Exercise Session 7

① (a) Assume $i \in k$. Let $a \in k^\times$ and let $E: y^2 = x^3 + ax$

Then E has CM by $\mathbb{Z}[i]$.

Consider

$$\sigma: E \xrightarrow{\sim} E, \quad x \mapsto -x, \; y \mapsto iy.$$

To show:

$$\sigma^2 = -1 \qquad (\text{then use } \mathbb{Z}[i] \to \mathrm{End}(E), \; i \mapsto \sigma)$$

1. Note

$$\sigma^2: x \mapsto x, \; y \mapsto -y$$

By explicit computation, this is $= -1$.

2. Note $\sigma^4 = 1$. Thus $(\sigma^2 - 1)(\sigma^2 + 1) = 0$ in $\mathrm{End}(E)$. But $\mathrm{End}(E)$ has no zero divisors $\Rightarrow \sigma^2 - 1 = 0$ or $\sigma^2 + 1 = 0$

But $\sigma^2 \neq 1 \Rightarrow \sigma^2 = -1$.

By ②: E is $\begin{cases} \text{ordinary} & \text{if } \mathrm{char}\, k \equiv 1\,(4) \\ \text{supersingular} & \text{if } \mathrm{char}\, k \equiv 3\,(4) \end{cases}$

(b) Assume $\omega \in k$. Let $b \in k^\times$ and let $E: y^2 = x^3 + b$.

Then E has CM by $\mathbb{Z}[\omega]$.

Consider

$$\tau: E \xrightarrow{\sim} E, \quad x \mapsto \omega x, \; y \mapsto y$$

Then $\tau^3 = 1$.

As in (a), get map

$$\mathbb{Z}[\omega] \to \mathrm{End}(E), \quad \omega \mapsto \tau$$

Rmk: $x \mapsto \omega x$, $y \mapsto -y$ has order 6! This is just $-\tau$. Similarly, $-\omega$ is primitive 6-th root of unity.

② char $k = p > 0$, E EC$/k$ with CM by $\mathcal{O}_K$, K a quadr. ext. of $\mathbb{Q}$.

($K = \mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z}$ square-free.

Then
$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & d \not\equiv 1 \ (4) \\ \mathbb{Z}\left[\frac{\sqrt{d}+1}{2}\right] & d \equiv 1 \ (4) \end{cases}$$
)

(a) If p does not split in K then E is supersingular.

(p splits in $\mathcal{O}_K \Leftrightarrow p\mathcal{O}_K = \mathfrak{P}_1 \mathfrak{P}_2$ with $\mathfrak{P}_1 \neq \mathfrak{P}_2$ prime ideals in $\mathcal{O}_K$)

To show: $E[p](\bar{k}) = 0$. Assume E is ordinary. Have map

$$\mathcal{O}_K \hookrightarrow \mathrm{End}(T_p E) \cong \mathbb{Z}_p$$
$$T_pE = \varprojlim E[p^n](\bar{k})$$

$\rightarrow \sqrt{d} \in \mathbb{Z}_p$.

Hence $p \nmid d$ and d mod p is a quadratic residue, i.e.

$d \equiv a^2 \bmod p$ for some $a \in \mathbb{F}_p$.

$\Rightarrow p$ splits in $\mathcal{O}_K$ by number theory.

Caution: Need a little extra work if $p = 2$.

(6) If p splits in K then E is ordinary.

Claim: $E[p] \cong G_1 \times G_2$, G_1, G_2 non-trivial k-group schemes.

Proof: Consider $\mathcal{O}_K/p \longrightarrow \mathrm{End}(E[p])$.

$$p \text{ splits} \longrightarrow \begin{array}{c} \mathcal{O}_K/p \\ \text{\rotatebox{90}{$\cong$}} \\ \mathbb{F}_p \times \mathbb{F}_p \end{array}$$

Let

$$G_1 = \ker((1,0)), \qquad G_2 = \ker((0,1))$$

1. $E[p] = G_1 \times G_2$ (check on S-points for $S \in Sch_k$)

To show: $E[p](S) = G_1(S) \times G_2(S)$

$G_1(S) = \ker\big((1,0)(S) : E[p](S) \rightarrow E[p](S)\big)$

$G_2(S) = $ — " — $(0,1)$ — " — —

2. Assume $G_1 = 0$. Then $\ker[p] \subseteq \ker(1,0)$

$\Rightarrow (1,0) \in \mathcal{O}_K$ is divisible by p in $\mathrm{End}(E)$.

$\Rightarrow (0,1) = (1,0)^*$ is divisible by p

$\Rightarrow G_2 = 0$ ↯ $\square$

(Recall $\mathrm{Lie}(G) = \mathrm{Map}_0(\mathrm{Spec}\, k[\varepsilon]/\varepsilon^2, G)$)

$$\begin{array}{c} \mathrm{Lie}(G_1 \times G_2) = \mathrm{Lie}(G_1) \times \mathrm{Lie}(G_2) \\ \shortparallel \\ \mathrm{Lie}(E[p]) \subseteq \mathrm{Lie}(E) \cong k \end{array}$$

$\Rightarrow \mathrm{Lie}(G_1) = 0$ or $\mathrm{Lie}(G_2) = 0$

$\Rightarrow G_1$ or G_2 is étale

$\Rightarrow G_1(\bar{k}) \neq 0$ or $G_2(\bar{k}) \neq 0$

$\Rightarrow E[p](\bar{k}) \neq 0$

$\Rightarrow E$ is ordinary.

(3) E EC$/k$.

(a) $\mathcal{L}$ line bundle on E. Define

$$\varphi_{\mathcal{L}} : E \to E^{\vee}$$

s.t.

$$\varphi_{\mathcal{L}}(k) : E(k) \to E^{\vee}(k) = \mathrm{Pic}^0(E)$$
$$x \longmapsto t_x^* \mathcal{L} \otimes \mathcal{L}^{-1}$$

Define $\forall T \in \mathrm{Sch}_S$

$t_x(T) : E_S(T) \to E_S(T)$

$a \mapsto a + x$

Yoneda:

Let $S \in \mathrm{Sch}_k$, $x \in E(S)$. This induces $t_x : E_S \xrightarrow{+x} E_S$ over S, where $E_S = E \times_k S$. Then let $\mathcal{L}_S = (E_S \to E)^* \mathcal{L}$ and

$$\varphi_{\mathcal{L}}(S) : x \longmapsto t_x^* \mathcal{L}_S \otimes \mathcal{L}_S^{-1} \in \mathrm{Pic}^0(E_S) / p_S^* \mathrm{Pic}(S)$$

(b) $\varphi_{\mathcal{L}}$ is linear in $\mathcal{L}$, hence defines grp hom

$$\varphi : \mathrm{Pic}(E) \to \mathrm{Hom}(E, E^{\vee})$$

Easy.

(c) $\varphi_{\mathcal{L}}$ depends only on $\deg \mathcal{L}$.

Enough to check: If $\deg \mathcal{L} = 0$ then $\varphi_{\mathcal{L}} = 0$.

Essential case: $\mathcal{L} = \mathcal{O}([y] - [0])$ for some $y \in E(k)$.

Then $\mathcal{L}_S = \mathcal{O}([y_S] - [0_S])$, $y_S : S \to E$ induced section.

$$t_x^* \mathcal{O}([y_S] - [0_S]) \otimes \mathcal{O}([y_S] - [0_S])^{-1}$$

by def of $y_s + x$ $= \mathcal{O}([y_s + x] - [x] - [y_s] + [0_s])$

$= \mathcal{O} \otimes p_S^* \mathcal{M} = \mathcal{O}$ in $E^\vee(S)$

for some $\mathcal{M} \in \mathrm{Pic}(S)$.

(d) Find $E \to E^\vee$ which is not in image of φ.

$$\varphi_{\mathcal{O}(0)} : E \xrightarrow{\sim} E^\vee, \quad x \mapsto \mathcal{O}([x] - [0])$$

$$\varphi_{\mathcal{O}(n0)} : E \xrightarrow{\sim} E^\vee \xrightarrow{[n]} E^\vee$$

$\rightsquigarrow$ Any CM is example.