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

Elliptische Kurven

Arbeitsblatt 22

Aufgaben

Aufgabe 22.1.*

Zeige, dass für beliebige reelle Zahlen die Abschätzung

$$\max(|a-b|, |b|) \geq \frac{1}{2}\max(|a|, |b|)$$

gilt.

Aufgabe 22.2.*

Es sei $\alpha \in \mathbb{R}$. Zeige, dass es ein $c \in \mathbb{R}_+$ derart gibt, dass

$$\max(|x-\alpha|, 1) \geq c \cdot \max(|x|, 1)$$

für alle $x \in \mathbb{R}$ gilt.

Aufgabe 22.3. Es sei $P(x)$ ein reelles Polynom vom Grad d. Zeige, dass es eine positive reelle Zahl c derart gibt, dass die Abschätzung

$$\max(|P(x)|, 1) \geq c \cdot \max\left(|x|^d, 1\right)$$

für alle $x \in \mathbb{R}$ gilt.

Aufgabe 22.4. Es seien $f, g \in K[X]$ teilerfremde Polynome über einem Körper K. Zeige, ohne den Hilbertschen Nullstellensatz heranzuziehen, dass das von den Homogenisierungen $F, G \in K[X, Y]$ erzeugte Ideal Potenzen von X und von Y enthält.

Im Falle eines Polynoms (anstatt einer rationalen Funktion) ergeben die beiden folgenden Aufgaben einen weiteren Beweis für Satz 22.1.

Aufgabe 22.5.*

Es sei K ein Zahlkörper, $F \in K[X]$ ein Polynom vom Grad d und $|-|$ ein Betrag auf K. Zeige, dass es eine positive reelle Zahl $c > 0$ derart gibt, dass

$$\max(|F(x)|, 1) \geq c \cdot \max\left(|x|^d, 1\right)$$

für alle $x \in K$ gilt.

Aufgabe 22.6. Beweise Satz 22.1 mit Hilfe von Aufgabe 21.5 für eine polynomiale Abbildung.

Aufgabe 22.7. Führe im Beweis zu Lemma 22.3 die Abschätzungen für die einzelnen Summanden durch.

Aufgabe 22.8. Zeige, dass eine elliptische Kurve über $\mathbb{R}$ nicht (als Gruppe) endlich erzeugt ist.

Aufgabe 22.9. Zeige, dass eine elliptische Kurve über einem algebraisch abgeschlossenen Körper K nicht (als Gruppe) endlich erzeugt ist.

Aufgabe 22.10. Es sei E eine elliptische Kurve über einem Zahlkörper K, gegeben durch eine Gleichung

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

mit $\lambda_i \in K$. Es sei eine reelle Einbettung $K \subseteq \mathbb{R}$ fixiert und es sei $E(\mathbb{R}) = S^1 \uplus S^1$ die zugehörige reelle Kurve, vergleiche Aufgabe 6.8. Man gebe ein Beispiel, wo die eine reelle Zusammenhangskomponente von $E(\mathbb{R})$ ein Erzeugendensystem von $E(K)$ enthält, die andere aber nicht.

Aufgabe 22.11. Es sei E eine elliptische Kurve über einem Zahlkörper K, gegeben durch eine Gleichung

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

mit $\lambda_i \in K$. Es sei eine reelle Einbettung $K \subseteq \mathbb{R}$ fixiert und es sei $E(\mathbb{R}) = S^1 \uplus S^1$ die zugehörige reelle Kurve, vergleiche Aufgabe 6.8. Man gebe ein Beispiel, wo die beiden reellen Zusammenhangskomponente von $E(\mathbb{R})$ jeweils kein Erzeugendensystem von $E(K)$ enthalten.

Aufgabe 22.12. Es sei E eine elliptische Kurve über einem Zahlkörper K, gegeben durch eine Gleichung

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

mit $\lambda_i \in K$. Es sei eine reelle Einbettung $K \subseteq \mathbb{R}$ fixiert und es sei $E(\mathbb{R}) = S^1 \uplus S^1$ die zugehörige reelle Kurve, vergleiche Aufgabe 6.8. Es sei r der Rang der Kurve. Zeige, dass beide reellen Zusammenhangskomponenten von $E(\mathbb{R})$ jeweils r Elemente besitzen, die jeweils $E(K)$ modulo Torsion erzeugen.

Aufgabe 22.13. Es sei E eine elliptische Kurve über einem Zahlkörper K, gegeben durch eine Gleichung

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

mit $\lambda_i \in K$. Es sei eine reelle Einbettung $K \subseteq \mathbb{R}$ fixiert und es sei $E(\mathbb{R}) = S^1 \uplus S^1$ die zugehörige reelle Kurve, vergleiche Aufgabe 6.8. Zeige, dass der Durchschnitt

$$E(K)_0 := E(K) \cap S^1$$

mit derjenigen Komponente, die das neutrale Element $\mathfrak{O}$ enthält, eine Untergruppe von $E(K)$ ist und dass eine kurze exakte Sequenz

$$0 \longrightarrow E(K)_0 \longrightarrow E(K) \longrightarrow \mathbb{Z}/(2) \longrightarrow 0$$

vorliegt.

Aufgabe 22.14.*

Es sei E eine elliptische Kurve über einem Zahlkörper K und es seien

$$\varphi_1, \varphi_2 \colon K \longrightarrow \mathbb{R}$$

reelle Einbettungen. Zeige, dass die zugehörigen elliptischen Kurven $E(\mathbb{R})_1$ und $E(\mathbb{R})_2$ nicht homöomorph (als topologischer Raum mit der metrischen Topologie) und nicht isomorph (als Gruppe) sein müssen.

Aufgabe 22.15. Es sei E eine elliptische Kurve über einem Zahlkörper K und es seien

$$\varphi_1, \varphi_2 \colon K \longrightarrow \mathbb{C}$$

komplexe Einbettungen. Zeige, dass zwischen den zugehörigen elliptischen Kurven $E(\mathbb{C})_1$ und $E(\mathbb{C})_2$ ein Gruppenisomorphismus vorliegt.

Abbildungsverzeichnis