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

Elliptische Kurven

Arbeitsblatt 25

Aufgaben

Aufgabe 25.1. Bestimme für die folgenden Punkte $P \in \mathbb{P}^2_{\mathbb{Q}}$ die Reduktionen modulo 5.

(1) $(7,\, 6,\, 11)$,
(2) $(5,\, 5,\, 5)$,
(3) $(4,\, 5,\, 6)$,
(4) $\left(\frac{3}{7},\, \frac{2}{9},\, \frac{-8}{11}\right)$,
(5) $\left(\frac{4}{25},\, \frac{5}{9},\, \frac{1}{100}\right)$,
(6) $\left(\frac{1}{25},\, \frac{1}{5},\, \frac{1}{125}\right)$.

Aufgabe 25.2. Bestimme für die folgenden Punkte $P \in \mathbb{P}^2_{\mathbb{Q}[\mathrm{i}]}$ die Reduktionen modulo dem maximalen Ideal (3) (mit dem Restekörper $\mathbb{Z}/(3)[\mathrm{i}]$)

(1) $(3 - \mathrm{i},\, 2 + 5\mathrm{i},\, 1 + 3\mathrm{i})$,
(2) $\left(\frac{2+8\mathrm{i}}{5},\, \frac{4-7\mathrm{i}}{15},\, \frac{12+5\mathrm{i}}{9}\right)$,
(3) $\left(\frac{9\mathrm{i}}{5},\, \frac{3}{5},\, \frac{7-11\mathrm{i}}{3}\right)$.

Aufgabe 25.3. Bestimme für die folgenden Punkte $P \in \mathbb{P}^2_{\mathbb{Q}[\mathrm{i}]}$ die Reduktionen modulo dem maximalen Ideal $(5, \mathrm{i} - 3)$ (mit dem Restekörper $\mathbb{Z}/(5)$)

(1) $(3 - \mathrm{i},\, 2 + 5\mathrm{i},\, 1 + 3\mathrm{i})$,
(2) $\left(\frac{2+8\mathrm{i}}{5},\, \frac{4-7\mathrm{i}}{15},\, \frac{12+5\mathrm{i}}{9}\right)$,
(3) $\left(\frac{9\mathrm{i}}{5},\, \frac{3}{5},\, \frac{7-11\mathrm{i}}{3}\right)$.

Aufgabe 25.4. Bestimme für die folgenden Punkte $P \in \mathbb{P}^2_{\mathbb{R}(t)}$ die Reduktionen modulo $t \mapsto 3$ und $t \mapsto \mathrm{i}$.

(1) $(5,\, -7,\, -3)$,
(2) $(t - 3,\, t^2,\, 2)$,
(3) $\left(\frac{t^2-1}{t^2},\, \frac{t}{t^4-5},\, \frac{t^3+t+2}{t}\right)$.

Aufgabe 25.5. Es sei R ein Dedekindbereich mit Quotientenkörper $Q = Q(R)$ und es sei $\mathfrak{m}$ ein maximales Ideal von R mit Restekörper $K = R/\mathfrak{m}$. Zeige, dass die Reduktion

$$\mathbb{P}^n_Q \longrightarrow \mathbb{P}^n_K$$

aus Lemma 25.1 surjektiv ist.

Aufgabe 25.6. Es sei R ein Dedekindbereich mit Quotientenkörper $Q = Q(R)$ und es sei $\mathfrak{m}$ ein maximales Ideal von R mit Restekörper $K = R/\mathfrak{m}$. Zeige, dass die Reduktion

$$\mathbb{P}^n_Q \longrightarrow \mathbb{P}^n_K$$

für $n \geq 1$ aus Lemma 25.1 nicht injektiv ist.

Aufgabe 25.7. Man gebe ein Beispiel einer unendlichen Punktmenge $M \subseteq \mathbb{P}^1_{\mathbb{Q}}$, deren Reduktion modulo p für jede Primzahl genau aus p Elementen besteht.

Aufgabe 25.8. Es sei $R = \mathbb{Z}[\sqrt{-5}]$ der quadratische Zahlbereich zu $\sqrt{-5} = \sqrt{5}\mathrm{i}$. Zeige, dass es für den Punkt

$$\left(2,\, 1 + \sqrt{-5}\right) \in \mathbb{P}^1_{Q(R)}$$

keine Repräsentierung in R gibt, mit der man sämtliche Reduktionen zu allen maximalen Idealen aus R durch komponentenweise Reduktion ausrechnen kann.

Aufgabe 25.9. Führe die Details der Überlegungen aus Beispiel 25.3 für Beispiel 2.8 aus.

Aufgabe 25.10. Es sei R ein Dedekindbereich mit Quotientenkörper $Q = Q(R)$ und es sei $\mathfrak{m}$ ein maximales Ideal von R mit Restekörper $K = R/\mathfrak{m}$. Begründe, dass es bei $n \geq 1$ keine sinnvolle Reduktion

$$\mathbb{A}^n_Q \longrightarrow \mathbb{A}^n_K$$

(ähnlich wie in Lemma 25.1) geben kann.

Aufgabe 25.11. Bestimme für die durch $y^2 = x^3 + 1$ gegebene elliptische Kurve die Reduktionen für die Punktemenge

$$\mathfrak{O},\ (-1,0),\ (0,1),\ (0,-1),\ (2,3),\ (2,-3)$$

für die Primzahlen $p = 2,3,5,7$. Für welche dieser Primzahlen ist die Reduktion wieder eine elliptische Kurve?

Aufgabe 25.12. Bestimme für die durch $y^2 = x^3 - x$ gegebene elliptische Kurve die Reduktionen für die Punktemenge

$$(0,0),\ (1,0),\ (-1,0),\ \mathfrak{O}$$

für die Primzahlen $p = 2,3,5,7$. Für welche dieser Primzahlen ist die Reduktion wieder eine elliptische Kurve?

Aufgabe 25.13. Zeige, dass für eine elliptische Kurve E über $\mathbb{Q}$ die Reduktionsabbildung

$$E(\mathbb{Q}) \longrightarrow E(\mathbb{Z}/(p))$$

im Allgemeinen nicht surjektiv ist.

Aufgabe 25.14. Es sei K ein Körper, $R = K[t]$ der Polynomring in einer Variablen und sei $K(t) = Q(K[t])$ sein Quotientenkörper. Wir betrachten die elliptische Kurve E über $K(t)$, die in Legendrescher Normalform

$$y^2 = x(x-1)(x-t)$$

gegeben sei.

(1) Zeige, dass man jede elliptische Kurve über K in Legendrescher Normalform als Reduktion von E mittels $t \mapsto \lambda$ im Sinne von Korollar 25.5 erhalten kann.
(2) Für welche $\lambda \in K$ ist die Reduktion keine elliptische Kurve?
(3) Welche $K(t)$-rationalen Punkte von E gibt es und welche Reduktionspunkte definieren sie?

Aufgabe 25.15. Es sei K ein Körper und $R = K[X,Y]$ mit dem Quotientenkörper $Q = Q(R) = K(X,Y)$. Es sei $\mathfrak{m} = (X,Y)$ mit dem Restekörper K. Zeige, dass es keine Reduktion

$$\mathbb{P}^1_Q \longrightarrow \mathbb{P}^1_K$$

(ähnlich wie in Lemma 25.1) geben kann.

Argumentiere mit dem projektiven Punkt (X,Y).

Aufgabe 25.16.*

Wir betrachten in $\mathbb{P}^2_{\mathbb{Q}}$ die endliche Punktemenge, die aus den drei Punkten $P_1 = (4,\,3,\,5)$, $P_2 = (6,\,6,\,6)$ und $P_3 = (1,\,3,\,5)$ besteht. Für welche Primzahlen p besteht die Reduktion dieser Punktemenge ebenfalls aus drei Punkten?

Aufgabe 25.17. Wir betrachten in $\mathbb{P}^2_{\mathbb{Q}}$ die endliche Punktemenge, die aus den vier Punkten $P_1 = (4, 0, 5)$, $P_2 = (5, 6, 6)$, $P_3 = (2, 1, 1)$ und $P_4 = (1, 0, 0)$ besteht. Für welche Primzahlen p besteht die Reduktion dieser Punktemenge ebenfalls aus vier Punkten?

Aufgabe 25.18. Bestimme für die beiden affinen Gleichungen

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

und

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

die nach Aufgabe 5.9 die gleiche elliptische Kurve über $\mathbb{Q}$ definieren, jeweils die Primzahlen p, für die die Kurve über $\mathbb{Z}/(p)$ glatt ist.

Aufgabe 25.19.*

Wir betrachten die durch die Gleichung

$$Y^2 = X^3 + \mathrm{i}$$

gegebene elliptische Kurve über $\mathbb{Q}[\mathrm{i}]$ und über $\mathbb{Z}[\mathrm{i}]$.

(1) Bestimme die Torsionsuntergruppe zur Ordnung 2 von $E(\mathbb{Q}[\mathrm{i}])$.
(2) Bestimme die Torsionsuntergruppe zur Ordnung 2 von $E(\mathbb{C})$.
(3) Bestimme die Torsionsuntergruppe zur Ordnung 2 von $E(\mathbb{Z}/(5))$, wobei der Reduktionshomomorphismus

$$\mathbb{Z}[\mathrm{i}] \longrightarrow \mathbb{Z}/(5),\ \mathrm{i} \longmapsto 2,$$

zugrunde liegt.
(4) Bestimme die Torsionsuntergruppe zur Ordnung 2 von $E(\mathbb{Z}/(5))$, wobei der Reduktionshomomorphismus

$$\mathbb{Z}[\mathrm{i}] \longrightarrow \mathbb{Z}/(5),\ \mathrm{i} \longmapsto 3,$$

zugrunde liegt.
(5) Bestimme die Torsionsuntergruppe zur Ordnung 2 von $E(\mathbb{F}_9)$, wobei der Reduktionshomomorphismus

$$\mathbb{Z}[\mathrm{i}] \longrightarrow \mathbb{F}_9 \cong \mathbb{Z}/(3)[\mathrm{i}] \cong \mathbb{Z}/(3)[T]/(T^2+1),\ \mathrm{i} \longmapsto \mathrm{i},$$

zugrunde liegt.

Aufgabe 25.20. Es sei E eine elliptische Kurve, die über $\mathbb{Z}$ definiert sei, und sei $P \in E(\mathbb{Q})$ ein $\mathbb{Q}$-rationaler Punkt von E. Zeige, dass P genau dann ein Torsionspunkt ist, wenn es eine natürliche Zahl n derart gibt, dass für alle Primzahlen p, für die die Reduktion modulo p eine elliptische Kurve ist, der zugehörige Punkt $\tilde{P} \in E(\mathbb{Z}/(p))$ eine Ordnung $\leq n$ besitzt.

AUFGABE 25.21. Man gebe für $n = 5, 6, 7, 13, 14, 15$ einen Punkt der durch $Y^2 = X^3 - n^2 X$ gegebenen elliptischen Kurve an, der kein Torsionspunkt ist.

Abbildungsverzeichnis