Contents

1 Hasse-Weil Theorem

p prime, $q = p^n$

$$\Phi : \bar{\mathbb{F}}_q \to \bar{\mathbb{F}}_q = \bar{\mathbb{F}}_p = \bigcup_n \mathbb{F}_{p^n}$$

$$\Phi(x) = x^q$$

it is a field homomorphism. Induces a map for $E/\mathbb{F}_q$

$$\Phi : E(\bar{\mathbb{F}}_q) \to E(\bar{\mathbb{F}}_q)$$

$$\Phi(x, y) = (x^q, y^q)$$

Frobenius is compatible wih group structure on $E(\bar{\mathbb{F}}_q)$.

1.1 Definition: Isogeny

E, E' are EC on K. An isogeny $\alpha : E \to E'$ is a rational map such that the induced map

$$E(\bar{K}) \to E'(\bar{K})$$

is a group homomorphism

1.2 Example: Frobenius

1.3 Isogeny $\alpha : E \to E$ is an endomorphism.

If $\alpha : E/K \to E'/K$ is an isogeny then

$$\alpha : E(L) \to E'(L)$$

for $K \subseteq L \subseteq \bar{K}$ is an isogeny.

$$E(L) \subseteq E(\bar{K})$$

1.4 Example

Let E/K be any EC, for all n multiplication by n is an endomorphism.

$$[n] : E \to E$$

$$P \to nP$$

Everything we do is polynomials and it preserves group structure.

1.5 Recall:

An isogeny $\alpha : E \to E'$ viewed as a rational map, has a canonical form.

$$\alpha(x, y) = (r_1(x), yr_2(x))$$

where $r_1(x) = \frac{p(x)}{q(x)}, r_2(x) = \frac{u(x)}{v(x)}$ and each quotient is reduced, so no common factors over $\bar{K}$.

If $q(x) = 0$ for some $x, y \in E(\bar{K})$, then we set $\alpha(x, y) = 0_{E'}$ and otherwise we showed $v(x) \neq 0$ and hence α is well defined.

1.6 Def

Let $\alpha : E/K \to E'/K$ be an isogeny.

1. The degree of α is $\deg(\alpha) = \max\{\deg(p), \deg(q)\}$.
2. α is called separable if the formal derivative $r_1'(x)$ is not identically zero $\quad p(x)q'(x) - p'(x)q(x) \neq 0$

$$\Phi_q = \alpha : E(\bar{\mathbb{F}}_q) \to E(\bar{\mathbb{F}}_q)$$
$$\infty \to \infty$$
$$(x, y) \to (x^q, y^q) \in E(\bar{\mathbb{F}}_q)$$
$$(y^q)^2 = (x^q)^3 + Ax^q + B$$
$$(y^2)^q = (x^3 + Ax + B)^q$$

Is Φ_q separable?

$$(x^q)' = qx^{q-1} = 0 \text{ in } \mathbb{F}_q$$

so it is not separable.

1.7 Prop

Let $\alpha : E \to E'$ be a nonzero isogeny. If α is separable then

$$\#\ker(\alpha : E(\bar{K}) \to E'(\bar{K})) = \deg(\alpha)$$

and otherwise $\#\ker(\alpha) < \deg(\alpha)$

1.7.1 Observe $\#E(\mathbb{F}_q) = \#\ker(\alpha)$

For $E/\mathbb{F}_q$

$$\alpha : \Phi_q^n - \mathrm{id} : E \to E$$
$$P \to \Phi_q^n(P) - P$$
$$\ker(\alpha : E(\bar{\mathbb{F}}_q) \to E(\bar{\mathbb{F}}_q)) = \#E(\mathbb{F}_{q^n})$$

(or without n easier)

For $E/\mathbb{F}_q$

$$\alpha : \Phi_q - \mathrm{id} : E \to E$$
$$P \to \Phi_q(P) - P$$
$$\ker(\alpha : E(\bar{\mathbb{F}}_q) \to E(\bar{\mathbb{F}}_q)) = \#E(\mathbb{F}_q)$$
$$P \in \ker(\alpha) \Leftrightarrow \Phi_q(P) - P = \infty$$
$$\Leftrightarrow \Phi_q(P) = P$$

we saw that these points P are exactly $E(\mathbb{F}_q)$

The only points frobenius acts as identity is those in $\mathbb{F}_q$, so only unchanged points are in the kernel. In higher extensions, frobenius doesn't act as the identity.

1.8 Proof

Since $\alpha \neq 0$ and is a group homomorphism on $E(\bar{K}) \to E'(\bar{K})$ it is non-constant.

Thus $\alpha : E(\bar{K}) \to E'(\bar{K})$ is surjective. Let $Q = (a, b) \in E'(\bar{K})$ and $P = (x_0, y_0) \in E(\bar{K})$.

1.9 Exercise: Show the prop on surjectivity generalizes to the case of $E \to E'$

Since $E'(\bar{K})$ is infinite we can choose Q st

1. $a, b \neq 0$
2. $\deg(p - qa) = \max\{\deg(p), \deg(q)\} = \deg(\alpha)$

the only case in which $\deg(p-qa) < \deg(\alpha)$ is when $\deg(p) = \deg(q)$ and their leading coefficients λ, δ respectively satisfy

$$\lambda - a\delta = 0 \Leftrightarrow a = \frac{\lambda}{\delta}$$

so we choose Q such that $a \neq \frac{\lambda}{\delta}$.

Since $\deg(p - aq) = \deg(\alpha)$, $p(x) - aq(x)$ has exactly $\deg(\alpha)$ roots over $\bar{K}$ (possibly repeated roots).

We claim that the number of distinct roots of $p - aq$ is exactly the number of sources P of Q (under α).

Since $(a, b) \neq (\infty, \infty)$, then

$$r_1(x_0) \neq 0 \Leftrightarrow q(x_0) \neq 0$$

since $b \neq 0$ and we have

$$y_0 r_2(x) = b$$

we have $y_0 = b/r_2(x_0)$, so y_0 is completely determined by x_0.

So it is enough to count the x_0's which in turn must satisfy $\frac{p(x_0)}{q(x_0)} = a$

$$\Leftrightarrow p(x_0) - aq(x_0) = 0$$

i.e the roots of $p - aq$

Since α is a group homomorphism on $E(\bar{K}) \to E'(\bar{K})$, then $\# \ker(\alpha)$ is the same as the number of sources of any given point $Q \in E'(\bar{K})$

Which is enough to analyze the number of distinct roots x_0 of $p - aq$.

x_0 is a repeated root of $p - aq \Leftrightarrow p(x_0) - aq(x_0) = 0$ and also $p'(x_0) - aq'(x_0) = 0$. Multiply both equations to get

$$ap(x_0)q'(x_0) = ap'(x_0)q(x_0)$$

Since $a \neq 0$

$$p(x_0)q'(x_0) - p'(x_0)q(x_0) = 0$$
$$r_1'(x_0) = 0$$

by the quotient rule applied to r_1'.

If α is not separable

$$r_1'(x) = 0$$

which means $p - aq$ has repeated roots and $\# \ker(\alpha) < \deg(\alpha)$.

If α is separable

$$r_1'(x) \neq 0$$

and hence has a finite number of roots S. We may add a constraint on the choice of Q saying that $a \notin r_1(S)$. Then since $r_1(x_0) = a$

$$x_0 \notin S$$

so $p - aq$ will not have repeated roots, i.e. $\# \ker(\alpha) = \deg(\alpha)$.

$$r_1'(x) = \frac{p(x)q'(x) - q'(x)p(x)}{q(x)^2}$$

2 Weil Pairing

Recall $\gcd(n, \mathrm{char} K) = 1$. For $Q \in E[n]$ take $f_Q \in K(E) : \mathrm{div}(f_Q) = n[Q] - n[\infty]$, there exists $g_Q \in K(E)$: $\mathrm{div}(g_Q^n) = \mathrm{div}(f_Q \circ [n])$.

For arbitrary $S \in E(K), P \in E[n]$

$$e_n(P, Q) = \frac{g_Q(S + P)}{g_Q(S)}$$

(this does not depend on the choice of S)

$$e_n : E[n] \times E[n] \to \mu_n(K)$$

2.1 $e_n(\alpha(P), \alpha(Q)) = e_n(P, Q)^{\deg \alpha}$

Let $\alpha : E \to E$ be a separable endomorphism.

Observe that $\alpha(P), \alpha(Q) \in E[n]$ since

$$n\alpha(P) = \alpha(nP) = \alpha(\infty) = \infty$$

Let $\{T_1, ..., T_k\} = \ker(\alpha)$. Since α is separable, $k = \deg(\alpha)$.

$$\begin{aligned}
\mathrm{div}(f_Q) &= n[Q] - n[\infty] \\
\mathrm{div}(f_{\alpha(Q)}) &= n[\alpha(Q)] - n[\infty] \\
g_Q^n &= f_Q \circ [n] \\
g_{\alpha(Q)}^n &= f_{\alpha(Q)} \circ [n]
\end{aligned}$$

Let $\tau_T : E \to E$ be $X \to X + T$ translation by T.

Then $\mathrm{div}(f_Q \circ \tau_{-T_i}) = n[Q + T_i] - n[T_i]$.

Now notice that $\mathrm{div}(f_{\alpha(Q)}) = n[\alpha(Q)] - n[\infty]$ and so

$$\begin{aligned}
\mathrm{div}(f_{\alpha(Q)} \circ \alpha) &= n \sum_{Q'':\alpha(Q'')=\alpha(Q)} [Q''] - n \sum_{T:\alpha(T)=\infty} [T] \\
&= n \sum_{i=1}^{k} ([Q + T_i] + [T_i]) \\
&= \mathrm{div}(\prod_{i=1}^{k} f_Q \circ \tau_{-T_i})
\end{aligned}$$

For $1 \leq i \leq k$ choose $T_i' \in E[n^2] : nT_i' = T_i$ then

$$\begin{aligned}
g_Q(S - T_i')^n &= f_Q \circ [n](S - T_i') \\
&= f_Q(nS - T_i)
\end{aligned}$$

by the definition of g_Q.

Now using this identity, we can see that

$$\begin{aligned}
\mathrm{div}(\prod_{i=1}^{k} (g_Q \circ \tau_{-T_i'})^n) &= \mathrm{div}(\prod_{i=1}^{k} f_Q \circ \tau_{-T_i} \circ [n]) \\
&= \mathrm{div}(f_{\alpha(Q)} \circ \alpha \circ [n])
\end{aligned}$$

where we use the expression from above for $\mathrm{div}(f_{\alpha(Q)} \circ \alpha)$.

Notice $\alpha \circ [n] = [n] \circ \alpha$ because $n\alpha(P) = \alpha(nP)$, so multiplication by n commutes with endormorphisms.

$$\begin{aligned}
\mathrm{div}(f_{\alpha(Q)} \circ \alpha \circ [n]) &= \mathrm{div}(f_{\alpha(Q)} \circ [n] \circ \alpha) \\
&= \mathrm{div}((g_{\alpha(Q)}^n) \circ \alpha) \\
&= \mathrm{div}((g_{\alpha(Q)} \circ \alpha)^n)
\end{aligned}$$

Finally we get

$$\prod_{i=1}^{k}(g_Q \circ \tau_{-T_i'}) = g_{\alpha(Q)} \circ \alpha$$

$$\begin{aligned} e_n(\alpha(P), \alpha(Q)) &= \frac{g_{\alpha(Q)}(\alpha(P) + \alpha(S))}{g_{\alpha(Q)}(\alpha(S))} \\ &= \prod_{i=1}^{k} \frac{g_Q(P + S - T_i')}{g_Q(S - T_i')} \\ &= \prod_{i=1}^{k} e_n(P, Q) = e_n(P, Q)^k \\ &= e_n(P, Q)^{\deg \alpha} \end{aligned}$$

3 General Direction

$$\begin{aligned} \#E(\mathbb{F}_q) &= \# \ker(\Phi_q - \mathrm{id}) \\ &= \deg(\Phi_q - \mathrm{id}) \end{aligned}$$

then we can estimate this degree.

4 Separable Map

Definition of separable map

$$\deg \alpha = \# \ker(\alpha)$$

alternatively $r_1'(x) \neq 0$.

$P, Q \in E[n]$ and α is separable then $e_n(\alpha(P), \alpha(Q)) = e_n(P, Q)^{\deg \alpha}$.

5 Invariance of Weil Pairing under "action of Galois group"

$$\mathrm{Gal}(\bar{K}/K) = \{\sigma \in \mathrm{Aut}(\bar{K}) : \sigma|_k = \mathrm{id}_K\}$$

$$\Phi_q \in \mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$$

5.1 Proposition

$$\sigma \in \mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$$

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

Note $\sigma P \in E$ since $\sigma(y)^2 = \sigma(x)^3 + A\sigma(x) + B$, and then adding is rational so $P \in E[n] \Rightarrow n \cdot \sigma P = \infty$.

Recall that $f_Q, g_Q \in K(E)$

$$\mathrm{div}(f_Q) = n[Q] - n[\infty]$$

and g_Q that satisfy

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

and for any $S \in E(K)$

$$e_n(P, Q) = \frac{g_Q(P + S)}{g_Q(S)}$$

Write out f_Q and then when it equals zero, applying σ you see that σQ is now a root of f_Q^σ, so

$$\mathrm{div}(f_Q^\sigma) = n[\sigma Q] - n[\infty]$$

and similarly for g_Q^σ.

$$\begin{aligned}(g_Q^\sigma)^n &= (g_Q^n)^\sigma \\ &= (f_Q \circ [n])^\sigma \\ &= f_Q^\sigma \circ [n]\end{aligned}$$

Thus

$$\begin{aligned}\sigma(e_n(P,Q)) &= \sigma(\frac{g_Q(P+S)}{g_Q(S)}) \\ &= \frac{g_Q^\sigma(\sigma P + \sigma S)}{g_Q^\sigma(\sigma S)} \\ &= e_n(\sigma P, \sigma Q)\end{aligned}$$

Where the last step comes from the construction of the Weil pairing. Namely $g_Q^\sigma = g_{\sigma Q}$.

$$\begin{aligned}(g_{\sigma Q})^n &= f_{\sigma Q} \circ [n] \\ &= f_Q^\sigma \circ [n] \\ &= (g_Q^n)^\sigma \\ &= (g_Q^\sigma)^n \\ &= (f_Q \circ [n])^\sigma \\ &= f_Q^\sigma \circ [n]\end{aligned}$$