

Übungsblatt 7

*Besprechung der mündlichen Aufgaben am 8. 12. 2022
Abgabe der schriftlichen Lösungen bis 13. 12. 2022, 23:59 Uhr*

Aufgabe 40

mündlich

Sei E eine durch die Gleichung $F(x, y) = 0$ im \mathbb{R}^2 definierte Kurve, wobei F die Form $F(x, y) = y^2 - x^3 - ax - b$ hat. Zeigen Sie, dass folgende Bedingungen äquivalent sind.

- (a) Das Polynom $p(x) = x^3 + ax + b$ hat eine mehrfache Nullstelle.
- (b) Es gilt $4a^3 = -27b^2$.
- (c) Es ex. ein Punkt $(x_0, y_0) \in E$, für den die partiellen Ableitungen $\frac{\delta F}{\delta x}(x_0, y_0)$ und $\frac{\delta F}{\delta y}(x_0, y_0)$ beide 0 sind. (Ein solcher Punkt heißt *singulär*.)

Aufgabe 41

mündlich

- (a) Geben Sie eine geometrische Bedingung dafür an, dass ein Punkt P auf einer elliptischen Kurve über \mathbb{R} die Ordnung 2, 3 oder 4 hat.
- (b) Zeigen Sie, dass eine elliptische Kurve $y^2 = x^3 + ax + b$ über \mathbb{F}_q nicht zyklisch ist, wenn das Polynom $x^3 + ax + b$ drei verschiedene Nullstellen in \mathbb{F}_q hat.

Aufgabe 42

mündlich

Eine elliptische Kurve E über \mathbb{F}_q ($q = 2^n$) enthält neben dem Punkt \mathcal{O} alle Lösungen $(x, y) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ einer Gleichung der Form

$$y^2 + cy = x^3 + ax + b \quad \text{oder} \quad y^2 + xy = x^3 + ax^2 + b .$$

Leiten Sie für Gleichungen der Form $y^2 + cy = x^3 + ax + b$ Formeln für die Koordinaten von $-P$ und $P+Q$ in Abhängigkeit der Koordinaten von $P = (x_1, y_1)$ und $Q = (x_2, y_2)$ her.

Hinweis: Bestimmen Sie hierzu wie in der Vorlesung die Koordinaten des Schnittpunktes der durch P und \mathcal{O} (bzw. durch P und Q) definierten Geraden mit der Kurve über \mathbb{R} und beachten Sie die Besonderheiten der Arithmetik in \mathbb{F}_{2^n} .

Aufgabe 43*mündlich*

Die Ursprungsgeraden

$$g(X, Y, Z) = \{(\lambda X, \lambda Y, \lambda Z) \mid \lambda \in \mathbb{R}\}, (X, Y, Z) \in \mathbb{R}^3 - \{(0, 0, 0)\}$$

bilden die Punkte der *projektiven Ebene*. Es gilt also $g(X, Y, Z) = g(X', Y', Z')$, falls ein $\lambda \in \mathbb{R} - \{0\}$ existiert mit $X' = \lambda X$, $Y' = \lambda Y$ und $Z' = \lambda Z$.

- Überlegen Sie, wie sich die affine Ebene \mathbb{R}^2 in die projektive Ebene einbetten lässt. (*Hinweis:* Verwenden Sie nur projektive Punkte der Form $g(X, Y, 1)$.)
- Zeigen Sie, dass von dieser Einbettung genau die projektiven Punkte der Form $g(X, Y, 0)$ nicht erfasst werden. Welche Punkte müsste man zum \mathbb{R}^2 hinzunehmen, damit diese Einbettung zu einem Isomorphismus wird? Geben Sie eine geometrische Interpretation dieser Punkte.
- Im \mathbb{R}^2 sei durch $F(x, y) = y^2 - x^3 - ax - b = 0$ eine Kurve definiert. Wie lässt sich hieraus eine Kurvengleichung $\tilde{F}(X, Y, Z) = 0$ für die Einbettung $\{g(x, y, 1) \mid F(x, y) = 0\}$ dieser Kurve in die projektive Ebene gewinnen?
- Für welche projektiven Punkte der Form $g(X, Y, 0)$ gilt ebenfalls $\tilde{F}(X, Y, Z) = 0$?

Aufgabe 44 Wieviele Punkte haben folgende ell. Kurven über \mathbb{F}_q ? **10 Punkte**

- $y^2 = x^3 - 1$ im Fall $q \equiv_6 5$ und
- $y^2 + y = x^3$ im Fall $q \equiv_3 2$.