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

Elliptische Kurven

Arbeitsblatt 6

Aufgaben

Aufgabe 6.1. Es sei M eine Menge mit einer Verknüpfung

$$*\colon M \times M \longrightarrow M,\ (P,Q) \longmapsto P*Q,$$

die für alle Elemente $P,Q,R,S \in M$ folgende Eigenschaften erfüllt.

(1) $P*Q = Q*P$
(2) $(P*Q)*P = Q$
(3) $((P*Q)*R)*S = P*((Q*S)*R)$.

Es sei $\mathfrak{O}$ ein beliebiges aber fest gewähltes Element aus M. (a) Zeige, dass die Verknüpfung

$$P+Q := (P*Q)*\mathfrak{O}$$

eine kommutative Gruppenstruktur auf M mit $\mathfrak{O}$ als neutralem Element definiert.

(b) Es sei nun $\mathfrak{O}'$ ein zweites Element aus M. Zeige, dass die durch $\mathfrak{O}$ und durch $\mathfrak{O}'$ definierten Gruppen isomorph sind.

Aufgabe 6.2. Begründe die Assoziativität der Verknüpfung in Satz 6.3 für die Fälle, wo manche der Schnittpunkte zusammenfallen.

Aufgabe 6.3.*

Berechne auf der durch

$$Y^2 = X^3+1$$

gegebenen elliptischen Kurve die Summen $(0,1)+(0,1)$ und $(0,1)+(0,1)+(0,1)$.

Aufgabe 6.4. Berechne auf der durch

$$Y^2 = X^3+1$$

gegebenen elliptischen Kurve die Summe $(2,3)+(3,\sqrt{28})$.

Aufgabe 6.5.*

Berechne auf der durch

$$Y^2 = X^3 + 4X$$

gegebenen elliptischen Kurve die Summe $(2,4)+(2,4)$.

Aufgabe 6.6. Berechne auf der durch

$$y^2 = x^3 - 25x$$

gegebenen elliptischen Kurve die Summe (vergleiche Beispiel 4.11)

$$\left(\frac{1681}{144}, \frac{62279}{1728}\right) + (5,\, 0)\ .$$

Bei den beiden folgenden Aufgaben verwende man, dass die einzige kompakte zusammenhängende reelle eindimensionale Mannigfaltigkeit die S^1 ist und dass die einzige eindimensionale kompakte zusammenhängende reelle Lie-Gruppe die S^1 mit der üblichen Verknüpfung ist.

Aufgabe 6.7. Es sei E eine elliptische Kurve über $\mathbb{R}$, gegeben in kurzer Weierstraßform $Y^2 = X^3 + aX + b$ mit $a, b \in \mathbb{R}$. Zeige, dass die folgenden Aussagen äquivalent sind.

(1) Das Polynom $X^3 + aX + b$ besitzt in $\mathbb{R}$ genau eine Nullstellen.
(2) $E(\mathbb{R})$ ist in der metrischen Topologie zusammenhängend.
(3) Es gilt die Homöomorphie $E(\mathbb{R}) \cong S^1$.
(4) Es ist $E(R) \cong S^1$ als reelle Lie-Gruppe.

Aufgabe 6.8. Es sei E eine elliptische Kurve über $\mathbb{R}$, gegeben in kurzer Weierstraßform $Y^2 = X^3 + aX + b$ mit $a, b \in \mathbb{R}$. Zeige, dass die folgenden Aussagen äquivalent sind.

(1) Das Polynom $X^3 + aX + b$ besitzt in $\mathbb{R}$ drei Nullstellen.
(2) $E(\mathbb{R})$ besteht in der metrischen Topologie aus zwei Zusammenhangskomponenten.
(3) Es gilt die Homöomorphie $E(\mathbb{R}) \cong S^1 \uplus S^1$.
(4) Es ist $E(R) \cong S^1 \times \mathbb{Z}/(2)$ als reelle Lie-Gruppe.

Aufgabe 6.9. Es sei E eine elliptische Kurve über $\mathbb{R}$, gegeben in kurzer Weierstraßform und Zerlegungsform $Y^2 = X^3 + aX + b = (X-\lambda_1)(X-\lambda_2)(X-\lambda_3)$ mit $a, b \in \mathbb{R}$ und $\lambda_1 < \lambda_2 < \lambda_3$. Wir setzen $B = (0, \lambda_2)$ und zerlegen $E(\mathbb{R}) = M \uplus N$ mit

$$M = \{P \in E(\mathbb{R}) \mid \lambda_1 \leq x(P) \leq \lambda_2\}$$

und

$$N = \{P \in E(\mathbb{R}) \mid x(P) \geq \lambda_3\}.$$

(1) Zeige, dass durch $P \mapsto P + B$ eine Bijektion zwischen M und N gegeben ist.
(2) Zeige, dass die Summe von zwei Punkten $P, Q \in M$ in N liegt.
(3) Zeige, dass die Summe von zwei Punkten $P, Q \in N$ wieder in N liegt.

Aufgabe 6.10. Bestimme auf der durch

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

gegebenen elliptischen Kurve E über $\mathbb{Z}/(3)$ die Gruppenstruktur von

$$E(\mathbb{Z}/(3)).$$

Die Lösung zur folgenden Aufgabe nimmt Bezug auf spätere Resultate. Man kann aber auch alles direkt berechnen.

Aufgabe 6.11.*

Bestimme auf der durch

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

gegebenen elliptischen Kurve E über $\mathbb{Z}/(5)$ die Gruppenstruktur von

$$E(\mathbb{Z}/(5)).$$

Aufgabe 6.12. Bestimme auf der durch

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

gegebenen elliptischen Kurve E über $\mathbb{Z}/(7)$ die Gruppenstruktur von

$$E(\mathbb{Z}/(7)).$$

Aufgabe 6.13.*

Überprüfe die zweite Darstellung aus Korollar 6.7, also

$$\begin{aligned} 2(x,y) &= \left(\frac{9x^4 + 6ax^2 + a^2}{4(x^3 + ax + b)} - 2x, \left(-\frac{(3x^2 + a)^3}{8(x^3 + ax + b)^2} + \frac{3x(3x^2 + a)}{2(x^3 + ax + b)} - 1 \right) y \right) \\ &= \left(\frac{x^4 - 2ax^2 - 8bx + a^2}{4(x^3 + ax + b)}, \frac{x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - a^3 - 8b^2}{8(x^3 + ax + b)^2} y \right). \end{aligned}$$

Aufgabe 6.14.*

Es sei E eine elliptische Kurve über einem Körper K mit kurzer Weierstraßgleichung $y^2 = x^3 + ax + b$. Wir betrachten den Ring

$$S = K[x_1, x_2, y_1, y_2]/(y_1^2 - x_1^3 - ax_1 - b, y_2^2 - x_2^3 - ax_2 - b),$$

in dem man die Gruppenstruktur auf der elliptischen Kurve mit rationalen Funktionen formulieren kann, siehe Satz 6.5.

(1) Zeige, dass eine endliche Erweiterung $K[x_1, x_2] \subseteq S$ vorliegt.
(2) Bestimme eine Ganzheitsgleichung für $y_2 - y_1$ über $K[x_1, x_2]$.
(3) Bestimme eine Ganzheitsgleichung für $\frac{y_2-y_1}{x_2-x_1}$ über $K(x_1, x_2)$.

vor.

Aufgabe 6.15.*

Es sei E eine elliptische Kurve über einem Körper K mit kurzer Weierstraßgleichung $y^2 = x^3 + ax + b$. Eliminiere in der Formel für die Addition (siehe Satz 6.5) die Terme y_1^1 und y_2^2 unter Verwendung der Kurvengleichung.

Aufgabe 6.16.*

Es sei

$$f_2(x) = \frac{x^4 - 2ax^2 - 8bx + a^2}{4(x^3 + ax + b)}$$

und

$$q_2(x) = \frac{x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - a^3 - 8b^2}{8(x^3 + ax + b)^2}.$$

Zeige $f_2' = 2q_2$.

Aufgabe 6.17.*

Schreibe f_{m+1} und q_{m+1} aus Korollar 6.8 ohne eine höhere Potenz von q_m.

Aufgabe 6.18.*

Es seien f_m und q_m wie in Korollar 6.8 definiert. Zeige $f_m' = mq_m$.

Aufgabe 6.19.*

Es sei

$$Y^2 = X^3 + rX^2 + sX + t$$

die Gleichung einer elliptischen Kurve. Zeige, dass die Verdoppelung eines Punktes (x, y) mit $y \neq 0$ durch

$$2(x, y) = \big(\alpha^2 - 2x - r,\, \alpha^3 - 3\alpha x - \alpha r + y\big)$$

mit $\alpha = \frac{3x^2+2rx+s}{2y}$ gegeben ist.

AUFGABE 6.20. Es sei

$$Y^2 = X^3 + rX^2 + sX + t$$

die Gleichung einer elliptischen Kurve E. Zeige, dass die Addition auf E im Sinne von Bemerkung 6.1 durch

$$(x_1, y_1) + (x_2, y_2) = \big(\alpha^2 - r - x_1 - x_2,\, \alpha\big(\alpha^2 - r - x_1 - x_2\big) + \beta\big)$$

mit $\alpha = \frac{y_2 - y_1}{x_2 - x_1}$ und $\beta = y_1 - \alpha x_1$ gegeben ist.

AUFGABE 6.21. Es sei

$$Y^2 = (X - \lambda_1)(X - \lambda_2)(X - \lambda_3)$$

die Gleichung einer elliptischen Kurve in Zerlegungsform. Zeige, dass die Verdoppelung eines Punktes (x, y) mit $y \neq 0$ durch

$$2(x, y) = \big(\alpha^2 - 2x + \lambda_1 + \lambda_2 + \lambda_3,\, \alpha^3 - 3\alpha x + \alpha(\lambda_1 + \lambda_2 + \lambda_3) + y\big)$$

mit $\alpha = \frac{3x^2 - 2(\lambda_1 + \lambda_2 + \lambda_3)x + \lambda_1\lambda_2 + \lambda_1\lambda_3 + \lambda_2\lambda_3}{2y}$ gegeben ist.

AUFGABE 6.22. Es sei $V_+(F) \subseteq \mathbb{P}^n_K$ eine glatte Hyperfläche vom Grad 3. Woran scheitert bei $n \geq 3$ die Idee, mit Hilfe des dritten Durchstoßungspunktes zu einer durch zwei Punkte $P, Q \in V_+(F)$ gegebenen Geraden eine Addition auf $V_+(F)$ zu definieren? Wie sieht es bei $n = 1$ aus?

AUFGABE 6.23. Bestimme auf der Fermat-Kubik in vier Variablen

$$V = V_+(X^3 + Y^3 + Z^3 + W^3) \subseteq \mathbb{P}^3_K$$

den dritten Durchstoßungspunkt der durch die beiden Punkte $(1, -1, 0, 0)$ und $(0, 0, 1, -1)$ gegebenen Gerade.

Abbildungsverzeichnis