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

Elliptische Kurven

Arbeitsblatt 19

Aufgaben

Aufgabe 19.1. Es sei V ein Vektorraum über einem Körper der Charakteristik 0. Zeige $V/2V = 0$.

Aufgabe 19.2. Es sei V ein Vektorraum über einem Körper der Charakteristik $\neq 2$. Zeige $V/2V = 0$.

Aufgabe 19.3. Es sei $G = \mathbb{Z}/(k)$ eine zyklische Gruppe. Bestimme $G/2G$.

Aufgabe 19.4. Es sei $\mathbb{Q}^2 \subseteq \mathbb{Q}_+$ die (multiplikative) Untergruppe der Quadrate innerhalb der positiven rationalen Zahlen und es sei $\sim$ die zugehörige Äquivalenzrelation auf $\mathbb{Q}_+$. Zeige, dass jede Äquivalenzklasse einen eindeutigen Repräsentanten besitzt, der durch eine natürliche Zahl gegeben ist, in deren Primfaktorzerlegung jeder Primfaktor einfach ist (die 1 erfülle diese Eigenschaft).

Aufgabe 19.5. Zeige, dass die beiden kommutativen Gruppen $(\mathbb{Q}, 0, +)$ und $(\mathbb{Q}_+, 1, \cdot)$ nicht isomorph sind.

Aufgabe 19.6. Bestimme die Restklassengruppe $\mathbb{R}^\times/(\mathbb{R}^\times)^2$.

Aufgabe 19.7. Es sei K ein endlicher Körper der Charakteristik $\neq 2$. Zeige

$$K^\times/\big(K^\times\big)^2 \cong \mathbb{Z}/(2).$$

Aufgabe 19.8. Es sei K ein Zahlkörper. Zeige, dass die Restklassengruppe $K^\times/(K^\times)^2$ unendlich ist.

Aufgabe 19.9.*

Es seien $\mu_1, \mu_2, \mu_3 \in K$ Elemente in einem Körper K. Zeige, dass

$$w = \mu_1\mu_2 + \mu_1\mu_3 + \mu_2\mu_3$$

und

$$z = -(\mu_1 + \mu_2 + \mu_3)w + \mu_1\mu_2\mu_3$$

die Gleichung $z^2 = (w + \mu_1^2)(w + \mu_2^2)(w + \mu_3^2)$ erfüllen.

Aufgabe 19.10.*

Es sei

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

die Gleichung einer elliptischen Kurve E in Zerlegungsform über einem Körper K mit $\lambda_1, \lambda_2, \lambda_3 \in K$. Es gelte $-\lambda_i = \mu_i^2$. Zeige, dass mit

$$w = \mu_1\mu_2 + \mu_1\mu_3 + \mu_2\mu_3$$

und

$$z = -(\mu_1 + \mu_2 + \mu_3)w + \mu_1\mu_2\mu_3$$

die Verdoppelungsgleichung $2(w, z) = (0, \mu_1\mu_2\mu_3)$ gilt.

Aufgabe 19.11.*

Wir betrachten die durch

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

gegebene elliptische Kurve über $\mathbb{Q}$. Zeige, dass der Punkt $(1, 0) \in E(\mathbb{Q})$ nach der Körpererweiterung $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{2}]$ einen Halbierungspunkt bekommt. Bestimme die Koordinaten (über $\mathbb{Q}[\sqrt{2}]$) eines solchen Halbierungspunktes.

Abbildungsverzeichnis