Exercise Session 6

(1) E EC$/k$, $E \hookrightarrow \mathbb{P}^2_k$ Weierstraß form, i.p. $x, y \in k(E)$, $e := \infty \in E(k)$.

Pick $p, q \in E(k)$.

(a) Up to scaling, $\exists!\ 0 \neq f \in \Gamma(E, \mathcal{O}(3e-p-q))$. It is of the form $f = ax + by + c$ for some $a, b, c \in k$ s.t. p, q lie on

$$L_{p,q} := V_+(ax + by + cz) \subseteq \mathbb{P}^2_k.$$

- By Riemann-Roch: $\dim_k \Gamma(E, \mathcal{O}(3e-p-q)) = 1$

  $\rightsquigarrow \exists!\ f \neq 0$ (up to scaling)

- $\Gamma(E, \mathcal{O}(3e)) = \mathrm{span}_k\langle 1, x, y\rangle$ (by construction of Weierstraß equation)

$$\begin{array}{c} \Gamma(E, \mathcal{O}(3e)) \\ \cup\!\vert \\ \Gamma(E, \mathcal{O}(3e-p-q)) \end{array}$$

$\Rightarrow f = ax + by + c$ for some $a, b, c \in k$.

- $p \neq e$: By def of $\mathcal{O}(3e-p-q)$, $f(p) = 0 \Rightarrow p \in L_{p,q}$.

  $p = e = [0:1:0]$: Must have $b = 0$, because y has pole of order 3 at e, so $y \notin \Gamma(E, \mathcal{O}(2e-q))$

(b) Get $0 \to \mathcal{O} \xrightarrow{f} \mathcal{O}(3e-p-q) \to \mathcal{F} \to 0$, where $\mathcal{F}$ is a skyscraper sheaf at $r = -(p+q)$.

Apply $\Gamma(E,-)$:

$$\begin{array}{ccccccc} 0 \to & \Gamma(E,\mathcal{O}) & \longrightarrow & \Gamma(E,\mathcal{O}(3e-p-q)) & \longrightarrow & \Gamma(E,\mathcal{F}) \\ & \parallel & & \parallel & & \parallel \\ & k & & k\cdot f & & \kappa(r) \\ & 1 & \longmapsto & f & \longmapsto & 0 \end{array}$$

$\Rightarrow f(r)=0$

On $\mathbb{A}^2_k \cap E$: $\mathcal{O}(3e-p-q) \hat{=} \mathfrak{m}_p\mathfrak{m}_q\, k[x,y]/(y^2-\dots)$

$$\Rightarrow \mathcal{O}(3e-p-q)/\mathcal{O} \hat{=} \mathfrak{m}_p\mathfrak{m}_q\, k[x,y]/(y^2-\dots)\Big/(ax+by+c)$$

At some point $s \in k(E)$,

$$\left(\mathcal{O}(3e-p-q)/\mathcal{O}\right)/\mathfrak{m}_s$$

If $s \neq p,q$, then this $= k[x,y]/(y^2-\dots)\big/(\mathfrak{m}_s, ax+by+c) = \begin{cases} 0 & s \notin V_{p,q} \\ k & s \in V_{p,q} \end{cases}$

(2) Let p be a prime, $q=p^n$, E EC$/\mathbb{F}_q$.

(a) $\forall \mathbb{F}_p$-scheme X, $F_X: X \to X$ absolute Frobenius. Show that

$$f := F_E^n : E \to E$$

is an isogeny of degree q.

$\leadsto$ Why not take $F_E : E \to E$? Not a morphism$/\mathbb{F}_q$!

- Isogeny $\Leftrightarrow$ non-constant. Clear for f.
  $+\ 0 \mapsto 0$

• $\deg f$:

1) Choose any $x \in E(\overline{\mathbb{F}}_q)$. Then $f^{-1}(x) = \{x\}$, hence $\deg f = e_x = q$.

2) $\deg f = [k(E) : k(E)^q] = [\mathbb{F}_q(t) : \mathbb{F}_q(t)^q] = q$.

$[k(E) : \mathbb{F}_q(t)^q] = [k(E) : k(E)^q] \cdot [k(E)^q : \mathbb{F}_q(t)^q]$

$= [k(E) : \mathbb{F}_q(t)] \cdot [\mathbb{F}_q(t) : \mathbb{F}_q(t)^q]$

(b) By analyzing $\ker(f)$, show if E is ordinary then $f \notin \mathbb{Z}$.

• Claim: $\ker(f)(\overline{\mathbb{F}}_q) = \ker\left(E(\overline{\mathbb{F}}_q) \xrightarrow{f} E(\overline{\mathbb{F}}_q)\right) = 0$

$$\begin{array}{ccc} \ker f & \rightarrow & E \\ \downarrow & & \downarrow f \\ k & \xrightarrow{e} & E \end{array} \quad \Rightarrow \quad |\ker f| = |f^{-1}(e)| = \{e\}$$

(Rmk: $\ker(f) \cong \begin{cases} \mu_q & E \text{ ordinary} \\ \alpha_q & E \text{ supersingular} \end{cases}$)

• If $f \in \mathbb{Z}$, then $f = [p^{n/2}]$, But $E[p^{n/2}](\overline{\mathbb{F}}_q) \neq 0$ if E ordinary.

(c) Assume E ordinary. Then $E[p^m](\overline{\mathbb{F}}_q) \cong \mathbb{Z}/p^m\mathbb{Z}$. $\forall m \geq 1$.

Use induction: Have sequence

$$\begin{array}{ccccccccc} 0 & \rightarrow & E[p^n] & \hookrightarrow & E[p^{n+1}] & \xrightarrow{p^n} & E[p] & \rightarrow & 0 \\ & & & & \downarrow & & \downarrow & & \\ & & & & E & \xrightarrow{p^n} & E & & \end{array}$$

Lemma: $Y \twoheadrightarrow X$ surj. map of k-varieties $\Rightarrow Y(\bar{k}) \twoheadrightarrow X(\bar{k})$ surj.

$$\rightsquigarrow 0 \to \underset{\mathbb{Z}/p^n\mathbb{Z}}{\underset{\cong}{E[p^n](\bar{\mathbb{F}}_q)}} \to E[p^{n+1}](\bar{\mathbb{F}}_q) \xrightarrow{p^n} \underset{\mathbb{Z}/p\mathbb{Z}}{\underset{\cong}{E[p](\bar{\mathbb{F}}_q)}} \to 0$$ exact by direct argument

$$\Rightarrow E[p^{n+1}](\bar{\mathbb{F}}_q) = \mathbb{Z}/p^{n+1}\mathbb{Z}$$

$\rightsquigarrow$ $\mathrm{End}(E)$ acts on $T_pE = \varprojlim E[p^n](\bar{\mathbb{F}}_q) \cong \mathbb{Z}_p$.

$\Rightarrow$ $\mathrm{End}^0(E) \longrightarrow \mathrm{End}(\mathbb{Q}_p) = \mathbb{Q}_p$ non-zero

$\Rightarrow$ automatically injective, as $\mathrm{End}^0(E)$ skew field.

$\rightsquigarrow$ $\mathrm{End}^0(E) \subseteq \mathbb{Q}_p$ $\rightsquigarrow$ $\mathrm{End}^0(E)$ commutative, hence quadr./$\mathbb{Q}$.

3 (a) $\varphi : E[p^n] \to E[p^n]$ $\rightsquigarrow$ $\varphi|_{E[p^{n-1}]} : E[p^{n-1}] \to E[p^{n-1}]$

(b) Argue as in lecture.