Exercise Sheet 7

Discussed on 09.06.2021

Problem 1. Let k be a field.

(a) Assume that k contains a primitive 4-th root of unity $i \in k$. Pick any $a \in k^\times$ and let E be the elliptic curve over k defined by the Weierstraß equation $y^2 = x^3 + ax$. By considering the automorphism $x \mapsto -x$, $y \mapsto iy$ of E, show that E admits complex multiplication by $\mathbb{Z}[i]$.

(b) Assume that k contains a primitive 3-rd root of unity $\omega \in k$. For any $b \in k^\times$, let E be the elliptic curve over k defined by the Weierstraß equation $y^2 = x^3 + b$. Show that E admits complex multiplication by $\mathbb{Z}[\omega]$.

Problem 2. Let k be a field of characteristic $p > 0$ and let E be an elliptic curve over k which admits complex multiplication by $\mathcal{O}_K$, where $\mathcal{O}_K$ is the ring of integers in some quadratic extension K of $\mathbb{Q}$.

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

Hint: Consider the induced action of $\mathcal{O}_K$ on T_pE (defined in problem 2 on sheet 6).

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

Hint: Show first that $E[p]$ splits as a product of two group schemes over k, then look at the Lie algebras to deduce that one of them must be étale.

Problem 3. Let k be a field and let E be an elliptic curve over k.

(a) Let $\mathcal{L}$ be a line bundle on E, let $x \in E(k)$ and let $t_x \colon E \to E$ denote the translation-by-x map. Then $t_x^*\mathcal{L} \otimes \mathcal{L}^{-1}$ is a line bundle of degree 0 on E and hence defines a point in $E^\vee(k)$. Use this idea to define a morphism $\varphi_\mathcal{L} \colon E \to E^\vee$ of elliptic curves over k.

(b) Show that the map $\varphi_\mathcal{L}$ defined in (a) is linear in $\mathcal{L}$ and hence defines a group homomorphism $\varphi \colon \operatorname{Pic}(E) \to \operatorname{Hom}(E, E^\vee)$.

(c) Show that $\varphi_\mathcal{L}$ depends only on the degree of $\mathcal{L}$, i.e. that φ factors over $\deg \colon \operatorname{Pic}(E) \to \mathbb{Z}$.

Hint: Use the ideas from the end of lecture 12.

(d) Give an example of an elliptic curve E and a homomorphism $E \to E^\vee$ not of the form $\varphi_\mathcal{L}$.