_Q^N(X)$$

$$\Rightarrow \left(\frac{g_Q(X+P)}{g_Q(X)}\right)^N = 1$$

$\Rightarrow$ $\downarrow$ is some N-th root of unity.

This does not depend on choice of X.

$$E \to \mathbb{P}^1 \quad \text{morphism}$$

$$X \mapsto \frac{g_Q(X+P)}{g_Q(X)}$$

Weil Pairing $\quad e_N : E[N] \times E[N] \to \mu_N$

$$(P, Q) \mapsto \frac{g_Q(X+P)}{g_Q(X)}$$

Properties of Weil Pairing

1) Bilinear in both variables

$$e_N(P_1+P_2, Q) = e_N(P_1, Q)\, e_N(P_2, Q)$$

$$e_N(P, Q_1+Q_2) = e_N(P, Q_1)\, e_N(P, Q_2)$$

2) Alternating

$$e_N(P, P) = 1$$

$$\Rightarrow e_N(P, Q) = e_N(Q, P)^{-1}$$

3) Non-degenerate

If $e_N(P, Q) = 1$ for all $Q \in E[N]$

$\Rightarrow P = \mathcal{O}$

If $e_N(P, Q) = 1$ for all $P \in E[N]$

$\Rightarrow Q = \mathcal{O}$

4) Galois- invariant

$$\sigma \in Gal(\overline{K}/K)$$

$$\sigma(e_N(P,Q)) = e_N(\sigma P, \sigma Q)$$

5) Compatibility among e_N's

If $S \in E[NN']$

$P \in E[N] \subseteq E[NN']$

$$e_{NN'}(S,P) = e_N(N'S, P)$$

Next time: 1) See a proof of these properties

2) Explicit applications in cryptography