Arithmetik Elliptischer Kurven

Universität Frankfurt
Institut für Mathematik
Marius Leonhardt

Blatt 03
Wintersemester 2024/25
Besprechung am ~~20.11.2024~~ 04.12.2024

Aufgabe 1 (Divisoren auf Elliptischer Kurve) Es sei K ein Körper und (E, O) eine Elliptische Kurve über K.

(a) Zeige, dass $D = \sum_P n_P P \in \mathrm{Div}(E)$ genau dann ein Hauptdivisor ist, falls $\sum_P n_P = 0$ (in $\mathbb{Z}$) und $\sum_P [n_P]P = O$ (in E).

(b) Begründe, dass die Folge

$$1 \longrightarrow \overline{K}^\times \longrightarrow \overline{K}(E)^\times \longrightarrow \mathrm{Div}^0(E) \longrightarrow E \longrightarrow 1$$

exakt ist, wobei die erste Abbildung die Inklusion ist, die zweite Abbildung durch $\mathrm{div}\colon \overline{K}(E)^\times \longrightarrow \mathrm{Div}^0(E)$ und die dritte Abbildung durch $j_O^{-1}\colon \mathrm{Div}^0(E) \longrightarrow E$ gegeben ist.[1] Wenn du magst, denke darüber nach, was passiert, wenn man $\mathrm{Gal}(\overline{K}/K)$-Invarianten nimmt.

Aufgabe 2 (Multiplikation mit n und Torsion) Es sei K ein Körper. Wir betrachten die Elliptische Kurve

$$E\colon \quad y^2 = x^3 + ax + b$$

über K sowie $P = (x_P, y_P) \in E \setminus E[2]$.

(a) Zeige, dass

$$[2]P = \big(\lambda^2 - 2x_P, -y_P - \lambda(\lambda^2 - 3x_P)\big)$$

gilt, wobei $\lambda = \frac{3x_P^2 + a}{2y_P}$ die Tangentensteigung im Punkt P ist.[2]

(b) Finde ein Polynom[3], dessen Nullstellen genau die x-Koordinaten der 3-Torsionspunkte sind. (*Hinweis:* $[3]T = O \Leftrightarrow [2]T = \ominus T$.)

(c) (Bonus) Zeige die Formel aus Beispiel 3.12: Auf der Kurve $E\colon y^2 = x(x^2 + ax + b)$ ist die Translation mit $P = (0, 0)$ gegeben durch $(x, y) \mapsto \left(\frac{b}{x}, -\frac{by}{x^2}\right)$.

Aufgabe 3 (Isogenien) Beweise Korollare 3.8 und 3.9, also:

(a) Für eine Isogenie $\Phi\colon E_1 \to E_2$ ist $E_1[\Phi] := \ker(\Phi)$ endlich von Ordnung $\deg_s(\Phi)$.

(b) $\mathrm{End}(E)$ ist ein (nicht notwendigerweise kommutativer) Ring und $[\cdot]\colon \mathbb{Z} \to \mathrm{End}(E)$ ist ein injektiver Ringhomomorphismus.

Bonusaufgabe 4 (Komplexe Multiplikation) Es sei E die über $\mathbb{Q}$ definierte Elliptische Kurve

$$E\colon y^2 = x^3 - x.$$

Finde einen (nicht notwendigerweise über $\mathbb{Q}$ definierten) Endomorphismus $\Phi\colon E \to E$ mit $\Phi^2 = [-1]$. (*Hinweis:* Es gilt $[-1]\colon (x, y) \mapsto (x, -y)$. Versuche eine ähnliche Substitution!) Zeige weiter, dass

$$[\cdot]\colon \mathbb{Z}[i] \to \mathrm{End}(E), \quad [a + bi] := [a] + [b]\Phi$$

ein injektiver Ringhomomorphismus[4] ist.

---

[1] Hier bezeichnet wie so oft E auch die Menge $E(\overline{K})$ der $\overline{K}$-Punkte von E.
[2] Insbesondere ist also die x-Koordinate $x([2]P)$ eine rationale Funktion von Grad 4 in $x(P)$.
[3] Ein solches Polynom heißt Divisionspolynom, vgl. [AEC, Exercise 3.7].
[4] Nach 3.10 ist $[\cdot]$ sogar ein Ringisomorphismus.