Recall: We were discussing Weil Pairing

$$e_N : E[N] \times E[N] \to \mu_N$$

(N was such that $\gcd(N, \mathrm{char}(K)) = 1$)
E/K

Finishing proof of Galois equivariance:

$\overline{K}$ Galois closure (or Algebraic closure)

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

$=$

{ Group of all automorphisms $\overline{K} \to \overline{K}$
they fix K }

Ex: $\mathbb{Q}(i)$ $\quad$ $\mathbb{Q}(i) = \{a+bi \mid a,b \in \mathbb{Q}\}$

$|$ $\quad$ If $\sigma \in \mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})$

$\mathbb{Q}$

$$\sigma(a+bi) = \sigma(a) + \sigma(b)\,\sigma(i)$$
$$= a + b\,\sigma(i)$$

i is root of x^2+1.

$$i^2+1 = 0$$

Apply σ to it

$$\sigma(i^2+1) = 0$$
$$\sigma(i)^2 + 1 = 0$$

$\sigma(i)$ is also a root of x^2+1.

$$\sigma(i) \begin{cases} \nearrow i \\ \searrow -i \end{cases}$$

$$\mathrm{Gal}\left(\mathbb{Q}(i)/\mathbb{Q}\right) = \left\{ \mathrm{Id},\ \begin{array}{l} \sigma : \mathbb{Q}(i) \to \mathbb{Q}(i) \\ \qquad i \mapsto -i \end{array} \right\}$$

Galois equivariance of Weil pairing

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

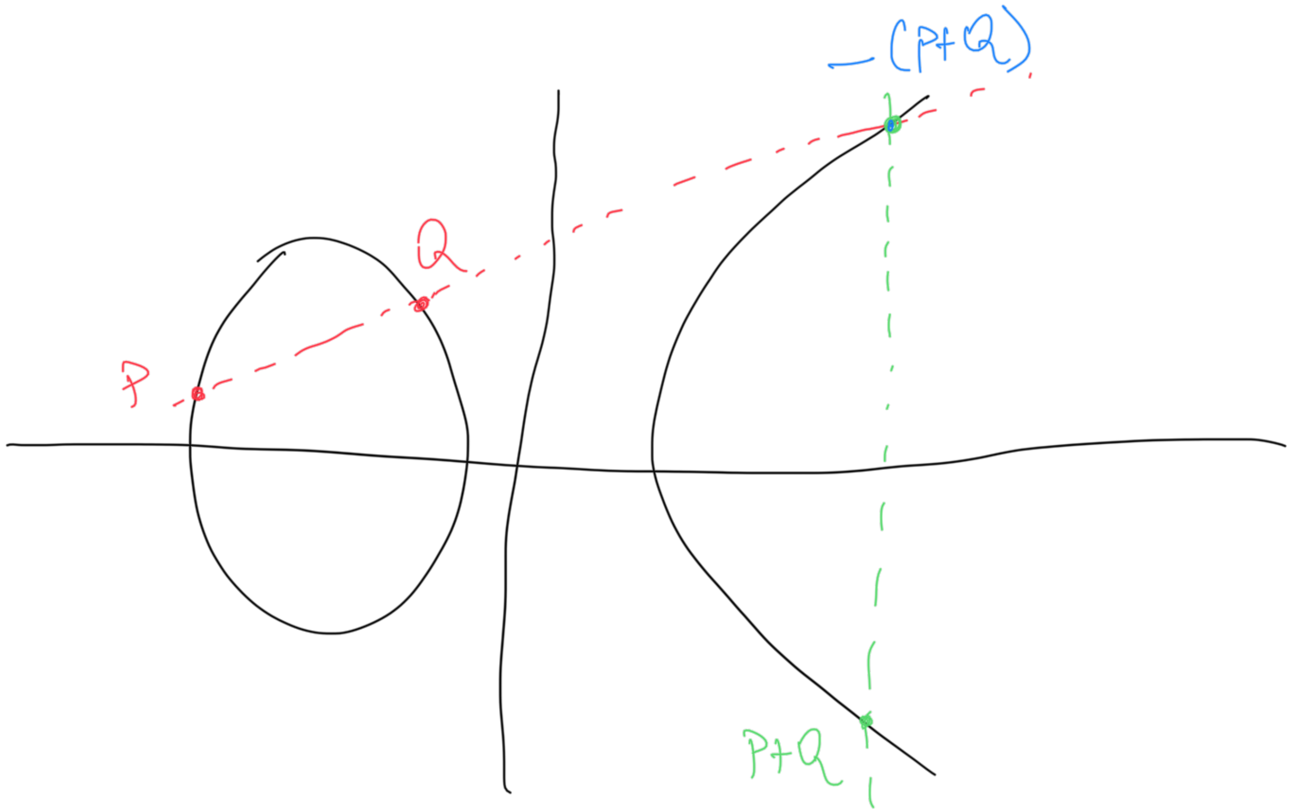
$$e_N(\sigma P, \sigma Q) = \frac{g_{\sigma Q}(X, \sigma P)}{g_{\sigma Q}(X)}$$

$$= \frac{g_{\sigma Q}(\sigma X, \sigma P)}{g_{\sigma Q}(\sigma X)}$$

$$= \frac{\sigma\left(g_Q(X, P)\right)}{\sigma\left(g_Q(X)\right)}$$

$$= \sigma\left(\frac{g_Q(X, P)}{g_Q(X)}\right) = \sigma\left(e_N(P,Q)\right)$$

Computing f used in Weil Pairing



Take $L_{P,Q}$ = Line joining P & Q

(If $P=Q$, we take the tangent line at P)

Zeroes of $L_{P,Q}$ are $\{P, Q, -(P+Q)\}$

Define $$g_{P,Q} := \frac{L_{P,Q}}{L_{(P+Q),-(P+Q)}}$$

Addition on Elliptic Curve

$$\mathrm{div}(L_{P,Q}) = P + Q + (\underline{-(P+Q)}) - 3\mathcal{O}$$

Formal Sum

$$\mathrm{div}\left(L_{(P+Q),\,-(P+Q)}\right) = (P+Q) + (-(P+Q)) + \mathcal{O} - 3\mathcal{O}$$

$$= (P+Q) + (-(P+Q)) - 2\mathcal{O}$$

$$\mathrm{div}(G_{P,Q}) = \mathrm{div}(L_{P,Q}) - \mathrm{div}\left(L_{(P+Q),\,-(P+Q)}\right)$$

$$= P+Q + \cancel{(-(P+Q))} - 3\mathcal{O} - (P+Q) - \cancel{(-(P+Q))} + 2\mathcal{O}$$

$$= P + Q - (P+Q) - \mathcal{O}$$

For each integer n we define $f_{n,P}$ as follows

$$f_{0,P} = f_{1,P} = 1$$

$$f_{n+1,P} = f_{n,P}\, G_{P,nP}$$

$$f_{-n,P} = \left(f_{n,P}\, G_{nP,-nP}\right)^{-1}$$

Propn: The following are true:

i) $\mathrm{div}\, f_{n,P} = nP - (n-1)\mathcal{O} - (nP)$

(If P is n-torsion, $nP = \mathcal{O}$
$$\mathrm{div}\, f_{n,P} = nP - (n-1)\mathcal{O} - \mathcal{O}$$
$$= nP - n\mathcal{O}$$
)

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: i) We will use induction on n.

for $n=0$ $\quad f_{0,P} = 1 \quad \mathrm{div}\,(f_{0,P}) = 0$

$$0P - (-1)\mathcal{O} - \mathcal{O} = 0P + \mathcal{O} - \mathcal{O} = 0$$

for $n=1$ $\quad f_{1,P} = 1 \quad \mathrm{div}\,(f_{1,P}) = 0$

$$P - P = 0$$

$$f_{n+1,P} = f_{n,P}\, g_{P,nP}$$

$$\mathrm{div}(f_{n+1,P}) = \mathrm{div}(f_{n,P}) + \mathrm{div}(g_{P,nP})$$

$$= nP - (n-1)O - \cancel{(nP)}$$

$$+ P + \cancel{(nP)} - ((n+1)P) - O$$

$$= (n+1)P - ((n+1)P) - nO$$

for $n < 0$

$$\mathrm{div}(f_{-n,P}) = -[\mathrm{div}(f_{n,P}) + \mathrm{div}(g_{nP,-nP})]$$

$$= -\Big[nP - (n-1)O - \cancel{(nP)} + \cancel{(nP)} + (-nP) - 2O\Big]$$

$$= -[nP + (-nP) - (n+1)O]$$

$$= (-n)P - (-nP) + (n+1)O$$

By induction, we have shown i)

2) $f_{m+n,P} = f_{m,P}\, f_{n,P}\, g_{mP,nP}$

$$\mathrm{div}(f_{m+n,P}) = (m+n)P - (m+n-1)O - ((m+n)P)$$

$$\mathrm{div}(f_{m,P}) + \mathrm{div}(f_{n,P}) + \mathrm{div}(g_{mP,nP})$$

$$\underline{mP} - (m-1)O - \cancel{(mP)}$$
$$+ nP - (n-1)O - \cancel{(nP)}$$
$$+ \cancel{(mP)} + \cancel{(nP)} - ((m+n)P) - O$$

$$= (m+n)P - (m+n-1)O - ((m+n)P)$$

$\Rightarrow$ Property 2.

3) $$f_{mn,P} = f_{m,P}^{n} f_{n,mP}$$

$$= f_{n,P}^{m} f_{m,nP}$$
(By symmetry of m & n)

$$\mathrm{div}(f_{mn,P}) = mnP - (mn-1)O - (mnP)$$
$$\mathrm{div}(f_{m,P}) + \mathrm{div}(f_{n,mP})$$
$$= n[mP - (m-1)O - (mP)]$$

$$+ n(mP) - (n-1)O - (nmP)$$

$$= nmP - n(m-1)O - \cancel{n(mP)}$$
$$+ \cancel{n(mP)} - (n-1)O - (mnP)$$

$$= nmP - [nm - \cancel{n} + \cancel{n} - 1]O - (mnP)$$

$$= nmP - [nm-1]O - (mnP)$$

divisors on both sides match, hence the functions are equal.

In next lecture, discuss frobenius maps, isogenies.