Übungsblatt 5

Aufgabe 33 ***mündlich***

Sei E die elliptische Kurve $y^2 = x^3 - 12x - 16$ über $\mathbb{R}$.

(a) Skizzieren Sie zeichnerisch den Verlauf von E.

(b) Berechnen Sie die Summe $P + Q$ für $P = (4, 0)$ und $Q = (5, 7)$.

(c) Berechnen Sie die Punkte $2P = P + P$ und $2Q = Q + Q$.

Aufgabe 34 ***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 35 ***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 36 ***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 $Z' = \lambda Z$.

(a) Überlegen Sie, wie sich die affine Ebene $\mathbb{R}^2$ in die projektive Ebene einbetten lässt. (*Hinweis:* Verwenden Sie nur projektive Punkte der Form $g(X, Y, 1)$.)

(b) 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.

(c) 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?

(d) Für welche projektiven Punkte der Form $g(X, Y, 0)$ gilt ebenfalls $\tilde{F}(X, Y, Z) = 0$?

Aufgabe 37 ***10 Punkte***

Sei E die elliptische Kurve $y^2 = x^3 - 7x - 6$ über $\mathbb{R}$.

(a) Skizzieren Sie zeichnerisch den Verlauf von E.

(b) Berechnen Sie die Summe $P + Q$ für $P = (4, \sqrt{30})$ und $Q = (3, 0)$.

(c) Berechnen Sie die Punkte $2P = P + P$ und $2Q = Q + Q$.