Exercise Sheet 9

Discussed on 23.06.2021

Problem 1 (CM Elliptic Curves)**.** Let K be an imaginary quadratic extension of $\mathbb{Q}$ and let k be an algebraically closed field. The aim is to classify all elliptic curves over k which have complex multiplication by K.

(a) Let $\mathcal{O} \subset K$ be an order, i.e. a subring of rank 2 over $\mathbb{Z}$. Show that there is a unique $f \in \mathbb{Z}_{\geq 1}$ such that $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$.

Hint: Consider $\mathcal{O}_K/\mathcal{O}$.

(b) Let $\Lambda \subset K$ be a lattice and define

$$\mathcal{O}_\Lambda := \{x \in K \mid x\Lambda \subseteq \Lambda\}.$$

Show that this is an order of K and that Λ is a projective module of rank 1 over $\mathcal{O}_\Lambda$ (i.e. a line bundle on $\operatorname{Spec} \mathcal{O}_\Lambda$). Show that this induces a bijection

$$\{\text{lattices } \Lambda \subset K\}/_{(a\Lambda\sim\Lambda,\ a\in K)} \;\cong\; \coprod_{f\in\mathbb{Z}_{\geq 1}} \operatorname{Pic}(\mathbb{Z} + f\mathcal{O}_K).$$

Hint: For each prime p consider the minimal $\mathcal{O}_{K_p}$-lattice L containing Λ_p. Show that there is $\alpha \in K_p^*$ with $\alpha L = \mathcal{O}_{K_p}$ and $1 \in \alpha\Lambda_p$, then argue as in (a).

(c) Assume that $\operatorname{char} k = 0$. Prove that all elliptic curves E over k with $\operatorname{End}^0(E) \cong K$ are isogenous. Deduce that there is a natural bijection

$$\{\text{ECs } E \text{ over } k \text{ with } \operatorname{End}^0(E) \cong K\}/_{\cong} \xleftrightarrow{\sim} \coprod_{f\in\mathbb{Z}_{\geq 1}} \operatorname{Pic}(\mathbb{Z} + f\mathcal{O}_K).$$

Hint: For the first part, reduce to the case $k = \mathbb{C}$.

(*d) Assume that $\operatorname{char} k = p > 0$. Use without proof that again all elliptic curves E over k with $\operatorname{End}^0(E) \cong K$ are isogenous. Prove that

$$\{\text{ECs } E \text{ over } k \text{ with } \operatorname{End}^0(E) \cong K\}/_{\cong} \xleftrightarrow{\sim} \coprod_{f\in\mathbb{Z}_{\geq 1},\ (f,p)=1} \operatorname{Pic}(\mathbb{Z} + f\mathcal{O}_K).$$

Definition. Let $X \to S$ be a map of schemes over $\mathbb{F}_p$. The *relative Frobenius* $F\colon X \to X^{(p)}$ is defined as follows. First recall the definition of the absolute Frobenii $F_S\colon S \to S$ and $F_X\colon X \to X$: They are the identity on the underlying topological spaces and the p-th power map on coordinate rings. Then define $X^{(p)}$ by the Fiber product diagram

$$\begin{tikzcd} X^{(p)} \arrow[r] \arrow[d] & X \arrow[d] \\ S \arrow[r, "F_S"] & S \end{tikzcd}$$

Now the map $F\colon X \to X^{(p)}$ is defined to be the S-morphism whose composition with $X^{(p)} \to X$ is the absolute Frobenius F_X. (It is certainly a good idea to work out an example of this, e.g. for $X = \mathbb{A}^1_S$.)

Problem 2 (Hasse Invariant)**.** Let p be a prime, S a noetherian $\mathbb{F}_p$-scheme and E an elliptic curve over S. Let $F\colon E \to E^{(p)}$ be the relative Frobenius, as defined above.

(a) Show that F is finite locally free of degree p. In particular $\ker F$ is a finite locally free group scheme over S. Show that $E^{(p)} = E/\ker F$.

Hint: Use the fiber criterion for flatness (Stacks Project Lemma 039E).

(b) Deduce that there is an S-morphism $V\colon E^{(p)} \to E$ such that $V \circ F = p$. It is called the *Verschiebung*.

(c) If $S = \operatorname{Spec} k$ for a field k, show that V is étale/inseparable if and only if E is ordinary/supersingular.

(d) Define the *Hodge bundle* $\omega_E := e^*\Omega^1_{E/S}$, where $e\colon S \to E$ is the neutral element section. Show that there is a natural isomorphism $\omega_{E^{(p)}} = \omega_E^{\otimes p}$.

(e) Show that pullback along V defines a map

$$V^*\colon \omega_E \to \omega_E^{\otimes p}.$$

The corresponding section $\mathrm{Ha}_E \in \Gamma(S, \omega_E^{\otimes(p-1)})$ is called the *Hasse invariant* of E. Deduce that

$$\{s \in S \mid E(s) \text{ supersingular}\} = V(\mathrm{Ha}_E).$$

In particular this is a closed subset of S.