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

$$E(\bar{K}) - > E'(\bar{K})$$

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