Arithmetik Elliptischer Kurven

Universität Frankfurt
Institut für Mathematik
Marius Leonhardt

Blatt 02
Wintersemester 2024/25
Besprechung am 13.11.2024

Aufgabe 1 (Verzweigungspunkte) Es sei K ein Körper mit $\mathrm{char}(K) \neq 2$, $\lambda \in K \setminus \{0,1\}$ und E die Elliptische Kurve

$$E\colon \quad y^2 = x(x-1)(x-\lambda).$$

Betrachte die rationale Abbildung $x\colon E \longrightarrow \mathbb{P}^1, \quad P \longmapsto [x(P):1]$. Bestimme die Verzweigungspunkte von x. Schlage die Formel von Riemann–Hurwitz nach und zeige (erneut), dass E Geschlecht 1 hat. Wiederhole das Ganze für y statt x.

Bonusaufgabe 2 ($\mathbb{P}^1$ II) Es sei K algebraisch abgeschlossen (vielleicht mit $\mathrm{char}(K) = 0$).

(a) Es sei $\Phi\colon \mathbb{P}^1 \to \mathbb{P}^1$ gegeben durch $\Phi([X:Y]) = [X^3(X-Y)^2 : Y^5]$. Bestimme $\deg(\Phi)$ sowie alle Verzweigungspunkte P und -indizes $e_\Phi(P)$ und verifiziere so für alle $Q \in \mathbb{P}^1$ die Formel

$$\sum_{R \in \Phi^{-1}(Q)} e_\Phi(R) = \deg(\Phi).$$

(b) Was sagt die Formel von Riemann–Hurwitz über die Abbildung aus (a)?

(c) Wenn du magst, denke darüber nach, was bei (a) und (b) für ein beliebiges nicht-konstantes $\Phi\colon \mathbb{P}^1 \to \mathbb{P}^1$, also $\Phi = [f:1]$ für ein nicht-konstantes $f \in K(x)$, passiert.

Bonusaufgabe 3 (Kurve von Geschlecht 1 vs. Elliptische Kurve) Es sei p eine Primzahl. Zeige, dass die über $\mathbb{Q}$ definierte, ebene, projektive Kurve

$$C\colon \quad X^3 + pY^3 + p^2Z^3 = 0$$

glatt ist, aber keinen $\mathbb{Q}$-rationalen Punkt besitzt (und damit keine Elliptische Kurve ist). Ist C eine Elliptische Kurve über einer endlichen Erweiterung von $\mathbb{Q}$?

Aufgabe 4 (Weierstraß-Gleichungen)

(a) Zeige, dass der Punkt $[0:1:0]$ auf der Kurve E aus Aufgabe 1 ein 'point of inflection'[1] ist.

Betrachte nun die über $\mathbb{Q}$ definierte, ebene, projektive Kurve

$$C_d\colon \quad U^d + V^d = W^d.$$

(b) ($d = 3$) Finde die 'points of inflection'[2] auf C_3 und bringe die Kurve C_3 in Weierstraß-Form. (*Hinweis*: Finde eine Koordinatentransformation, die einen von dir gewählten 'point of inflection' P auf $[0:1:0]$ und seine Tangente auf $\{Z=0\}$ abbildet.)

(c) ($d = 4$) Es seien $x, y \in \mathbb{Q}(C_4)$ gegeben durch $x = \frac{W^2}{U^2}$ und $y = \frac{V^2W}{U^3}$. Zeige, dass

$$y^2 = x^3 - x$$

und bestimme damit alle $\mathbb{Q}$-rationalen Punkte auf C_4. (*Hinweis:* Du darfst ohne Beweis verwenden, dass 1 keine kongruente Zahl ist.)

Aufgabe 5 (Addition auf Elliptischer Kurve) Es sei E die über $\mathbb{Q}$ definierte Elliptische Kurve

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

und $P = (0,0) \in E(\mathbb{Q})$. Zeichne $E(\mathbb{R})$. Bestimme[3] Δ_E und $j(E)$. Berechne nP für $n \in \{2,3,4,5\}$. (Wenn du magst, mach weiter mit $n \in \{6,7,8\}$. Was fällt dir bei den Nennern der Koordinaten auf?)

Aufgabe 6 (Quadratische Twists) Es sei E eine Elliptische Kurve definiert über $\mathbb{Q}$, gegeben durch die Weierstraß-Gleichung

$$E\colon \quad y^2 = f(x).$$

(a) Bestimme für $d \in \mathbb{Q}^\times$ eine Weierstraß-Gleichung für $E_d\colon dy^2 = f(x)$.

(b) Benutze das Gruppengesetz auf $E\colon \quad y^2 = x^3 - 25x$, um zwei Dreiecke mit rationalen Seitenlängen und Flächeninhalt 5 zu finden. (Hinweis: Blatt 1, Aufgabe 4)

(c) Zeige, dass im Falle $j(E) \neq 0, 1728$ jeder Twist[4] von E isomorph zu einem E_d ist. Ist d eindeutig?

---

[1] Das heißt, seine Tangente schneidet die Kurve mit Vielfachheit 3.
[2] Diese sind gerade die Nullstellen der Determinante der Hesse-Matrix des homogenen Polynoms.
[3] Formeln hierfür sind in [Si, AEC, III.1, S. 42]; Achtung: $b_2 = a_1^2 + 4a_2$.
[4] Ein *Twist* von E ist eine Elliptische Kurve E' definiert über $\mathbb{Q}$, die $\overline{\mathbb{Q}}$-isomorph zu E ist.