Arithmetik Elliptischer Kurven

Universität Frankfurt
Institut für Mathematik
Marius Leonhardt

Blatt 07
Wintersemester 2024/25
Besprechung am 12.02.2025

Aufgabe 1 (Diverses) Betrachte die über $\mathbb{Q}$ definierte Elliptische Kurve

$$E\colon \quad y^2 + xy = x^3 - 2x + 1$$

mit Diskriminante $\Delta = -61$.

(a) Bestimme $\#\widetilde{E}_p(\mathbb{F}_p)$ für $p \leq 7$, wobei $\widetilde{E}_p$ die Reduktion von E modulo p bezeichne.

(b) Bestimme $E(\mathbb{Q})_{\text{tors}}$.

(c) Zeige, dass die Ordnung von $E(\mathbb{Q}_2)_{\text{tors}}$ ein Teiler von 8 ist.

(d) Es sei $P = (0,1) \in E(\mathbb{Q})$. Zeige, dass $7P$ und $9P$ keine ganzzahligen Koordinaten haben. (Du sollst die Punkte nicht berechnen; sie lauten $7P = \left(\frac{157728}{4092529}, -\frac{8115092999}{8279186167}\right)$ und $9P = \left(-\frac{3971776544}{99083300625}, \frac{33045229680632279}{31188945954234375}\right)$.)

Aufgabe 2 (Torsionsuntergruppe) Bestimme jeweils die Torsionsuntergruppe von $E(\mathbb{Q})$ für

(a) $E\colon y^2 + y = x^3 + x^2$.

(b) $E\colon y^2 + xy + y = x^3$.

Bonusaufgabe 3 (Torsionspunkte) Es sei E eine Elliptische Kurve über $\mathbb{Q}$ gegeben durch eine Weierstraß-Gleichung mit $a_1, \dots, a_6 \in \mathbb{Z}$. Sei weiter $O \neq T = (x,y) \in E(\mathbb{Q})_{\text{tors}}$.

(a) Zeige mit Hilfe der formalen Gruppe $\widehat{E}$:

(i) $4x, 8y \in \mathbb{Z}$.

(ii) Falls $2 | a_1$ oder $2T \neq O$, so gilt $x, y \in \mathbb{Z}$. (*Hinweis*: Überlege, wann T in $\widehat{E}(2\mathbb{Z}_2)$ liegen kann. Es gilt $-T = (x, -y - a_1x - a_3)$.)

(b) (Lutz–Nagell) Zeige: Ist E gegeben durch eine kurze Weierstraß-Gleichung der Form $y^2 = x^3 + ax + b =: f(x)$ mit $a, b \in \mathbb{Z}$, so gilt $x, y \in \mathbb{Z}$ und entweder $y = 0$ oder $y^2 | (4a^3 + 27b^2)$.

(*Hinweis*: Falls $2T = (x_2, y_2) \neq O$, so gilt $x_2 = \left(\frac{f'(x)}{2y}\right)^2 - 2x$. Außerdem gilt $(3x^2 + 4a)f'(x)^2 - 27(x^3 + ax - b)f(x) = 4a^3 + 27b^2$ in $\mathbb{Z}[x]$.)

Bonusaufgabe 4 (Kummer-Paarung) Es sei K ein Körper mit $\mu_n \subset K$, wobei $n \in \mathbb{N}$ mit $\operatorname{char}(K) \nmid n$. Es sei $\Delta \subset K^\times/(K^\times)^n$ eine endliche Untergruppe und $L = K(\sqrt[n]{\Delta})$. Betrachte die Kummer-Paarung

$$\begin{aligned} \langle \cdot, \cdot \rangle\colon \quad \operatorname{Gal}(L/K) \times \Delta &\longrightarrow \mu_n \\ (\sigma, [x]) &\longmapsto \frac{\sigma(\sqrt[n]{x})}{\sqrt[n]{x}}. \end{aligned}$$

Zeige:

(a) $\langle \cdot, \cdot \rangle$ ist wohldefiniert, also unabhängig von der Wahl von x und $\sqrt[n]{x}$.

(b) $\langle \cdot, \cdot \rangle$ ist bilinear.

(c) $\langle \cdot, \cdot \rangle$ ist nicht-ausgeartet, induziert also injektive Gruppenhomomorphismen $\operatorname{Gal}(L/K) \to \operatorname{Hom}(\Delta, \mu_n)$ und $\Delta \to \operatorname{Hom}(\operatorname{Gal}(L/K), \mu_n)$

(d) Zeige, dass die Abbildungen in (c) bijektiv sind. (*Hinweis:* Verwende (mit oder ohne Beweis) $\#\operatorname{Hom}(A, \mathbb{C}^\times) = \#A$ für jede endliche abelsche Gruppe A.)

Aufgabe 5 (Schwache Version von Mordell–Weil: Reduktion) Es sei E eine Elliptische Kurve über K, $n \geq 2$ nicht durch $\operatorname{char}(K)$ teilbar und L/K eine endliche Galoiserweiterung mit $E[n] \subset E(L)$.

(a) Konstruiere eine injektive Abbildung $\lambda\colon \big(E(L) \cap [n]^{-1}(E(K))\big)/E(K) \longrightarrow \operatorname{Abb}(\operatorname{Gal}(L/K), E[n]), Q \longmapsto \lambda_Q$ (*Hinweis:* Kummer-Paarung. Weder λ_Q noch λ müssen Homomorphismen sein.)

(b) Folgere, dass $E(K)/nE(K) \longrightarrow E(L)/nE(L)$ endlichen Kern hat. Schließe, dass $E(K)/nE(K)$ endlich ist, falls $E(L)/nE(L)$ endlich ist. (Wer Gruppenkohomologie kennt, kann (b) auch ohne (a) zeigen.)

Bonusaufgabe 6 (Kanonische Höhe) Es sei E eine Elliptische Kurve über $\mathbb{Q}$. Zeige, dass die Folge $4^{-n}h(2^nP)$ für $P \in E(\mathbb{Q})$ konvergiert. Zeige weiter, dass es eine Konstante $c > 0$ gibt mit $|\widehat{h}(P) - h(P)| \leq c$ für alle $P \in E(\mathbb{Q})$.