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

Elliptische Kurven

Arbeitsblatt 18

Aufgaben

Eine kommutative Gruppe G heißt *torsionsfrei*, wenn für jedes Element $x \in G$, $x \neq 0$, und $n \in \mathbb{N}_+$ gilt $nx \neq 0$.

Aufgabe 18.1. Zeige, dass die Torsionsuntergruppe einer kommutativen Gruppe G in der Tat eine Untergruppe ist.

Aufgabe 18.2. Es sei $T \subseteq G$ die Torsionsuntergruppe einer kommutativen Gruppe G. Zeige, dass die Restklassengruppe G/T torsionsfrei ist.

Aufgabe 18.3. Es sei G eine kommutative Gruppe. Zeige, dass zu jedem $m \in \mathbb{N}_+$ eine kurze exakte Sequenz

$$0 \longrightarrow \operatorname{Tor}_m(G) \longrightarrow G \xrightarrow{\cdot m} mG \longrightarrow 0$$

vorliegt.

Aufgabe 18.4. Es sei R ein kommutativer Ring. Zeige, dass die Einheitswurzeln in R die Torsionsuntergruppe der Einheitengruppe ist.

Aufgabe 18.5. Es sei G eine kommutative Gruppe und $m \in \mathbb{N}_+$. Zeige, dass die Torsionsuntergruppe zur Ordnung m $\operatorname{Tor}_m(G)$ in natürlicher Weise ein $\mathbb{Z}/(m)$-Modul ist.

Aufgabe 18.6. Es sei G eine kommutative Gruppe mit n^2 Elementen derart, dass für jedes Element $x \in G$ die Beziehung $nx = 0$ gilt. Zeige

$$G \cong \mathbb{Z}/(n) \times \mathbb{Z}/(n),$$

Aufgabe 18.7. Es sei G eine kommutative Gruppe und seien $m, n \in \mathbb{N}_+$ teilerfremd. Zeige, dass die Torsionsuntergruppe zur Ordnung mn $\operatorname{Tor}_{mn}(G)$ die direkte Summe aus den Torsionsuntergruppen $\operatorname{Tor}_m(G)$ und $\operatorname{Tor}_n(G)$ ist.

Aufgabe 18.8.*

Zeige, dass es in der Restklassengruppe $\mathbb{Q}/\mathbb{Z}$ zu jedem $n \in \mathbb{N}_+$ Elemente gibt, deren Ordnung gleich n ist.

Aufgabe 18.9. Zeige, dass die Restklassengruppe $\mathbb{Q}/\mathbb{Z}$ unendlich ist und jedes Element eine endliche Ordnung besitzt.

Aufgabe 18.10. Zeige, dass für die Torsionsuntergruppen von $\mathbb{Q}/\mathbb{Z}$ die Gleichheit

$$\mathrm{Tor}_m(\mathbb{Q}/\mathbb{Z}) = \{[0], [\frac{1}{m}], [\frac{2}{m}], \ldots, [\frac{m-1}{m}]\} \cong \mathbb{Z}/(m)$$

gilt.

Aufgabe 18.11. Zeige, dass ein Körper K genau dann die Charakteristik 0 besitzt, wenn die additive Gruppe $(K, +, 0)$ torsionsfrei ist.

Aufgabe 18.12. Es sei $\Gamma \subseteq \mathbb{C}$ ein Gitter und $E = \mathbb{C}/\Gamma$ der zugehörige komplexe Torus. Zeige, dass die Torsionsuntergruppe zur Ordnung m von E in kanonischer Weise isomorph zur Restklassengruppe $\frac{1}{m}\Gamma/\Gamma$ ist, und das diese wiederum isomorph zu $\Gamma/m\Gamma$ ist.

Aufgabe 18.13.*

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

$$Y^2 = X^3 - X + 6$$

gegeben ist.

(1) Bestimme die Torsionsuntergruppe der Ordnung 2 für $E(\mathbb{R})$.
(2) Bestimme die Torsionsuntergruppe der Ordnung 2 für $E(\mathbb{C})$.
(3) Parametrisiere den oberen Bogen von $E(\mathbb{R})$ als Funktion über einem geeigneten Definitionsbereich.
(4) Bestimme die Koordinaten der Punkte von $E(\mathbb{R})$, wo die Funktion aus (3) lokale Extrema annimmt.
(5) Beschreibe eine endliche Körpererweiterung $\mathbb{Q} \subseteq K$ derart, dass die Punkte aus Teil (4) zu $E(K)$ gehören.

Aufgabe 18.14. Es sei

$$Y^2 = X^3 + aX + b$$

die Gleichung einer elliptischen Kurve über einem algebraisch abgeschlossenen Körper K und es sei $\{\mathfrak{O}, P_1, P_2, P_3\}$ die Untergruppe der Elemente der Ordnung ≤ 2. Man beschreibe einen Hauptdivisor, bei dem genau diese vier Punkte nichttrivial vorkommen.

Für die beiden folgenden Aufgaben ziehe man Aufgabe 6.7 und Aufgabe 6.8 heran.

Aufgabe 18.15. 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 Nullstelle.
(2) Die Torsionsuntergruppe zur Ordnung 2, $\mathrm{Tor}_2(E(\mathbb{R}))$, ist isomorph zu $\mathbb{Z}/(2)$.
(3) Es ist $E(R) \cong S^1$ als reelle Lie-Gruppe.
(4) Die Torsionsuntergruppe zur Ordnung m, $\mathrm{Tor}_m(E(\mathbb{R}))$, ist isomorph zu $\mathbb{Z}/(m)$ für alle $m \in \mathbb{N}_+$.

Aufgabe 18.16. 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) Die Torsionsuntergruppe zur Ordnung 2, $\mathrm{Tor}_2(E(\mathbb{R}))$, ist isomorph zu $\mathbb{Z}/(2) \times \mathbb{Z}/(2)$.
(3) Es ist $E(R) \cong S^1 \times \mathbb{Z}/(2)$ als reelle Lie-Gruppe.
(4) Die Torsionsuntergruppe zur Ordnung m, $\mathrm{Tor}_m(E(\mathbb{R}))$, ist isomorph zu $\mathbb{Z}/(m) \times \mathbb{Z}/(2)$ für alle geraden $m \geq 2$ (und isomorph zu $\mathbb{Z}/(m)$ für m ungerade).

Aufgabe 18.17. 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 $\lambda_1 < \lambda_2 < \lambda_3$. Begünde durch eine Skizze, dass $(\lambda_3, 0)$ einen Halbierungspunkt besitzt und dass $(\lambda_1, 0)$ und $(\lambda_2, 0)$ keinen Halbierungspunkt besitzen.

Aufgabe 18.18.*

Bestimme für die elliptische Kurve $Y^2 = X^3 + X$ die reelle und die komplexe Torsionsuntergruppe zur Ordnung 2.

Aufgabe 18.19.*

Bestimme für die elliptische Kurve $Y^2 = X^3 + 2$ die Torsionsuntergruppe zur Ordnung 2 für die Körper

(1)
$$K = \mathbb{Q},$$

(2)
$$K = \mathbb{Q}[\sqrt[3]{2}],$$

(3)
$$K = \mathbb{Q}[\sqrt[3]{2}, \sqrt{-3}].$$

Aufgabe 18.20. Bestimme für die durch $Y^2 = X^3+7X$ gegebene elliptische Kurve E den kleinsten Zahlkörper K, für den die Torsionsuntergruppe zur Ordnung 2 von $E(K)$ isomorph zu $\mathbb{Z}/(2) \times \mathbb{Z}/(2)$ ist.

Aufgabe 18.21.*

Es sei E eine elliptische Kurve über einem Körper K, die durch eine affine Gleichung
$$Y^2 = X^3 + aX + b$$
gegeben sei. Es sei $K \subseteq K(t)$ der Funktionenkörper in einer Variablen über K. Es sei (t, u) ein Punkt der Kurve über einem Erweiterungskörper $L \supseteq K(t)$. Zeige, dass (t, u) in E_L unendliche Ordnung besitzt.

Aufgabe 18.22. Es sei G eine kommutative Gruppe, sei ℓ eine Primzahl. Zeige, dass der Tate-Modul in natürlicher Weise ein $\hat{\mathbb{Z}}_\ell$-Modul ist.

Aufgabe 18.23.*

Es sei ℓ eine Primzahl. Zeige, dass für den Tate-Modul von $\mathbb{Q}/\mathbb{Z}$ die Gleichheit
$$T_\ell(\mathbb{Q}/\mathbb{Z}) = \hat{\mathbb{Z}}_\ell$$
gilt.

Aufgabe 18.24. Es sei ℓ eine Primzahl. Berechne den Tate-Modul $T_\ell(S^1)$ zur Kreisgruppe S^1.

Aufgabe 18.25. Es sei $\Gamma \subseteq \mathbb{C}$ ein Gitter und $E = \mathbb{C}/\Gamma$ der zugehörige komplexe Torus. Es sei ℓ eine Primzahl. Zeige, dass unter den natürlichen Identifizierungen

$$\Gamma/\ell^n\Gamma \cong \operatorname{Tor}_{\ell^n}(E)$$

mit $[g] \mapsto \frac{1}{\ell^n}[g]$ (vergleiche Aufgabe 18.12) die Diagramme

$$\begin{array}{ccc} \Gamma/\ell^{n+1}\Gamma & \longrightarrow & \Gamma/\ell^n\Gamma \\ \downarrow & & \downarrow \\ \operatorname{Tor}_{\ell^{n+1}}(E) & \stackrel{\cdot\ell}{\longrightarrow} & \operatorname{Tor}_{\ell^n}(E) \end{array}$$

kommutieren, wobei oben die natürliche Restklassenabbildung zur Untergruppe $\ell^{n+1}\Gamma \subseteq \ell^n\Gamma$ steht. Man folgere, dass der Tate-Modul $T_\ell(E)$ kanonisch isomorph zu $\varprojlim_{n\in\mathbb{N}} \Gamma/\ell^n\Gamma$ ist.

Aufgabe 18.26.*

Es sei $\Gamma \subseteq \mathbb{C}$ ein Gitter und $E = \mathbb{C}/\Gamma$ der zugehörige komplexe Torus. Es sei ℓ eine Primzahl. Zeige, dass ein Isomorphismus $\Gamma \cong \mathbb{Z}^2$ einen Isomorphismus

$$T_\ell(E) \cong \hat{\mathbb{Z}}_\ell \times \hat{\mathbb{Z}}_\ell$$

induziert.

Aufgabe 18.27. Es seien $\Gamma_1, \Gamma_2 \subseteq \mathbb{C}$ Gitter und $E_1 = \mathbb{C}/\Gamma_1$, $E_2 = \mathbb{C}/\Gamma_2$, die zugehörigen komplexen Tori. Es sei $s \in \mathbb{C}$, $s \neq 0$, mit $s\Gamma_1 \subseteq \Gamma_2$ und es sei

$$\varphi\colon\ E_1 \longrightarrow E_2$$

die zugehörige Isogenie (vergleiche Lemma 10.7). Es sei ℓ eine Primzahl. Zeige, dass der zugehörige Homomorphismus der Tate-Moduln

$$\varphi_\ell\colon\ T_\ell(E_1) \longrightarrow T_\ell(E_2)$$

(siehe Satz 18.13) unter den kanonischen Isomorphismen

$$T_\ell(E_1) \cong \varprojlim_{n\in\mathbb{N}} \Gamma_1/\ell^n\Gamma_1$$

und

$$T_\ell(E_2) \cong \varprojlim_{n\in\mathbb{N}} \Gamma_2/\ell^n\Gamma_2$$

aus Aufgabe 18.25 mit dem projektiven Limes zu $s\colon\ \Gamma_1/\ell^n\Gamma_1 \to \Gamma_2/\ell^n\Gamma_2$ übereinstimmt.

Aufgabe 18.28.*

Es sei $\Gamma \subseteq \mathbb{C}$ ein Gitter und $E = \mathbb{C}/\Gamma$ der zugehörige komplexe Torus. Es sei $s \in \mathbb{C}$, $s \neq 0$, mit $s\Gamma \subseteq \Gamma$ und es sei

$$\varphi\colon\ E \longrightarrow E$$

die zugehörige Isogenie. Zeige, dass der Grad von φ mit der Determinante von

$$s\colon\ \Gamma \longrightarrow \Gamma$$

und mit der Determinante des zugehörigen Endomorphismus des Tate-Moduls

$$\varphi_\ell\colon\ T_\ell(E) \longrightarrow T_\ell(E)$$

für jede Primzahl ℓ übereinstimmt.

Abbildungsverzeichnis