Fachbereich Mathematik und Statistik
Dr. Michele Serra
Prof. Dr. Salma Kuhlmann
SS 2023

Universität Konstanz

Introduction to Elliptic Curves

Exercise Sheet 2
Group law on cubics

Let K be a field with $\operatorname{char} K \neq 2, 3$.

Exercise 5 *Explicit formula for an elliptic curve in short Weierstraß form* **(4 points)**
Let $E : Y^2 = X^3 + aX + b$. Let $P_1 = (x_1, x_2)$ and $P_2 = (x_2, y_2)$ be two points on $E \cap \{Z \neq 0\}$. Set

$$\begin{cases} m = \frac{3x_1^2+a}{2y_1} & \text{if } x_1 = x_2 \wedge y_1 = y_2 \neq 0 \\ m = \frac{y_1-y_2}{x_1-x_2} & \text{otherwise} \end{cases}$$

Show that $P_1 + P_2 = (x_3, y_3)$ where $x_3 = m^2 - x_1 - x_2$ and $y_3 = -y_1 - m(x_3 - x_1)$.
The cases where $P_1 = O$ or $P_1 = O$ are known.

Exercise 6 **(2+2 points)**

(a) Deduce that, if $K \subseteq L \subseteq \bar{K}$ is an extension of K, then $(E(L), +)$ is a subgroup of $(E(\bar{K}), +)$.

(b) Derive a formula for the opposite $-P$ of a point $P = (x, y) \in E(\bar{K})$ when E is an elliptic curve given by a

- medium Weierstraß equation: $E\colon Y^2 = X^3 + a_2X^2 + a_4X + a_6$;
- long Weierstraß equation: $E\colon Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$.

Exercise 7 *Group law for "additive" singular cubics* **(4 points)**
We have encountered the two possible types of singular cubics. Let

$$C : Y^2 = f(X) = X^3 + aX + b$$

We know that C is singular if and only if $\Delta = -4a^3 - 27b^2 = 0$, in which case f has a double root $\alpha \in \bar{K}$. We saw that the only singularity occurs then at the point $P_0 = (\alpha, 0)$ (in affine coordinates).
Let $C_{ns}(\bar{K}) := C(\bar{K}) \setminus \{P_0\}$.
Assuming α is a triple root of f, show that the map

$$\begin{array}{rcl} \phi\colon (C_ns(\bar{K}), \oplus) & \longrightarrow & (\bar{K}, +) \\ (x, y) & \longmapsto & \frac{x}{y} \end{array}$$

is an isomorphism of abelian groups, where $(\bar{K}, +)$ is the additive group of $\bar{K}$ and $\oplus$ is defined on $C_ns(\bar{K}$ in the same way as for elliptic curves.

Because of this isomorphism we call such singular cubics *additive.*
In the case where f has a double root (at 0) and a simple root α, one can show that

(i) $(C_n s(\bar{K}), \oplus) \simeq (\bar{K}^\times, \cdot)$, if $\alpha \in K$ – *split-multiplicative*

(ii) $(C_n s(\bar{K}), \oplus) \simeq \{r + s\alpha : r, s \in K,\ r^2 - s^2\alpha^2 = 1\} \subseteq (K(\alpha), \cdot)$ – *non-split-multiplicative*

Exercise 8 **(2+2 points)**

(a) Let $E\colon Y^2 = X^3 + 73$ and let $P = (2, 9)$ and $Q = (3, 10)$. Note that $P, Q \in E(\mathbb{Q})$.
Compute $-P$, $2P := P + P$ and $P + Q$.

(b) Now let $E\colon Y^2 = X^3 + 10X + 6$. Find all points of order 2 of $E(\bar{\mathbb{Q}})$, i.e., P such that $2P = O$.

Please hand in your solutions by ***Wednesday, 17 May 2023, 13:30h*** *in the* ***postbox by F409*** *or per e-mail to your tutor.*