29. January 2015

# Exercise sheet 8
# Elliptic Curves [1]

Kay Rülling

**Exercise 8.1.** Let $K$ be a field of characteristic $\neq 2$ and $E$ an elliptic curve over $k$ given by the equation $y^2 = x^3 + ax + b$. Denote by $E_2$ the group scheme of 2-torsion points in $E$.

Show:

$$E_2(K) \cong \mathbb{Z}/2 \oplus \mathbb{Z}/2 \text{ (as abstract groups)}$$
$$\iff x^3 + ax + b = (x-\alpha)(x-\beta)(x-\gamma), \quad \alpha, \beta, \gamma \in K.$$

**Exercise 8.2.** Let $E$ be an elliptic curve over $\mathbb{Q}$ with $E_2(\mathbb{Q}) \cong \mathbb{Z}/2 \oplus \mathbb{Z}/2$ and discriminant $\Delta$. By the Mordell-Weil Theorem we can write $E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus T$, where $T$ is a finite torsion group.

(1) Show that $T/2T = \mathbb{Z}/2 \oplus \mathbb{Z}/2$.
(2) Show $r \leq 2 \cdot \#\{p \in \mathbb{N} \text{ prime with } p|2\Delta\}$. (*Hint:* Use (1) and that the cardinality of $E(\mathbb{Q})/2E(\mathbb{Q})$ is bounded by the 2nd Selmer group $S^{(2)}(E/Q)$.)

**Exercise 8.3.** Let $G$ be a finite group, $H \subset G$ a normal subgroup and $M$ a $G$-module.

(1) Let $f : G/H \to M^H$ be a crossed homomorphism and denote by $\mathrm{Inf}(f)$ the composition
$$G \to G/H \xrightarrow{f} M^H \hookrightarrow M.$$
Show that this induces a well defined homomorphism
$$\mathrm{Inf} : H^1(G/H, M^H) \to H^1(G, M).$$
(2) Show that there is a short exact sequence
$$0 \to H^1(G/H, M^H) \xrightarrow{\mathrm{Inf}} H^1(G, M) \xrightarrow{\mathrm{Res}} H^1(H, M).$$
(3) Generalize the above to the case of a profinite group $G$ with a closed subgroup $H$ and an discrete $G$-module $M$.

[1]This exercise sheet will be discussed on February 3. If you have questions or remarks please contact `kay.ruelling@fu-berlin.de` or `l.zhang@fu-berlin.de`

**Exercise 8.4.** Denote by $H : \mathbb{P}^n(\bar{\mathbb{Q}}) \to \mathbb{R}_{\geq 1}$ the absolute height function and for an algebraic number $x \in \bar{\mathbb{Q}}$ set $H(x) := H((x : 1))$.

Show for $x \in \bar{\mathbb{Q}}^\times$ we have

$$H(x) = 1 \Longleftrightarrow x \text{ is a root of } 1.$$

To this end proceed as follows:

(1) Show this '$\Leftarrow$' direction.
(2) Let $K$ be a number field and set $S = \{x \in K^\times \mid H(x) = 1\}$.
  (a) Show $S$ is a subgroup of $K^\times$.
  (b) Let $x \in S$ and $f = T^d + a_{d-1}T^{d-1} + \ldots + a_0$ the minimal polynomial of $x$ with $a_i \in \mathbb{Q}$. Show that $H((1 : a_{d-1} : \ldots : a_0)) \leq 2^{d-1}$.
  (c) Conclude that there is a constant $C$ such that $H_K(x) \leq C$, for all $x \in S$.
  (d) Conclude that $S$ is a finite group.
(3) Conclude.