Prof. Dr. H. Brenner **Osnabrück WS 2021/2022**

Elliptische Kurven

Arbeitsblatt 5

Aufgaben

Aufgabe 5.1. Bestimme die Wendepunkte der projektiven Kurve

$$V_+(YZ^2 - X^3) \subseteq \mathbb{P}^2_K$$

über einem Körper K.

Aufgabe 5.2. Es sei K ein Körper der Charakteristik $\neq 3$ und sei $F = X^3 + Y^3 + Z^3$.

(1) Bestimme die Hesse-Matrix von F.
(2) Bestimme die Determinante der Hesse-Matrix von F.
(3) Bestimme die Schnittpunkte von $V_+(F)$ mit der projektiven Nullstellenmenge zur Determinate der Hesse-Matrix von F über $K = \mathbb{C}$
(4) Bestimme für jeden Schnittpunkt aus Teil (3) die Tangente und bestätige Lemma 5.1.

Aufgabe 5.3.*

Es sei $F = X^3 + aXZ^2 + bZ^3 - Y^2Z \in K[X, Y, Z]$ über einem Körper K mit gewissen $a, b \in K$.

(1) Bestimme die Hesse-Matrix zu F.
(2) Bestimme die Hesse-Matrix von F im Punkt $(0, 1, 0)$.
(3) Bestimme ein nichttriviales Element des Kernes der Hesse-Matrix von F im Punkt $(0, 1, 0)$.

Aufgabe 5.4.*

Zeige, dass ein Polynom $X^3 + aX + b$ genau dann keine mehrfachen Nullstellen (und zwar auch nach keiner Körpererweiterung) besitzt, wenn die Diskriminante $4a^3 + 27b^2$ von 0 verschieden ist.

Aufgabe 5.5. Es sei $F \in \mathbb{Q}[X]$ ein irreduzibles Polynom vom Grad 3. Zeige, dass F entweder eine oder drei reelle Nullstellen besitzt.

Aufgabe 5.6.*

Finde acht Punkte (x, y) mit ganzzahligen Komponenten, die die Bedingung

$$y^2 = x^3 + 17$$

erfüllen.

Aufgabe 5.7.*

Wir betrachten die elliptische Kurve E, die durch die affine Gleichung

$$Y^2 = X^3 - X$$

gegeben ist.

(1) Parametrisiere den oberen Bogen von $E(\mathbb{R})$ für $x \in [-1, 0]$.
(2) Bestimme den Punkt P aus $E(\mathbb{R})$ mit $x \in [-1, 0]$ und mit der maximalen y-Koordinate.
(3) Beschreibe eine endliche Körpererweiterung $\mathbb{Q} \subseteq K$ derart, dass $P \in E(K)$ liegt.

Aufgabe 5.8. Es sei R ein Integritätsbereich mit Quotientenkörper $K = Q(R)$ und es sei $y^2 = x^3 + ax + b$ die Gleichung für eine elliptische Kurve über K. Zeige, dass es eine lineare Transformation derart gibt, dass in der neuen Gleichung für die Kurve die Koeffizienten aus R sind.

Die vorstehende Aufgabe ist der Grund, warum man elliptische Kurven über $\mathbb{Q}$ direkt über $\mathbb{Z}$ realisieren kann. Es ist aber ein diffiziles Problem, was die optimale Realisierung über $\mathbb{Z}$ ist. Siehe die folgende Aufgabe und Aufgabe 25.18.

Aufgabe 5.9.*

Zeige, dass die beiden affinen Gleichungen

$$Y^2 = X^3 + 16$$

und

$$V^2 + V = U^3$$

die gleiche elliptische Kurve über $\mathbb{Q}$ definieren.

Aufgabe 5.10. Wir betrachten die durch $y^2 = x^3 + ax + b$ bzw. $y^2 = x^3 + a'x + b'$ gegebenen elliptischen Kurven C und C' in kurzer Weierstraßform, wobei die Beziehung $c^4a' = a$ und $c^6b' = b$ mit einem $c \in K$, $c \neq 0$, gelte. Zeige, dass die beiden Kurven die gleiche j-Invariante besitzen.

Aufgabe 5.11. Bestimme die Diskriminante und die j-Invariante der durch die Gleichung

$$y^2 = x^3 + x$$

gegebenen elliptischen Kurve.

Aufgabe 5.12. Bestimme die Diskriminante und die j-Invariante der durch die Gleichung

$$y^2 = x^3 + 1$$

gegebenen elliptischen Kurve.

Aufgabe 5.13.*

Berechne

$$(-x^2 + x - 1)^3 .$$

Aufgabe 5.14.*

Berechne

$$(-2x^3 + 3x^2 + 3x - 2)^2$$

Aufgabe 5.15.*

Finde eine lineare Substitution $X = \alpha Y + \beta$ mit $\alpha, \beta \in \mathbb{C}$ derart, dass aus dem Polynom $X^3 - 1$ ein Polynom in Y entsteht, das 0 und 1 als Nullstellen besitzt. Wie lautet die dritte Nullstelle?

Aufgabe 5.16.*

Wir betrachten die rationale Funktion

$$F(\lambda) = \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2}$$

in der Variablen λ.

(1) Zeige
$$F(1 - \lambda) = F(\lambda).$$
(2) Zeige
$$F(\frac{1}{\lambda}) = F(\lambda).$$
(3) Zeige
$$F(\frac{1}{1-\lambda}) = F(\frac{\lambda - 1}{\lambda}) = F(\frac{\lambda}{\lambda - 1}) = F(\lambda).$$

Abbildungsverzeichnis