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

Elliptische Kurven

Arbeitsblatt 7

Aufgaben

Aufgabe 7.1. Sei K ein Körper und $\mathbb{P}^n_K$ der projektive Raum. Zeige, dass die Konstanten die einzigen globalen algebraischen Funktionen sind, d.h. es gilt

$$\Gamma\left(\mathbb{P}^n_K, \mathcal{O}_{\mathbb{P}^n_K}\right) = K.$$

Aufgabe 7.2. Es sei

$$U = D_+(X_0) \cup D_+(X_1) \subseteq \mathbb{P}^n_K.$$

Zeige

$$\Gamma\left(U, \mathcal{O}_{\mathbb{P}^n_K}\right) = K.$$

Aufgabe 7.3. Es sei $f \in K[X_0, X_1, \ldots, X_n]$ ein homogenes Polynom vom Grad d und sei

$$D_+(f) \subseteq \mathbb{P}^n_K$$

die zugehörige offene Teilmenge des projektiven Raumes. Zeige, dass zu jedem homogenen Polynom $h \in K[X_0, X_1, \ldots, X_n]$ vom Grad e die rationale Funktion $\frac{h}{f^n}$ unter der Bedingung $e = nd$ eine algebraische Funktion

$$\frac{h}{f^n} \colon D_+(f) \longrightarrow K$$

definiert.

Aufgabe 7.4. Sei $R \subseteq S$ eine endliche Ringerweiterung und sei $f \in R$. Zeige: Wenn f, aufgefasst in S, eine Einheit ist, dann ist f eine Einheit in R.

Aufgabe 7.5. Begründe, dass $K[y,z] \subseteq K[x,y,z]/(x^2+yz^2+z^{m+1})$ endlich ist. Wie sieht es über $K[x,y]$ bzw. $K[x,z]$ aus?

Aufgabe 7.6. Begründe, dass $K[x,y] \subseteq K[x,y,z]/(xy-z^n)$ endlich ist. Wie sieht es über $K[x,z]$ bzw. $K[y,z]$ aus?

AUFGABE 7.7. Es sei R ein kommutativer Ring und

$$S = R[X_1, \ldots, X_n]/\mathfrak{a}$$

eine (als Algebra) endlich erzeugte R-Algebra, die ganz über R sei. Zeige, dass S ein endlich erzeugter R-Modul ist.

AUFGABE 7.8. Es sei K ein Körper und sei $P \in K[X]$ ein nichtkonstantes Polynom. Zeige, dass P nicht algebraisch über K ist.

AUFGABE 7.9. Es sei K ein Körper und $L = K(X)$ der Quotientenkörper des Polynomrings $K[X]$. Es sei M, $K \subseteq M \subseteq L$, $M \neq K$, ein Zwischenkörper. Zeige, dass $M \subseteq L$ eine endliche Körpererweiterung ist.

Es sei K ein Körper und sei A eine kommutative K-Algebra. Man nennt Elemente $f_1, \ldots, f_n \in A$ *algebraisch abhängig*, wenn es ein von 0 verschiedenes Polynom $P \in K[X_1, \ldots, X_n]$ mit

$$P(f_1, \ldots, f_n) = 0$$

gibt.

AUFGABE 7.10. Es sei $K[X_1, \ldots, X_n]$ der Polynomring über einem Körper K. Zeige, dass die Variablen $X_1, \ldots, X_n$ algebraisch unabhängig sind.

AUFGABE 7.11. Es sei $K[X_1, \ldots, X_n]$ der Polynomring über einem Körper K und seien $n + 1$ Polynome $f_1, \ldots, f_{n+1} \in K[X_1, \ldots, X_n]$ gegeben. Zeige, dass diese algebraisch abhängig sind.

AUFGABE 7.12. Es sei

$$\varphi \colon \mathbb{A}_K^m \longrightarrow \mathbb{A}_K^n$$

eine polynomiale Abbildung zwischen affinen Räumen mit $m < n$. Zeige, dass φ nicht surjektiv ist.

AUFGABE 7.13. Es sei A eine kommutative K-Algebra über einem Körper K und seien n Elemente $f_1, \ldots, f_n \in A$ gegeben. Zeige, dass diese Elemente genau dann algebraisch unabhängig sind, wenn die von diesen Elementen erzeugte K-Algebra $K[f_1, \ldots, f_n]$ isomorph zum Polynomring $K[X_1, \ldots, X_n]$ ist.

Aufgabe 7.14. Es sei K ein algebraisch abgeschlossener Körper und $F \in K[X,Y]$ ein nichtkonstantes Polynom. Zeige, dass der Restklassenring

$$K[X,Y]/(F)$$

eine endliche $K[T]$-Algebra ist.

Aufgabe 7.15. Seien R, S, T kommutative Ringe und seien $\varphi : R \to S$ und $\psi : S \to T$ Ringhomomorphismen derart, dass S endlich über R und T endlich über S ist. Zeige, dass dann auch T endlich über R ist.

Aufgabe 7.16.*

Es sei K ein Körper und es sei eine endliche Ringerweiterung der Form
$K[X] \subseteq K[X][Y]/\big(Y^n + P_{n-1}(X)Y^{n-1} + \cdots + P_2(X)Y^2 + P_1(X)Y + P_0(X)\big)$
mit $P_i(X) \in K[X]$ gegeben, wobei der Erweiterungsring integer sei. Es sei k derart, dass der Grad von P_i höchstens $k(n-i)$ ist für alle

$$i = 0, 1, \ldots, n-1.$$

Zeige, dass dann YX^{-k} eine Ganzheitsgleichung vom Grad n über $K[X^{-1}]$ erfüllt, und dass die zugehörige Erweiterungsalgebra den gleichen Quotientenkörper besitzt.

Aufgabe 7.17. Es sei $F \in K[X]$ ein Polynom. Interpretiere F als Morphismus

$$F\colon \mathbb{P}^1_K \longrightarrow \mathbb{P}^1_K.$$

Was ist $F(\infty)$?

Aufgabe 7.18. Es sei $F = G/H$ eine rationale Funktion über dem Körper K. Interpretiere F als Morphismus

$$F\colon \mathbb{P}^1_K \longrightarrow \mathbb{P}^1_K.$$

Aufgabe 7.19.*

Bestimme zu einem Punkt $(a,b) \in \mathbb{P}^1$ die Gleichung für die Urbildgerade zur Projektion weg von einem Punkt

$$\mathbb{P}^2_K \setminus \{(1,0,0)\} \longrightarrow \mathbb{P}^1_K,\ (x,y,z) \longmapsto (y,z).$$

Aufgabe 7.20. Zeige, dass es einen Morphismus

$$V(X^2 - Y^3) \supseteq U = V(X^2 - Y^3) \setminus \{(0,0)\} \longrightarrow \mathbb{A}^1$$

gibt, den man nicht auf $V(X^2 - Y^3)$ ausdehnen kann.

Aufgabe 7.21. Zeige, dass die Einschränkung der Projektion weg von einem Punkt

$$\mathbb{P}^2_K \setminus \{P\} \longrightarrow \mathbb{P}^1_K$$

auf eine jede Gerade $G \subset \mathbb{P}^2_K$, die nicht durch P geht, einen Isomorphismus induziert.

Aufgabe 7.22.*

Es sei K ein algebraisch abgeschlossener Körper, sei

$$C = V_+\big(X^2 + Y^2 + Z^2\big) \subset \mathbb{P}^2_K$$

und sei

$$\varphi\colon C \longrightarrow \mathbb{P}^1_K$$

der durch die Projektion weg vom Punkt

$$\mathbb{P}^2_K \setminus \{(1,0,0)\} \longrightarrow \mathbb{P}^1_K,\ (x,y,z) \longmapsto (y,z),$$

definierte Morphismus. Bestimme das Urbild des Punktes $(3,5) \in \mathbb{P}^1_K$.

Der Beweis der folgenden Aussage erfordert das Konzept der Separabilität für Polynome und den Charakterisierungssatz für separable Polynome.

Aufgabe 7.23.*

Es sei K ein algebraisch abgeschlossener Körper der Charakteristik 0 und sei $C \subset \mathbb{P}^2_K$ eine irreduzible ebene projektive Kurve vom Grad d und sei

$$\varphi\colon C \longrightarrow \mathbb{P}^1_K$$

der durch eine Projektion weg von einem Punkt $P \notin C$ definierte Morphismus. Zeige, dass bis auf endlich viele Ausnahmen die Faser zu jedem Punkt $t \in \mathbb{P}^1_K$ aus genau d Punkten besteht.

Aufgabe 7.24.*

Es sei K ein algebraisch abgeschlossener Körper der Charakteristik $p > 0$ und sei $C = V(YZ^{p-1} + X^p) \subset \mathbb{P}^2_K$. Zeige, dass der durch die Projektion weg vom Punkt $(1,0,0)$ definierte Morphismus

$$\varphi\colon C \longrightarrow \mathbb{P}^1_K$$

bijektiv ist.

Aufgabe 7.25. Es sei K ein Körper und sei $C \subset \mathbb{P}^2_K$ eine ebene projektive Kurve. Es sei $P \in C$ ein Punkt der Kurve und sei

$$\varphi\colon C \setminus \{P\} \longrightarrow \mathbb{P}^1_K$$

der durch die Projektion weg vom Punkt definierte Morphismus. Bei dieser Abbildung wird also ein Punkt $Q \in C$, $Q \neq P$, auf die durch Q und P gegebene *Sekante* abgebildet.

(1) Sei $K = \mathbb{C}$ und sei Q_n eine Folge auf C, die in der komplexen Topologie gegen P konvergiert. Konvergiert $\varphi(Q_n)$?
(2) Besitzt $\varphi(Q_n)$ einen Häufungspunkt?
(3) Sei P ein glatter Punkt. Zeige, dass es eine Fortsetzung des Morphismus auf ganz C gibt.

Aufgabe 7.26. Diskutiere die Situation aus Aufgabe 7.25 für das Achsenkreuz

$$V_+(YZ) \subset \mathbb{P}^2$$

und den Kreuzungspunkt $(1, 0, 0)$.

Aufgabe 7.27. Es sei $F = G/H$ eine rationale Funktion über den reellen Zahlen $\mathbb{R}$ (oder den komplexen Zahlen $\mathbb{C}$) mit dem zugehörigen Morphismus

$$F\colon \mathbb{P}^1_{\mathbb{K}} \longrightarrow \mathbb{P}^1_{\mathbb{K}}.$$

Zeige, dass

$$F(\infty) = c \in \mathbb{P}^1_{\mathbb{K}}$$

genau dann gilt, wenn die Folge

$$\frac{G(n)}{H(n)}$$

für $n \to \infty$ gegen c konvergiert (was für $c = \infty$ sinnvoll zu interpretieren ist).

Aufgabe 7.28. Es sei K ein algebraisch abgeschlossener Körper und $C \subset \mathbb{P}^2_K$ eine glatte Kurve vom Grad $d \geq 2$. Zeige, dass es einen Morphismus $C \to \mathbb{P}^1_K$ derart gibt, dass jede Faser aus maximal $d - 1$ Punkten besteht.

Aufgabe 7.29. Es sei $C = V_+(X^3 + Y^3 + Z^3) \subset \mathbb{P}^2_K$ die *Fermat-Kubik* über einem algebraisch abgeschlossenen Körper der Charakteristik $\neq 3$. Beschreibe explizit einen Morphismus $C \to \mathbb{P}^1_K$, bei dem über jedem Punkt maximal zwei Punkte liegen.

Abbildungsverzeichnis