Arithmetik Elliptischer Kurven

Universität Frankfurt
Institut für Mathematik
Marius Leonhardt

Blatt 01
Wintersemester 2024/25
Besprechung am 30.10.2024

Aufgabe 1 (Affine und projektive Kurven) Lies die ersten beiden Abschnitte (ohne die letzte Seite) von Appendix A in Silverman-Tate: Rational Points on Elliptic Curves. Überlege dir Fragen und bringe sie zur nächsten Vorlesung (23.10.) mit. Überlege dir Beispiele und Gegenbeispiele für die wichtigsten Objekte, z.B. für affine und projektive Kurven und ihre singulären und nicht-singulären Punkte. Wer möchte, kann über die Aufgaben A.5, A.8 und A.9 nachdenken.

Aufgabe 2 (Glattheit) Es sei K algebraisch abgeschlossen mit $\operatorname{char}(K) \neq 2$ und $f \in K[x]$ vom Grad $\deg(f) \geq 3$. Weiter sei C der projektive Abschluss (in $\mathbb{P}^2$) der affinen ebenen Kurve

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

(a) Zeige, dass im Fall $\deg(f) = 3$ die Kurve C genau dann glatt ist, wenn f paarweise verschiedene Nullstellen hat. (*Hinweis*: Betrachte den Punkt im Unendlichen separat.)

(b) Was passiert für $\deg(f) \geq 4$?

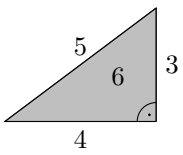
Aufgabe 3 (Gruppengesetz) Es sei K ein Körper mit $\operatorname{char}(K) \neq 2$ und E/K die (affine) Kurve gegeben durch

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

mit $f(x) \in K[x]$ vom Grad 3 ohne mehrfache Nullstelle in $\overline{K}$. Weiter seien $P, Q \in E(K)$ zwei K-rationale Punkte auf E mit verschiedenen x-Koordinaten. Zeige, dass die Gerade L durch P und Q die Kurve E in genau einem weiteren Punkt $R \in \overline{K}^2$ schneidet, und dass R Koordinaten in K hat.

Waren alle Voraussetzungen in dieser Aufgabe wirklich notwendig? Finde außerdem den Fehler in der Formulierung dieser Aufgabe und überlege, wie sie hätte formuliert werden müssen.

Aufgabe 4 (Kongruente Zahlen) Eine positive rationale Zahl D heißt *kongruent*, falls es ein rechtwinkliges Dreieck mit rationalen Seitenlängen mit Flächeninhalt D gibt. Zum Beispiel ist $D = 6$ kongruent.



Zeige, dass D genau dann kongruent ist, wenn die Elliptische Kurve

$$E_D\colon \quad Dy^2 = x^3 - x$$

einen rationalen Punkt $(x, y) \in E_D(\mathbb{Q})$ mit $y \neq 0$ hat.[1]

Aufgabe 5 (Divisoren) Es sei K ein Körper mit $\operatorname{char}(K) \neq 2$, $\lambda \in K \setminus \{0, 1\}$ und E die Elliptische Kurve

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

(a) Bestimme $\operatorname{div}(x)$ und $\operatorname{div}(y)$.

(b) Zeige, dass $\omega = \frac{dx}{y}$ keine Null- oder Polstellen hat.

Aufgabe 6 ($\mathbb{P}^1$) Es sei $K = \overline{K}$ und $\infty = [1 : 0] \in \mathbb{P}^1$. Die Koordinate auf $\mathbb{P}^1$ heiße x.

(a) Schau die Definition des Funktionenkörpers einer glatten Kurve nach und "zeige" $K(\mathbb{P}^1) = K(x)$.

(b) Es sei $f \in K[x] \setminus \{0\}$. Bestimme $\operatorname{ord}_\infty(f)$ und den Divisor $\operatorname{div}(f)$. Verifiziere $\deg(\operatorname{div}(f)) = 0$.

(c) Zeige $\operatorname{div}(dx) = -2\infty$. Folgere, dass 0 das einzige holomorphe Differential auf $\mathbb{P}^1$ ist, also $g(\mathbb{P}^1) = 0$.

(d) Was sagt der Satz von Riemann–Roch[2] für $\mathbb{P}^1$? Bestimme für alle $n \in \mathbb{Z}$ eine Basis von $\mathcal{L}(n\infty)$.

---

[1] *Hinweis*: Schränke dich auf quadratfreie $D \in \mathbb{N}$ ein und benutze die Beschreibung Pythagoreischer Tripel aus der Vorlesung.
[2] Dieser Teil wird erst nach der Vorlesung vom 30.10. Sinn ergeben.