

# Contents

<b>1</b>	<b>Hasse-Weil Theorem</b>	<b>1</b>
1.1	Definition: Isogeny . . . . .	1
1.2	Example: Frobenius . . . . .	1
1.3	Isogeny $\alpha : E \rightarrow E$ is an endomorphism. . . . .	1
1.4	Example . . . . .	1
1.5	Recall: . . . . .	2
1.6	Def . . . . .	2
1.7	Prop . . . . .	2
1.7.1	Observe $\#E(\mathbb{F}_q) = \# \ker(\alpha)$ . . . . .	2
1.8	Proof . . . . .	3
1.9	Exercise: Show the prop on surjectivity generalizes to the case of $E \rightarrow E'$ . . . . .	3
<b>2</b>	<b>Weil Pairing</b>	<b>4</b>
2.1	$e_n(\alpha(P), \alpha(Q)) = e_n(P, Q)^{\deg \alpha}$ . . . . .	4

## 1 Hasse-Weil Theorem

$p$  prime,  $q = p^n$

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

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

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

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

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

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

### 1.1 Definition: Isogeny

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

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

is a group homomorphism

### 1.2 Example: Frobenius

### 1.3 Isogeny $\alpha : E \rightarrow E$ is an endomorphism.

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

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

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.

$$[n] : E \rightarrow E$$

$$P \rightarrow nP$$

Everything we do is polynomials and it preserves group structure.

## 1.5 Recall:

An isogeny  $\alpha : E \rightarrow E'$  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  $\alpha$  is well defined.

## 1.6 Def

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

1. The degree of  $\alpha$  is  $\deg(\alpha) = \max\{\deg(p), \deg(q)\}$ .
2.  $\alpha$  is called separable if the formal derivative  $r'_1(x)$  is not identically zero  $p(x)q'(x) - p'(x)q(x) \neq 0$

$$\Phi_q = \alpha : E(\bar{\mathbb{F}}_q) \rightarrow E(\bar{\mathbb{F}}_q)$$

$$\infty \rightarrow \infty$$

$$(x, y) \rightarrow (x^q, y^q) \in E(\bar{\mathbb{F}}_q)$$

$$(y^q)^2 = (x^q)^3 + Ax^q + B$$

$$(y^2)^q = (x^3 + Ax + B)^q$$

Is  $\Phi_q$  separable?

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

so it is not separable.

## 1.7 Prop

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

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

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

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

For  $E/\mathbb{F}_q$

$$\alpha : \Phi_q^n - \text{id} : E \rightarrow E$$

$$P \rightarrow \Phi_q^n(P) - P$$

$$\ker(\alpha : E(\bar{\mathbb{F}}_q) \rightarrow E(\bar{\mathbb{F}}_q)) = \#E(\mathbb{F}_{q^n})$$

(or without  $n$  easier)

For  $E/\mathbb{F}_q$

$$\alpha : \Phi_q - \text{id} : E \rightarrow E$$

$$P \rightarrow \Phi_q(P) - P$$

$$\ker(\alpha : E(\bar{\mathbb{F}}_q) \rightarrow E(\bar{\mathbb{F}}_q)) = \#E(\mathbb{F}_q)$$

$$P \in \ker(\alpha) \Leftrightarrow \Phi_q(P) - P = \infty$$

$$\Leftrightarrow \Phi_q(P) = P$$

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  $E(\bar{K}) \rightarrow E'(\bar{K})$  it is non-constant.

Thus  $\alpha : E(\bar{K}) \rightarrow E'(\bar{K})$  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 $E \rightarrow E'$

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  $\lambda, \delta$  respectively satisfy

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

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

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

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

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  $\alpha$  is a group homomorphism on  $E(\bar{K}) \rightarrow E'(\bar{K})$ , 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  $a \neq 0$

$$\begin{aligned} p(x_0)q'(x_0) - p'(x_0)q(x_0) &= 0 \\ r'_1(x_0) &= 0 \end{aligned}$$

by the quotient rule applied to  $r'_1$ .

If  $\alpha$  is not separable

$$r'_1(x) = 0$$

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

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

## 2 Weil Pairing

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

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  $S$ )

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

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

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

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

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

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

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

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

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

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

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

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

$$\begin{aligned} \text{div}\left(\prod_{i=1}^k (g_Q \circ \tau_{-T'_i})^n\right) &= \text{div}\left(\prod_{i=1}^k f_Q \circ \tau_{-T_i} \circ [n]\right) \\ &= \text{div}(f_{\alpha(Q)} \circ \alpha \circ [n]) \end{aligned}$$

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

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

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

Finally we get

$$\begin{aligned}
\prod_{i=1}^k (g_Q \circ \tau_{-T'_i}) &= g_{\alpha(Q)} \circ \alpha \\
e_n(\alpha(P), \alpha(Q)) &= \frac{g_{\alpha(Q)}(\alpha(P) + \alpha(S))}{g_{\alpha(Q)}(\alpha(S))} \\
&= \prod_{i=1}^k \frac{g_Q(P + S - T'_i)}{g_Q(S - T'_i)} \\
&= \prod_{i=1}^k e_n(P, Q) = e_n(P, Q)^k \\
&= e_n(P, Q)^{\deg \alpha}
\end{aligned}$$