Math 5020 - Elliptic Curves

Homework 2 (3.4 (use SAGE), 3.5, 3.8, and the exercise below)

3.4 *Referring to example (2.4), express each of the points P_2, P_4, P_5, P_6, P_7, P_8 in the form $[m]P_1 + [n]P_3$ with $m, n \in \mathbb{Z}$.*

3.5 *Let E/K be given by a singular Weierstrass equation.*

(a) *Suppose that E has a node, and let the tangent lines at the node be $y = \alpha_i x + \beta_i, i = 1, 2$.*

(i) *If $\alpha_1 \in K$, prove that $\alpha_2 \in K$ and*

$$E_{ns}(K) \cong K^*.$$

(ii) *If $\alpha_1 \notin K$, prove that $L = K(\alpha_1, \alpha_2)$ is a quadratic extension of K. From (i), $E_{ns}(K) \subset E_{ns}(L) \cong L^*$. Show that*

$$E_{ns}(K) \cong \{t \in L^* : \mathrm{N}_{L/K}(t) = 1\}.$$

(b) *Suppose that E has a cusp. Prove that*

$$E_{ns}(K) \cong K^+.$$

3.8 (a) *Let $E/\mathbb{C}$ be an elliptic curve. There is a lattice $L \subset \mathbb{C}$ and a complex analytic isomorphism of groups $\mathbb{C}/L \cong E(\mathbb{C})$. Then $\deg[m] = m^2$ and $E[m] = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.*

(b) *Let E/K be an elliptic curve with $\mathrm{char}(K) = 0$. Then $\deg[m] = m^2$.*

Problem 1 *Let $E/\mathbb{Q}$ be an elliptic curve given by a Weierstrass equation of the form $y^2 = f(x)$, where $f(x) \in \mathbb{Z}[x]$ is a monic cubic polynomial with distinct roots (over $\bar{\mathbb{Q}}$).*

(a) *Show that $P = (x, y) \in E(\bar{\mathbb{Q}})$ is a torsion point of exact order 2 if and only if $y = 0$ and $f(x) = 0$.*

(b) *Let us define $\mathbb{Q}(E[2])$ by*

$$\mathbb{Q}(E[2]) = \mathbb{Q}(\{x, y : P = (x, y) \in E[2]\}).$$

Show that Gal$(\mathbb{Q}(E[2])/\mathbb{Q})$ is isomorphic to a subgroup of $\mathrm{GL}(2, \mathbb{F}_2)$, unique up to conjugation. Note that the isomorphism is not canonical, because it depends on a choice of basis for $E[2]$.

(c) *Prove that $S_3 \cong \mathrm{GL}(2, \mathbb{F}_2)$. List all subgroups of $\mathrm{GL}(2, \mathbb{F}_2)$.*

(d) *For every subgroup $G \leq \mathrm{GL}(2, \mathbb{F}_2)$, either find an elliptic curve $E/\mathbb{Q}$ and an isomorphism*

$$\mathit{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \cong G$$

or prove that no such curve exists. For example, $y^2 = x^3 - x$ affords $G = \{\mathrm{Id}\}$.

(e) *The elliptic curve $y^2 = x^3 + 2x^2 - 3x$ satisfies $E(\mathbb{Q})[4] = \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, i.e. the full 2-torsion is defined over $\mathbb{Q}$ and there is also a point of order 4 defined over $\mathbb{Q}$. Describe the possible isomorphism types of Gal$(\mathbb{Q}(E[4])/\mathbb{Q})$ as a subgroup of $\mathrm{GL}(2, \mathbb{Z}/4\mathbb{Z})$.*