Exercise Session 10

① $S_0 \hookrightarrow S$ thickening (e.g. $\operatorname{Spec} R \to \operatorname{Spec} R[\varepsilon]/\varepsilon^2$). Let

X, Y abelian schemes$/S$, $f_0 : X|_{S_0} \to Y|_{S_0}$ hom.

Then there is at most one lift of f_0 to a hom. $f : X \to Y$.

Suppose $f, f' : X \to Y$ are two lifts. Wlog. S connected. Apply the Rigidity Lemma to $f - f'$! Have $(f-f')(s_0)(X_{s_0}) = \{0\}$ for any $s_0 \in S$ (since $(f-f')|_{S_0} = 0$).

$\Rightarrow f - f'$ factors as $g \circ (X \to S) = 0$

$g = f \circ e$ (e.g. by proof of rigidity)

② $k = \bar{k}$, $\operatorname{char} k = p > 0$.

Thm: Every finite grp scheme over k of order p is isomorphic to $\mathbb{Z}/p\mathbb{Z}$, α_p or μ_p.

(a) $\operatorname{End}(\mu_p) = \{ \varphi : k[T]/(T^p - 1) \to k[T]/(T^p-1) \mid P(T_1 T_2) = P(T_1)P(T_2) \}$

$T \longmapsto p$

$= \{ T \mapsto T^n \mid n \in \{0, \dots, p-1\} \}$

$= \mathbb{Z}/p\mathbb{Z}$

$$\mathrm{End}(\alpha_p) = \left\{ \varphi: k[T]/T^p \to k[T]/T^p \;\middle|\; a \in k \right\}$$
$$T \longmapsto aT$$

E supersingular EC$/k$

<u>Claim:</u> Let $F: E \to E^{(p)}$ be the relative Frobenius. Then $\ker(F) \cong \alpha_p$.

<u>Proof:</u> By above thm, have $\ker F \in \{\mathbb{Z}/p\mathbb{Z}, \mu_p, \alpha_p\}$.

- $\ker F \not\cong \mathbb{Z}/p\mathbb{Z}$, because $\ker F$ is connected (a "fat point")

- $\ker F \not\cong \mu_p$: Assume $\ker F \cong \mu_p$. Then $\mathrm{End}(\ker F) = \mathbb{Z}/p\mathbb{Z}$.

Recall: There is a valuation

$$v: \mathrm{End}^0(E) \to \mathbb{Z} \cup \{\infty\}, \quad \phi \mapsto v_p(\deg \phi).$$

(cf Lecture 16, page 11). It extends to a valuation

$$v: \mathrm{End}^0(E)_p = \mathrm{End}^0(E) \otimes_{\mathbb{Q}} \mathbb{Q}_p \longrightarrow \mathbb{Z} \cup \{\infty\}.$$

By lecture 17, page 4,

$$E \text{ supersingular} \Rightarrow \dim_{\mathbb{Q}} \mathrm{End}^0(E) = 4$$

By lecture 11, page 18, there are, up to isom., only 2 quaternion algebras over $\mathbb{Q}_p$: $M_2(\mathbb{Q}_p)$ and skew field

Actually, by lecture 11, page 19, we have that $\mathrm{End}^0(E)_p$ is a skew field.

Moreover,

$$\mathcal{O} = \mathrm{End}(E)_p = \left\{ x \in \mathrm{End}^0(E)_p \;\middle|\; v(x) \geq 0 \right\}$$

(by lecture 16, page 12)

Let $\mathfrak{m} := \{x \in \mathcal{O} \mid v(x) > 0\}$. Then $\mathcal{O}/\mathfrak{m}$ is a (skew) field.

It has $\dim_{\mathbb{F}_p} \mathcal{O}/\mathfrak{m} \geq 2$ because $\mathcal{O}$ has rank 4 and $v(p) = 2$

$(\rightsquigarrow \mathcal{O}/p$ has $\mathbb{F}_p$-dim 4 and $p = \mathfrak{m}^2)$

$\Rightarrow$ there is no ring hom. $\mathcal{O}/\mathfrak{m} \to \mathbb{F}_p$.

On the other hand $\mathrm{End}(E) \to \mathrm{End}(\ker F)$ induces a map

$\mathcal{O}/\mathfrak{m} \to \mathrm{End}(\ker F) = \mathbb{Z}/p\mathbb{Z}$ ↯

(b) $\mathrm{Hom}(\mu_p, \alpha_p) = 0$ (as in (a))

$\Rightarrow$ Every subgroup $G \subseteq (\alpha_p)^n$ of order p is isom. to α_p.

(c) Let $X = E^n$. Then

$$\{\text{closed subgrps } K \subset X \text{ of order } p\} \cong \mathbb{P}^{n-1}(k)$$

- Any such K lies in $(\ker F)^n$.

By lecture 15, page 14: There is only one order-p subgrp of E, necessarily it's $\ker F$ (E supersingular!)

Given K, look at the projections $K \hookrightarrow E^n \xrightarrow{p_i} E$. Then

$\ker f_i \in \{0, K\}$. If $\ker f_i = 0$, $f_i : K \hookrightarrow E$ is closed immersion, hence $K = \ker F$. If $\ker f_i = K$, $f_i = 0$.

$\rightsquigarrow f_i$ factors over $\ker F$.

$\bullet \ \{K \subset X \ \dots\} \cong \{K \subset (\alpha_p)^m \text{ closed subgrp of order } p\}$

$$= \{\operatorname{im} f \mid f : \alpha_p \hookrightarrow (\alpha_p)^m\}$$

$$= \{\operatorname{im} f \mid f \in \underbrace{Hom(\alpha_p, (\alpha_p)^m)}_{= k^m \setminus 0 \text{ by (a)}} \setminus 0\}$$

$$= (k^m \setminus 0)/Aut(\alpha_p)$$

$$= (k^m \setminus 0)/k^\times$$

$$= \mathbb{P}^{m-1}(k).$$

(d) Show that for only finitely many K's, $X/K \cong E_1 \times \dots \times E_m$ for some EC's $E_1, \dots, E_m$.

$\bullet$ There are only finitely many possibilities for $E_1, \dots, E_m$:

Suppose $X/K \cong E_1 \times \dots \times E_m$. Then

$$\exists \varphi : E^m \to E_1 \times \dots \times E_m \quad \text{s.t. } \ker \varphi \text{ has order } p$$

Then

j-th factor of E^m

$$\varphi = (\varphi_{ij})_{i,j} \quad \text{with } \varphi_{ij} : E \to E_i \qquad \left(Hom(E^m, E_1 \times \dots \times E_m) = \prod_i Hom(E, E_i)^m\right)$$

For each i, we have some j s.t. $\varphi_{ij} \neq 0$.

$\Rightarrow E_i$ isogenous to E

By lecture 17, page 5: only fin. many such E_i's.

• Fix $E_1 \times \dots \times E_m$.

$$\{\ker\varphi \mid \varphi : E^m \to E_1 \times \dots \times E_m \text{ s.t. } \ker\varphi \text{ has order } p\}$$

$$= \{\ker\varphi \mid \varphi \in \underbrace{\mathrm{Hom}(E^m, E_1 \times \dots \times E_m)/p}_{\text{finite!}} \text{ s.t. } \ker\varphi \text{ has order } p\}$$

is finite.