Homework sheet 13

Due date: Monday, 21.1.13 at 12 noon

1. Let $\mathrm{char}(k) \neq 2$ and let $a, b \in k$, $\tilde{a} := -2a$, $\tilde{b} := a^2 - 4b$ with $b \neq 0$, $\tilde{b} \neq 0$. Let E and $\tilde{E}$ be given in Weierstraß equations

$$E: \ y^2 = x^3 + ax^2 + bx \qquad \text{and} \qquad \tilde{E}: \ \tilde{y}^2 = \tilde{x}^3 + \tilde{a}\tilde{x}^2 + \tilde{b}\tilde{x}.$$

Consider the isogenies:

$$\varphi : E \to \tilde{E}, \quad \varphi^*(\tilde{x}) = \tfrac{y^2}{x^2}, \quad \varphi^*(\tilde{y}) = \tfrac{y(x^2-b)}{x^2}$$

$$\psi : \tilde{E} \to E, \quad \psi^*(x) = \tfrac{\tilde{y}^2}{4\tilde{x}^2}, \quad \psi^*(y) = \tfrac{\tilde{y}(\tilde{x}^2-\tilde{b})}{8\tilde{x}^2}$$

   (a) Prove that φ and ψ are separable. Hint: $\varphi^*\omega \neq 0$.

   (b) Determine $\ker\varphi$, $\ker\psi$, $\deg\varphi$ as well as $\deg\psi$.

   (c) Prove that $\psi \circ \varphi = [2] : E \to E$ and $\varphi \circ \psi = [2] : \tilde{E} \to \tilde{E}$.

   (d) Let $P \in E(k^{\mathrm{alg}})$ with $\varphi(P) \in \ker\psi$, $\varphi(P) \neq 0$, e.g. $P = (\alpha : 0 : 1)$ for $\alpha \in k^{\mathrm{alg}}$ with $\alpha^2 + \alpha a + b = 0$. Prove that

$$E[2](k^{\mathrm{alg}}) = \{0, P\} \oplus \ker\varphi \cong (\mathbb{Z}/2)^2. \qquad \textit{(8 points)}$$

2. Find integral group schemes E, E' over k with neutral elements $0 \in E(K)$ and $0' \in E'(k)$, as well as a morphism $\varphi : E \to E'$ of k-schemes, which satisfies $\varphi(0) = 0'$, but is not a homomorphism of group schemes. Insofar Proposition 2.4.4 is a special property of elliptic curves resp. more generally proper integral group schemes. *(2 points)*

3. The elliptic curve E over $\mathbb{F}_2$ is given by the Weierstraß equation $y^2+y = x^3+a_6$ with $a_6 \in \mathbb{F}_2$.

   (a) Prove that $[2] = \varphi \circ \mathrm{Fr}_4$ and $\widehat{\mathrm{Fr}}_2 = \varphi \circ \mathrm{Fr}_2$ for a suitable $\varphi \in \mathrm{Aut}(E)$.

   (b) Use that to determine $E[2](k^{\mathrm{alg}})$ (cf. Exercise 3, sheet 12).

   (c) Compute $\deg(1 - \mathrm{Fr}_{2^r})$ for $r = 1, \ldots, 8$ with the help of $\widehat{\mathrm{Fr}}_{2^r}$. Check your result by computing $\#E(\mathbb{F}_{2^r})$ directly. *(6 points)*

4. $\star$ Figure out where you encounter elliptic curves in everyday life. You won't believe it. A possible keyword is *ECC*.

5. Welche Zusammenhänge, Details, Inhalte oder Fragen sollen in der Übung am 23.1. besprochen werden? *(2 points)*